UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	ISSUE DATE	PATENT NO.	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/823,916	04/24/2018	9954872	067292-5005-US01	5143

24341 7590 04/04/2018

Morgan, Lewis & Bockius LLP (PA)
1400 Page Mill Road
Palo Alto, CA 94304-1124

ISSUE NOTIFICATION

The projected patent number and issue date are specified above.

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(application filed on or after May 29, 2000)

The Patent Term Adjustment is 0 day(s). Any patent to issue from the above-identified application will include an indication of the adjustment on the front page.

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (http://pair.uspto.gov).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Application Assistance Unit (AAU) of the Office of Data Management (ODM) at (571)-272-4200.

APPLICANT(s) (Please see PAIR WEB site http://pair.uspto.gov for additional applicants):

Alen Capalik, Pacific Palisades, CA;
COUNTERTACK INC., Santa Monica, CA;
David Andrews, Los Angeles, CA;
Ben Becker, Santa Monica, CA;

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The USA offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to encourage and facilitate business investment. To learn more about why the USA is the best country in the world to develop technology, manufacture products, and grow your business, visit SelectUSA.gov.

PART B - FEE(S) TRANSMITTAL

Electronically filed March 14, 2018

Complete and send this form with applicable fee(s), to: Mail — Mail Stop ISSUE FEE, Commissioner of Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450
or Fax — (571) 273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advanced orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS

MORGAN, LEWIS & BOCKIUS LLP
1400 Page Mill Road
Palo Alto, CA 94304

Note: A certificate of mailing below can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing.

Certificate of Mailing

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)

(Signature)

(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTY'S DOCKET NO.	CONFIRMATION NO.
14/823,916	08/11/2015	Alen Capalik	067292-5005-US01	5143

TITLE OF INVENTION **SYSTEM AND METHOD FOR IDENTIFYING UNAUTHORIZED ACTIVITIES ON A COMPUTER SYSTEM USING A DATA STRUCTURE MODEL**

APPLN. TYPE	ENTITY STATUS	ISSUE FEE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	480	0	480	03/15/2018

EXAMINER	ART UNIT	CLASS-SUB CLASS
NGUYEN, THU HAT	2444	726-023000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).
☐ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.
☐ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list (1) the names of up to 3 registered patent attorneys or agents OR, alternatively, (2) the name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed

1. **Morgan, Lewis & Bockius LLP**
2.
3.

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE: COUNTERTACK INC.

(B) RESIDENCE: (CITY and STATE OR COUNTRY) Santa Monica, CA

Please check the appropriate assignee category or categories (will not be printed on the patent) ☐ Individual ☒ Corporation or other private group entity ☐ Government

4a. The following fee(s) are submitted:
☒ Issue Fee
☐ Advanced Order - # of Copies ____

4b. Payment of Fee(s): (**Please first reapply any previously paid issue fee shown above.**)
☐ A check in the amount of the fee(s) enclosed
☐ Payment by credit card. Form PTO-2038 is attached.
☒ The Director is hereby authorized to charge the required fee(s), or credit any overpayment, to Deposit Account Number 50-0310 (order no. 067292-5005-US01).

5. **Change in Small Entity Status** (from status indicated above)
☐ a. Applicant certifying micro entity status. See 37 CFR 1.29.
NOTE: Absent a valid certification of Micro Entity (see form PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.

☐ Applicant asserting small entity status. See 37 CFR 1.27.
NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.

☐ Applicant changing to regular undiscounted fee status.
NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be sign in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature __/ Tae-Woong Koo __ Date: March 14, 2018

Printed Name: Tae-Woong Koo Registration No. 59,649

DB2/ 32976206.1

Electronic Patent Application Fee Transmittal				
Application Number:	14823916			
Filing Date:	11-Aug-2015			
Title of Invention:	System and Method for Identifying Unauthorized Activities on a Computer System using a Data Structure Model			
First Named Inventor/Applicant Name:	Alen Capalik			
Filer:	Tae-Woong Koo			
Attorney Docket Number:	067292-5005-US01			
Filed as Small Entity				
Filing Fees for Utility under 35 USC 111(a)				
Description	**Fee Code**	**Quantity**	**Amount**	**Sub-Total in USD($)**
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
UTILITY APPL ISSUE FEE	2501	1	480	480

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Miscellaneous:				
		Total in USD ($)		**480**

Electronic Acknowledgement Receipt	
EFS ID:	32043945
Application Number:	14823916
International Application Number:	
Confirmation Number:	5143
Title of Invention:	System and Method for Identifying Unauthorized Activities on a Computer System using a Data Structure Model
First Named Inventor/Applicant Name:	Alen Capalik
Customer Number:	24341
Filer:	Tae-Woong Koo
Filer Authorized By:	
Attorney Docket Number:	067292-5005-US01
Receipt Date:	14-MAR-2018
Filing Date:	11-AUG-2015
Time Stamp:	01:48:18
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	DA
Payment was successfully received in RAM	$480
RAM confirmation Number	031418INTEFSW00009580500310
Deposit Account	
Authorized User	
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Issue Fee Payment (PTO-85B)	067292-5005-US01_IssueFeePmt.pdf	127210 f659c472f15ffc592ac4edbd1a07fbb8952e1c41	no	1
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	30562 c3b742a97137b0a910460313cd726a804c82c2e7	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	157772		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.
National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.
New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/823,916	08/11/2015	Alen Capalik	067292-5005-US01	5143

24341 7590 01/08/2018
Morgan, Lewis & Bockius LLP (PA)
1400 Page Mill Road
Palo Alto, CA 94304-1124

EXAMINER	
NGUYEN, THU HA T	

ART UNIT	PAPER NUMBER
2444	

NOTIFICATION DATE	DELIVERY MODE
01/08/2018	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

padocketingdepartment@morganlewis.com
vskliba@morganlewis.com

UNITED STATES DEPARTMENT OF COMMERCE
U.S. Patent and Trademark Office
Address : COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450

APPLICATION NO./ CONTROL NO.	FILING DATE	FIRST NAMED INVENTOR / PATENT IN REEXAMINATION	ATTORNEY DOCKET NO.
14/823,916	11 August, 2015	CAPALIK ET AL.	067292-5005-US01

Morgan, Lewis & Bockius LLP (PA)
1400 Page Mill Road
Palo Alto, CA 94304-1124

EXAMINER	
THU HA NGUYEN	
ART UNIT	PAPER
2444	20180103

DATE MAILED:

Please find below and/or attached an Office communication concerning this application or proceeding.

Commissioner for Patents

IDS filed 12/12/17 has been considered and placed in file.

/THU HA NGUYEN/
Primary Examiner, Art Unit 2444

PTO-90C (Rev.04-03)

Receipt date: 12/12/2017

INFORMATION DISCLOSURE STATEMENT BY APPLICANT Substitute for Form 1449-PTO				Electronically filed December 12, 2017	
				Application Number	14/823,916
				Filing Date	August 11, 2015
				First Named Inventor	Alen Capalik
				Art Unit	2444
				Examiner Name	Nguyen, Thu Ha T.
Sheet	1	of	1	Attorney Docket Number	067292-5005-US01

NON PATENT LITERATURE DOCUMENTS		
Examiner Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published
		CounterTack Inc., Communication Pursuant to Article 94(3), EP11729826.5, 22JUN2017, 5 pgs.
		CounterTack Inc., Intent to Grant, EP11731194.4, 20JUL2017, 6 pgs.
		CounterTack Inc., International Preliminary Report on Patentability, PCTUS2016/012533, 11JUL2017, 8 pgs.
		CounterTack Inc., Office Action, CA 2,689,126, received on 02JUN2017, 3 pgs

Examiner Signature	/THU HA T NGUYEN/	Date Considered	01/03/2018

DB2/ 32379771.1

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /T.T.N/

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

NOTICE OF ALLOWANCE AND FEE(S) DUE

24341 7590 12/15/2017
Morgan, Lewis & Bockius LLP (PA)
1400 Page Mill Road
Palo Alto, CA 94304-1124

EXAMINER
NGUYEN, THU HA T

ART UNIT	PAPER NUMBER
2444	

DATE MAILED: 12/15/2017

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/823,916	08/11/2015	Alen Capalik	067292-5005-US01	5143

TITLE OF INVENTION: System and Method for Identifying Unauthorized Activities on a Computer System using a Data Structure Model

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$480	$0	$0	$480	03/15/2018

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the ENTITY STATUS shown above. If the ENTITY STATUS is shown as SMALL or MICRO, verify whether entitlement to that entity status still applies.

If the ENTITY STATUS is the same as shown above, pay the TOTAL FEE(S) DUE shown above.

If the ENTITY STATUS is changed from that shown above, on PART B - FEE(S) TRANSMITTAL, complete section number 5 titled "Change in Entity Status (from status indicated above)".

For purposes of this notice, small entity fees are 1/2 the amount of undiscounted fees, and micro entity fees are 1/2 the amount of small entity fees.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed and an extra copy of the form should be submitted. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Maintenance fees are due in utility patents issuing on applications filed on or after Dec. 12, 1980. It is patentee's responsibility to ensure timely payment of maintenance fees when due. More information is available at www.uspto.gov/PatentMaintenanceFees.

PTOL-85 (Rev. 02/11)

IPR2025-00068
CrowdStrike EX1002 Page 10

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail **Mail Stop ISSUE FEE**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

24341 7590 12/15/2017
Morgan, Lewis & Bockius LLP (PA)
1400 Page Mill Road
Palo Alto, CA 94304-1124

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission
I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/823,916	08/11/2015	Alen Capalik	067292-5005-US01	5143

TITLE OF INVENTION: System and Method for Identifying Unauthorized Activities on a Computer System using a Data Structure Model

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$480	$0	$0	$480	03/15/2018

EXAMINER	ART UNIT	CLASS-SUBCLASS
NGUYEN, THU HA T	2444	726-023000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).
- ❑ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.
- ❑ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list
(1) The names of up to 3 registered patent attorneys or agents OR, alternatively,
(2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.
1 _____
2 _____
3 _____

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE (B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent) : ❑ Individual ❑ Corporation or other private group entity ❑ Government

4a. The following fee(s) are submitted:
- ❑ Issue Fee
- ❑ Publication Fee (No small entity discount permitted)
- ❑ Advance Order - # of Copies _____

4b. Payment of Fee(s): **(Please first reapply any previously paid issue fee shown above)**
- ❑ A check is enclosed.
- ❑ Payment by credit card. Form PTO-2038 is attached.
- ❑ The director is hereby authorized to charge the required fee(s), any deficiency, or credits any overpayment, to Deposit Account Number _____ (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)
- ❑ Applicant certifying micro entity status. See 37 CFR 1.29 — NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.
- ❑ Applicant asserting small entity status. See 37 CFR 1.27 — NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.
- ❑ Applicant changing to regular undiscounted fee status. — NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature _____ Date _____

Typed or printed name _____ Registration No. _____

PTOL-85 Part B (10-13) Approved for use through 10/31/2013. OMB 0651-0033 U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

IPR2025-00068
CrowdStrike EX1002 Page 11

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/823,916	08/11/2015	Alen Capalik	067292-5005-US01	5143

24341 7590 12/15/2017

Morgan, Lewis & Bockius LLP (PA)
1400 Page Mill Road
Palo Alto, CA 94304-1124

EXAMINER	
NGUYEN, THU HA T	

ART UNIT	PAPER NUMBER
2444	

DATE MAILED: 12/15/2017

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(Applications filed on or after May 29, 2000)

The Office has discontinued providing a Patent Term Adjustment (PTA) calculation with the Notice of Allowance.

Section 1(h)(2) of the AIA Technical Corrections Act amended 35 U.S.C. 154(b)(3)(B)(i) to eliminate the requirement that the Office provide a patent term adjustment determination with the notice of allowance. See Revisions to Patent Term Adjustment, 78 Fed. Reg. 19416, 19417 (Apr. 1, 2013). Therefore, the Office is no longer providing an initial patent term adjustment determination with the notice of allowance. The Office will continue to provide a patent term adjustment determination with the Issue Notification Letter that is mailed to applicant approximately three weeks prior to the issue date of the patent, and will include the patent term adjustment on the patent. Any request for reconsideration of the patent term adjustment determination (or reinstatement of patent term adjustment) should follow the process outlined in 37 CFR 1.705.

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

PTOL-85 (Rev. 02/11)

IPR2025-00068
CrowdStrike EX1002 Page 12

OMB Clearance and PRA Burden Statement for PTOL-85 Part B

The Paperwork Reduction Act (PRA) of 1995 requires Federal agencies to obtain Office of Management and Budget approval before requesting most types of information from the public. When OMB approves an agency request to collect information from the public, OMB (i) provides a valid OMB Control Number and expiration date for the agency to display on the instrument that will be used to collect the information and (ii) requires the agency to inform the public about the OMB Control Number's legal significance in accordance with 5 CFR 1320.5(b).

The information collected by PTOL-85 Part B is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450. Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Notice of Allowability	Application No. 14/823,916	Applicant(s) CAPALIK ET AL.	
	Examiner THU HA NGUYEN	Art Unit 2444	AIA (First Inventor to File) Status No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *amendment filed 11/06/17*.
   ☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on_____.
2. ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.
3. ☒ The allowed claim(s) is/are *1-21*. As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.
4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   Certified copies:

   a) ☐ All b) ☐ Some *c) ☐ None of the:
   1. ☐ Certified copies of the priority documents have been received.
   2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
   3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☒ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date 5/31/17
3. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
4. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
5. ☐ Examiner's Amendment/Comment
6. ☒ Examiner's Statement of Reasons for Allowance
7. ☐ Other _____.

/THU HA NGUYEN/
Primary Examiner, Art Unit 2444

The present application is being examined under the pre-AIA first to invent provisions.

Reasons for Allowance

1. Claims 1- 21 are allowed.

2. The following is the examiner's statement of reasons for allowance:

3. Claims 1-21 are allowable over prior arts because the cited prior art of record fails to teach or render obvious the claimed limitations in combination with the specific added limitation recited in each of independent claims 1, 19 and 20 (and associated dependent claims).

4. This communication warrants no examiner's reason for allowance, as applicant's reply makes evident the reason for allowance, satisfying the record as whole as required by rule 37 CFR 1.104 (e). In this case, the substance of applicant's remark filed on November 06, 2017 with respect to arguments and amendment that point out and make clear the reason claims are patentable over the prior art of record. Thus, the reason for allowance is in all probability evident from the record and no statement for examiner's reason for allowance is necessary (see MPEP 13202.14).

5. Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thu Ha Nguyen, whose telephone number is (571) 272-

3989. The examiner can normally be reached Monday through Friday from 8:00 AM to 6:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Peter-Anthony Pappas, can be reached at (571) 272-7646.

The fax phone numbers for the organization where this application or proceeding is assigned are (571) 273-8300 for regular communications.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/THU HA NGUYEN/

Primary Examiner, Art Unit 2444

Notice of References Cited	Application/Control No. 14/823,916	Applicant(s)/Patent Under Reexamination CAPALIK ET AL.	
	Examiner THU HA NGUYEN	Art Unit 2444	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-2008/0222729 A1	09-2008	Chen; Songqing	G06F21/566	726/24
*	B	US-2011/0321165 A1	12-2011	Capalik; Alen	G06F11/3471	726/25
*	C	US-2011/0321166 A1	12-2011	Capalik; Alen	H04L63/1416	726/25
*	D	US-8,204,984 B1	06-2012	Aziz; Ashar	H04L63/0227	709/224
*	E	US-8,776,050 B2	07-2014	Plouffe; Jerry	G06F9/45537	718/1
*	F	US-8,943,506 B2	01-2015	Tang; Changbin	G06F9/45558	718/1
*	G	US-8,949,826 B2	02-2015	Fitzgerald; Joseph	G06F9/45537	718/1
	H	US-				
	I	US-				
	J	US-				
	K	US-				
	L	US-				
	M	US-				

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	CPC Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Receipt date: 05/31/2017

INFORMATION DISCLOSURE STATEMENT BY APPLICANT Substitute for Form 1449-PTO				Electronically filed May 31, 2017	
				Application Number	14/823,916
				Filing Date	August 11, 2015
				First Named Inventor	Alen Capalik
				Art Unit	2444
				Examiner Name	Nguyen, Thu Ha T.
Sheet	1	of	1	Attorney Docket Number	067292-5005-US01

NON PATENT LITERATURE DOCUMENTS		
Examiner Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published
		Capalik, Final Office Action, US 14/542,376, 24APR2017, 17 pgs.

Examiner Signature	/THU HA T NGUYEN/	Date Considered	11/27/2017

DB2/ 31520280.1

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /T.T.N/

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

BIB DATA SHEET

CONFIRMATION NO. 5143

SERIAL NUMBER	FILING or 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
14/823,916	08/11/2015 RULE	726	2444	067292-5005-US01

APPLICANTS
COUNTERTACK INC., Santa Monica, CA;

INVENTORS
Alen Capalik, Pacific Palisades, CA;
David Andrews, Los Angeles, CA;
Ben Becker, Santa Monica, CA;

**** CONTINUING DATA ***************************
This application is a CON of 13/163,590 06/17/2011 PAT 9106697
which claims benefit of 61/358,367 06/24/2010

**** FOREIGN APPLICATIONS ***************************

**** IF REQUIRED, FOREIGN FILING LICENSE GRANTED **** ** SMALL ENTITY **
09/18/2015

Foreign Priority claimed ❑ Yes ☑ No 35 USC 119(a-d) conditions met ❑ Yes ☑ No Verified and Acknowledged /THU HA T NGUYEN/ Examiner's Signature	❑ Met after Allowance Initials	STATE OR COUNTRY	SHEETS DRAWINGS	TOTAL CLAIMS	INDEPENDENT CLAIMS
		CA	17	20	3

ADDRESS
Morgan, Lewis & Bockius LLP (PA)
1400 Page Mill Road
Palo Alto, CA 94304-1124
UNITED STATES

TITLE
System and Method for Identifying Unauthorized Activities on a Computer System using a Data Structure Model

FILING FEE RECEIVED	FEES: Authority has been given in Paper	❑ All Fees
840	No._____ to charge/credit DEPOSIT ACCOUNT	❑ 1.16 Fees (Filing)
	No._____ for following:	❑ 1.17 Fees (Processing Ext. of time)
		❑ 1.18 Fees (Issue)
		❑ Other _____
		❑ Credit

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14823916	CAPALIK ET AL.
	Examiner	**Art Unit**
	THU HA NGUYEN	2444

CPC						
Symbol					**Type**	**Version**
H04L		63	/	1416	F	2013-01-01
H04L		63	/	1491	I	2013-01-01
			/			
			/			
			/			
			/			
			/			
			/			
			/			
			/			
			/			
			/			
			/			
			/			
			/			

CPC Combination Sets						
Symbol				**Type**	**Set**	**Ranking**	**Version**
			/				
			/				

NONE (Assistant Examiner)	(Date)	**Total Claims Allowed:** 21	
/THU HA NGUYEN/ Primary Examiner.Art Unit 2444 (Primary Examiner)	11/27/17 (Date)	O.G. Print Claim(s) 1	O.G. Print Figure 1

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14823916	CAPALIK ET AL.
	Examiner	**Art Unit**
	THU HA NGUYEN	2444

US ORIGINAL CLASSIFICATION		INTERNATIONAL CLASSIFICATION	
CLASS	SUBCLASS	CLAIMED	NON-CLAIMED
726	23	G 0 6 F 11 / 00 (2006.01.01)	

CROSS REFERENCE(S)					
CLASS	SUBCLASS (ONE SUBCLASS PER BLOCK)				
726	1	2	26		

NONE		Total Claims Allowed:	
(Assistant Examiner)	(Date)	21	
/THU HA NGUYEN/ Primary Examiner.Art Unit 2444	11/27/17	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	1

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14823916	CAPALIK ET AL.
	Examiner	**Art Unit**
	THU HA NGUYEN	2444

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☒ T.D. ☐ R.1.47

Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original
1	1	17	17												
2	2	18	18												
3	3	20	19												
4	4	21	20												
5	5	19	21												
6	6														
7	7														
8	8														
9	9														
10	10														
11	11														
12	12														
13	13														
14	14														
15	15														
16	16														

NONE (Assistant Examiner)	(Date)	**Total Claims Allowed:** 21	
/THU HA NGUYEN/ Primary Examiner.Art Unit 2444 (Primary Examiner)	11/27/17 (Date)	O.G. Print Claim(s) 1	O.G. Print Figure 1

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	0	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 same associat$6 same auth$7 same fingerprint$4 and 726/1.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2017/11/27 14:10
L2	0	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 same associat$6 same auth$7 same fingerprint$4 and 726/2.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2017/11/27 14:10
L5	0	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 same associat$6 same auth$7 same fingerprint$4 and 726/23.ccls.	US-PGPUB; USPAT; JPO; DERWENT	OR	OFF	2017/11/27 14:10
L6	0	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 same associat$6 same auth$7 same fingerprint$4 and 726/26.ccls.	US-PGPUB; USPAT; JPO; DERWENT	OR	OFF	2017/11/27 14:10
L7	0	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 same associat$6 same auth$7 same fingerprint$4 and 726/27.ccls.	US-PGPUB; USPAT; JPO; DERWENT	OR	OFF	2017/11/27 14:10
L11	0	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 same associat$6 same auth$7 same fingerprint$4 and H04l63/1491.cpc.	US-PGPUB; USPAT; JPO; DERWENT	OR	OFF	2017/11/27 14:12
L12	36	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and 709/223.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2017/11/27 14:13
L13	76	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and 709/224.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2017/11/27 14:13
L15	161	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and fingerprint$4 and auth$9 and (compar$4 or match$4 or map$4) and prevent$4 and attack$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2017/11/27 14:13
L20	1	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and fingerprint$4 and auth$9 and (compar$4 or match$4 or map$4) and prevent$4 and attack$4 and 726/2.ccls.	US-PGPUB; USPAT; JPO; DERWENT	OR	OFF	2017/11/27 14:14
L21	5	monitor$4 same ((virtual adj machine$4) or	US-PGPUB;	OR	OFF	2017/11/27

		VM or VMM) same (activit$4 or event$4) and fingerprint$4 and auth$9 and (compar$4 or match$4 or map$4) and prevent$4 and attack$4 and 726/26.ccls.	USPAT; JPO; DERWENT			14:14
L22	1	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and fingerprint$4 and auth$9 and (compar$4 or match$4 or map$4) and prevent$4 and attack$4 and 726/27.ccls.	US-PGPUB; USPAT; JPO; DERWENT	OR	OFF	2017/11/27 14:14
L25	5	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) same fingerprint$4 same decoy$4 same unauthor$5	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2017/11/27 14:25
L33	131	monitor$4 same (activit$4 or event$4) and source and target$4 and fingerprint$4 and G06F21/566.cpc.	US-PGPUB; USPAT; JPO; DERWENT	OR	OFF	2017/11/27 14:29
L34	131	monitor$4 same (activit$4 or event$4) and source and target$4 and fingerprint$4 and 726/1-2.ccls.	US-PGPUB; USPAT; JPO; DERWENT	OR	OFF	2017/11/27 14:31
L35	129	monitor$4 same (activit$4 or event$4) and source and target$4 and fingerprint$4 and 726/26.ccls.	US-PGPUB; USPAT; JPO; DERWENT	OR	OFF	2017/11/27 14:31
L36	95	monitor$4 same (activit$4 or event$4) and source and target$4 and fingerprint$4 and 726/27.ccls.	US-PGPUB; USPAT; JPO; DERWENT	OR	OFF	2017/11/27 14:31

EAST Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L3	0	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 same associat$6 same auth$7 same fingerprint$4 and 726/2.ccls.	US-PGPUB; USPAT	OR	OFF	2017/11/27 14:10
L4	0	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 same associat$6 same auth$7 same fingerprint$4 and 726/23.ccls.	US-PGPUB; USPAT	OR	OFF	2017/11/27 14:10
L8	0	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 same associat$6 same auth$7 same fingerprint$4 and 726/27.ccls.	US-PGPUB; USPAT	OR	OFF	2017/11/27 14:10
L9	0	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 same associat$6 same auth$7 same fingerprint$4 and H04l63/1416.cpc.	US-PGPUB; USPAT	OR	OFF	2017/11/27 14:11
L10	0	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 same associat$6 same auth$7 same fingerprint$4 and H04l63/1491.cpc.	US-PGPUB; USPAT	OR	OFF	2017/11/27 14:12
L14	76	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and 709/224.ccls.	US-PGPUB; USPAT	OR	OFF	2017/11/27 14:13

L16	161	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and fingerprint$4 and auth$9 and (compar$4 or match$4 or map$4) and prevent$4 and attack$4	US-PGPUB; USPAT	OR	OFF	2017/11/27 14:13
L17	4	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and fingerprint$4 and auth$9 and (compar$4 or match$4 or map$4) and prevent$4 and attack$4 and 709/223-224.ccls.	US-PGPUB; USPAT	OR	OFF	2017/11/27 14:14
L18	3	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and fingerprint$4 and auth$9 and (compar$4 or match$4 or map$4) and prevent$4 and attack$4 and 726/1.ccls.	US-PGPUB; USPAT	OR	OFF	2017/11/27 14:14
L19	1	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and fingerprint$4 and auth$9 and (compar$4 or match$4 or map$4) and prevent$4 and attack$4 and 726/2.ccls.	US-PGPUB; USPAT	OR	OFF	2017/11/27 14:14
L23	1	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and fingerprint$4 and auth$9 and (compar$4 or match$4 or map$4) and prevent$4 and attack$4 and 726/27.ccls.	US-PGPUB; USPAT	OR	OFF	2017/11/27 14:14
L24	5	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and fingerprint$4 and auth$9 and (compar$4 or match$4 or map$4) and prevent$4 and attack$4 and 726/26.ccls.	US-PGPUB; USPAT	OR	OFF	2017/11/27 14:14
L26	5	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) same fingerprint$4 same decoy$4 same unauthor$5	US-PGPUB; USPAT	OR	OFF	2017/11/27 14:25
L27	8	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and fingerprint$4 and G06F21/50.cpc.	US-PGPUB; USPAT	OR	OFF	2017/11/27 14:25
L28	37	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and fingerprint$4 and auth$9 and (compar$4 or match$4 or map$4) and prevent$4 and attack$4 and H04L63/1416.cpc.	US-PGPUB; USPAT	OR	OFF	2017/11/27 14:25
L29	12	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and fingerprint$4 and G06F21/52.cpc.	US-PGPUB; USPAT	OR	OFF	2017/11/27 14:25
L30	8	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) same fingerprint$4 and auth$9 and (compar$4 or match$4 or map$4) and prevent$4 same attack$4	US-PGPUB; USPAT	OR	OFF	2017/11/27 14:28
L31	52	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and fingerprint$4 and G06F21/566.cpc.	US-PGPUB; USPAT	OR	OFF	2017/11/27 14:29
L32	131	monitor$4 same (activit$4 or event$4) and source and target$4 and fingerprint$4 and G06F21/566.cpc.	US-PGPUB; USPAT	OR	OFF	2017/11/27 14:29
L37	95	monitor$4 same (activit$4 or event$4) and	US-	OR	OFF	2017/11/27

		source and target$4 and fingerprint$4 and 726/27.ccls.	PGPUB; USPAT			14:31

11/27/2017 2:42:29 PM
C:\Users\tnguyen39\Documents\EAST\Workspaces\14823916.wsp

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14823916	CAPALIK ET AL.
	Examiner	Art Unit
	THU HA NGUYEN	2453

CPC- SEARCHED		
Symbol	Date	Examiner
H04L63/1416; 63/1491	08/22/16	THN
Update search (search note attached)	11/27/17	THN

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner
726	23, 25	08/22/16	THN
Update search		05/30/17	THN
Update search		11/27/17	THN
726	1, 2, 26, 27	11/27/17	THN

* See search history printout included with this form or the SEARCH NOTES box below to determine the scope of the search.

SEARCH NOTES		
Search Notes	Date	Examiner
East, Derwent, JPO, EPO, USPG-Pub search	08/22/16	THN
Inventor name, assignee name search	08/22/16	THN
Update search	05/30/17	THN
Update search	11/27/17	THN
East search note attached	11/27/17	THN

INTERFERENCE SEARCH

US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner
726	1, 2, 26	11/27/17	THN

IPR2025-00068
CrowdStrike EX1002 Page 28

Document code: WFEE

United States Patent and Trademark Office
Sales Receipt for Accounting Date: 01/22/2018

SBROWN2 SALE #00000016 Mailroom Dt: 12/12/2017 500310 14823916
01 FC : 2806 90.00 DA

INFORMATION DISCLOSURE STATEMENT BY APPLICANT Substitute for Form 1449-PTO				Electronically filed December 12, 2017	
				Application Number	14/823,916
				Filing Date	August 11, 2015
				First Named Inventor	Alen Capalik
				Art Unit	2444
				Examiner Name	Nguyen, Thu Ha T.
Sheet	1	of	1	Attorney Docket Number	067292-5005-US01

NON PATENT LITERATURE DOCUMENTS		
Examiner Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published
		CounterTack Inc., Communication Pursuant to Article 94(3), EP11729826.5, 22JUN2017, 5 pgs.
		CounterTack Inc., Intent to Grant, EP11731194.4, 20JUL2017, 6 pgs.
		CounterTack Inc., International Preliminary Report on Patentability, PCTUS2016/012533, 11JUL2017, 8 pgs.
		CounterTack Inc., Office Action, CA 2,689,126, received on 02JUN2017, 3 pgs

Examiner Signature		Date Considered	

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY
(Chapter I of the Patent Cooperation Treaty)

(PCT Rule 44*bis*)

Applicant's or agent's file reference 067292-5007WO	**FOR FURTHER ACTION**	See item 4 below
International application No. PCT/US2016/012533	International filing date *(day/month/year)* 07 January 2016 (07.01.2016)	Priority date *(day/month/year)* 07 January 2015 (07.01.2015)
International Patent Classification (8th edition unless older edition indicated) See relevant information in Form PCT/ISA/237		
Applicant COUNTERTACK, INC.		

1. This international preliminary report on patentability (Chapter I) is issued by the International Bureau on behalf of the International Searching Authority under Rule 44 *bis*.1(a).

2. This REPORT consists of a total of 8 sheets, including this cover sheet.

   In the attached sheets, any reference to the written opinion of the International Searching Authority should be read as a reference to the international preliminary report on patentability (Chapter I) instead.

3. This report contains indications relating to the following items:

☒	Box No. I	Basis of the report
☐	Box No. II	Priority
☐	Box No. III	Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
☐	Box No. IV	Lack of unity of invention
☒	Box No. V	Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
☐	Box No. VI	Certain documents cited
☐	Box No. VII	Certain defects in the international application
☒	Box No. VIII	Certain observations on the international application

4. The International Bureau will communicate this report to designated Offices in accordance with Rules 44*bis*.3(c) and 93*bis*.1 but not, except where the applicant makes an express request under Article 23(2), before the expiration of 30 months from the priority date (Rule 44*bis* .2).

	Date of issuance of this report 11 July 2017 (11.07.2017)
The International Bureau of WIPO 34, chemin des Colombettes 1211 Geneva 20, Switzerland Facsimile No. +41 22 338 82 70	Authorized officer Agnès Wittmann-Regis e-mail: pct.team6@wipo.int

Form PCT/IB/373 (January 2004)

PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

To:

see form PCT/ISA/220

PCT

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

(PCT Rule 43*bis*.1)

Date of mailing
(day/month/year) see form PCT/ISA/210 (second sheet)

Applicant's or agent's file reference
see form PCT/ISA/220

FOR FURTHER ACTION
See paragraph 2 below

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/US2016/012533	07.01.2016	07.01.2015

International Patent Classification (IPC) or both national classification and IPC
INV. H04L29/06 G06F9/445 G06F21/55 G06F9/45 G06F9/30

Applicant
COUNTERTACK, INC.

1. This opinion contains indications relating to the following items:

- ☒ Box No. I Basis of the opinion
- ☐ Box No. II Priority
- ☐ Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- ☐ Box No. IV Lack of unity of invention
- ☒ Box No. V Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step and industrial applicability; citations and explanations supporting such statement
- ☐ Box No. VI Certain documents cited
- ☐ Box No. VII Certain defects in the international application
- ☒ Box No. VIII Certain observations on the international application

2. **FURTHER ACTION**

If a demand for international preliminary examination is made, this opinion will usually be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notifed the International Bureau under Rule 66.1*bis*(b) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

Name and mailing address of the ISA:	Date of completion of this opinion	Authorized Officer
European Patent Office D-80298 Munich Tel. +49 89 2399 - 0 Fax: +49 89 2399 - 4465	see form PCT/ISA/210	Rey, Salvador Telephone No. +49 89 2399-0

Form PCT/ISA/237 (Cover Sheet) (January 2015)

Box No. I Basis of the opinion

1. With regard to the **language**, this opinion has been established on the basis of:

   ☒ the international application in the language in which it was filed.

   ☐ a translation of the international application into , which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1 (b)).

2. ☐ This opinion has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43*bis*.1(a))

3. ☐ With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, this opinion has been established on the basis of a sequence listing:

   a. ☐ forming part of the international application as filed:

      ☐ in the form of an Annex C/ST.25 text file.

      ☐ on paper or in the form of an image file.

   b. ☐ furnished together with the international application under PCT Rule 13*ter*.1(a) for the purposes of international search only in the form of an Annex C/ST.25 text file.

   c. ☐ furnished subsequent to the international filing date for the purposes of international search only:

      ☐ in the form of an Annex C/ST.25 text file (Rule 13*ter*.1(a)).

      ☐ on paper or in the form of an image file (Rule 13*ter*.1(b) and Administrative Instructions, Section 713).

4. ☐ In addition, in the case that more than one version or copy of a sequence listing has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that forming part of the application as filed or does not go beyond the application as filed, as appropriate, were furnished.

5. Additional comments:

Box No. V Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes:	Claims	5, 21
	No:	Claims	1-4, 6-20, 22-26
Inventive step (IS)	Yes:	Claims	
	No:	Claims	1-26
Industrial applicability (IA)	Yes:	Claims	1-26
	No:	Claims	

2. Citations and explanations

see separate sheet

Box No. VIII Certain observations on the international application

The following observations on the clarity of the claims, description, and drawings or on the question whether the claims are fully supported by the description, are made:

see separate sheet

Re Item V

Reasoned statement with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1 Reference is made to the following documents:

D1 US 2014/108635 A1 (KHEMANI PRAKASH [US] ET AL) 17 April 2014 (2014-04-17)

2 The present application does not meet the criteria of Article 33(1) PCT, because the subject-matter of claims 1 and 14 is not new in the sense of Article 33(2) PCT.

2.1 D1 discloses the following features of claim 1 (references between parentheses):

A computer implemented method of monitoring a collector computer system, the collector computer system comprising one or more processors (fig. 1d, 2b, par. 0077-0079, monitoring service including data collection, analysis and reporting; monitoring service including monitoring agents; monitoring agent including software and/or hardware for performing collection activities on an appliance; fig. 7a, par. 0187-0188, configure policies corresponding to plurality of appliances) and memory storing an interpreter and compiled instructions for execution by the one or more processors (fig. 2B, par. 0109-110, policy engine in appliance provides a configuration mechanism to allow a user to define or configure a caching policy; policy engine comprises functions or operations), said method comprising:
receiving machine interpretable code that is configured for interpretation by the interpreter, wherein the machine interpretable code is not directly executable by the one or more processors (par. 0180, a policy being interpreted at run-time on a policy engine, or being compiled before its execution) and the machine interpretable code includes: information identifying a first set of one or more monitoring targets within the collector computer system, a method for monitoring the first set of one or more monitoring targets, and predefined reporting criteria (par. 0130 the appliance inspects and intercepts attacks; par. 0180-0181, policies directing behaviour of the appliance including monitoring agents; policy comprising a rule evaluated at run-time with respect to objects, methods and operators);
interpreting the machine interpretable code with the interpreter to obtain the first set of one or more monitoring targets, the method for monitoring the first set of one or more monitoring targets, and the predefined reporting criteria (par. 0180, policy interpreted at run-time);

monitoring, using the one or more processors, at least a subset of the first set of one or more monitoring targets for candidate activity that satisfies the predefined reporting criteria by executing compiled instructions that correspond to the method for monitoring the first set of one or more monitoring targets; obtaining candidate event information that is associated with the candidate activity; and reporting the candidate event information to a computer system that is distinct from the collector computer system (par. 0077, agent of the monitoring service performs data collection, aggregation and reporting).

3 The objection above applies *mutatis mutandis* to corresponding independent system claims 10 and 12, and independent non-transitory computer readable storage medium claims 11 and 13.

4 The subject-matter of claim 14 is also not new as it is further disclosed in D1, fig. 7a, par. 0187-0188, configuration interface to configure policies corresponding to plurality of appliances, thus distributing the policies for these appliances from the device on which they are configured.

5 The objection above applies *mutatis mutandis* to corresponding independent system claims 23 and 25, and independent non-transitory computer readable storage medium claims 24 and 26.

6 Dependent claims 2-9 and 15-22 do not appear to contain any additional features which, in combination with the features of any claim to which they refer, meet the requirements of the PCT in respect of novelty and/or inventive step, as these are considered to further specify alternatives and implementation details which are either well known and thus obvious to the skilled person or disclosed in the prior art and which cannot be considered to involve an inventive step. See relevant passages of the International Search Report. In particular,

6.1 Claims 2 and 18: D1 also discloses object-oriented expressions for use in a policy engine using syntax of script languages, par. 0167-0168.

6.2 Claims 3 and 19: D1 also discloses the monitoring service performing monitoring of network infrastructure elements such as an appliance or network connection, par. 0079.

6.3 Claim 5 and 21: D1 also discloses the following features of claim 5 (references between parentheses):

The method of any of claims 1-4 (see point 2.1), wherein the receiving, the interpreting, the monitoring, and the obtaining are performed while the collector computer system is in a first state, the method further including: while

the collector computer system is in a second state that is distinct from the first state (no technical constraint is determined by this definition, since the state is determined by the actions performed and not inversely):
having at disposal~~receiving~~ machine executable code that is configured for execution by the one or more processors and that is not configured for interpretation by the interpreter (par. 0180, policy compiled before its execution, in opposition of being interpreted at run-time), wherein the machine executable code includes information identifying a second set of one or more monitoring targets, and second predefined reporting criteria;
monitoring using the one or more processors, the second set of the one or more monitoring targets for additional candidate activity that satisfies the second predefined reporting criteria by executing the machine executable code;
obtaining additional candidate event information that is associated with the additional candidate activity; and
reporting the additional candidate event information to the computer system that is distinct from the collector computer system (see point 2.1).

6.3.1 The subject-matter of claim 5 differs from D1 in that it further defines the policy being compiled prior to being received.

6.3.2 The difference above is considered as the obvious solution to the problem of how to execute a policy in compiled format in the absence of a local compiler in the appliance. Thus, the skilled person would arrive to the subject-matter of claim 5 when starting from D1 trying to solve the above mentioned problem without exercising inventive skill.

6.4 The subject-matter of claim 9 is also disclosed in D1, see fig. 2a, policy engine located in kernel space.

Re Item VIII

Certain observations on the international application

7 The application does not meet the requirements of Article 6 PCT, because claim 1 is not clear.

7.1 The imprecise statements in the description on paragraphs 0019 and 0047, indicating "incorporated by reference in its entirety" of prior applications, furthermore with a filing date earlier than twelve months of the current

application, imply that the subject-matter for which protection is sought may be different to that defined by the claims, thereby resulting in lack of clarity (Article 6 PCT) when used to interpret them.

Electronic Acknowledgement Receipt	
EFS ID:	31207763
Application Number:	14823916
International Application Number:	
Confirmation Number:	5143
Title of Invention:	System and Method for Identifying Unauthorized Activities on a Computer System using a Data Structure Model
First Named Inventor/Applicant Name:	Alen Capalik
Customer Number:	24341
Filer:	Tae-Woong Koo/Edith Fuentes
Filer Authorized By:	Tae-Woong Koo
Attorney Docket Number:	067292-5005-US01
Receipt Date:	12-DEC-2017
Filing Date:	11-AUG-2015
Time Stamp:	19:16:49
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		067292-5005US01_IDS.pdf	237332 8d5c944ee2214cb8fb8e59c0bef238b135096f76	yes	5

	Multipart Description/PDF files in .zip description				
	Document Description		**Start**	**End**	
	Transmittal Letter		1	4	
	Information Disclosure Statement (IDS) Form (SB08)		5	5	
Warnings:					
Information:					
2	Non Patent Literature	CounterTack_Comm-Pursuant-Article-94-3-EP11729826-5_22JUN2017.pdf	162362 8ce0725b0f3befcacc3220cd54a2ab3357415ffb	no	5
Warnings:					
Information:					
3	Non Patent Literature	CounterTack_Intent-to-Grant-EP11731194-4_20JUL2017.pdf	229029 6f6e637a4419cb7f5e7c113737bb4375d380f6f8	no	6
Warnings:					
Information:					
4	Non Patent Literature	Countertack_International-Preliminary-Rpt-Patentability-PCTUS2016012533_11JUL2017.pdf	304049 c0733c75d1e1e0de2cb32741687b3768ca2aa7b4	no	8
Warnings:					
Information:					
5	Non Patent Literature	CounterTack_Office-Action-CA2689126_received-02JUN2017.pdf	224667 8f4d6b6caac202f2222eb240c84322f99a3ca410	no	3
Warnings:					
Information:					
		Total Files Size (in bytes):	1157439		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Electronically filed December 12, 2017

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application of:	Capalik et al.	Confirmation No.:	5143
Serial No.:	14/823,916	Art Unit:	2444
Filed:	August 11, 2015	Examiner:	Nguyen, Thu Ha T.
For:	System and Method for Identifying Unauthorized Activities on a Computer System using a Data Structure Model	Attorney Docket No.:	067292-5005-US01

INFORMATION DISCLOSURE STATEMENT

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

In accordance with the duty of disclosure provisions of 37 C.F.R. §1.56, there is hereby provided certain information which the Examiner may consider material to the examination of the subject U.S. patent application. It is requested that the Examiner make this information of record if it is deemed material to the examination of the application.

1. Enclosures accompanying this Information Disclosure Statement are:

1a. ☒ A list of all patents, publications, applications, or other information submitted for consideration by the office.

1b. A legible copy of:

☐ Each foreign patent;

☐ Each publication or that portion which caused it to be listed on the PTO-1449;

☐ For each cited pending U.S. application, the application specification including the claims, and any drawing of the application, or portion of the application which caused it to be listed on the PTO-1449 including any claims directed to that portion;

☒ all other information or portion which caused it to be listed on the PTO-1449.

1c. ☐ An English language copy of search report(s) from a counterpart foreign application or PCT International Search Report.

1d. ☐ Explanations of relevancy (ATTACHMENT 1(d), hereto) or English language

IPR2025-00068
CrowdStrike EX1002 Page 42

abstracts of the non-English language publications.

2. ☒ This Information Disclosure Statement is filed under 37 C.F.R. §1.97(b):

☐ Within three months of the filing date of a national application other than a continued prosecution application under §1.53(d);

☐ Within three months of the date of entry of the national stage as set forth in §1.491 in an international application;

☐ Before the mailing of the first Office action on the merits;

☒ Before the mailing of a first Office action after the filing of a request for continued examination under §1.114.

3. ☐ This Information Disclosure Statement is filed under 37 C.F.R. §1.97(c) after the period specified in 37 C.F.R. §1.97(b), but before the mailing date of any of a final action under 37 C.F.R. §1.113, a notice of allowance under 37 C.F.R. §1.311 or an action that otherwise closes prosecution in the application.

(Check either Item 3a, 3b or 3c)

3a. ☐ The Certification Statement in Item 5 below is applicable. Accordingly, no fee is required.

3b. ☐ The $180.00 (large entity) fee set forth in 37 C.F.R. §1.17(p) in accordance with 37 C.F.R. §1.97(c) is to be charged to Morgan, Lewis & Bockius LLP Deposit Account No. 50-0310 (order no.).

3c. ☐ The $90.00 (small entity) fee set forth in 37 C.F.R. §1.17(p) in accordance with 37 C.F.R. §1.97(c) is to be charged to Morgan, Lewis & Bockius LLP Deposit Account No. 50-0310 (order no. 067292-5005-US01).

(Items 3b or 3c to be checked if any reference known for more than 3 months)

4. ☐ This Information Disclosure Statement is filed under 37 C.F.R. §1.97(d) after the period specified in 37 C.F.R. §1.97(c), but on or before the date of payment of the issue fee.

(Check Item 4a, and 4b or 4c)

4a. ☐ The Certification Statement in Item 5 below is applicable.

4b. ☐ The $180.00 (large entity) fee set forth in 37 C.F.R. §1.17(p) in accordance with 37 C.F.R. §1.97(c) is to be charged to Morgan, Lewis & Bockius LLP Deposit Account No. 50-0310 (order no.).

4c. ☐ The $90.00 (small entity) fee set forth in 37 C.F.R. §1.17(p) in accordance with 37 C.F.R. §1.97(c) is to be charged to Morgan, Lewis & Bockius LLP Deposit Account No. 50-0310 (order no.).

5. ☐ Certification Statement (applicable if Item 3a or Item 4a is checked)

(Check either Item 5a, 5b, 5c or 5d)

5a. ☐ In accordance with 37 C.F.R. §1.97(e)(1), it is certified that each item of information contained in this information disclosure statement was first cited in a communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of this Information Disclosure Statement.

5b. ☐ In accordance with 37 C.F.R. §1.97(e)(2), it is certified that no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 C.F.R. §1.56(c) more than three months prior to the filing of this information disclosure statement.

5c. ☐ Each item of information contained in this information disclosure statement was cited in a communication from a foreign patent office in a counterpart application, and the communication was not **received** by any individual designated in 37 C.F.R. §1.56(c) more than thirty days prior to the filing of this information disclosure statement.

5d. ☐ Pursuant to 37 C.F.R. §1.704(d), each item of information contained in this information disclosure statement was cited in a communication from a foreign patent office in a counterpart application, and the communication was not **received** by any individual designated in 37 C.F.R. §1.56(c) more than thirty days prior to the filing of this information disclosure statement.

6. ☐ Copies of each cited U.S. patent and each U.S. patent application publication are not enclosed pursuant to the USPTO OG Notice dated 05 August 2003 waiving the requirement under 37 C.F.R. 1.98(a)(2)(i) for U.S. patent applications filed after June 30, 2003.

7. ☐ This application is a continuation application under 37 C.F.R. §1.53(b) or (d).

(Check appropriate Items 7a, 7b and/or 7c)

7a. ☐ A Petition to Withdraw from issue under 37 C.F.R. §1.313(b)(5) is concurrently filed herewith.

7b. ☐ Copies of publications listed on Form PTO-1449 from prior application Serial No. , filed on , of which this application claims priority under 35 U.S.C. §120, are not being submitted pursuant to 37 C.F.R. §1.98(d).

7c. ☐ Copies of the publications listed on the attached Form PTO-1449 that were not previously cited in prior application Serial No. , filed on , are provided herewith.

8. ☐ This is a Supplemental Information Disclosure Statement. (Check Item 8a)

8a. ☐ This Supplemental Information Disclosure Statement under 37 C.F.R. §1.97(f) supplements the Information Disclosure Statement filed on . A bona fide attempt was made to comply with 37 C.F.R. §1.98, but inadvertent omissions were made. These omissions have been corrected herein. Accordingly, additional time is

IPR2025-00068
CrowdStrike EX1002 Page 44

requested so that this Supplemental Information Disclosure Statement can be considered as if properly filed on .

9. ☐ In accordance with 37 C.F.R. §1.98, a concise explanation of what is presently understood to be the relevance of each non-English language publication is:

(Check Item 9a, 9b, or 9c)

9a. ☐ satisfied because all non-English language publications were cited on the enclosed English language copy of the PCT International Search Report or the search report from a counterpart foreign application indicating the degree of relevance found by the foreign office.

9b. ☐ set forth in the application.

9c. ☐ enclosed as an attachment hereto.

10. ☒ The Commissioner is authorized to charge any additional fee required or credit any overpayment for this Information Disclosure Statement and/or Petition to Morgan, Lewis & Bockius LLP Deposit Account No. 50-0310 (order no. 067292-5005-US01).

11. ☒ No admission is made that the information cited in this Statement is, or is considered to be, material to patentability nor a representation that a search has been made (other than a search report of a foreign counterpart application or PCT International Search Report if submitted herewith). 37 C.F.R. §§1.97(g) and (h).

Respectfully submitted,

Date: December 12, 2017

59,649

Tae-Woong Koo (Reg. No.)
MORGAN, LEWIS & BOCKIUS LLP
1400 Page Mill Road
Palo Alto, CA 94304
(650) 843-4000

IPR2025-00068
CrowdStrike EX1002 Page 45

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
14/823,916	08/11/2015	Alen Capalik	067292-5005-US01

CONFIRMATION NO. 5143

24341
Morgan, Lewis & Bockius LLP (PA)
1400 Page Mill Road
Palo Alto, CA 94304-1124

POA ACCEPTANCE LETTER

OC000000095359397

Date Mailed: 11/13/2017

NOTICE OF ACCEPTANCE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 11/06/2017.

The Power of Attorney in this application is accepted. Correspondence in this application will be mailed to the above address as provided by 37 CFR 1.33.

Questions about the contents of this notice and the requirements it sets forth should be directed to the Office of Data Management, Application Assistance Unit, at **(571) 272-4000** or **(571) 272-4200** or **1-888-786-0101**.

/mteklemichael/

Application Number	Application/Control No.	Applicant(s)/Patent under Reexamination	
	14/823,916	CAPALIK ET AL.	

Document Code - DISQ	Internal Document – DO NOT MAIL

TERMINAL DISCLAIMER	☒ APPROVED	☐ DISAPPROVED
Date Filed : 06 November, 2017	**This patent is subject to a Terminal Disclaimer**	

Approved/Disapproved by:

/CRYSTAL QUEEN/

Technology Center: PLRC

Telephone: _____

U.S. Patent and Trademark Office

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
14/823,916	08/11/2015	Alen Capalik	067292-5005-US01

CONFIRMATION NO. 5143

24341
Morgan, Lewis & Bockius LLP (PA)
1400 Page Mill Road
Palo Alto, CA 94304-1124

POA ACCEPTANCE LETTER

OC000000095324217

Date Mailed: 11/09/2017

NOTICE OF ACCEPTANCE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 11/06/2017.

The Power of Attorney in this application is accepted. Correspondence in this application will be mailed to the above address as provided by 37 CFR 1.33.

Questions about the contents of this notice and the requirements it sets forth should be directed to the Office of Data Management, Application Assistance Unit, at **(571) 272-4000** or **(571) 272-4200** or **1-888-786-0101**.

/ltaba/

REQUEST FOR CONTINUED EXAMINATION (RCE) TRANSMITTAL

Address to:
Mail Stop RCE
Commissioner of Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Electronically filed	November 6, 2017
Application Number	14/823,916
Filing Date	August 11, 2015
First Named Inventor	Alen Capalik
Art Unit	2444
Examiner Name	NGUYEN, THU HA T
Attorney Docket No.	067292-5005-US01

This is a Request for Continued Examination (RCE) under 37 C.F.R. § 1.114 of the above-identified application. Request for Continued Examination (RCE) practice under 37 CFR 1.114 does not apply to any utility or plant application filed prior to June 8, 1995, or to any design application.

1. Submission required under 37 C.F.R. § 1.114
   - a. ☐ Previously submitted
     - i. ☐ Consider the amendment(s)/reply under 37 C.F.R. § 1.116 previously filed on _____ (Any unentered amendment(s) referred to above will be entered).
     - ii. ☐ Consider the arguments in the Appeal Brief or Reply Brief previously filed _____
     - iii. ☐ Other _____
   - b. ☒ Enclosed
     - i. ☒ Amendment/Reply
     - ii. ☐ Affidavit(s)/Declaration(s)
     - iii. ☐ Information Disclosure Statement (IDS)
     - iv. ☐ Other _____
2. Miscellaneous
   - a. ☐ Suspension of action on the above-identified application is requested under 37 C.F.R. § 1.103(c) for a period of _____ months. (Period of suspension shall not exceed 3 months; Fee under 37 C.F.R. § 1.17(i) required)
   - b. ☐ Other _____
3. Fees — The RCE fee under 37 C.F.R. § 1.17(e) is required by 37 C.F.R. § 1.114 when the RCE is filed.
   - a. ☒ The Director is hereby authorized to charge the following fees, any underpayment of fees, or credit any overpayments, to Morgan, Lewis & Bockius LLP Deposit Account No. 50-0310 (order no. 067292-5005-US01).
     - i. ☒ (1st request) RCE fee required under 37 C.F.R. § 1.17(e)(1), estimated to be $ 1200 (large entity) or **$600 (small entity)**
     - ii. ☐ (2nd or subsequent request) RCE fee required under 37 C.F.R. § 1.17(e)(2), estimated to be $ 1700 (large entity) or $850 (small entity)
     - iii. ☒ Extension of time fee required under 37 C.F.R. §§ 1.136 and 1.17, estimated to be $ 300 for a two month(s) extension, the request for which is being made herewith
     - iv. ☒ Other Terminal Disclaimer
   - b. ☐ Check in the amount of $ _____ enclosed
   - c. ☐ Payment by credit card (Form PTO-2038 enclosed)

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT REQUIRED

Name (Print/Type)	Tae-Woong Koo	*Registration No. (Attorney/Agent)*	59,649
Signature		*Date*	November 6, 2017

CERTIFICATE OF MAILING OR TRANSMISSION

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Mail Stop RCE, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, or by facsimile transmitted to fax no. 1-703- to the U.S. Patent and Trademark Office on the date indicated below.

Name (Print/Type)		*Registration No. (Attorney/Agent)*	
Signature		*Date*	

DB2/ 32236724.1

REMARKS

This amendment responds to the office action mailed June 6, 2017. In the office action, the Examiner rejected:

- claims 1-20 on the ground of nonstatutory double patenting over claims 1-23 of U.S. Patent No. 9,106,697; and
- claims 1-20 under pre-AIA 35 U.S. C. 103(a) over Jiang U.S. Pub. No. 2008/0320594, in view of Aziz et al., U.S. Pub. No. 2012/0331553.

Interview Summary

Applicant's representatives, Tae-Woong Koo and Koji Yoshida, thank Examiner Nguyen for her helpful comments during the telephone interview on September 27, 2017. During the interview, amendments to independent claim 1 were discussed. Examiner Nguyen indicated that the amendments discussed during the interview would overcome the current §103 rejections of claim 1, but an additional search would be required. No agreement was reached in terms of the allowability of the claims.

McKesson Statement

The pending application is related to:

- U.S. Patent No. 9,106,697, which issued from U.S. Patent Application Serial No. 13/163,590, which is a parent application of this application;
- U.S. Patent No. 8,429,746, which issued from U.S. Patent Application Serial No. 11/488,743.
- U.S. Patent No. 8,484,152, which issued from U.S. Patent Application Serial No. 12/459,203;
- U.S. Patent No. 8,656,493, which issued from U.S. Patent Application Serial No. 13/759,335;
- U.S. Patent No. 8,769,689, which issued from U.S. Patent Application Serial No. 12/386,970;
- U.S. Patent No. 8,789,189, which issued from U.S. Patent Application Serial No. 13/163,578;
- U.S. Patent No. 9,311,482, which issued from U.S. Patent Application Serial No. 13/200,504;

IPR2025-00068
CrowdStrike EX1002 Page 50

- U.S. Patent No. 9,792,444, which issued from U.S. Patent Application Serial No. 15/063,312;
- U.S. Patent Application Serial No. 14/542,376, which has been allowed;
- U.S. Patent Application Serial No. 11/788,795, which has been abandoned;
- U.S. Patent Application Serial No. 14/990,575; and
- U.S. Patent Application Serial No. 14/317,958.

The Examiner is encouraged to review the art made of record, Office Action(s) and the Notices of Allowance in the above-mentioned related applications, all of which are available on PAIR.

Amendments to the Claims

Claims 1-3, 15, 17, and 19-20 have been amended for clarity. Claim 21 has been added. Support for the claim revisions and the new claim can be found at least in original claims and paragraphs [0066]-[0067], [0069]-[0070], [0072] and [0103]-[0104] of the specification as originally filed.

No new matter has been added. With respect to all amendments, Applicant has not dedicated or abandoned any unclaimed subject matter. Moreover, Applicant has not acquiesced to any characterizations of the invention, nor any rejections or objections of the claims, made by the Examiner.

REMARKS CONCERNING NONSTATUTORY DOUBLE PATENTING REJECTIONS

The Applicant submits a Terminal Disclaimer for the present application over U.S. Patent No. 9,106,697 to overcome the nonstatutory obviousness-type double patenting rejection. Accordingly, withdrawal of this rejection is respectfully requested.

REMARKS CONCERNING REJECTIONS UNDER 35 U.S.C. 103

To establish prima facie obviousness of a claimed invention, all the claim elements must be taught or suggested by the prior art. *In re Royka*, 490 F.2d 981, 180 USPQ 580 (CCPA 1974). Indeed, the Board of Patent Appeal and Interferences repeatedly confirmed that a proper obviousness determination requires an Examiner to make "a searching comparison of the claimed invention - including all its limitations - with the teaching of the prior art." See *In re Wada and Murphy*, Appeal 2007-3733, citing *In re Ochiai*, 71 F.3d 1565, 1572 (Fed. Cir. 1995) (emphasis in original). Finding all the claim elements in the prior art is

IPR2025-00068
CrowdStrike EX1002 Page 51

necessary, but not sufficient. *KSR Intern. Co. v. Teleflex Inc.*, 127 S.Ct. 1727, 1741 (2007) ("a patent composed of several elements is not proved obvious merely by demonstrating that each of its elements was, independently, known in the prior art"). "All words in a claim must be considered in judging the patentability of that claim against the prior art." *In re Wilson*, 424 F.2d 1382, 1385, 165 USPQ 494, 496 (CCPA 1970).

Amended claim 1 recites:

> monitoring activity on the first computer system;
>
> identifying a plurality of activities being performed at the first computer system, wherein each of the activities includes an activity source, an activity target, and an association between the activity source and the activity target;
>
> storing in the memory a data structure that identifies the activity sources, the activity targets, and the associations for the plurality of activities; and
>
> transmitting to one or more computer systems other than the first computer system information identifying one or more of the activity sources, the activity targets, and the associations for preventing future attacks, to the one or more computer systems, associated with the one or more of the activity sources, the activity targets, and the associations.

A combination of Jiang and Aziz does not teach or suggest the features above in amended claim 1. With respect to these features (before amendment), the Examiner states, *inter alia*:

> Aziz teaches … transmitting one or more of the activity source, activity target and associations to prevent future attacks associated with the one or more of the activity sources, the activity targets, and the associations (abstract, 0175-0180).[1]

Relevant portions of paragraphs [0175]-[0180] of Aziz are reproduced below to facilitate the Examiner's review.

> [0175] As the analysis environment 750 simulates the transmission of the network data, behavior of the virtual machine 815 can be closely monitored for unauthorized activity. …
>
> [0176] In some embodiments, the analysis environment 750 monitors and analyzes the behavior of the virtual machine 815 in order to determine a specific type of malware or the presence of an illicit computer user. … By simulating the transmission of suspicious network data and analyzing the response of the virtual machine, the analysis environment 750 can identify known and previously

[1] Office action dated June 6, 2017, p. 7.

IPR2025-00068
CrowdStrike EX1002 Page 52

> unidentified malware and the activities of illicit computer users before a computer system is damaged or compromised.
>
> ...
>
> [0180] In step 910, the transmission of the network data is orchestrated to analyze unauthorized activity. In one example, the transmission of the network data over a network is simulated to analyze the resulting action of the destination device. The simulation can be monitored and analyzed to identify the effects of malware or illegitimate computer use.

As shown above, paragraphs [0175]-[0180] of Aziz describe simulating transmission of the network data. However, paragraphs [0175]-[0180] of Aziz do not teach or suggest "transmitting to one or more computer systems other than the first computer system information identifying one or more of the activity sources, the activity targets, and the associations for preventing future attacks…" as required in claim 1. Simulating the transmission of the network data does not teach or suggest "one or more of the activity sources, the activity targets, and the associations." Furthermore, what is simulated in Aziz is the transmission of the network data, and not the information identifying "one or more of the activity sources, the activity targets, and the associations." If the transmitted network data in Aziz is replaced with the processed information, namely information identifying one or more of the activity sources, the activity targets, and the associations, the modification would interfere with the simulation of the transmission of the network data as described in Aziz, which would render the combination inoperable for the intended purpose. Thus, a person having ordinary skill in the art would not combine the disclosure of Jiang and the disclosure of Aziz as suggested by the Examiner. "the claimed combination cannot change the principle of operation of the primary reference or render the reference inoperable for its intended purpose. "[T]he claimed combination cannot change the principle of operation of the primary reference or render the reference inoperable for its intended purpose." MPEP § 2145(III). Also *see* MPEP § 2143.01.

Independent claims 19 and 20, as amended, include analogous features, and thus are also patentable over the cited references for analogous reasons.

New claim 21 is also patentable over the cited references, because the cited references do not teach or suggest the features of claim 21. Applicant respectfully requests that the Examiner consider claim 21 with a view toward allowance.

IPR2025-00068
CrowdStrike EX1002 Page 53

By responding in the foregoing remarks only to particular positions asserted by the Examiner, Applicant does not necessarily acquiesce in other positions that have not been explicitly addressed. In addition, the Applicant's arguments for the patentability of a claim should not be understood as implying that no other reasons for the patentability of that claim exist.

In light of the above amendments and remarks, Applicant respectfully requests that the Examiner reconsider this application with a view towards allowance. The Examiner is invited to call the undersigned attorney at (650) 843-4000, if a telephone call could help resolve any remaining items.

Respectfully submitted,

Date: November 6, 2017

/ Tae-Woong Koo / 59,649

Tae-Woong Koo (Reg. No.)
MORGAN, LEWIS & BOCKIUS LLP
1400 Page Mill Road
Palo Alto, CA 94304
(650) 843-4000

IPR2025-00068
CrowdStrike EX1002 Page 54

IN THE CLAIMS:

Please rewrite the pending claims as follows:

1. (Currently Amended) A computer implemented method of identifying unauthorized activities on a first computer system attached to a computer network, wherein the first computer system comprises one or more processors and memory, the method comprising:

monitoring activity on the first computer system;

identifying a plurality of activities being performed at the first computer system, wherein each of the activities includes an activity source, an activity target, and an association between the activity source and the activity target;

storing in the memory a data structure that identifies the activity sources, the activity targets, and the associations for the plurality of activities; and

transmitting to one or more computer systems other than the first computer system information identifying one or more of the activity sources, the activity targets, and the associations for [[to]] preventing future attacks, to the one or more computer systems, associated with the one or more of the activity sources, the activity targets, and the associations.

2. (Currently Amended) The method of claim 1, wherein the monitoring further comprises monitoring all activity on the first computer system.

3. (Currently Amended) The method of claim 1, further comprising:

creating, from the stored information, a fingerprint indicative of the activity on the first computer system.

4. (Original) The method of claim 1, wherein the activities comprise two or more of: a file initiating an execution of an instruction, an instruction reading a file, an instruction writing to a file, and receiving data through the network.

5. (Original) The method of claim 1, wherein a respective activity target comprises one of: a file, a user, an instruction, a thread, data stream, and network socket connections.

6. (Original) The method of claim 1, wherein a respective activity source comprises one of: a file, a user, an instruction, a thread, data stream, and network socket connections.

7. (Original) The method of claim 1, further comprising:

IPR2025-00068
CrowdStrike EX1002 Page 55

graphically displaying at least a subset of the stored activities.

8. (Original) The method of claim 7, wherein the displaying includes visually distinguishing at least a subset of the associations.

9. (Original) The method of claim 1, wherein an activity target of a first activity of the plurality of activities is an activity source of a second activity of the plurality of activities.

10. (Original) The method of claim 1, further comprising:

identifying a respective association between a first activity source and a first activity target as unauthorized, wherein the first activity target, when associated as a second activity source with a second activity target, causes unauthorized activities on the second activity target.

11. (Original) The method of claim 10, further comprising:

tracking a transfer of malicious associations over time.

12. (Original) The method of claim 1, further comprising:

identifying activity sources that are affected by unauthorized activities.

13. (Original) The method of claim 12, wherein the identifying activity sources that are affected by unauthorized activities includes identifying activity sources that request to access a portion of memory that is set as non-executable.

14. (Original) The method of claim 12, wherein:

instructions executed by the one or more processors have respective privilege levels;

respective activity sources have respective privilege levels; and

the identifying activity sources that are affected by unauthorized activities includes identifying activity sources that request to execute underprivileged instructions.

15. (Currently Amended) The method of claim 12, wherein the identifying activity sources that are affected by unauthorized activities includes identifying data stream incoming from outside the first computer system.

16. (Original) The method of claim 1, further comprising:

determining an activity status for the stored events, the activity status comprising one of:

IPR2025-00068
CrowdStrike EX1002 Page 56

a complete status, representing that a source of unauthorized activities is identified, and each activity target in the stored activities is associated with the source through one or more associations; and

an incomplete status, which represents that the source of unauthorized activities is not identified, or at least one activity target in the stored activities is not associated with the source through one or more associations.

17. (Currently Amended) The method of claim 1, further comprising:

determining an activity level representing a frequency of unauthorized activities on the first computer system during a predefined time interval.

18. (Original) The method of claim 1, further comprising:

identifying a respective activity as unauthorized based on a determination that the respective activity is associated with an unauthorized activity that is distinct from the respective activity.

19. (Currently Amended) A first computer system, comprising:

one or more processors; and

memory storing one or more programs, the one or more programs including instructions for:

monitoring activity on the first computer system;

identifying a plurality of activities being performed at the first computer system, where each of the activities includes an activity source, an activity target, and an association between the activity source and the activity target;

storing in the memory a data structure that identifies the activity sources, the activity targets, and the associations for the plurality of activities; and

transmitting to one or more computer systems other than the first computer system information identifying one or more of the activity sources, the activity targets, and the associations for [[to]] preventing future attacks, to the one or more computer systems, associated with the one or more of the activity sources, the activity targets, and the associations.

20. (Currently Amended) A computer readable storage medium, including one or more programs for execution by one or more processors of a first computer system, the one or more programs including instructions for:

IPR2025-00068
CrowdStrike EX1002 Page 57

monitoring activity on the first computer system;

identifying a plurality of activities being performed at the first computer system, where each of the activities includes an activity source, an activity target, and an association between the activity source and the activity target;

storing in memory of the first computer system a data structure that identifies the activity sources, the activity targets, and the associations for the plurality of activities; and

transmitting to one or more computer systems other than the first computer system information identifying one or more of the activity sources, activity targets, and associations for [[to]] preventing future attacks, to the one or more computer systems, associated with the one or more of the activity sources, the activity targets, and the associations.

21. (New) The method of claim 1, wherein the association includes a type that represents whether or not the activity source has modified the activity target to perform the unauthorized activities.

IPR2025-00068
CrowdStrike EX1002 Page 58

Electronically filed November 6, 2017

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application of:	Alen Capalik	Confirmation No.:	5143
Serial No.:	14/823,916	Art Unit:	2444
Filed:	August 11, 2015	Examiner:	NGUYEN, THU HA T
For:	System and Method for Identifying Unauthorized Activities on a Computer System using a Data Structure Model	Attorney Docket No.:	067292-5005-US01

RESPONSE TO FINAL OFFICE ACTION AND INTERVIEW SUMMARY

FILED WITH A REQUEST FOR CONTINUED EXAMINATION

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

The enclosed Amendment is in response to the Final Office Action dated June 6, 2017, for the above identified patent application.

Petition for Extension of Time under 37 CFR 1.136. It is respectfully requested that the time for response to the Office Action dated June 6, 2017, be extended for a period of two (2) months from September 6, 2017 to November 6, 2017.

The Commissioner is hereby authorized to charge any required fee(s) to Morgan, Lewis & Bockius LLP Deposit Account No. 50-0310 (order no. 067292-5005-US01).

IPR2025-00068
CrowdStrike EX1002 Page 59

Electronically filed November 6, 2017

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application of:	Alen Capalik	Confirmation No.:	5143
Serial No.:	14/823,916	Art Unit:	2444
Filed:	August 11, 2015	Examiner:	NGUYEN, THU HA T
For:	System and Method for Identifying Unauthorized Activities on a Computer System using a Data Structure Model	Attorney Docket No.:	067292-5005-US01

TERMINAL DISCLAIMER

Mail Stop Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Applicant, CounterTack Inc., is the assignee of the entire 100% right, title and interest in and to the above identified application by virtue of assignments recorded on July 7, 2015 at reel/frame 036074 / 0499.

Applicant hereby disclaims, except as provided below, the terminal part of the statutory term of any patent granted on the above identified application which would extend beyond the expiration date of the full statutory term of U.S. Patent No. 9,106,697 (the "prior patent"), which issued on August 11, 2015, as the term of said prior patent is presently shortened by any terminal disclaimer. Applicant hereby agrees that any patent so granted on the above identified application shall be enforceable only for and during such period that it and the prior patent are commonly owned.

Applicant further agrees that this agreement is to run with any patent granted on the above identified application and is to be binding upon the grantee, its successors, or assigns.

Applicant does not disclaim any terminal part of the term of any patent granted on the above identified application that would extend to the expiration date of the full statutory term of

IPR2025-00068
CrowdStrike EX1002 Page 60

said prior patent, "as the term of said prior patent is presently shortened by any terminal disclaimer," in the event that said prior patent later expires for failure to pay a maintenance fee, is held unenforceable, is found invalid by a court of competent jurisdiction, is statutorily disclaimed in whole or terminally disclaimed under 37 C.F.R. 1.321, has all claims canceled by a reexamination certificate, is reissued, or is otherwise terminated prior to the expiration of its full statutory term as presently shortened by any terminal disclaimer.

The undersigned is empowered to act on behalf of and as a representative of Countertack Inc. The undersigned is an attorney of record.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both, and that such willful false statements may jeopardize the validity of the application or any patent issuing thereon.

The fee under 37 CFR 1.20(d) is $160. The Commissioner is authorized to charge any required fees or credit any overpayments to our Deposit Account No. 50-0310 (order no. 067292-5005-US01).

Signed this 6th day of November, 2017.

By: / Tae-Woong Koo /
Tae-Woong Koo (Reg. No. 59,649)
Attorney of Record for Assignee, CounterTack Inc.
Telephone Number: 650-843-4000

IPR2025-00068
CrowdStrike EX1002 Page 61

Electronically filed November 6, 2017

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application of:	Alen Capalik	Confirmation No.:	5143
Serial No.:	14/823,916	Art Unit	2444
Filed:	August 11, 2015	Examiner:	NGUYEN, THU HA T
For:	System and Method for Identifying Unauthorized Activities on a Computer System using a Data Structure Model	Attorney Docket No.:	067292-5005-US01

STATEMENT UNDER 37 C.F.R. § 3.73(c)

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

CounterTack, Inc., a corporation, states that it is the assignee of the entire right, title and interest in the patent application identified above by virtue of an assignment from the inventor(s) of the parent of the patent application/patent identified above:

1.	From:	CAPALIK, ALEN, ANDREWS, DAVID, BECKER, BEN				
	To:	NEURALIQ				
	Recorded:	June 27, 2011	Reel:	026504	Frame:	0689
2.	From:	NEURALIQ, INC.				
	To:	COUNTERTACK, INC.				
	Recorded:	July 7, 2015	Reel:	036074	Frame:	0499

The undersigned is authorized to act on behalf of the assignee.

Date: November 6, 2017

/ Tae-Woong Koo / 59,649

Tae-Woong Koo (Reg. No.)
MORGAN, LEWIS & BOCKIUS LLP
1400 Page Mill Road
Palo Alto, CA 94304
(650) 843-4000

IPR2025-00068
CrowdStrike EX1002 Page 62

POWER OF ATTORNEY TO PROSECUTE APPLICATIONS BEFORE THE UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

I hereby revoke all previous powers of attorney given in the application identified in the attached statement under pre-AIA 37 CFR 3.73(b) or post AIA-37 CFR 3.73(c).

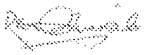
I hereby appoint the practitioners of Morgan, Lewis & Bockius LLP, Customer Number **24341** as attorneys or agents to represent the undersigned and to transact all business before the United States Patent and Trademark Office (USPTO) in connection with any and all patent applications and patents assigned only to the undersigned according to the USPTO assignment records or assignment documents attached to this form in accordance with pre-AIA 37 CFR 3.73(b) or post AIA-37 CFR 3.73(c), said appointment to be to the exclusion of the inventor(s) and their attorney(s) in accordance with the provisions of 37 C.F.R. § 3.71, provided that, if any one of these attorneys ceases being affiliated with the law firm of Morgan, Lewis & Bockius LLP as partner, counsel, or employee, then the appointment of that attorney and all powers derived therefrom shall terminate on the date such attorney ceases being so affiliated.

Please change the correspondence address for the application identified in the attached statement under pre pre-AIA 37 CFR 3.73(b) or post AIA-37 CFR 3.73(c) to the address associated with Customer Number **24341**.

Assignee Name and Address: CounterTack, Inc.
1639 11th Street, #119,
Santa Monica, CA 90404

SIGNATURE of Assignee of Record

The undersigned whose signature and title is supplied below is authorized to act on behalf of the assignee.

Signature			
Name	Raj Dodhiawala	Date	July 24, 2017
Title	Chief Product Officer	Telephone	425-985-4204

A copy of this form, together with a statement under 37 C.F.R. § 3.73(b) (Form PTO/SB96 or equivalent) is required to be filed in each application in which this form is used. The statement under 37 C.F.R. § 3.73(b) may be completed by one of the practitioners appointed in this form if the appointed practitioner is authorized to act on behalf of the assignee and must identify the application in which this Power of Attorney is to be filed.

Send to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450

DB2/ 26261822.1

Electronic Patent Application Fee Transmittal	
Application Number:	14823916
Filing Date:	11-Aug-2015
Title of Invention:	System and Method for Identifying Unauthorized Activities on a Computer System using a Data Structure Model
First Named Inventor/Applicant Name:	Alen Capalik
Filer:	Tae-Woong Koo
Attorney Docket Number:	067292-5005-US01
Filed as Small Entity	
Filing Fees for Utility under 35 USC 111(a)	

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
CLAIMS IN EXCESS OF 20	2202	1	40	40
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Extension - 2 months with $0 paid	2252	1	300	300
Miscellaneous:				
RCE- 1st Request	2801	1	600	600
STATUTORY OR TERMINAL DISCLAIMER	2814	1	160	160
		Total in USD ($)		**1100**

Electronic Acknowledgement Receipt	
EFS ID:	30870266
Application Number:	14823916
International Application Number:	
Confirmation Number:	5143
Title of Invention:	System and Method for Identifying Unauthorized Activities on a Computer System using a Data Structure Model
First Named Inventor/Applicant Name:	Alen Capalik
Customer Number:	24341
Filer:	Tae-Woong Koo
Filer Authorized By:	
Attorney Docket Number:	067292-5005-US01
Receipt Date:	06-NOV-2017
Filing Date:	11-AUG-2015
Time Stamp:	20:10:41
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	DA
Payment was successfully received in RAM	$1100
RAM confirmation Number	110717INTEFSW00006824500310
Deposit Account	
Authorized User	
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Request for Continued Examination (RCE)	067292_5005US01_RCE.pdf	85923 272811126d73ea8ea07908ac8dbe8a1f03a321a3	no	1
Warnings:					
This is not a USPTO supplied RCE SB30 form.					
Information:					
2		067292_5005_US01_AMEND.pdf	147096 062389856ce5a696b913d2e36edb9ec6c6c5f821	yes	10

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Applicant Arguments/Remarks Made in an Amendment	6	10
	Claims	2	5
	Response After Final Action	1	1

Warnings:					
Information:					
3	Terminal Disclaimer Filed	067292_5005US01_Ter_Dis.pdf	106096 db174345bcb452510bec25ec27787f27e786e416	no	2
Warnings:					
Information:					
4	Assignee showing of ownership per 37 CFR 3.73	067292_5005US01_STMT_POA.pdf	64349 0f2f4f7f264f0e06740fd9f30e5fe7a059765245	no	1
Warnings:					
Information:					

5	Power of Attorney	067292_5010US01_POA.pdf	613085 ff61827b59ab60c461af3daf5397f051cba2662a	no	1
Warnings:					
Information:					
6	Fee Worksheet (SB06)	fee-info.pdf	35555 bfebb5a641d7e4fe4cd4e864704290e75bcea189	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	1052104		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/SB/06 (09-11)
Approved for use through 1/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 14/823,916	Filing Date 08/11/2015	☐ To be Mailed

ENTITY: ☐ LARGE ☒ SMALL ☐ MICRO

APPLICATION AS FILED – PART I

	(Column 1)	(Column 2)		
FOR	NUMBER FILED	NUMBER EXTRA	RATE ($)	FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	21 minus 20 =	*	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	5 minus 3 =	*	X $ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	

APPLICATION AS AMENDED – PART II

AMENDMENT	11/06/2017	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 21	Minus	** 20	=	X $ =	
	Independent (37 CFR 1.16(h))	* 3	Minus	***3	=	X $ =	
	☐ Application Size Fee (37 CFR 1.16(s))						
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
						TOTAL ADD'L FEE	

AMENDMENT		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	*	Minus	**	=	X $ =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	X $ =	
	☐ Application Size Fee (37 CFR 1.16(s))						
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
						TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

LIE
PEGGY S. YARBOROUGH

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**
If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/823,916	08/11/2015	Alen Capalik	067292-5005-US01	5143

24341 7590 06/06/2017
Morgan, Lewis & Bockius LLP (PA)
1400 Page Mill Road
Palo Alto, CA 94304-1124

EXAMINER	
NGUYEN, THU HA T	

ART UNIT	PAPER NUMBER
2444	

NOTIFICATION DATE	DELIVERY MODE
06/06/2017	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

padocketingdepartment@morganlewis.com
vskliba@morganlewis.com

Office Action Summary	Application No. 14/823,916	Applicant(s) CAPALIK ET AL.	
	Examiner THU HA NGUYEN	Art Unit 2444	AIA (First Inventor to File) Status No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTHS FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *02/28/17*.

☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims*

5)☒ Claim(s) *1-20* is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6)☐ Claim(s) _____ is/are allowed.

7)☒ Claim(s) *1-20* is/are rejected.

8)☐ Claim(s) _____ is/are objected to.

9)☐ Claim(s) _____ are subject to restriction and/or election requirement.

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a)☐ All b)☐ Some** c)☐ None of the:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

** See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☒ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b) Paper No(s)/Mail Date *02/28/17, 08/10/16*.

3) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

4) ☐ Other: _____.

The present application is being examined under the pre-AIA first to invent provisions.

DETAILED ACTION

1. Claims **1- 20** are presented for examination.

2. Claims 1-3, 17, and 19-20 are currently amended.

Response to Arguments

3. Applicant's arguments filed 02/28/17 have been fully considered but they are not persuasive because of the following reasons:

4. Applicant argues that Jiang does not disclose "an activity source, an activity target, and an association between the activity source and the activity target".

5. In response to applicant's argument, the examiner submits that Aziz teaches wherein each of the activities includes an activity source, an activity target, and an association between the activity source and the activity target as shown in par. 0052-0058, 0087, 0090, 0108-0109 (*monitoring the plurality of ports of the computer network 110*).

6. Applicant argues that Aziz does not teach or suggest the claimed storing operation, namely "storing in the memory a data structure that identifies the activity sources, the activity targets, and the associations for the plurality of activities".

7. In response to applicant's argument, the examiner submits that Aziz does teach this feature as shown in par. 0019, 0050-0051, 0108-0109, 00116, 159-0161, 0179, 0190-0193 (*database 210 stores the identifier of source of computer worm and the recovery script of the computer worm*).

Double Patenting

8. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on nonstatutory double patenting provided the reference application or patent either is shown to be commonly owned with the examined application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement. See MPEP § 717.02 for applications subject to examination under the first inventor to file provisions of the AIA as explained in MPEP § 2159. See MPEP §§ 706.02(l)(1) - 706.02(l)(3) for applications not subject to examination under the first inventor to file

provisions of the AIA. A terminal disclaimer must be signed in compliance with 37 CFR 1.321(b).

The USPTO Internet website contains terminal disclaimer forms which may be used. Please visit www.uspto.gov/patent/patents-forms. The filing date of the application in which the form is filed determines what form (e.g., PTO/SB/25, PTO/SB/26, PTO/AIA/25, or PTO/AIA/26) should be used. A web-based eTerminal Disclaimer may be filled out completely online using web-screens. An eTerminal Disclaimer that meets all requirements is auto-processed and approved immediately upon submission. For more information about eTerminal Disclaimers, refer to www.uspto.gov/patents/process/file/efs/guidance/eTD-info-I.jsp.

Claims 1-20 rejected on the ground of nonstatutory double patenting as being unpatentable over claims 1-23 of U.S. Patent No. 9,106,697. Although the claims at issue are not identical, they are not patentably distinct from each other because the current claims of instant application encompass the same subject matter as the patented claims, but with obvious wording variations.

Claims 1-20 of instant application is directed toward identifying unauthorized activities on a computer system in which a virtual machine monitor supervising the virtual machine (VM) by monitoring activity on the VM; identifying and storing a plurality of activities performed by the VM, each of the activities includes activity source, activity target, and an association between activity source and activity target; and transmitting one or more activity source, activity target and associations to prevent further attacks.

Claims 1-23 of the Patent also mentions identifying unauthorized activities on a decoy computer system in which a virtual machine monitor supervising the virtual machine (VM) by monitoring activity on the VM; identifying and storing a plurality of activities performed by the VM, each of the activities includes activity source, activity target, and an association between activity source and activity target; creating a fingerprint indicative of the activity on the VM; and transmitting the fingerprint to prevent further attacks that comprise the same or similar activities as indicated by the fingerprint.

As can be seen there are some different between the claims; however, the differences are obvious and therefore, the claims are not patentably distinct from one another because the claims of the current application encompass the same subject matter as the patented claims.

Claim Rejections - 35 USC § 103

9. The following is a quotation of pre-AIA 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

10. Claims 1-20 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over **Jiang** U.S. Pub. No. **2008/0320594**, in view of **Aziz et al.,** U.S. Pub. No. **2012/0331553**.

11. As to claim 1, 20, **Jiang** teaches the invention as claimed, including a computer implemented method of identifying unauthorized activities on computer system attached to a computer network, wherein the system comprises one or more processors and memory, the method comprising:

monitoring activity on the computer system (fig. 4, par. 0031, 0033, 0039-0062, 0065-00067 –*VMWatcher can be used to create malware detection apparatus such as computer, processor or other devices such as PDA*);

identifying a plurality of activities being performed at the computer system (par. 0035, 0048-0050, 0059-0062 –*VM states and events*).

Jiang does not explicitly teach wherein each of the activities includes an activity source, an activity target, and an association between the activity source and the activity target; storing in the memory a data structure that identifies the activity sources, the activity targets, and the associations for the plurality of activities; and transmitting one or more of the activity source, activity target and associations to prevent future attacks associated with the one or more of the activity sources, the activity targets, and the associations.

Aziz teaches wherein each of the activities includes an activity source, an activity target, and an association between the activity source and the activity target (par. 0052-0058, 0087, 0090, 0108);

storing in the memory a data structure that identifies the activity sources, the activity targets, and the associations for the plurality of activities (par. 0019, 0050-0051, 0159-0161, 0179, 0190-0193); and

transmitting one or more of the activity source, activity target and associations to prevent future attacks associated with the one or more of the activity sources, the activity targets, and the associations (abstract, 0175-0180).

It would have been obvious to one of ordinary skill in the art at the time of the invention was made to combine the teaching of **Jiang and Aziz** in order to preventing the spread of malware.

12. As to claim 2, **Jiang** teaches the invention as claimed, including the method of claim 1, wherein the monitoring further comprises monitoring all activity on the virtual machine, and all activity on the computer system (par. 0064-0067, 0212).

13. As to claim 3, **Aziz** teaches the invention as claimed, including the method of claim 1, wherein the fingerprint includes files that are affected by the unauthorized activities on the virtual machine (par. 0022, 0165-0166).

14. As to claim 4, **Aziz** teaches the invention as claimed, including the method of claim 1, wherein the fingerprint includes processes that are affected by the unauthorized activities on the computer system (par. 0022, 0165-0166).

15. As to claim 5, **Jiang** teaches the invention as claimed, including the method of claim 1, wherein the activities comprise two or more of: a file initiating an execution of an instruction, an instruction reading a file, an instruction writing to a file, and receiving data through the network (abstract, par. 0102-0107).

16. As to claim 6, **Jiang** teaches the invention as claimed, including the method of claim 1, wherein a respective activity target comprises one of: a file, a user, an instruction, a thread, data stream, and network socket connections (par. 0032-0044).

17. As to claim 7, **Jiang** teaches the invention as claimed, including the method of claim 1, wherein a respective activity source comprises one of: a file, a user, an instruction, a thread, data stream, and network socket connections (par. 0032-0064, 0074-0077).

18. As to claim 8, **Jiang** teaches the invention as claimed, including the method of claim 1, further comprising graphically displaying at least a subset of the stored activities (par. 0090).

19. As to claim 9, **Jiang** teaches the invention as claimed, including the method of claim 8, wherein the displaying includes visually distinguishing at least a subset of the associations (par. 0032-0033, 0044, 0077).

20. As to claim 10, **Jiang** teaches the invention as claimed, including the method of claim 8, wherein the subset of activities includes a first activity and a second activity, and the activity target of the first activity is the activity source of the second activity (par. 0074-0075, 0077).

21. As to claim 11, **Jiang** teaches the invention as claimed, including the method of claim 1, further comprising identifying a respective association between a first activity source and a first activity target as unauthorized, wherein the first activity target, when associated as a second activity source with a second activity target, causes unauthorized activities on the second activity target (par. 0022, 0165-0166).

22. As to claim 12, **Aziz** teaches the invention as claimed, including the method of claim 11, further comprising tracking a transfer of malicious associations over time (par. 0098, 0101-0103, 0127, 0249).

23. As to claim 13, **Jiang** teaches the invention as claimed, including the method of claim 1, further comprising identifying activity sources that are affected by unauthorized activities (par. 0022, 0165-0166).

24. As to claim 14, **Jiang** teaches the invention as claimed, including the method of claim 13, wherein the identifying activity sources that are affected by unauthorized activities includes identifying activity sources that request to access a portion of memory that is set as non-executable (par. 0022, 0165-0166).

25. As to claim 15, **Jiang** teaches the invention as claimed, including the method of claim 13, wherein: instructions executed by the one or more processors have respective privilege levels; respective activity sources have respective privilege levels; and the identifying activity sources that are affected by unauthorized activities includes identifying activity sources that request to execute underprivileged instructions (par. 0102).

26. As to claim 16, **Jiang** teaches the invention as claimed, including the method of claim 13, wherein the identifying activity sources that are affected by unauthorized activities includes identifying data stream incoming from outside the computer system (abstract, par. 0029-0030, 0033-0043).

27. As to claim 17, **Jiang** teaches the invention as claimed, including the method of claim 1, further comprising determining an activity status for the stored events, the activity status comprising one of: a complete status, representing that a source of unauthorized activities is identified, and each activity target in the stored

activities is associated with the source through one or more associations; and an incomplete status, which represents that the source of unauthorized activities is not identified, or at least one activity target in the stored activities is not associated with the source through one or more associations (par. 0022, 0165-0166).

28. As to claim 18, **Jiang** teaches the invention as claimed, including the method of claim 1, further comprising determining an activity level representing a frequency of unauthorized activities on the virtual machine during a predefined time interval (par. 0119-0120).

29. As to claim 19, 20, **Jiang** teaches the invention as claimed, including a computer system, comprising:

one or more processors (par. 0043); and

memory storing one or more programs, the one or more programs including instructions for (fig. 3);

monitoring activity on the computer system (fig. 4, par. 0031, 0033, 0039-0062, 0065-00067-*VMWatcher*);

identifying a plurality of activities being performed at the computer system (par. 0035, 0048-0050, 0059-0061 –*VM states and events*).

Jiang does not explicitly teach where each of the activities includes an activity source, an activity target, and an association between the activity source and the activity target; storing in the memory a data structure that identifies the activity sources,

the activity targets, and the associations for the plurality of activities; and transmitting one or more of the activity source, the activity target and the associations to prevent future attacks associated with the one or more of the activity sources, the activity targets, and the associations.

Aziz teaches where each of the activities includes an activity source, an activity target, and an association between the activity source and the activity target (par. 0052-0058, 0087, 0090, 0108);

storing in the memory a data structure that identifies the activity sources, the activity targets, and the associations for the plurality of activities (par. 0019, 0050-0051, 0159-0161, 0179, 0190-0193);

transmitting one or more of the activity source, the activity target and the associations to prevent future attacks associated with the one or more of the activity sources, the activity targets, and the associations (abstract, 0175-0180).

It would have been obvious to one of ordinary skill in the art at the time of the invention was made to combine the teaching of **Jiang and Aziz** in order to preventing the spread of malware.

Conclusion

30. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within

TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

31. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thu Ha Nguyen, whose telephone number is (571) 272-3989. The examiner can normally be reached Monday through Friday from 8:30 AM to 5:00 PM.

32. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Peter-Anthony Pappas can be reached on 571-272-7646. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

33. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a

USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/THU HA NGUYEN/

Primary Examiner, Art Unit 2453

Notice of References Cited	Application/Control No. 14/823,916	Applicant(s)/Patent Under Reexamination CAPALIK ET AL.	
	Examiner THU HA NGUYEN	Art Unit 2444	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
	A	US-				
	B	US-				
	C	US-				
	D	US-				
	E	US-				
	F	US-				
	G	US-				
	H	US-				
	I	US-				
	J	US-				
	K	US-				
	L	US-				
	M	US-				

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	CPC Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	Dagon et al. HoneyStat: Local Worm Detection Using Honeypots, pp. 39-58, 2004
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Receipt date: 08/10/2016

INFORMATION DISCLOSURE STATEMENT BY APPLICANT Substitute for Form 1449-PTO				Electronically filed August 10, 2016	
				Application Number	14/823,916
				Filing Date	August 11, 2015
				First Named Inventor	Alen Capalik
				Art Unit	2453
				Examiner Name	Nguyen, Thu Ha T.
Sheet	1	of	1	Attorney Docket Number	067292-5005US01

U.S. PATENT DOCUMENTS					
Examiner Initials	Cite No.[1]	Document Number Number - Kind Code[2]	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		2006/0101516 A1	05-11-2006	Sudaharan et al.	
		2010/0153693 A1	06-17-2010	Stall et al.	
		2010/0306179 A1	12-02-2010	Lim	
		2012/0167063 A1	06-28-2012	Detwiler et al.	
		2014/0108635 A1	04-17-2014	Khemani et al.	

NON PATENT LITERATURE DOCUMENTS		
Examiner Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published
		Capalik, Office Action, US 14/542,376, 22JUN2016, 13 pgs
		CounterTack Inc., International Search Report and Written Opinion, PCTUS2016/012533, 16JUN2016, 12 pgs.

Examiner Signature	/THU HA T NGUYEN/	Date Considered	05/29/2017

DB2/ 30492683.1

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /T.T.N/

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14823916	CAPALIK ET AL.
	Examiner	**Art Unit**
	THU HA NGUYEN	2453

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	08/08/2016	05/30/2017							
	1	✓	✓							
	2	✓	✓							
	3	✓	✓							
	4	✓	✓							
	5	✓	✓							
	6	✓	✓							
	7	✓	✓							
	8	✓	✓							
	9	✓	✓							
	10	✓	✓							
	11	✓	✓							
	12	✓	✓							
	13	✓	✓							
	14	✓	✓							
	15	✓	✓							
	16	✓	✓							
	17	✓	✓							
	18	✓	✓							
	19	✓	✓							
	20	✓	✓							

Receipt date: 12/22/2016

INFORMATION DISCLOSURE STATEMENT BY APPLICANT Substitute for Form 1449-PTO				Electronically filed December 22, 2016	
				Application Number	14/823,916
				Filing Date	August 11, 2015
				First Named Inventor	Alen Capalik
				Art Unit	2444
				Examiner Name	Nguyen, Thu Ha T.
Sheet	1	of	1	Attorney Docket Number	067292-5005US01

NON PATENT LITERATURE DOCUMENTS		
Examiner Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published
		CounterTack Inc., Decision to Grant, EP15174670.8, 14SEP2016, 5 pgs.
		CounterTack Inc., Certificate of Grant, EP15174670.8, 14SEP2016, 1 pg.

Examiner Signature	/THU HA T NGUYEN/	Date Considered	05/29/2017

DB2/ 30917637.1

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /T.T.N/

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14823916	CAPALIK ET AL.
	Examiner	Art Unit
	THU HA NGUYEN	2453

CPC- SEARCHED		
Symbol	Date	Examiner
H04L63/1416; 63/1491	08/22/16	THN

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner
726	23, 25	08/22/16	THN
Update search		05/30/17	THN

SEARCH NOTES		
Search Notes	Date	Examiner
East, Derwent, JPO, EPO, USPG-Pub search	08/22/16	THN
Inventor name, assignee name search	08/22/16	THN
Update search	05/30/17	THN

INTERFERENCE SEARCH			
US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner

INFORMATION DISCLOSURE STATEMENT BY APPLICANT Substitute for Form 1449-PTO				Electronically filed May 31, 2017	
				Application Number	14/823,916
				Filing Date	August 11, 2015
				First Named Inventor	Alen Capalik
				Art Unit	2444
				Examiner Name	Nguyen, Thu Ha T.
Sheet	1	of	1	Attorney Docket Number	067292-5005-US01

NON PATENT LITERATURE DOCUMENTS		
Examiner Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published
		Capalik, Final Office Action, US 14/542,376, 24APR2017, 17 pgs.

Examiner Signature		Date Considered	

DB2/ 31520280.1

Electronic Patent Application Fee Transmittal	
Application Number:	14823916
Filing Date:	11-Aug-2015
Title of Invention:	System and Method for Identifying Unauthorized Activities on a Computer System using a Data Structure Model
First Named Inventor/Applicant Name:	Alen Capalik
Filer:	Tae-Woong Koo/Edith Fuentes
Attorney Docket Number:	067292-5005-US01
Filed as Small Entity	
Filing Fees for Utility under 35 USC 111(a)	

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
SUBMISSION- INFORMATION DISCLOSURE STMT	2806	1	90	90
		Total in USD ($)		**90**

Electronic Acknowledgement Receipt	
EFS ID:	29361828
Application Number:	14823916
International Application Number:	
Confirmation Number:	5143
Title of Invention:	System and Method for Identifying Unauthorized Activities on a Computer System using a Data Structure Model
First Named Inventor/Applicant Name:	Alen Capalik
Customer Number:	24341
Filer:	Tae-Woong Koo/Edith Fuentes
Filer Authorized By:	Tae-Woong Koo
Attorney Docket Number:	067292-5005-US01
Receipt Date:	31-MAY-2017
Filing Date:	11-AUG-2015
Time Stamp:	20:43:48
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	DA
Payment was successfully received in RAM	$90
RAM confirmation Number	060117INTEFSW00007432500310
Deposit Account	
Authorized User	
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		067292-5005US01_IDS.pdf	223396 16585631ec6ef020d97c15ac018eebb819b4010b	yes	5
	Multipart Description/PDF files in .zip description				
	Document Description		**Start**	**End**	
	Transmittal Letter		1	4	
	Information Disclosure Statement (IDS) Form (SB08)		5	5	
Warnings:					
Information:					
2	Other Reference-Patent/App/Search documents	Capalik_Final-Office-Action-US14542376_24APR2017.pdf	585775 91bdb994b72197cf6d8813f6e409bd0cdaa5dd5d	no	17
Warnings:					
Information:					
3	Fee Worksheet (SB06)	fee-info.pdf	30745 28692052d55f082a0c4eef58b16885dd54e13dc5	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	839916		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Electronically filed May 31, 2017

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application of:	Capalik et al.	Confirmation No.:	5143
Serial No.:	14/823,916	Art Unit:	2444
Filed:	August 11, 2015	Examiner:	Nguyen, Thu Ha T.
For:	System and Method for Identifying Unauthorized Activities on a Computer System using a Data Structure Model	Attorney Docket No.:	067292-5005-US01

INFORMATION DISCLOSURE STATEMENT

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

In accordance with the duty of disclosure provisions of 37 C.F.R. §1.56, there is hereby provided certain information which the Examiner may consider material to the examination of the subject U.S. patent application. It is requested that the Examiner make this information of record if it is deemed material to the examination of the application.

1. Enclosures accompanying this Information Disclosure Statement are:

1a. ☒ A list of all patents, publications, applications, or other information submitted for consideration by the office.

1b. A legible copy of:

☐ Each foreign patent;

☐ Each publication or that portion which caused it to be listed on the PTO-1449;

☐ For each cited pending U.S. application, the application specification including the claims, and any drawing of the application, or portion of the application which caused it to be listed on the PTO-1449 including any claims directed to that portion;

☒ all other information or portion which caused it to be listed on the PTO-1449.

1c. ☐ An English language copy of search report(s) from a counterpart foreign application or PCT International Search Report.

1d. ☐ Explanations of relevancy (ATTACHMENT 1(d), hereto) or English language

IPR2025-00068
CrowdStrike EX1002 Page 96

abstracts of the non-English language publications.

2. ☐ This Information Disclosure Statement is filed under 37 C.F.R. §1.97(b):

☐ Within three months of the filing date of a national application other than a continued prosecution application under §1.53(d);

☐ Within three months of the date of entry of the national stage as set forth in §1.491 in an international application;

☐ Before the mailing of the first Office action on the merits;

☐ Before the mailing of a first Office action after the filing of a request for continued examination under §1.114.

3. ☒ This Information Disclosure Statement is filed under 37 C.F.R. §1.97(c) after the period specified in 37 C.F.R. §1.97(b), but before the mailing date of any of a final action under 37 C.F.R. §1.113, a notice of allowance under 37 C.F.R. §1.311 or an action that otherwise closes prosecution in the application.

(Check either Item 3a, 3b or 3c)

3a. ☐ The Certification Statement in Item 5 below is applicable. Accordingly, no fee is required.

3b. ☐ The $180.00 (large entity) fee set forth in 37 C.F.R. §1.17(p) in accordance with 37 C.F.R. §1.97(c) is to be charged to Morgan, Lewis & Bockius LLP Deposit Account No. 50-0310 (order no.).

3c. ☒ The $90.00 (small entity) fee set forth in 37 C.F.R. §1.17(p) in accordance with 37 C.F.R. §1.97(c) is to be charged to Morgan, Lewis & Bockius LLP Deposit Account No. 50-0310 (order no. 067292-5005-US01).

(Items 3b or 3c to be checked if any reference known for more than 3 months)

4. ☐ This Information Disclosure Statement is filed under 37 C.F.R. §1.97(d) after the period specified in 37 C.F.R. §1.97(c), but on or before the date of payment of the issue fee.

(Check Item 4a, and 4b or 4c)

4a. ☐ The Certification Statement in Item 5 below is applicable.

4b. ☐ The $180.00 (large entity) fee set forth in 37 C.F.R. §1.17(p) in accordance with 37 C.F.R. §1.97(c) is to be charged to Morgan, Lewis & Bockius LLP Deposit Account No. 50-0310 (order no.).

4c. ☐ The $90.00 (small entity) fee set forth in 37 C.F.R. §1.17(p) in accordance with 37 C.F.R. §1.97(c) is to be charged to Morgan, Lewis & Bockius LLP Deposit Account No. 50-0310 (order no.).

5. ☐ Certification Statement (applicable if Item 3a or Item 4a is checked)

IPR2025-00068
CrowdStrike EX1002 Page 97

(Check either Item 5a, 5b, 5c or 5d)

5a. ☐ In accordance with 37 C.F.R. §1.97(e)(1), it is certified that each item of information contained in this information disclosure statement was first cited in a communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of this Information Disclosure Statement.

5b. ☐ In accordance with 37 C.F.R. §1.97(e)(2), it is certified that no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 C.F.R. §1.56(c) more than three months prior to the filing of this information disclosure statement.

5c. ☐ Each item of information contained in this information disclosure statement was cited in a communication from a foreign patent office in a counterpart application, and the communication was not **received** by any individual designated in 37 C.F.R. §1.56(c) more than thirty days prior to the filing of this information disclosure statement.

5d. ☐ Pursuant to 37 C.F.R. §1.704(d), each item of information contained in this information disclosure statement was cited in a communication from a foreign patent office in a counterpart application, and the communication was not **received** by any individual designated in 37 C.F.R. §1.56(c) more than thirty days prior to the filing of this information disclosure statement.

6. ☐ Copies of each cited U.S. patent and each U.S. patent application publication are not enclosed pursuant to the USPTO OG Notice dated 05 August 2003 waiving the requirement under 37 C.F.R. 1.98(a)(2)(i) for U.S. patent applications filed after June 30, 2003.

7. ☐ This application is a continuation application under 37 C.F.R. §1.53(b) or (d).

(Check appropriate Items 7a, 7b and/or 7c)

7a. ☐ A Petition to Withdraw from issue under 37 C.F.R. §1.313(b)(5) is concurrently filed herewith.

7b. ☐ Copies of publications listed on Form PTO-1449 from prior application Serial No. , filed on , of which this application claims priority under 35 U.S.C. §120, are not being submitted pursuant to 37 C.F.R. §1.98(d).

7c. ☐ Copies of the publications listed on the attached Form PTO-1449 that were not previously cited in prior application Serial No. , filed on , are provided herewith.

8. ☐ This is a Supplemental Information Disclosure Statement. (Check Item 8a)

8a. ☐ This Supplemental Information Disclosure Statement under 37 C.F.R. §1.97(f) supplements the Information Disclosure Statement filed on . A bona fide attempt was made to comply with 37 C.F.R. §1.98, but inadvertent omissions were made. These omissions have been corrected herein. Accordingly, additional time is

IPR2025-00068
CrowdStrike EX1002 Page 98

requested so that this Supplemental Information Disclosure Statement can be considered as if properly filed on .

9. ☐ In accordance with 37 C.F.R. §1.98, a concise explanation of what is presently understood to be the relevance of each non-English language publication is:

(Check Item 9a, 9b, or 9c)

9a. ☐ satisfied because all non-English language publications were cited on the enclosed English language copy of the PCT International Search Report or the search report from a counterpart foreign application indicating the degree of relevance found by the foreign office.

9b. ☐ set forth in the application.

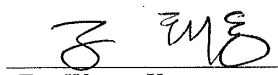
9c. ☐ enclosed as an attachment hereto.

10. ☒ The Commissioner is authorized to charge any additional fee required or credit any overpayment for this Information Disclosure Statement and/or Petition to Morgan, Lewis & Bockius LLP Deposit Account No. 50-0310 (order no. 067292-5005-US01).

11. ☒ No admission is made that the information cited in this Statement is, or is considered to be, material to patentability nor a representation that a search has been made (other than a search report of a foreign counterpart application or PCT International Search Report if submitted herewith). 37 C.F.R. §§1.97(g) and (h).

Respectfully submitted,

Date: May 31, 2017



59,649
(Reg. No.)

Tae-Woong Koo
MORGAN, LEWIS & BOCKIUS LLP
1400 Page Mill Road
Palo Alto, CA 94304
(650) 843-4000

IPR2025-00068
CrowdStrike EX1002 Page 99

Electronically filed February 28, 2017

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application of:	Alen Capalik	Confirmation No.:	5143
Serial No.:	14/823,916	Art Unit:	2444
Filed:	August 11, 2015	Examiner:	NGUYEN, THU HA T
For:	System and Method for Identifying Unauthorized Activities on a Computer System using a Data Structure Model	Attorney Docket No.:	067292-5005-US01

AMENDMENT

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

The enclosed Amendment is in response to the Office Action dated August 30, 2016 for the above identified patent application.

Petition for Extension of Time under 37 CFR 1.136. It is respectfully requested that the time for response to the Office Action dated August 30, 2016 be extended for a period of three (3) months from November 30, 2016 to February 28, 2017.

The Commissioner is hereby authorized to charge any required fee(s) to Morgan, Lewis & Bockius LLP Deposit Account No. 50-0310 (order no. 067292-5005-US01).

IPR2025-00068
CrowdStrike EX1002 Page 100

Electronic Patent Application Fee Transmittal	
Application Number:	14823916
Filing Date:	11-Aug-2015
Title of Invention:	System and Method for Identifying Unauthorized Activities on a Computer System using a Data Structure Model
First Named Inventor/Applicant Name:	Alen Capalik
Filer:	Tae-Woong Koo/Lata Olivier
Attorney Docket Number:	067292-5005-US01
Filed as Small Entity	
Filing Fees for Utility under 35 USC 111(a)	

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension - 3 months with $0 paid	2253	1	700	700
Miscellaneous:				
		Total in USD ($)		**700**

Electronic Acknowledgement Receipt	
EFS ID:	28494874
Application Number:	14823916
International Application Number:	
Confirmation Number:	5143
Title of Invention:	System and Method for Identifying Unauthorized Activities on a Computer System using a Data Structure Model
First Named Inventor/Applicant Name:	Alen Capalik
Customer Number:	24341
Filer:	Tae-Woong Koo
Filer Authorized By:	
Attorney Docket Number:	067292-5005-US01
Receipt Date:	28-FEB-2017
Filing Date:	11-AUG-2015
Time Stamp:	21:05:55
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	DA
Payment was successfully received in RAM	$700
RAM confirmation Number	030117INTEFSW00009022500310
Deposit Account	
Authorized User	
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		067292_5010US01_AMEND.pdf	141387 40dc001e3f05970c664f5ce318cb2458d5270383	yes	11

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Applicant Arguments/Remarks Made in an Amendment	6	11
	Claims	2	5
	Amendment/Req. Reconsideration-After Non-Final Reject	1	1

Warnings:

Information:

2	Fee Worksheet (SB06)	fee-info.pdf	30723 1848488b5cc04bb3c59255664512e90291e36281	no	2

Warnings:

Information:

Total Files Size (in bytes):	172110

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

REMARKS

This amendment responds to the office action mailed August 30, 2016. In the office action, the Examiner rejected:

- claims 1-20 on the ground of nonstatutory double patenting over claims 1-23 of U.S. Patent No. 9,106,697; and
- claims 1-20 under pre-AIA 35 U.S.C. 103(a) over Jiang U.S. Pub. No. 2008/0320594 and Aziz et al., U.S. Pub. No. 2012/0331553.

After entry of this amendment, the pending claims are: claims 1-20.

McKesson Statement

The pending application is related to:

- U.S. Patent Application Serial No. 14/542,376;
- U.S. Patent No. 8,656,493, which issued from U.S. Patent Application Serial No. 13/759,335;
- U.S. Patent No. 9,106,697, which issued from U.S. Patent Application Serial No. 13/163,590, which is a parent application of this application;
- U.S. Patent No. 8,789,189, which issued from U.S. Patent Application Serial No. 13/163,578;
- U.S. Patent Application Serial No. 11/788,795; and
- U.S. Patent No. 8,429,746, which issued from U.S. Patent Application Serial No. 11/488,743.

The Examiner is encouraged to review the art made of record, Office Action(s) and the Notices of Allowance in the above-mentioned related applications, all of which are available on PAIR.

Amendments to the Claims

Claims 1-3, 17, and 19-20 have been amended for clarity. Support for the claim revisions can be found at least in original claims, paragraphs [0067]-[0072] of the specification, and Figures 5A-5B as originally filed.

No new matter has been added. With respect to all amendments, Applicant has not dedicated or abandoned any unclaimed subject matter. Moreover, Applicant has not

IPR2025-00068
CrowdStrike EX1002 Page 106

acquiesced to any characterizations of the invention, nor any rejections or objections of the claims, made by the Examiner.

REMARKS CONCERNING NONSTATUTORY DOUBLE PATENTING REJECTIONS

Because the claims can be amended during the course of prosecution, Applicant respectfully requests that the Examiner reconsider the nonstatutory double-patenting rejection of claims 1-20 over claims 1-20 of U.S. Patent No. 9,106,697, when at least one independent claim of this application has been allowed or noted as being allowable over the cited references.

REMARKS CONCERNING REJECTIONS UNDER 35 U.S.C. 103

To establish prima facie obviousness of a claimed invention, all the claim elements must be taught or suggested by the prior art. *In re Royka*, 490 F.2d 981, 180 USPQ 580 (CCPA 1974). Indeed, the Board of Patent Appeal and Interferences repeatedly confirmed that a proper obviousness determination requires an Examiner to make "a searching comparison of the claimed invention - including all its limitations - with the teaching of the prior art." See *In re Wada and Murphy*, Appeal 2007-3733, citing *In re Ochiai*, 71 F.3d 1565, 1572 (Fed. Cir. 1995) (emphasis in original). Finding all the claim elements in the prior art is necessary, but not sufficient. *KSR Intern. Co. v. Teleflex Inc.*, 127 S.Ct. 1727, 1741 (2007) ("a patent composed of several elements is not proved obvious merely by demonstrating that each of its elements was, independently, known in the prior art"). "All words in a claim must be considered in judging the patentability of that claim against the prior art." *In re Wilson*, 424 F.2d 1382, 1385, 165 USPQ 494, 496 (CCPA 1970).

Amended claim 1 recites:

> monitoring activity on the computer system;
>
> identifying a plurality of activities being performed at the computer system, wherein each of the activities includes an activity source, an activity target, and an association between the activity source and the activity target;
>
> storing in the memory a data structure that identifies the activity sources, the activity targets, and the associations for the plurality of activities; and
>
> transmitting one or more of the activity sources, the activity targets, and the associations to prevent future attacks associated with the one or more of the activity sources, the activity targets, and the associations.

IPR2025-00068
CrowdStrike EX1002 Page 107

With respect to this claim (before amendments), the Examiner states:

> Jiang teaches … identifying a plurality of activities being performed at the virtual machine, wherein each of the activities includes an activity source, an activity target, and an association between the activity source and the activity target (par. 0035, 0048-0050, 0059-0061 - VM states and events).
>
> Jiang does not explicitly teach storing in the memory the activity sources, activity targets, and associations; and transmitting one or more of the activity source, activity target and associations to prevent future attacks.
>
> Aziz teaches storing in the memory the activity sources, activity targets, and associations (par. 0019, 0050-0051, 0159-0161, 0179, 0190-0193) …
>
> It would have been obvious to one of ordinary skill in the art at the time of the invention was made to combine the teaching of Jiang and Aziz in order to preventing the spread of malware.[1]

However, paragraphs [0035], [0048]-[0050] and [0059]-[0061] of Jiang, cited by the Examiner, state (emphasis added):

> [0035] … The open-source VMMs (QEMU, Xen, and UML) allow full access to low-level VM states and events. …
>
> [0048] … the instructions may further include, as shown in FIG. 2, retrieving for inspection virtual machine internal system events from the virtual resources S210. … The virtual machine internal system events may comprise virtual memory events and/or virtual disk events.
>
> [0049] … the instructions further include interpreting the **virtual memory events** and/or **virtual disk events** S220. After interpretation, the instructions may further include transparently encapsulating and presenting the interpreted virtual memory events and/or the interpreted virtual disk events to the anti-malware software S230.
>
> [0050] Interpreting either or both these types of events also help enable guest function extrapolation. Just as with the virtual machine internal system states, extrapolation can aid in extracting semantic-rich data … from the virtual machine internal system events.
>
> [0059] Not only can the malware detection system 305 retrieve, interpret, and transparently encapsulate and present virtual machine internal system states, but it can also do the same for **virtual machine internal system events**. Such events can be retrieved from the virtual resources 340 for inspection. Retrieval of these events is also based on non-intrusive virtual machine introspection without perturbing their execution. The **virtual machine internal system events** may comprise **virtual memory events** … and **virtual disk events** ….

[1] Office action dated August 30, 2016, pp. 5-6.

IPR2025-00068
CrowdStrike EX1002 Page 108

> [0060] The malware detection system 305 may use the virtual machine inspector 362 may be configured to retrieve the virtual memory events from a virtual machine monitor .... Generally running between the host operating system ... and the virtual machine ..., the virtual machine monitor ... may be configured to intercept the virtual memory events. Upon interception, the guest function extrapolator 364 may extract semantic-rich data by interpreting the virtual memory events. Afterwards, the transparent presenter 366 may encapsulate and present the interpreted virtual memory events to the anti-malware software. Like above, the anti-malware software ... may be configured to use the virtual memory events to detect system compromises.
>
> [0061] Similarly, the malware detection system 305 may also use the virtual machine inspector 362 to retrieve the virtual disk events from a virtual machine monitor .... The virtual machine monitor ..., running between the host operating system ... and the virtual machine ... may be configured to intercept the virtual disk events. After interception, the guest function extrapolator 364 may extract semantic-rich data by interpreting the virtual disk events. Then, the transparent presenter 366 may encapsulate and present the interpreted virtual disk events to the anti-malware software ... for detecting any system comprise.

As shown above, paragraphs [0035], [0048]-[0050] and [0059]-[0061] of Jiang describe a malware detection system that detects virtual memory events and virtual disk events. These detected events in Jiang are interrupt, memory, and I/O access events.[2] Even if these events were targets, which they are not, Jiang simply does not disclose all of "an activity **source**, an activity **target**, and an **association between the activity source and the activity target**." As such, Jiang simply does not teach or even suggest the above-recited features. Aziz is not cited for, nor does it teach or suggest the above-recited features.

In addition, paragraphs [0019], [0050]-[0051], [0159]-[0161], [0179], and [0190]-[0193] of Aziz, cited by the Examiner, state:

> [0019] The controller can be further configured to receive other network data from the communication network, scan the other network data for unauthorized activity based on the unauthorized activity signature, and block the other network data based on the scan. Further, the controller can be configured to store the unauthorized activity signature and send the unauthorized signature to another digital device.
>
> [0050] The controller 115 controls the operation of the computing systems 120 and the gateway 125 to orchestrate network activities in the computer worm sensor 105. In one embodiment, the orchestrated network activities are a predetermined sequence of network activities in the computer network 110, which represents an orchestrated behavior of the computer network 110. ...

[2] *See* paragraph [0067] of Jiang.

IPR2025-00068
CrowdStrike EX1002 Page 109

> [0051] Anomalous behavior may include a communication anomaly, like an unexpected network communication, or an execution anomaly, for example, an unexpected execution of computer program code. If the controller 115 identifies an anomalous behavior, the computer network 110 is deemed to be infected with a computer worm. In this way, the controller 115 can detect the presence of a computer worm in the computer network 110 based on an anomalous behavior of the computer worm in the computer network 110. The controller 115 then creates an identifier (i.e., a "definition" of the anomalous behavior), which can be used for detecting the computer worm in another computer network, such as the communication network 130.
>
> [0159] The heuristic module 730 can retain data packets belonging to a particular data flow previously copied by the tap 715. …
>
> [0160] In some embodiments, the heuristic module 730 performs heuristic and/or probability analysis on a set of data packets belonging to a data flow and then stores the data packets within a buffer or other memory. …
>
> [0161] In some embodiments, an optional buffer receives the flagged network data from the heuristic module 730. …
>
> [0179] Step 905 can alternatively include flagging network data as suspicious based on policies such as the identity of a source device, a destination device, or the activity of the network data. …
>
> [0190] In other embodiments, the heuristic module 730 serially applies heuristics and/or probabilistic analysis to both the first network data and the second network data. …
>
> [0191] The heuristic module 730 can independently apply heuristics and probability analysis to different network data. …
>
> [0192] The heuristic module 730 may comprise an optional buffer to buffer the network data flagged a suspicious. …
>
> [0193] The heuristic module 730 can retain data packets belonging to a variety of different network data previously copied by the tap 715. …

As shown above, Aziz describes storing the unauthorized activity signature and sending the unauthorized signature to another digital device. However, Aziz is silent as to how the unauthorized activity signature is configured. More importantly, Aziz does not teach or suggest the claimed storing operation, namely "storing in the memory a data structure that identifies the activity sources, the activity targets, and the associations for the plurality of activities."

Because Jiang and Aziz, separately or in combination, do not teach or suggest all of the claimed features, claim 1 and its dependent claims are patentable over Jiang and Aziz. Claims 19 and 20 are also patentable over Jiang and Aziz for analogous reasons.

IPR2025-00068
CrowdStrike EX1002 Page 110

By responding in the foregoing remarks only to particular positions asserted by the Examiner, Applicant does not necessarily acquiesce in other positions that have not been explicitly addressed. In addition, the Applicant's arguments for the patentability of a claim should not be understood as implying that no other reasons for the patentability of that claim exist.

In light of the above amendments and remarks, Applicant respectfully requests that the Examiner reconsider this application with a view towards allowance. The Examiner is invited to call the undersigned attorney at (650) 843-4000, if a telephone call could help resolve any remaining items.

Respectfully submitted,

Date: February 28, 2017

/ Tae-Woong Koo / 59,649

Tae-Woong Koo (Reg. No.)

MORGAN, LEWIS & BOCKIUS LLP
1400 Page Mill Road
Palo Alto, CA 94304
(650) 843-4000

IPR2025-00068
CrowdStrike EX1002 Page 111

IN THE CLAIMS:

Please rewrite the pending claims as follows:

1. (Currently amended) A computer implemented method of identifying unauthorized activities on a computer system attached to a computer network, wherein the computer system comprises [[:]] one or more processors [[;]] and memory, ~~storing: a virtual machine; and a virtual machine monitor supervising the virtual machine,~~ the method comprising: ~~, at the virtual machine monitor:~~

monitoring activity on the computer system; ~~virtual machine;~~

identifying a plurality of activities being performed at the computer system, ~~virtual machine,~~ wherein each of the activities includes an activity source, an activity target, and an association between the activity source and the activity target;

storing in the memory a data structure that identifies the activity sources, the activity targets, and the associations for the plurality of activities; and

transmitting one or more of the activity sources, the activity targets, and the associations to prevent future attacks associated with the one or more of the activity sources, the activity targets, and the associations.

2. (Currently amended) The method of claim 1, wherein the monitoring further comprises monitoring all activity on the computer system. ~~virtual machine, and all activity on the virtual machine is assumed to be unauthorized.~~

3. (Currently amended) The method of claim 1, further comprising:

creating, from the stored information, a fingerprint indicative of the activity on the computer system. ~~virtual machine.~~

4. (Original) The method of claim 1, wherein the activities comprise two or more of: a file initiating an execution of an instruction, an instruction reading a file, an instruction writing to a file, and receiving data through the network.

5. (Original) The method of claim 1, wherein a respective activity target comprises one of: a file, a user, an instruction, a thread, data stream, and network socket connections.

6. (Original) The method of claim 1, wherein a respective activity source comprises one of: a file, a user, an instruction, a thread, data stream, and network socket connections.

IPR2025-00068
CrowdStrike EX1002 Page 112

7. (Original) The method of claim 1, further comprising:
graphically displaying at least a subset of the stored activities.

8. (Original) The method of claim 7, wherein the displaying includes visually distinguishing at least a subset of the associations.

9. (Original) The method of claim 1, wherein an activity target of a first activity of the plurality of activities is an activity source of a second activity of the plurality of activities.

10. (Original) The method of claim 1, further comprising:
identifying a respective association between a first activity source and a first activity target as unauthorized, wherein the first activity target, when associated as a second activity source with a second activity target, causes unauthorized activities on the second activity target.

11. (Original) The method of claim 10, further comprising:
tracking a transfer of malicious associations over time.

12. (Original) The method of claim 1, further comprising:
identifying activity sources that are affected by unauthorized activities.

13. (Original) The method of claim 12, wherein the identifying activity sources that are affected by unauthorized activities includes identifying activity sources that request to access a portion of memory that is set as non-executable.

14. (Original) The method of claim 12, wherein:
instructions executed by the one or more processors have respective privilege levels;
respective activity sources have respective privilege levels; and
the identifying activity sources that are affected by unauthorized activities includes identifying activity sources that request to execute underprivileged instructions.

15. (Original) The method of claim 12, wherein the identifying activity sources that are affected by unauthorized activities includes identifying data stream incoming from outside the computer system.

16. (Original) The method of claim 1, further comprising:

IPR2025-00068
CrowdStrike EX1002 Page 113

determining an activity status for the stored events, the activity status comprising one of:

a complete status, representing that a source of unauthorized activities is identified, and each activity target in the stored activities is associated with the source through one or more associations; and

an incomplete status, which represents that the source of unauthorized activities is not identified, or at least one activity target in the stored activities is not associated with the source through one or more associations.

17. (Currently amended) The method of claim 1, further comprising:

determining an activity level representing a frequency of unauthorized activities on the computer system ~~virtual machine~~ during a predefined time interval.

18. (Original) The method of claim 1, further comprising:

identifying a respective activity as unauthorized based on a determination that the respective activity is associated with an unauthorized activity that is distinct from the respective activity.

19. (Currently amended) A computer system, comprising:

one or more processors; and

memory storing one or more programs, the one or more programs including instructions for:

~~a virtual machine;~~

~~a virtual machine monitor supervising the virtual machine; and~~

~~one or more programs, the one or more programs including instructions for:~~

monitoring activity on the computer system; ~~virtual machine;~~

identifying a plurality of activities being performed at the computer system, ~~virtual machine,~~ where each of the activities includes an activity source, an activity target, and an association between the activity source and the activity target;

storing in the memory a data structure that identifies the activity sources, the activity targets, and the associations for the plurality of activities; and

transmitting one or more of the activity sources, the activity targets, and the associations to prevent future attacks associated with the one or more of the activity sources, the activity targets, and the associations.

IPR2025-00068
CrowdStrike EX1002 Page 114

20. (Currently amended) A computer readable storage medium, including one or more programs for execution by one or more processors of a computer system, the one or more programs including instructions for:

monitoring activity on the computer system; ~~virtual machine;~~

identifying a plurality of activities being performed at the computer system, ~~virtual machine,~~ where each of the activities includes an activity source, an activity target, and an association between the activity source and the activity target;

storing in [[the]] memory of the computer system a data structure that identifies the activity sources, the activity targets, and the associations for the plurality of activities; and

transmitting one or more of the activity sources, activity targets, and associations to prevent future attacks associated with the one or more of the activity sources, the activity targets, and the associations.

IPR2025-00068
CrowdStrike EX1002 Page 115

PTO/SB/06 (09-11)
Approved for use through 1/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 14/823,916	Filing Date 08/11/2015	☐ To be Mailed

ENTITY: ☐ LARGE ☒ SMALL ☐ MICRO

APPLICATION AS FILED – PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	RATE ($)	FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	

APPLICATION AS AMENDED – PART II

AMENDMENT 02/28/2017

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	* 20	Minus	** 20	= 0	X $40 =	0
Independent (37 CFR 1.16(h))	* 3	Minus	***3	= 0	X $210 =	0
☐ Application Size Fee (37 CFR 1.16(s))						
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
					TOTAL ADD'L FEE	0

AMENDMENT

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	*	Minus	**	=	X $ =	
Independent (37 CFR 1.16(h))	*	Minus	***	=	X $ =	
☐ Application Size Fee (37 CFR 1.16(s))						
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
					TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

LIE
LAVINIA JOHNSON

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**
If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT Substitute for Form 1449-PTO				Electronically filed December 22, 2016	
				Application Number	14/823,916
				Filing Date	August 11, 2015
				First Named Inventor	Alen Capalik
				Art Unit	2444
				Examiner Name	Nguyen, Thu Ha T.
Sheet	1	of	1	Attorney Docket Number	067292-5005US01

NON PATENT LITERATURE DOCUMENTS		
Examiner Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published
		CounterTack Inc., Decision to Grant, EP15174670.8, 14SEP2016, 5 pgs.
		CounterTack Inc., Certificate of Grant, EP15174670.8, 14SEP2016, 1 pg.

Examiner Signature		Date Considered	

DB2/ 30917637.1

Electronic Patent Application Fee Transmittal	
Application Number:	14823916
Filing Date:	11-Aug-2015
Title of Invention:	System and Method for Identifying Unauthorized Activities on a Computer System using a Data Structure Model
First Named Inventor/Applicant Name:	Alen Capalik
Filer:	Tae-Woong Koo/Lamesha Robertson
Attorney Docket Number:	067292-5005-US01
Filed as Small Entity	
Filing Fees for Utility under 35 USC 111(a)	

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
SUBMISSION- INFORMATION DISCLOSURE STMT	2806	1	90	90
		Total in USD ($)		**90**

Electronic Acknowledgement Receipt	
EFS ID:	27886251
Application Number:	14823916
International Application Number:	
Confirmation Number:	5143
Title of Invention:	System and Method for Identifying Unauthorized Activities on a Computer System using a Data Structure Model
First Named Inventor/Applicant Name:	Alen Capalik
Customer Number:	24341
Filer:	Tae-Woong Koo/Lamesha Robertson
Filer Authorized By:	Tae-Woong Koo
Attorney Docket Number:	067292-5005-US01
Receipt Date:	22-DEC-2016
Filing Date:	11-AUG-2015
Time Stamp:	17:29:58
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	DA
Payment was successfully received in RAM	$90
RAM confirmation Number	122316INTEFSW00005493500310
Deposit Account	
Authorized User	
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		067292_5005US01_IDS.pdf	221911 7a1dd4513d6bca5af0b9c551e76f9514bcf2314a	yes	5
	Multipart Description/PDF files in .zip description				
	Document Description		**Start**	**End**	
	Transmittal Letter		1	4	
	Information Disclosure Statement (IDS) Form (SB08)		5	5	
Warnings:					
Information:					
2	Non Patent Literature	CounterTack_DOG_EP_151746 70_8_14_SEP_2016.pdf	32919 05f7c70e1667950e3f6fa8b504277726404ba0d2	no	1
Warnings:					
Information:					
3	Non Patent Literature	CounterTack_COG_EP_151746 70_8_14_Sep_2016.pdf	35140 82706514b45372cd5ad3b6206536dc683d69e976	no	1
Warnings:					
Information:					
4	Fee Worksheet (SB06)	fee-info.pdf	30847 3d1249e761a72aa82976023ba0ae1bf2e30dbcdc	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	320817		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Electronically filed December 22, 2016

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application of:	Capalik et al	Confirmation No.:	5143
Serial No.:	14/823,916	Art Unit:	2444
Filed:	August 11, 2015	Examiner:	Nguyen, Thu Ha T.
For:	System and Method for Identifying Unauthorized Activities on a Computer System using a Data Structure Model	Attorney Docket No.:	067292-5005US01

INFORMATION DISCLOSURE STATEMENT

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

In accordance with the duty of disclosure provisions of 37 C.F.R. §1.56, there is hereby provided certain information which the Examiner may consider material to the examination of the subject U.S. patent application. It is requested that the Examiner make this information of record if it is deemed material to the examination of the application.

1. Enclosures accompanying this Information Disclosure Statement are:

1a. ☒ A list of all patents, publications, applications, or other information submitted for consideration by the office.

1b. A legible copy of:

☐ Each foreign patent;

☐ Each publication or that portion which caused it to be listed on the PTO-1449;

☐ For each cited pending U.S. application, the application specification including the claims, and any drawing of the application, or portion of the application which caused it to be listed on the PTO-1449 including any claims directed to that portion;

☒ all other information or portion which caused it to be listed on the PTO-1449.

1c. ☐ An English language copy of search report(s) from a counterpart foreign application or PCT International Search Report.

1d. ☐ Explanations of relevancy (ATTACHMENT 1(d), hereto) or English language abstracts of the non-English language publications.

IPR2025-00068
CrowdStrike EX1002 Page 123

2. ☐ This Information Disclosure Statement is filed under 37 C.F.R. §1.97(b):

☐ Within three months of the filing date of a national application other than a continued prosecution application under §1.53(d);

☐ Within three months of the date of entry of the national stage as set forth in §1.491 in an international application;

☐ Before the mailing of the first Office action on the merits;

☐ Before the mailing of a first Office action after the filing of a request for continued examination under §1.114.

3. ☒ This Information Disclosure Statement is filed under 37 C.F.R. §1.97(c) after the period specified in 37 C.F.R. §1.97(b), but before the mailing date of any of a final action under 37 C.F.R. §1.113, a notice of allowance under 37 C.F.R. §1.311 or an action that otherwise closes prosecution in the application.

(Check either Item 3a, 3b or 3c)

3a. ☐ The Certification Statement in Item 5 below is applicable. Accordingly, no fee is required.

3b. ☐ The $180.00 (large entity) fee set forth in 37 C.F.R. §1.17(p) in accordance with 37 C.F.R. §1.97(c) is to be charged to Morgan, Lewis & Bockius LLP Deposit Account No. 50-0310 (order no.).

3c. ☒ The $90.00 (small entity) fee set forth in 37 C.F.R. §1.17(p) in accordance with 37 C.F.R. §1.97(c) is to be charged to Morgan, Lewis & Bockius LLP Deposit Account No. 50-0310 (order no. 067292-5005US01).

(Items 3b or 3c to be checked if any reference known for more than 3 months)

4. ☐ This Information Disclosure Statement is filed under 37 C.F.R. §1.97(d) after the period specified in 37 C.F.R. §1.97(c), but on or before the date of payment of the issue fee.

(Check Item 4a, and 4b or 4c)

4a. ☐ The Certification Statement in Item 5 below is applicable.

4b. ☐ The $180.00 (large entity) fee set forth in 37 C.F.R. §1.17(p) in accordance with 37 C.F.R. §1.97(c) is to be charged to Morgan, Lewis & Bockius LLP Deposit Account No. 50-0310 (order no.).

4c. ☐ The $90.00 (small entity) fee set forth in 37 C.F.R. §1.17(p) in accordance with 37 C.F.R. §1.97(c) is to be charged to Morgan, Lewis & Bockius LLP Deposit Account No. 50-0310 (order no.).

5. ☐ Certification Statement (applicable if Item 3a or Item 4a is checked)

(Check either Item 5a, 5b, 5c or 5d)

5a. ☐ In accordance with 37 C.F.R. §1.97(e)(1), it is certified that each item of information contained in this information disclosure statement was first cited in a communication from a foreign patent office in a counterpart foreign application

IPR2025-00068
CrowdStrike EX1002 Page 124

not more than three months prior to the filing of this Information Disclosure Statement.

5b. ☐ In accordance with 37 C.F.R. §1.97(e)(2), it is certified that no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 C.F.R. §1.56(c) more than three months prior to the filing of this information disclosure statement.

5c. ☐ Each item of information contained in this information disclosure statement was cited in a communication from a foreign patent office in a counterpart application, and the communication was not **received** by any individual designated in 37 C.F.R. §1.56(c) more than thirty days prior to the filing of this information disclosure statement.

5d. ☐ Pursuant to 37 C.F.R. §1.704(d), each item of information contained in this information disclosure statement was cited in a communication from a foreign patent office in a counterpart application, and the communication was not **received** by any individual designated in 37 C.F.R. §1.56(c) more than thirty days prior to the filing of this information disclosure statement.

6. ☐ Copies of each cited U.S. patent and each U.S. patent application publication are not enclosed pursuant to the USPTO OG Notice dated 05 August 2003 waiving the requirement under 37 C.F.R. 1.98(a)(2)(i) for U.S. patent applications filed after June 30, 2003.

7. ☐ This application is a continuation application under 37 C.F.R. §1.53(b) or (d).

(Check appropriate Items 7a, 7b and/or 7c)

7a. ☐ A Petition to Withdraw from issue under 37 C.F.R. §1.313(b)(5) is concurrently filed herewith.

7b. ☐ Copies of publications listed on Form PTO-1449 from prior application Serial No. , filed on , of which this application claims priority under 35 U.S.C. §120, are not being submitted pursuant to 37 C.F.R. §1.98(d).

7c. ☐ Copies of the publications listed on the attached Form PTO-1449 that were not previously cited in prior application Serial No. , filed on , are provided herewith.

8. ☐ This is a Supplemental Information Disclosure Statement. (Check Item 8a)

8a. ☐ This Supplemental Information Disclosure Statement under 37 C.F.R. §1.97(f) supplements the Information Disclosure Statement filed on . A bona fide attempt was made to comply with 37 C.F.R. §1.98, but inadvertent omissions were made. These omissions have been corrected herein. Accordingly, additional time is requested so that this Supplemental Information Disclosure Statement can be considered as if properly filed on .

9. ☐ In accordance with 37 C.F.R. §1.98, a concise explanation of what is presently understood to be the relevance of each non-English language publication is:

(Check Item 9a, 9b, or 9c)

9a. ☐ satisfied because all non-English language publications were cited on the enclosed English language copy of the PCT International Search Report or the search report from a counterpart foreign application indicating the degree of relevance found by the foreign office.

9b. ☐ set forth in the application.

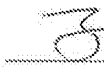
9c. ☐ enclosed as an attachment hereto.

10. ☒ The Commissioner is authorized to charge any additional fee required or credit any overpayment for this Information Disclosure Statement and/or Petition to Morgan, Lewis & Bockius LLP Deposit Account No. 50-0310 (order no. 067292-5005US01).

11. ☒ No admission is made that the information cited in this Statement is, or is considered to be, material to patentability nor a representation that a search has been made (other than a search report of a foreign counterpart application or PCT International Search Report if submitted herewith). 37 C.F.R. §§1.97(g) and (h).

Respectfully submitted,

Date: December 19, 2016



59,649
Tae-Woong Koo (Reg. No.)
MORGAN, LEWIS & BOCKIUS LLP
1400 Page Mill Road
Palo Alto, CA 94304
(650) 843-4000

IPR2025-00068
CrowdStrike EX1002 Page 126

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/823,916	08/11/2015	Alen Capalik	067292-5005-US01	5143

24341 7590 08/30/2016
Morgan, Lewis & Bockius LLP (PA)
1400 Page Mill Road
Palo Alto, CA 94304-1124

EXAMINER	
NGUYEN, THU HA T	

ART UNIT	PAPER NUMBER
2453	

NOTIFICATION DATE	DELIVERY MODE
08/30/2016	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

padocketingdepartment@morganlewis.com
vskliba@morganlewis.com

Office Action Summary	Application No. 14/823,916	Applicant(s) CAPALIK ET AL.	
	Examiner THU HA NGUYEN	Art Unit 2453	AIA (First Inventor to File) Status No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTHS FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *12/10/15*.

☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims*

5)☒ Claim(s) *1-20* is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6)☐ Claim(s) _____ is/are allowed.

7)☒ Claim(s) *1-20* is/are rejected.

8)☐ Claim(s) _____ is/are objected to.

9)☐ Claim(s) _____ are subject to restriction and/or election requirement.

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a)☐ All b)☐ Some** c)☐ None of the:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

** See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☒ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b) Paper No(s)/Mail Date *12/10/15; 02/05/16*.

3) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

4) ☐ Other: _____.

IPR2025-00068
CrowdStrike EX1002 Page 128

The present application is being examined under the pre-AIA first to invent provisions.

DETAILED ACTION

1. Claims **1- 20** are presented for examination.

Double Patenting

2. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the “right to exclude” granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on nonstatutory double patenting provided the reference application or patent either is shown to be commonly owned with the examined application, or claims an invention made as a

result of activities undertaken within the scope of a joint research agreement. See MPEP § 717.02 for applications subject to examination under the first inventor to file provisions of the AIA as explained in MPEP § 2159. See MPEP §§ 706.02(l)(1) - 706.02(l)(3) for applications not subject to examination under the first inventor to file provisions of the AIA. A terminal disclaimer must be signed in compliance with 37 CFR 1.321(b).

The USPTO Internet website contains terminal disclaimer forms which may be used. Please visit www.uspto.gov/patent/patents-forms. The filing date of the application in which the form is filed determines what form (e.g., PTO/SB/25, PTO/SB/26, PTO/AIA/25, or PTO/AIA/26) should be used. A web-based eTerminal Disclaimer may be filled out completely online using web-screens. An eTerminal Disclaimer that meets all requirements is auto-processed and approved immediately upon submission. For more information about eTerminal Disclaimers, refer to www.uspto.gov/patents/process/file/efs/guidance/eTD-info-I.jsp.

Claims 1-20 rejected on the ground of nonstatutory double patenting as being unpatentable over claims 1-23 of U.S. Patent No. 9,106,697. Although the claims at issue are not identical, they are not patentably distinct from each other because the current claims of instant application encompass the same subject matter as the patented claims, but with obvious wording variations.

Claims 1-20 of instant application is directed toward identifying unauthorized activities on a computer system in which a virtual machine monitor supervising the virtual machine (VM) by monitoring activity on the VM; identifying and storing a plurality

of activities performed by the VM, each of the activities includes activity source, activity target, and an association between activity source and activity target; and transmitting one or more activity source, activity target and associations to prevent further attacks.

Claims 1-23 of the Patent also mentions identifying unauthorized activities on a decoy computer system in which a virtual machine monitor supervising the virtual machine (VM) by monitoring activity on the VM; identifying and storing a plurality of activities performed by the VM, each of the activities includes activity source, activity target, and an association between activity source and activity target; creating a fingerprint indicative of the activity on the VM; and transmitting the fingerprint to prevent further attacks that comprise the same or similar activities as indicated by the fingerprint.

As can be seen there are some different between the claims; however, the differences are obvious and therefore, the claims are not patentably distinct from one another because the claims of the current application encompass the same subject matter as the patented claims.

Claim Rejections - 35 USC § 103

3. The following is a quotation of pre-AIA 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1-20 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over **Jiang** U.S. Pub. No. **2008/0320594**, in view of **Aziz et al.,** U.S. Pub. No. **2012/0331553**.

5. As to claim 1, 20, **Jiang** teaches the invention as claimed, including a computer implemented method of identifying unauthorized activities on computer system attached to a computer network, wherein the system comprises: one or more processors; and memory storing:

a virtual machine (fig. 3, virtual machine 310); and

a virtual machine monitor supervising the virtual machine, the method comprising, at the virtual machine monitor (fig. 3, VM monitor 370):

monitoring activity on the virtual machine (par. 0031, 0033, 0039-0061, 0065-00067 -*VMWatcher*);

identifying a plurality of activities being performed at the virtual machine, wherein each of the activities includes an activity source, an activity target, and an association between the activity source and the activity target (par. 0035, 0048-0050, 0059-0061 – *VM states and events*).

Jiang does not explicitly teach storing in the memory the activity sources, activity targets, and associations; and transmitting one or more of the activity source, activity target and associations to prevent future attacks.

Aziz teaches storing in the memory the activity sources, activity targets, and associations (par. 0019, 0050-0051, 0159-0161, 0179, 0190-0193); and

transmitting one or more of the activity source, activity target and associations to prevent future attacks (abstract, 0175-0180).

It would have been obvious to one of ordinary skill in the art at the time of the invention was made to combine the teaching of **Jiang and Aziz** in order to preventing the spread of malware.

6. As to claim 2, **Jiang** teaches the invention as claimed, including the method of claim 1, wherein the monitoring further comprises monitoring all activity on the virtual machine, and all activity on the virtual machine is assumed to be unauthorized (par. 0064-0067, 0212).

7. As to claim 3, **Aziz** teaches the invention as claimed, including the method of claim 1, wherein the fingerprint includes files that are affected by the unauthorized activities on the virtual machine (par. 0022, 0165-0166).

8. As to claim 4, **Aziz** teaches the invention as claimed, including the method of claim 1, wherein the fingerprint includes processes that are affected by the unauthorized activities on the virtual machine (par. 0022, 0165-0166).

9. As to claim 5, **Jiang** teaches the invention as claimed, including the method of claim 1, wherein the activities comprise two or more of: a file initiating an execution of an instruction, an instruction reading a file, an instruction writing to a file, and receiving data through the network (abstract, par. 0102-0107).

10. As to claim 6, **Jiang** teaches the invention as claimed, including the method of claim 1, wherein a respective activity target comprises one of: a file, a user, an instruction, a thread, data stream, and network socket connections (par. 0032-0044).

11. As to claim 7, **Jiang** teaches the invention as claimed, including the method of claim 1, wherein a respective activity source comprises one of: a file, a user, an instruction, a thread, data stream, and network socket connections (par. 0032-0064, 0074-0077).

12. As to claim 8, **Jiang** teaches the invention as claimed, including the method of claim 1, further comprising graphically displaying at least a subset of the stored activities (par. 0090).

13. As to claim 9, **Jiang** teaches the invention as claimed, including the method of claim 8, wherein the displaying includes visually distinguishing at least a subset of the associations (par. 0032-0033, 0044, 0077).

14. As to claim 10, **Jiang** teaches the invention as claimed, including the method of claim 8, wherein the subset of activities includes a first activity and a second activity, and the activity target of the first activity is the activity source of the second activity (par. 0074-0075, 0077).

15. As to claim 11, **Jiang** teaches the invention as claimed, including the method of claim 1, further comprising identifying a respective association between a first activity source and a first activity target as unauthorized, wherein the first activity target, when associated as a second activity source with a second activity target, causes unauthorized activities on the second activity target (par. 0022, 0165-0166).

16. As to claim 12, **Aziz** teaches the invention as claimed, including the method of claim 11, further comprising tracking a transfer of malicious associations over time (par. 0098, 0101-0103, 0127, 0249).

17. As to claim 13, **Jiang** teaches the invention as claimed, including the method of claim 1, further comprising identifying activity sources that are affected by unauthorized activities (par. 0022, 0165-0166).

18. As to claim 14, **Jiang** teaches the invention as claimed, including the method of claim 13, wherein the identifying activity sources that are affected by

unauthorized activities includes identifying activity sources that request to access a portion of memory that is set as non-executable (par. 0022, 0165-0166).

19. As to claim 15, **Jiang** teaches the invention as claimed, including the method of claim 13, wherein: instructions executed by the one or more processors have respective privilege levels; respective activity sources have respective privilege levels; and the identifying activity sources that are affected by unauthorized activities includes identifying activity sources that request to execute underprivileged instructions (par. 0102).

20. As to claim 16, **Jiang** teaches the invention as claimed, including the method of claim 13, wherein the identifying activity sources that are affected by unauthorized activities includes identifying data stream incoming from outside the computer system (abstract, par. 0029-0030, 0033-0043).

21. As to claim 17, **Jiang** teaches the invention as claimed, including the method of claim 1, further comprising determining an activity status for the stored events, the activity status comprising one of: a complete status, representing that a source of unauthorized activities is identified, and each activity target in the stored activities is associated with the source through one or more associations; and an incomplete status, which represents that the source of unauthorized activities is not

identified, or at least one activity target in the stored activities is not associated with the source through one or more associations (par. 0022, 0165-0166).

22. As to claim 18, **Jiang** teaches the invention as claimed, including the method of claim 1, further comprising determining an activity level representing a frequency of unauthorized activities on the virtual machine during a predefined time interval (par. 0119-0120).

23. As to claim 19, 20, **Jiang** teaches the invention as claimed, including a system, comprising:

one or more processors (par. 0043); and

memory storing: a virtual machine (fig. 3);

a virtual machine monitor supervising the virtual machine (fig. 3); and

one or more programs, the one or more programs including instructions for: monitoring activity on the virtual machine (par. par. 0031, 0033, 0039-0061, 0065-00067-*VMWatcher*);

identifying a plurality of activities being performed at the virtual machine, where each of the activities includes an activity source, an activity target, and an association between the activity source and the activity target (par. 0035, 0048-0050, 0059-0061 – *VM states and events*).

Jiang does not explicitly teach storing in the memory the activity sources, activity targets, and associations; and transmitting one or more of the activity source, activity target and associations to prevent future attacks.

Aziz teaches storing in the memory the activity sources, activity targets, and associations (par. 0019, 0050-0051, 0159-0161, 0179, 0190-0193);

transmitting one or more of the activity source, activity target and associations to prevent future attacks (abstract, 0175-0180).

It would have been obvious to one of ordinary skill in the art at the time of the invention was made to combine the teaching of **Jiang and Aziz** in order to preventing the spread of malware.

Conclusion

24. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

25. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thu Ha Nguyen, whose telephone number is (571) 272-3989. The examiner can normally be reached Monday through Friday from 8:30 AM to 5:00 PM.

26. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Krista Zele can be reached on 571-272-7288. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

27. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/THU HA NGUYEN/

Primary Examiner, Art Unit 2453

Notice of References Cited	Application/Control No. 14/823,916	Applicant(s)/Patent Under Reexamination CAPALIK ET AL.	
	Examiner THU HA NGUYEN	Art Unit 2453	Page 1 of 3

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-2003/0023656 A1	01-2003	Hutchison, Gordon Douglas	G06F9/524	718/100
*	B	US-2006/0136720 A1	06-2006	Armstrong; Benjamin	G06F21/53	713/164
*	C	US-2006/0294592 A1	12-2006	Polyakov; Alexey A.	G06F21/566	726/24
*	D	US-2007/0180450 A1	08-2007	CROFT; Richard Jason	G06F3/1415	718/1
*	E	US-2007/0250930 A1	10-2007	Aziz; Ashar	G06F21/554	726/24
*	F	US-2008/0005782 A1	01-2008	Aziz; Ashar	G06F9/45537	726/3
*	G	US-2008/0177994 A1	07-2008	Mayer; Yaron	G06F9/4418	713/2
*	H	US-2008/0222729 A1	09-2008	Chen; Songqing	H04L63/145	726/24
*	I	US-2008/0320594 A1	12-2008	Jiang; Xuxian	G06F21/566	726/24
*	J	US-7,581,219 B2	08-2009	Neiger; Gilbert	G06F12/1491	711/6
*	K	US-7,596,654 B1	09-2009	Wong; Kai C.	G06F12/0813	703/21
*	L	US-2009/0307273 A1	12-2009	Johnson; William D.	G06F21/55	1/1
*	M	US-2010/0042632 A1	02-2010	Johnson; William D.	G06F11/3476	707/725

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	CPC Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Notice of References Cited	Application/Control No. 14/823,916	Applicant(s)/Patent Under Reexamination CAPALIK ET AL.	
	Examiner THU HA NGUYEN	Art Unit 2453	Page 2 of 3

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-2011/0060947 A1	03-2011	Song; Zhexuan	G06F21/53	714/37
*	B	US-2011/0179136 A1	07-2011	Twitchell, JR.; Robert W.	H04L45/586	709/217
*	C	US-2011/0239291 A1	09-2011	SOTKA; SCOTT	H04L63/1408	726/14
*	D	US-2012/0179904 A1	07-2012	Dunn; Chris	G06F21/575	713/155
*	E	US-2012/0255018 A1	10-2012	Sallam; Ahmed Said	G06F12/14	726/24
*	F	US-2012/0255012 A1	10-2012	Sallam; Ahmed Said	G06F21/52	726/24
*	G	US-2012/0331553 A1	12-2012	Aziz; Ashar	G06F21/554	726/23
*	H	US-8,365,180 B2	01-2013	Kawasaki; Shinichiro	G06F9/45516	718/1
*	I	US-8,448,170 B2	05-2013	Wipfel; Robert	H04L9/3213	718/1
*	J	US-8,539,582 B1	09-2013	Aziz; Ashar	G06F21/554	713/150
*	K	US-2013/0238785 A1	09-2013	Hawk; Ryan	G06F9/5072	709/224
*	L	US-8,572,613 B1	10-2013	Brandwine; Eric J.	G06F9/45533	714/38.1
*	M	US-2013/0304903 A1	11-2013	Mick; Jason	H04L43/0817	709/224

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Notice of References Cited	Application/Control No. 14/823,916	Applicant(s)/Patent Under Reexamination CAPALIK ET AL.	
	Examiner THU HA NGUYEN	Art Unit 2453	Page 3 of 3

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-2014/0026121 A1	01-2014	Jackson; Wayne	G06F9/44521	717/124
*	B	US-8,683,548 B1	03-2014	Curry; Samuel	G06F21/57	713/152
*	C	US-2014/0096131 A1	04-2014	Sonnek; Jason D.	G06F21/53	718/1
*	D	US-8,776,050 B2	07-2014	Plouffe; Jerry	G06F9/45537	718/1
*	E	US-8,943,506 B2	01-2015	Tang; Changbin	G06F9/45558	718/1
*	F	US-8,949,826 B2	02-2015	Fitzgerald; Joseph	G06F9/45537	718/1
	G	US-				
	H	US-				
	I	US-				
	J	US-				
	K	US-				
	L	US-				
	M	US-				

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

IPR2025-00068
CrowdStrike EX1002 Page 142

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

BIB DATA SHEET

CONFIRMATION NO. 5143

SERIAL NUMBER	FILING or 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
14/823,916	08/11/2015 RULE	726	2453	067292-5005-US01

APPLICANTS
COUNTERTACK INC., Santa Monica, CA;

INVENTORS
Alen Capalik, Pacific Palisades, CA;
David Andrews, Los Angeles, CA;
Ben Becker, Santa Monica, CA;

**** CONTINUING DATA ***************************
This application is a CON of 13/163,590 06/17/2011 PAT 9106697
which claims benefit of 61/358,367 06/24/2010

**** FOREIGN APPLICATIONS ***************************

**** IF REQUIRED, FOREIGN FILING LICENSE GRANTED **** ** SMALL ENTITY **
09/18/2015

Foreign Priority claimed ❑ Yes ☑ No 35 USC 119(a-d) conditions met ❑ Yes ☑ No Verified and Acknowledged /THU HA T NGUYEN/ Examiner's Signature	❑ Met after Allowance Initials	STATE OR COUNTRY	SHEETS DRAWINGS	TOTAL CLAIMS	INDEPENDENT CLAIMS
		CA	17	20	3

ADDRESS
Morgan, Lewis & Bockius LLP (PA)
1400 Page Mill Road
Palo Alto, CA 94304-1124
UNITED STATES

TITLE
System and Method for Identifying Unauthorized Activities on a Computer System using a Data Structure Model

FILING FEE RECEIVED	FEES: Authority has been given in Paper	❑ All Fees
800	No._____ to charge/credit DEPOSIT ACCOUNT	❑ 1.16 Fees (Filing)
	No._____ for following:	❑ 1.17 Fees (Processing Ext. of time)
		❑ 1.18 Fees (Issue)
		❑ Other _____
		❑ Credit

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	2	"20050136570".did.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L2	2	"20050136725".did.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L3	2	"20060136725".did.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L4	2	"20060136720".did.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L5	5	"2007000689".did.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L6	2	"20070002689".did.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L7	2	"20060294592".did.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L8	0	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) same source same target$4 same figureprint$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L9	0	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and figureprint$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L10	173	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and fingerprint$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L11	5	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) same source same target$4 same fingerprint$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L12	20	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) same fingerprint$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20

L13	5	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) same fingerprint$4 same decoy$4 same unauthor$6	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L14	8	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) same fingerprint$4 and auth$9 and prevent$4 same attack$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L15	8	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) same fingerprint$4 and auth$9 and (compar$4 or match$4 or map$4) and prevent$4 same attack$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L16	8	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) same fingerprint$4 and auth$9 and (compar$4 or match$4 or map$4) and prevent$4 and attack$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L17	118	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and fingerprint$4 and auth$9 and (compar$4 or match$4 or map$4) and prevent$4 and attack$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L18	11	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and fingerprint$4 and auth$9 and (compar$4 or match$4 or map$4) and prevent$4 and attack$4 and 726/25.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L19	4	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and fingerprint$4 and auth$9 and (compar$4 or match$4 or map$4) and prevent$4 and attack$4 and 709/223-224.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L20	25	("20010011254" | "20020194437" | "20040153672" | "20040177269" | "20070240221" | "20080127114" | "20100095281" | "5621886" | "5740413" | "6343280" | "6446062" | "7996836").PN.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L21	7	("20010011254" | "20020194437" | "20040153672" | "20040177269" | "20070240221" | "20080127114" | "20100095281" | "5621886" | "5740413" | "6343280" | "6446062" | "7996836").PN. and (virtual adj machine$4)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L22	2	"20050136570".did.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L23	2	"20050136725".did.	US-PGPUB;	OR	OFF	2016/08/22

			USPAT; EPO; JPO; DERWENT			14:20
L24	2	"20060136725".did.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L25	2	"20060136720".did.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L26	5	"2007000689".did.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L27	2	"20070002689".did.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L28	2	"20060294592".did.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L29	0	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) same source same target$4 same figureprint$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L30	0	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and figureprint$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L31	173	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and fingerprint$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L32	5	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) same source same target$4 same fingerprint$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L33	20	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) same fingerprint$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L34	5	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) same fingerprint$4 same decoy$4 same unauthor$6	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L35	8	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) same fingerprint$4 and auth$9 and prevent$4 same attack$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L36	8	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) same fingerprint$4 and auth$9 and (compar$4 or match$4 or map$4) and prevent$4 same attack$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20

L37	8	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) same fingerprint$4 and auth$9 and (compar$4 or match$4 or map$4) and prevent$4 and attack$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L38	118	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and fingerprint$4 and auth$9 and (compar$4 or match$4 or map$4) and prevent$4 and attack$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L39	11	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and fingerprint$4 and auth$9 and (compar$4 or match$4 or map$4) and prevent$4 and attack$4 and 726/25.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L40	4	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and fingerprint$4 and auth$9 and (compar$4 or match$4 or map$4) and prevent$4 and attack$4 and 709/223-224.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L41	21	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and (finger adj print$4)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L42	10653	718/1.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L43	1	L41 and L42	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L44	6880	718/100.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L45	0	L41 and L44	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L46	1	L38 and L44	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L47	0	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and (finger adj print$4) and auth$9 and (compar$4 or match$4 or map$4) and "7263".ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L48	0	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and (finger adj print$4) and auth$9 and (compar$4 or match$4 or map$4) and "726/3".ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20

IPR2025-00068
CrowdStrike EX1002 Page 147

L49	0	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and (finger adj print$4) and auth$9 and (compar$4 or match$4 or map$4) and 726/3.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L50	0	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and (finger adj print$4) and auth$9 and (compar$4 or match$4 or map$4) and 726/14-15.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L51	1	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and (finger adj print$4) and auth$9 and (compar$4 or match$4 or map$4) and 726/24-26.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L52	1	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and (finger adj print$4) and auth$9 and (compar$4 or match$4 or map$4) and 726/22.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L53	1	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and (finger adj print$4) and auth$9 and (compar$4 or match$4 or map$4) and 726/11.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L54	257	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and 718/1.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L55	13	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and 718/100.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L56	104	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and 709/223-224.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L57	10653	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 same associat$6 same auth$7 same fingerprint$4 718/1.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L58	0	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 same associat$6 same auth$7 same fingerprint$4 and 718/1.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L59	0	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 same auth$7 same fingerprint$4 and 718/1.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L60	0	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 same auth$7 same	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20

IPR2025-00068
CrowdStrike EX1002 Page 148

		fingerprint$4 and 718/100.ccls.				
L61	0	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and auth$7 same fingerprint$4 and 718/100.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L62	5	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and auth$4 and 709/223-224.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L73	2	"20080320594".did.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2016/08/22 14:20
L74	2	"20120331553".did.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2016/08/22 14:20
L75	2	"20120331553".did.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L76	2	"20080320594".did.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L77	29	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and fingerprint$4 and G06F21/554.cpc.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L78	29	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and fingerprint$4 and G06F21/56.cpc.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L79	38	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and fingerprint$4 and G06F21/566.cpc.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L80	1	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and fingerprint$4 and G06F21/51.cpc.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L81	10	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and fingerprint$4 and G06F21/52.cpc.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L82	6	monitor$4 same ((virtual adj machine$4) or VM or VMM) same	US-PGPUB; USPAT; EPO;	OR	OFF	2016/08/22 14:20

		(activit$4 or event$4) and source and target$4 and fingerprint$4 and G06F21/50.cpc.	JPO; DERWENT			
L83	41	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and fingerprint$4 and H04L63/145.cpc.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L84	28	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and fingerprint$4 and H04L63/1491.cpc.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L85	47	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and fingerprint$4 and 726/22-25.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L86	23	CAPALIK-ALEN.inv.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2016/08/22 14:20
L87	19	CAPALIK-ALEN.inv. and virtual$4	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2016/08/22 14:20
L88	13	CAPALIK-ALEN.inv. and virtual$4 and monitor$4	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2016/08/22 14:20
L89	9	ANDREWS-DAVID.inv. and virtual$4 and monitor$4	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2016/08/22 14:20
L90	6	BECKER-BEN.inv. and virtual$4 and monitor$4	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2016/08/22 14:20
L91	2	"20050136570".did.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L92	2	"20050136725".did.	US-PGPUB; USPAT; EPO; JPO;	OR	OFF	2016/08/22 14:20

			DERWENT			
L93	2	"20060136725".did.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L94	2	"20060136720".did.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L95	5	"2007000689".did.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L96	2	"20070002689".did.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L97	2	"20060294592".did.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L98	0	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) same source same target$4 same figureprint$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L99	0	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and figureprint$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L100	173	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and fingerprint$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L101	5	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) same source same target$4 same fingerprint$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L102	20	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) same fingerprint$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L103	5	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) same fingerprint$4 same decoy$4 same unauthor$6	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L104	8	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) same fingerprint$4 and auth$9 and prevent$4 same attack$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L105	8	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) same fingerprint$4 and auth$9 and (compar$4 or match$4 or map$4) and prevent$4 same attack$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L106	8	monitor$4 same ((virtual adj machine$4) or VM or VMM) same	US-PGPUB; USPAT; EPO;	OR	OFF	2016/08/22 14:20

IPR2025-00068
CrowdStrike EX1002 Page 151

		(activit$4 or event$4) same fingerprint$4 and auth$9 and (compar$4 or match$4 or map$4) and prevent$4 and attack$4	JPO; DERWENT			
L107	118	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and fingerprint$4 and auth$9 and (compar$4 or match$4 or map$4) and prevent$4 and attack$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L108	11	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and fingerprint$4 and auth$9 and (compar$4 or match$4 or map$4) and prevent$4 and attack$4 and 726/25.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L109	4	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and fingerprint$4 and auth$9 and (compar$4 or match$4 or map$4) and prevent$4 and attack$4 and 709/223-224.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L110	25	("20010011254" | "20020194437" | "20040153672" | "20040177269" | "20070240221" | "20080127114" | "20100095281" | "5621886" | "5740413" | "6343280" | "6446062" | "7996836").PN.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L111	7	("20010011254" | "20020194437" | "20040153672" | "20040177269" | "20070240221" | "20080127114" | "20100095281" | "5621886" | "5740413" | "6343280" | "6446062" | "7996836").PN. and (virtual adj machine$4)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L112	2	"20050136570".did.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L113	2	"20050136725".did.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L114	2	"20060136725".did.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L115	2	"20060136720".did.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L116	5	"2007000689".did.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L117	2	"20070002689".did.	US-PGPUB; USPAT; EPO; JPO;	OR	OFF	2016/08/22 14:20

			DERWENT			
L118	2	"20060294592".did.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L119	0	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) same source same target$4 same figureprint$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L120	0	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and figureprint$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L121	173	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and fingerprint$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L122	5	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) same source same target$4 same fingerprint$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L123	20	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) same fingerprint$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L124	5	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) same fingerprint$4 same decoy$4 same unauthor$6	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L125	8	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) same fingerprint$4 and auth$9 and prevent$4 same attack$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L126	8	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) same fingerprint$4 and auth$9 and (compar$4 or match$4 or map$4) and prevent$4 same attack$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L127	8	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) same fingerprint$4 and auth$9 and (compar$4 or match$4 or map$4) and prevent$4 and attack$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L128	118	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and fingerprint$4 and auth$9 and (compar$4 or match$4 or map$4) and prevent$4 and attack$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L129	11	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and fingerprint$4 and auth$9 and (compar$4 or match$4 or map$4) and prevent$4 and attack$4 and 726/25.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20

L130	4	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and fingerprint$4 and auth$9 and (compar$4 or match$4 or map$4) and prevent$4 and attack$4 and 709/223-224.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L131	21	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and (finger adj print$4)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L132	10653	718/1.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L133	1	L131 and L132	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L134	6880	718/100.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L135	0	L131 and L134	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L136	1	L128 and L134	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L137	0	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and (finger adj print$4) and auth$9 and (compar$4 or match$4 or map$4) and "7263".ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L138	0	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and (finger adj print$4) and auth$9 and (compar$4 or match$4 or map$4) and "726/3".ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L139	0	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and (finger adj print$4) and auth$9 and (compar$4 or match$4 or map$4) and 726/3.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L140	0	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and (finger adj print$4) and auth$9 and (compar$4 or match$4 or map$4) and 726/14-15.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L141	1	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and (finger adj print$4) and auth$9 and (compar$4 or match$4 or map$4) and 726/24-26.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L142	1	monitor$4 same ((virtual adj	US-PGPUB;	OR	OFF	2016/08/22

IPR2025-00068
CrowdStrike EX1002 Page 154

		machine$4) or VM or VMM) same (activit$4 or event$4) and (finger adj print$4) and auth$9 and (compar$4 or match$4 or map$4) and 726/22.ccls.	USPAT; EPO; JPO; DERWENT			14:20
L143	1	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and (finger adj print$4) and auth$9 and (compar$4 or match$4 or map$4) and 726/11.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L144	257	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and 718/1.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L145	13	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and 718/100.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L146	104	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and 709/223-224.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L147	10653	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 same associat$6 same auth$7 same fingerprint$4 718/1.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L148	0	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 same associat$6 same auth$7 same fingerprint$4 and 718/1.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L149	0	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 same auth$7 same fingerprint$4 and 718/1.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L150	0	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 same auth$7 same fingerprint$4 and 718/100.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L151	0	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and auth$7 same fingerprint$4 and 718/100.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L152	5	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and auth$4 and 709/223-224.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L153	2	"20080320594".did.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2016/08/22 14:20

L154	2	"20120331553".did.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2016/08/22 14:20
L155	2	"20120331553".did.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L156	2	"20080320594".did.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L157	29	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and fingerprint$4 and G06F21/554.cpc.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L158	29	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and fingerprint$4 and G06F21/56.cpc.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L159	38	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and fingerprint$4 and G06F21/566.cpc.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L160	1	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and fingerprint$4 and G06F21/51.cpc.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L161	10	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and fingerprint$4 and G06F21/52.cpc.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L162	6	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and fingerprint$4 and G06F21/50.cpc.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L163	41	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and fingerprint$4 and H04L63/145.cpc.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L164	28	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and fingerprint$4 and H04L63/1491.cpc.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L165	47	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and fingerprint$4 and 726/22-25.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20

EAST Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L63	21	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and (finger adj print$4)	US-PGPUB; USPAT; * No UPAD	OR	OFF	2016/08/22 14:20
L64	7038	718/1.ccls.	US-PGPUB; USPAT; * No UPAD	OR	OFF	2016/08/22 14:20
L65	5120	718/100.ccls.	US-PGPUB; USPAT; * No UPAD	OR	OFF	2016/08/22 14:20
L66	13	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and 718/100.ccls.	US-PGPUB; USPAT; * No UPAD	OR	OFF	2016/08/22 14:20
L67	5	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and auth$4 and 709/223-224.ccls.	US-PGPUB; USPAT; * No UPAD	OR	OFF	2016/08/22 14:20
L68	0	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and auth$4 and 713/155.ccls.	US-PGPUB; USPAT; * No UPAD	OR	OFF	2016/08/22 14:20
L69	2	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and auth$4 and 713/164-165.ccls.	US-PGPUB; USPAT; * No UPAD	OR	OFF	2016/08/22 14:20
L70	8	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) same fingerprint$4 and auth$9 and prevent$4 same attack$4	US-PGPUB; USPAT; * No UPAD	OR	OFF	2016/08/22 14:20
L71	104	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and 709/223-224.ccls.	US-PGPUB; USPAT; * No UPAD	OR	OFF	2016/08/22 14:20
L72	171	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and fingerprint$4	US-PGPUB; USPAT; * No UPAD	OR	OFF	2016/08/22 14:20
L166	21	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and (finger adj print$4)	US-PGPUB; USPAT; * No UPAD	OR	OFF	2016/08/22 14:20

L167	7038	718/1.ccls.	US-PGPUB; USPAT; * No UPAD	OR	OFF	2016/08/22 14:20
L168	5120	718/100.ccls.	US-PGPUB; USPAT; * No UPAD	OR	OFF	2016/08/22 14:20
L169	5	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and auth$4 and 709/223-224.ccls.	US-PGPUB; USPAT; * No UPAD	OR	OFF	2016/08/22 14:20
L170	0	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and auth$4 and 713/155.ccls.	US-PGPUB; USPAT; * No UPAD	OR	OFF	2016/08/22 14:20
L171	2	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and auth$4 and 713/164-165.ccls.	US-PGPUB; USPAT; * No UPAD	OR	OFF	2016/08/22 14:20
L172	8	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) same fingerprint$4 and auth$9 and prevent$4 same attack$4	US-PGPUB; USPAT; * No UPAD	OR	OFF	2016/08/22 14:20
L173	104	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and 709/223-224.ccls.	US-PGPUB; USPAT; * No UPAD	OR	OFF	2016/08/22 14:20
L174	171	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and fingerprint$4	US-PGPUB; USPAT; * No UPAD	OR	OFF	2016/08/22 14:20
L175	41	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and fingerprint$4 and H04L63/145.cpc.	US-PGPUB; USPAT; * No UPAD	OR	OFF	2016/08/22 14:20
L176	27	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and fingerprint$4 and H04L63/1491.cpc.	US-PGPUB; USPAT; * No UPAD	OR	OFF	2016/08/22 14:20
L177	6	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and fingerprint$4 and G06F21/50.cpc.	US-PGPUB; USPAT; * No UPAD	OR	OFF	2016/08/22 14:20
L178	8	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) same fingerprint$4 and auth$9 and prevent$4 same attack$4	US-PGPUB; USPAT; * No UPAD	OR	OFF	2016/08/22 14:20

L179	13	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and 718/100.ccls.	US-PGPUB; USPAT; * No UPAD	OR	OFF	2016/08/22 14:20

8/22/2016 2:46:23 PM
C:\Users\tnguyen39\Documents\EAST\Workspaces\14823916.wsp

INFORMATION DISCLOSURE CITATION IN A PATENT PTO 1449				Electronically filed	*February 5, 2016*
				Application Number	*14/823,916*
				Filing Date	*August 11, 2015*
				First Named Inventor	*Alen Capalik*
				Group Art Unit	*2431*
				Examiner Name	*To be assigned*
Sheet	1	of	1	Attorney Docket Number	*067292-5005-US01*

U.S. PATENT DOCUMENTS

Examiner Initials	Cite No.	Document Number Number - Kind Code[1]	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pgs, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	A1	8,776,050 B2	07-08-2014	Plouffe et al.	
	A2	8,943,506 B2	01-27-2015	Tang et al.	
	A3	8,949,826 B2	02-03-2015	Fitzgerald et al.	

FOREIGN PATENT DOCUMENTS

Examiner Initials	Cite No.	Foreign Patent Document Country Code[2] - Number[3] - Kind Code[4] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pgs, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T Yes

OTHER NON PATENT LITERATURE DOCUMENTS

Examiner Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published
	C1	Capalik, Certificate of Grant, AU2011271157, 07JAN2016, 1 pg.
	C2	NeuralIQ Inc., Office Action, AU 2008242296, 05APR2012, 2 pgs
	C3	NeuralIQ Inc., Examination Report, AU2011271157, 13MAR2015, 4 pgs.

Examiner Signature	/THU HA T NGUYEN/	Date Considered	08/22/2016

DB2/ 28134257.1

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /T.T.N/

INFORMATION DISCLOSURE CITATION IN A PATENT PTO 1449				Electronically filed	*December 10, 2015*
				Application Number	*14/823,916*
				Filing Date	*August 11, 2015*
				First Named Inventor	*Alen Capalik*
				Group Art Unit	*2431*
				Examiner Name	*To be assigned*
Sheet	1	of	5	Attorney Docket Number	*067292-5005-US01*

U.S. PATENT DOCUMENTS					
Examiner Initials	Cite No.	Document Number Number - Kind Code[1]	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pgs, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	A1	2001/0011254 A1	08-02-2001	Clark	
	A2	2002/0099752 A1	07-25-2002	Markos et al.	
	A3	2002/0166063 A1	11-07-2002	Lachman, III et al.	
	A4	2002/0194437 A1	12-19-2002	Kapoor et al.	
	A5	2003/0023656 A1	01-30-2003	Hutchison et al.	
	A6	2003/0120935 A1	06-26-2003	Teal et al.	
	A7	2004/0025052 A1	02-05-2004	Dickenson	
	A8	2004/0153672 A1	08-05-2004	Watt et al.	
	A9	2004/0177269 A1	09-09-2004	Belnet et al.	
	A10	2004/0225877 A1	11-11-2004	Huang	
	A11	2005/0229250 A1	10-13-2005	Ring et al.	
	A12	2006/0018466 A1	01-26-2006	Adelstein et al.	
	A13	2006/0031673 A1	02-09-2006	Beck et al.	
	A14	2006/0136720 A1	06-22-2006	Armstrong et al.	
	A15	2006/0242703 A1	10-26-2006	Abeni	
	A16	2006/0288414 A1	12-21-2006	Kuroda	
	A17	2006/0294592 A1	12-28-2006	Polyakov et al.	
	A18	2007/0002689 A1	01-04-2007	Mateescu et al.	
	A19	2007/0101431 A1	05-03-2007	Clift et al.	
	A20	2007/0180450 A1	08-02-2007	Croft et al.	
	A21	2007/0180529 A1	08-02-2007	Costea et al.	
	A22	2007/0240221 A1	10-11-2007	Tuvell et al.	
	A23	2007/0250930 A1	10-25-2007	Aziz et al.	
	A24	2008/0005782 A1	01-03-2008	Aziz	
	A25	2008/0016571 A1	01-17-2008	Chang	
	A26	2008/0127114 A1	05-29-2008	Vasudevan	

Examiner Signature		Date Considered	

DB2/ 27215619.1

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /T.T.N/

INFORMATION DISCLOSURE CITATION IN A PATENT PTO 1449				Electronically filed	*December 10, 2015*
				Application Number	*14/823,916*
				Filing Date	*August 11, 2015*
				First Named Inventor	*Alen Capalik*
				Group Art Unit	*2431*
				Examiner Name	*To be assigned*
Sheet	2	of	5	Attorney Docket Number	*067292-5005-US01*

	A27	2008/0177994 A1	07-24-2008	Mayer	
	A28	2008/0222729 A1	09-11-2008	Chen et al.	
	A29	2008/0320594 A1	12-25-2008	Jiang	
	A30	2009/0307273 A1	12-10-2009	Johnson et al.	
	A31	2010/0042632 A1	02-18-2010	Johnson et al.	
	A32	2010/0095281 A1	04-15-2010	Raber	
	A33	2011/0060947 A1	03-10-2011	Song et al.	
	A34	2011/0179136 A1	07-21-2011	Twitchell	
	A35	2011/0239291 A1	09-29-2011	Sotka	
	A36	2012/0174186 A1	07-05-2012	Aziz et al.	
	A37	2012/0179904 A1	07-12-2012	Dunn et al.	
	A38	2012/0255012 A1	10-04-2012	Sallam	
	A39	2012/0255018 A1	10-04-2012	Sallam	
	A40	2012/0331553 A1	12-27-2012	Azizi et al.	
	A41	2013/0047257 A1	02-21-2013	Aziz	
	A42	2013/0238785 A1	09-12-2013	Hawk et al.	
	A43	2013/0254870 A1	09-26-2013	Sotka	
	A44	2013/0304903 A1	11-14-2013	Mick et al.	
	A45	2014/0026121 A1	01-23-2014	Jackson et al.	
	A46	2014/0096131 A1	04-03-2014	Sonneck et al.	
	A47	5,339,426	08-16-1994	Aoshima	
	A48	5,621,886	04-15-1997	Alpert et al.	
	A49	5,664,159	09-02-1997	Richter et al.	
	A50	5,740,413	04-14-1998	Alpert et al.	
	A51	6,009,274	12-28-1999	Fletcher et al.	
	A52	6,279,113 B1	08-21-2001	Vaidya	
	A53	6,343,280 B2	01-29-2002	Clark	
	A54	6,360,327 B1	03-19-2002	Hobson	
	A55	6,446,062 B1	09-03-2002	Levine et al.	
	A56	7,222,366 B2	05-22-2007	Bruton, III et al.	
	A57	7,392,543 B2	06-24-2008	Szor	

Examiner Signature		Date Considered	

DB2/ 27215619.1

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /T.T.N/

INFORMATION DISCLOSURE CITATION IN A PATENT PTO 1449				Electronically filed	*December 10, 2015*
				Application Number	*14/823,916*
				Filing Date	*August 11, 2015*
				First Named Inventor	*Alen Capalik*
				Group Art Unit	*2431*
				Examiner Name	*To be assigned*
Sheet	3	of	5	Attorney Docket Number	*067292-5005-US01*

	A58	7,464,407 B2	12-09-2008	Nakae et al.	
	A59	7,581,219 B2	08-25-2009	Neiger et al	
	A60	7,596,654 B1	09-29-2009	Wong	
	A61	7,996,836 B1	08-09-2011	McCorkendale et al.	
	A62	8,539,582 B1	09-17-2013	Aziz et al	
	A63	8,365,180 B2	01-29-2013	Kawasaki et al.	
	A64	8,448,170 B2	05-21-2013	Wipfel et al.	
	A65	8,539,582 B1	09-17-2013	Aziz et al.	
	A66	8,572,613 B1	10-29-2013	Brandwine	
	A67	8,683,548 B1	03-25-2014	Curry et al.	

FOREIGN PATENT DOCUMENTS

Examiner Initials	Cite No.	Foreign Patent Document Country Code[2] - Number[3] - Kind Code[4] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pgs, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T Yes
	B1	JP 2005-316779	11-10-2005	Intelligent Cosmos Research Institute		
	B2	WO 2006/113781 A1	10-26-2006	University of Columbia		
	B3	WO 2007/027739	03-08-2007	Microsoft Corp.		

OTHER NON PATENT LITERATURE DOCUMENTS

Examiner Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published
	C1	Asrigo, Using VMM-Based Sensors to Monitor Honeypots, 14JUN2006, 11 pgs
	C2	Capalik, Final Office Action, US 11/788,795, 14AUG2014, 18 pgs
	C3	Capalik, Examiner's Answer, US 11/788,795, 31MAY2011, 19 pgs
	C4	Capalik, Notice of Allowance, US 11/788,743, 24OCT2012, 9 pgs
	C5	Capalik, Notice of Allowance, US 13/759,335, 09OCT2013, 10 pgs
	C6	Capalik,Notice of Allowance, US 13/163,590, 10APR2015, 5 pgs
	C7	Capalik, Final Office Action, US 13/163,590, 15AUG2014, 11 pgs
	C8	Capalik, Notice of Allowance, US 13/163,590, 01MAY2014, 5 pgs

Examiner Signature	/THU HA T NGUYEN/	Date Considered	08/22/2016

DB2/ 27215619.1

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /T.T.N/

INFORMATION DISCLOSURE CITATION IN A PATENT PTO 1449				Electronically filed	*December 10, 2015*
				Application Number	*14/823,916*
				Filing Date	*August 11, 2015*
				First Named Inventor	*Alen Capalik*
				Group Art Unit	*2431*
				Examiner Name	*To be assigned*
Sheet	4	of	5	Attorney Docket Number	*067292-5005-US01*

	C9	Capalik, Office Action, US 13/163,590, 25OCT2013, 11 pgs
	C10	Capalik, Office Action, US 11/488,743, 04AUG2010, 22 pgs
	C11	Capalik, Office Action, US 11/488,743, 16FEB2010, 23 pgs
	C12	Capalik, Office Action, US 11/488,743, 18JAN2011, 23 pgs
	C13	Capalik, Office Action, US 11/488,743, 30JUL2009, 21 pgs
	C14	Capalik, Office Action, US 11/788,795, 01DEC2010, 19 pgs
	C15	Capalik, Office Action, US 11/788,795, 09JUN2010, 14 pgs
	C16	Capalik, Office Action, US 13/163,578, 01NOV2013, 15 pgs
	C17	Capalik, Office Action, US 13/759,335, 14JUN2013, 32 pgs
	C18	Capalik, Office Action, US 14/542,376, 23JUL2015, 10 pgs
	C19	CounterTack Inc., Certificate of Grant, EP08745858.4, 05AUG2015, 1 pg.
	C20	CounterTack Inc., Extended European Search Report, EP15174670.8, 11NOV2015, 4 pgS.
	C21	Dagon et al., "HoneyStat: Local Worm Detection Using Honeypots," Recent Advances in Intrusion Detection, Springer Berlin Heidelberg, 2004, 20 pgs.
	C22	Debug Register, Aus Lowlevel, 22MAR2010, 2 pgs
	C23	European Network of Affined Honeypots, D1.2: Attack Detection and Signature Generation, 11MAY2006
	C24	Anonymous, Wikipedia, "Honeypot (Computing)" http://en.wikipedia.org/wiki/Honeypot, 17JUL2006, 4 pgs
	C25	Anonymous, Wikipedia, "Intrusion-Detection System" http://en.wikipedia.org/wiki/Intrusion_detection_system, 17JUL2006, 3 pgs
	C26	ISR, PCT/US08/60336, 11AUG2008
	C27	Joshi, Detecting Past and Present Intrusions Through Vulnerability Specific Predicates, SOSP'05, Brighton, UK, 23-26OCT2005, 14 pgs
	C28	Krapf, XEN memory management, 30OCT2007, 5 pgs
	C29	Liang, Fast and Automated Generation of Attach Signatures: A Basis for Building Self-Protecting Servers, 7-11NOV2005
	C30	Litty, Hypervisor support for identifying covertly executing binaries, 31DEC2008, 16 pgs
	C31	NeuralIQ Inc., Decision to Grant a Patent, JP 2010-504185, 26JUL2013, 1 pg
	C32	Debug Register, Aus Lowlevel, 22MAR2010, 2 pgs
	C33	European Network of Affined Honeypots, D1.2: Attack Detection and Signature Generation, 11MAY2006
	C34	NeuralIQ Inc., Extended European Search Report, 08745858-4, 12JUN2014, 4 pgs
	C35	NeuralIQ Inc., International Search Report / Written Opinion, PCT/US2011/041119, 04OCT2011, 12 pgs

Examiner Signature	/THU HA T NGUYEN/	Date Considered	08/22/2016

DB2/ 27215619.1

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /T.T.N/

INFORMATION DISCLOSURE CITATION IN A PATENT PTO 1449				Electronically filed	*December 10, 2015*
				Application Number	*14/823,916*
				Filing Date	*August 11, 2015*
				First Named Inventor	*Alen Capalik*
				Group Art Unit	*2431*
				Examiner Name	*To be assigned*
Sheet	5	of	5	Attorney Docket Number	*067292-5005-US01*

	C36	NeuralIQ Inc., International Search Report / Written Opinion, PCT/US2011/041122, 21SEP2011, 12 pgs
	C37	NeuralIQ Inc., Notice of Reasons for Rejection, JP 2010-504185, 15MAR2013, 4 pgs
	C38	NeuralIQ Inc., Office Action, CA 2,689,126, 15AUG2012, 3 pgs
	C39	NeuralIQ Inc., Office Action, CA 2,689,126, 23JAN2014, 3 pgs
	C40	NeuralIQ Inc., Office Action, CA 2,689,126, 06MAR2015, 3 pgs
	C41	NeuralIQ Inc., Patent Examination Report No. 1, AU 2011271157, 16DEC2013, 4 pgs
	C42	Provos, A Virtual Honeypot Framework, 21OCT2003, 11 pgs
	C43	Shibuya, A study for some experiences of the Operation of Highly Interactive Decoy System, 10AUG2004, 10 pgs
	C44	Tian, A Study of Intrusion Signature Based on Honeypot, Parallel and Distributed Computing, Applications and Technologies, PDCAT'2005, 08DEC2005, pp. 125-129
	C45	Zhang, Honeypot: a supplemented active defense system for network security, Parallel and Distributed Computing, Applications and Technologies, PDCAT'2003, 29AUG2003, pp. 231-235

Examiner Signature	/THU HA T NGUYEN/	Date Considered	08/22/2016

DB2/ 27215619.1

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /T.T.N/

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14823916	CAPALIK ET AL.
	Examiner	Art Unit
	THU HA NGUYEN	2453

CPC- SEARCHED		
Symbol	Date	Examiner
H04L63/1416; 63/1491	08/22/16	THN

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner
726	23, 25	08/22/16	THN

SEARCH NOTES		
Search Notes	Date	Examiner
East, Derwent, JPO, EPO, USPG-Pub search	08/22/16	THN
Inventor name, assignee name search	08/22/16	THN

INTERFERENCE SEARCH			
US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14823916	CAPALIK ET AL.
	Examiner	Art Unit
	THU HA NGUYEN	2453

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	08/08/2016								
	1	✓								
	2	✓								
	3	✓								
	4	✓								
	5	✓								
	6	✓								
	7	✓								
	8	✓								
	9	✓								
	10	✓								
	11	✓								
	12	✓								
	13	✓								
	14	✓								
	15	✓								
	16	✓								
	17	✓								
	18	✓								
	19	✓								
	20	✓								

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	2	"20050136570".did.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L2	2	"20050136725".did.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L3	2	"20060136725".did.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L4	2	"20060136720".did.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L5	5	"2007000689".did.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L6	2	"20070002689".did.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L7	2	"20060294592".did.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L8	0	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) same source same target$4 same figureprint$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L9	0	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and figureprint$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L10	173	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and fingerprint$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L11	5	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) same source same target$4 same fingerprint$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L12	20	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) same fingerprint$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20

L13	5	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) same fingerprint$4 same decoy$4 same unauthor$6	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L14	8	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) same fingerprint$4 and auth$9 and prevent$4 same attack$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L15	8	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) same fingerprint$4 and auth$9 and (compar$4 or match$4 or map$4) and prevent$4 same attack$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L16	8	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) same fingerprint$4 and auth$9 and (compar$4 or match$4 or map$4) and prevent$4 and attack$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L17	118	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and fingerprint$4 and auth$9 and (compar$4 or match$4 or map$4) and prevent$4 and attack$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L18	11	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and fingerprint$4 and auth$9 and (compar$4 or match$4 or map$4) and prevent$4 and attack$4 and 726/25.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L19	4	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and fingerprint$4 and auth$9 and (compar$4 or match$4 or map$4) and prevent$4 and attack$4 and 709/223-224.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L20	25	("20010011254" | "20020194437" | "20040153672" | "20040177269" | "20070240221" | "20080127114" | "20100095281" | "5621886" | "5740413" | "6343280" | "6446062" | "7996836").PN.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L21	7	("20010011254" | "20020194437" | "20040153672" | "20040177269" | "20070240221" | "20080127114" | "20100095281" | "5621886" | "5740413" | "6343280" | "6446062" | "7996836").PN. and (virtual adj machine$4)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L22	2	"20050136570".did.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L23	2	"20050136725".did.	US-PGPUB;	OR	OFF	2016/08/22

			USPAT; EPO; JPO; DERWENT			14:20
L24	2	"20060136725".did.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L25	2	"20060136720".did.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L26	5	"2007000689".did.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L27	2	"20070002689".did.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L28	2	"20060294592".did.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L29	0	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) same source same target$4 same figureprint$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L30	0	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and figureprint$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L31	173	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and fingerprint$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L32	5	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) same source same target$4 same fingerprint$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L33	20	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) same fingerprint$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L34	5	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) same fingerprint$4 same decoy$4 same unauthor$6	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L35	8	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) same fingerprint$4 and auth$9 and prevent$4 same attack$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L36	8	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) same fingerprint$4 and auth$9 and (compar$4 or match$4 or map$4) and prevent$4 same attack$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20

L37	8	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) same fingerprint$4 and auth$9 and (compar$4 or match$4 or map$4) and prevent$4 and attack$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L38	118	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and fingerprint$4 and auth$9 and (compar$4 or match$4 or map$4) and prevent$4 and attack$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L39	11	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and fingerprint$4 and auth$9 and (compar$4 or match$4 or map$4) and prevent$4 and attack$4 and 726/25.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L40	4	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and fingerprint$4 and auth$9 and (compar$4 or match$4 or map$4) and prevent$4 and attack$4 and 709/223-224.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L41	21	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and (finger adj print$4)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L42	10653	718/1.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L43	1	L41 and L42	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L44	6880	718/100.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L45	0	L41 and L44	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L46	1	L38 and L44	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L47	0	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and (finger adj print$4) and auth$9 and (compar$4 or match$4 or map$4) and "7263".ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L48	0	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and (finger adj print$4) and auth$9 and (compar$4 or match$4 or map$4) and "726/3".ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20

L49	0	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and (finger adj print$4) and auth$9 and (compar$4 or match$4 or map$4) and 726/3.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L50	0	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and (finger adj print$4) and auth$9 and (compar$4 or match$4 or map$4) and 726/14-15.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L51	1	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and (finger adj print$4) and auth$9 and (compar$4 or match$4 or map$4) and 726/24-26.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L52	1	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and (finger adj print$4) and auth$9 and (compar$4 or match$4 or map$4) and 726/22.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L53	1	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and (finger adj print$4) and auth$9 and (compar$4 or match$4 or map$4) and 726/11.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L54	257	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and 718/1.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L55	13	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and 718/100.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L56	104	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and 709/223-224.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L57	10653	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 same associat$6 same auth$7 same fingerprint$4 718/1.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L58	0	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 same associat$6 same auth$7 same fingerprint$4 and 718/1.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L59	0	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 same auth$7 same fingerprint$4 and 718/1.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L60	0	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 same auth$7 same	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20

IPR2025-00068
CrowdStrike EX1002 Page 172

		fingerprint$4 and 718/100.ccls.				
L61	0	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and auth$7 same fingerprint$4 and 718/100.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L62	5	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and auth$4 and 709/223-224.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L73	2	"20080320594".did.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2016/08/22 14:20
L74	2	"20120331553".did.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2016/08/22 14:20
L75	2	"20120331553".did.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L76	2	"20080320594".did.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L77	29	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and fingerprint$4 and G06F21/554.cpc.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L78	29	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and fingerprint$4 and G06F21/56.cpc.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L79	38	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and fingerprint$4 and G06F21/566.cpc.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L80	1	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and fingerprint$4 and G06F21/51.cpc.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L81	10	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and fingerprint$4 and G06F21/52.cpc.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L82	6	monitor$4 same ((virtual adj machine$4) or VM or VMM) same	US-PGPUB; USPAT; EPO;	OR	OFF	2016/08/22 14:20

		(activit$4 or event$4) and source and target$4 and fingerprint$4 and G06F21/50.cpc.	JPO; DERWENT			
L83	41	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and fingerprint$4 and H04L63/145.cpc.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L84	28	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and fingerprint$4 and H04L63/1491.cpc.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L85	47	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and fingerprint$4 and 726/22-25.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L86	23	CAPALI K-ALEN.inv.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2016/08/22 14:20
L87	19	CAPALI K-ALEN.inv. and virtual$4	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2016/08/22 14:20
L88	13	CAPALI K-ALEN.inv. and virtual$4 and monitor$4	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2016/08/22 14:20
L89	9	ANDREWS-DAVI D.inv. and virtual$4 and monitor$4	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2016/08/22 14:20
L90	6	BECKER-BEN.inv. and virtual$4 and monitor$4	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2016/08/22 14:20
L91	2	"20050136570".did.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L92	2	"20050136725".did.	US-PGPUB; USPAT; EPO; JPO;	OR	OFF	2016/08/22 14:20

			DERWENT			
L93	2	"20060136725".did.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L94	2	"20060136720".did.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L95	5	"2007000689".did.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L96	2	"20070002689".did.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L97	2	"20060294592".did.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L98	0	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) same source same target$4 same figureprint$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L99	0	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and figureprint$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L100	173	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and fingerprint$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L101	5	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) same source same target$4 same fingerprint$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L102	20	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) same fingerprint$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L103	5	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) same fingerprint$4 same decoy$4 same unauthor$6	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L104	8	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) same fingerprint$4 and auth$9 and prevent$4 same attack$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L105	8	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) same fingerprint$4 and auth$9 and (compar$4 or match$4 or map$4) and prevent$4 same attack$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L106	8	monitor$4 same ((virtual adj machine$4) or VM or VMM) same	US-PGPUB; USPAT; EPO;	OR	OFF	2016/08/22 14:20

		(activit$4 or event$4) same fingerprint$4 and auth$9 and (compar$4 or match$4 or map$4) and prevent$4 and attack$4	JPO; DERWENT			
L107	118	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and fingerprint$4 and auth$9 and (compar$4 or match$4 or map$4) and prevent$4 and attack$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L108	11	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and fingerprint$4 and auth$9 and (compar$4 or match$4 or map$4) and prevent$4 and attack$4 and 726/25.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L109	4	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and fingerprint$4 and auth$9 and (compar$4 or match$4 or map$4) and prevent$4 and attack$4 and 709/223-224.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L110	25	("20010011254" | "20020194437" | "20040153672" | "20040177269" | "20070240221" | "20080127114" | "20100095281" | "5621886" | "5740413" | "6343280" | "6446062" | "7996836").PN.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L111	7	("20010011254" | "20020194437" | "20040153672" | "20040177269" | "20070240221" | "20080127114" | "20100095281" | "5621886" | "5740413" | "6343280" | "6446062" | "7996836").PN. and (virtual adj machine$4)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L112	2	"20050136570".did.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L113	2	"20050136725".did.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L114	2	"20060136725".did.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L115	2	"20060136720".did.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L116	5	"2007000689".did.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L117	2	"20070002689".did.	US-PGPUB; USPAT; EPO; JPO;	OR	OFF	2016/08/22 14:20

			DERWENT			
L118	2	"20060294592".did.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L119	0	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) same source same target$4 same figureprint$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L120	0	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and figureprint$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L121	173	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and fingerprint$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L122	5	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) same source same target$4 same fingerprint$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L123	20	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) same fingerprint$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L124	5	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) same fingerprint$4 same decoy$4 same unauthor$6	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L125	8	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) same fingerprint$4 and auth$9 and prevent$4 same attack$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L126	8	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) same fingerprint$4 and auth$9 and (compar$4 or match$4 or map$4) and prevent$4 same attack$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L127	8	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) same fingerprint$4 and auth$9 and (compar$4 or match$4 or map$4) and prevent$4 and attack$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L128	118	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and fingerprint$4 and auth$9 and (compar$4 or match$4 or map$4) and prevent$4 and attack$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L129	11	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and fingerprint$4 and auth$9 and (compar$4 or match$4 or map$4) and prevent$4 and attack$4 and 726/25.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20

L130	4	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and fingerprint$4 and auth$9 and (compar$4 or match$4 or map$4) and prevent$4 and attack$4 and 709/223-224.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L131	21	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and (finger adj print$4)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L132	10653	718/1.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L133	1	L131 and L132	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L134	6880	718/100.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L135	0	L131 and L134	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L136	1	L128 and L134	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L137	0	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and (finger adj print$4) and auth$9 and (compar$4 or match$4 or map$4) and "7263".ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L138	0	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and (finger adj print$4) and auth$9 and (compar$4 or match$4 or map$4) and "726/3".ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L139	0	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and (finger adj print$4) and auth$9 and (compar$4 or match$4 or map$4) and 726/3.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L140	0	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and (finger adj print$4) and auth$9 and (compar$4 or match$4 or map$4) and 726/14-15.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L141	1	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and (finger adj print$4) and auth$9 and (compar$4 or match$4 or map$4) and 726/24-26.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L142	1	monitor$4 same ((virtual adj	US-PGPUB;	OR	OFF	2016/08/22

IPR2025-00068
CrowdStrike EX1002 Page 178

		machine$4) or VM or VMM) same (activit$4 or event$4) and (finger adj print$4) and auth$9 and (compar$4 or match$4 or map$4) and 726/22.ccls.	USPAT; EPO; JPO; DERWENT			14:20
L143	1	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and (finger adj print$4) and auth$9 and (compar$4 or match$4 or map$4) and 726/11.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L144	257	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and 718/1.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L145	13	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and 718/100.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L146	104	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and 709/223-224.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L147	10653	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 same associat$6 same auth$7 same fingerprint$4 718/1.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L148	0	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 same associat$6 same auth$7 same fingerprint$4 and 718/1.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L149	0	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 same auth$7 same fingerprint$4 and 718/1.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L150	0	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 same auth$7 same fingerprint$4 and 718/100.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L151	0	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and auth$7 same fingerprint$4 and 718/100.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L152	5	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and auth$4 and 709/223-224.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L153	2	"20080320594".did.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2016/08/22 14:20

L154	2	"20120331553".did.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2016/08/22 14:20
L155	2	"20120331553".did.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L156	2	"20080320594".did.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L157	29	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and fingerprint$4 and G06F21/554.cpc.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L158	29	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and fingerprint$4 and G06F21/56.cpc.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L159	38	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and fingerprint$4 and G06F21/566.cpc.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L160	1	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and fingerprint$4 and G06F21/51.cpc.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L161	10	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and fingerprint$4 and G06F21/52.cpc.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L162	6	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and fingerprint$4 and G06F21/50.cpc.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L163	41	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and fingerprint$4 and H04L63/145.cpc.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L164	28	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and fingerprint$4 and H04L63/1491.cpc.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20
L165	47	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and fingerprint$4 and 726/22-25.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:20

IPR2025-00068
CrowdStrike EX1002 Page 180

L180	0	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and fingerprint$4 and auth$9 and (compar$4 or match$4 or map$4) and prevent$4 and attack$4 and 726/023.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:49
L181	28	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and fingerprint$4 and auth$9 and (compar$4 or match$4 or map$4) and prevent$4 and attack$4 and H04L63/1416.cpc.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:49
L182	30	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and fingerprint$4 and auth$9 and (compar$4 or match$4 or map$4) and prevent$4 and attack$4 and H04L63/1491.cpc.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2016/08/22 14:49

EAST Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L63	21	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and (finger adj print$4)	US-PGPUB; USPAT; * No UPAD	OR	OFF	2016/08/22 14:20
L64	7038	718/1.ccls.	US-PGPUB; USPAT; * No UPAD	OR	OFF	2016/08/22 14:20
L65	5120	718/100.ccls.	US-PGPUB; USPAT; * No UPAD	OR	OFF	2016/08/22 14:20
L66	13	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and 718/100.ccls.	US-PGPUB; USPAT; * No UPAD	OR	OFF	2016/08/22 14:20
L67	5	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and auth$4 and 709/223-224.ccls.	US-PGPUB; USPAT; * No UPAD	OR	OFF	2016/08/22 14:20
L68	0	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and auth$4 and 713/155.ccls.	US-PGPUB; USPAT; * No UPAD	OR	OFF	2016/08/22 14:20
L69	2	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and auth$4 and 713/164-165.ccls.	US-PGPUB; USPAT; * No	OR	OFF	2016/08/22 14:20

			UPAD			
L70	8	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) same fingerprint$4 and auth$9 and prevent$4 same attack$4	US-PGPUB; USPAT; * No UPAD	OR	OFF	2016/08/22 14:20
L71	104	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and 709/223-224.ccls.	US-PGPUB; USPAT; * No UPAD	OR	OFF	2016/08/22 14:20
L72	171	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and fingerprint$4	US-PGPUB; USPAT; * No UPAD	OR	OFF	2016/08/22 14:20
L166	21	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and (finger adj print$4)	US-PGPUB; USPAT; * No UPAD	OR	OFF	2016/08/22 14:20
L167	7038	718/1.ccls.	US-PGPUB; USPAT; * No UPAD	OR	OFF	2016/08/22 14:20
L168	5120	718/100.ccls.	US-PGPUB; USPAT; * No UPAD	OR	OFF	2016/08/22 14:20
L169	5	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and auth$4 and 709/223-224.ccls.	US-PGPUB; USPAT; * No UPAD	OR	OFF	2016/08/22 14:20
L170	0	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and auth$4 and 713/155.ccls.	US-PGPUB; USPAT; * No UPAD	OR	OFF	2016/08/22 14:20
L171	2	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and auth$4 and 713/164-165.ccls.	US-PGPUB; USPAT; * No UPAD	OR	OFF	2016/08/22 14:20
L172	8	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) same fingerprint$4 and auth$9 and prevent$4 same attack$4	US-PGPUB; USPAT; * No UPAD	OR	OFF	2016/08/22 14:20
L173	104	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and 709/223-224.ccls.	US-PGPUB; USPAT; * No UPAD	OR	OFF	2016/08/22 14:20
L174	171	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and fingerprint$4	US-PGPUB; USPAT; * No	OR	OFF	2016/08/22 14:20

			UPAD			
L175	41	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and fingerprint$4 and H04L63/145.cpc.	US-PGPUB; USPAT; * No UPAD	OR	OFF	2016/08/22 14:20
L176	27	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and fingerprint$4 and H04L63/1491.cpc.	US-PGPUB; USPAT; * No UPAD	OR	OFF	2016/08/22 14:20
L177	6	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and fingerprint$4 and G06F21/50.cpc.	US-PGPUB; USPAT; * No UPAD	OR	OFF	2016/08/22 14:20
L178	8	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) same fingerprint$4 and auth$9 and prevent$4 same attack$4	US-PGPUB; USPAT; * No UPAD	OR	OFF	2016/08/22 14:20
L179	13	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and 718/100.ccls.	US-PGPUB; USPAT; * No UPAD	OR	OFF	2016/08/22 14:20

8/22/2016 2:54:51 PM
C:\Users\tnguyen39\Documents\EAST\Workspaces\14823916.wsp

INFORMATION DISCLOSURE STATEMENT BY APPLICANT Substitute for Form 1449-PTO				Electronically filed August 10, 2016	
				Application Number	14/823,916
				Filing Date	August 11, 2015
				First Named Inventor	Alen Capalik
				Art Unit	2453
				Examiner Name	Nguyen, Thu Ha T.
Sheet	1	of	1	Attorney Docket Number	067292-5005US01

U.S. PATENT DOCUMENTS					
Examiner Initials	Cite No.[1]	Document Number Number - Kind Code[2]	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		2006/0101516 A1	05-11-2006	Sudaharan et al.	
		2010/0153693 A1	06-17-2010	Stall et al.	
		2010/0306179 A1	12-02-2010	Lim	
		2012/0167063 A1	06-28-2012	Detwiler et al.	
		2014/0108635 A1	04-17-2014	Khemani et al.	

NON PATENT LITERATURE DOCUMENTS		
Examiner Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published
		Capalik, Office Action, US 14/542,376, 22JUN2016, 13 pgs
		CounterTack Inc., International Search Report and Written Opinion, PCTUS2016/012533, 16JUN2016, 12 pgs.

Examiner Signature		Date Considered	

DB2/ 30492683.1

PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference	**FOR FURTHER ACTION**	see Form PCT/ISA/220 as well as, where applicable, item 5 below.
067292-5007WO		
International application No.	International filing date *(day/month/year)*	(Earliest) Priority Date *(day/month/year)*
PCT/US2016/012533	7 January 2016 (07-01-2016)	7 January 2015 (07-01-2015)
Applicant		
COUNTERTACK, INC.		

This international search report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This international search report consists of a total of 4 sheets.

[X] It is also accompanied by a copy of each prior art document cited in this report.

1. **Basis of the report**
   a. With regard to the **language,** the international search was carried out on the basis of:
      [X] the international application in the language in which it was filed
      [ ] a translation of the international application into _____, which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b))
   b. [ ] This international search report has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43.6*bis*(a)).
   c. [ ] With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, see Box No. I.

2. [ ] **Certain claims were found unsearchable** (See Box No. II)

3. [ ] **Unity of invention is lacking** (see Box No III)

4. With regard to the **title,**
   [X] the text is approved as submitted by the applicant
   [ ] the text has been established by this Authority to read as follows:

5. With regard to the **abstract,**
   [X] the text is approved as submitted by the applicant
   [ ] the text has been established, according to Rule 38.2, by this Authority as it appears in Box No. IV. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority

6. With regard to the **drawings,**
   a. the figure of the **drawings** to be published with the abstract is Figure No. 1
      [X] as suggested by the applicant
      [ ] as selected by this Authority, because the applicant failed to suggest a figure
      [ ] as selected by this Authority, because this figure better characterizes the invention
   b. [ ] none of the figures is to be published with the abstract

IPR2025-00068
CrowdStrike EX1002 Page 185

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2016/012533

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L29/06 G06F9/445 G06F21/55 G06F9/45 G06F9/30
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2014/108635 A1 (KHEMANI PRAKASH [US] ET AL) 17 April 2014 (2014-04-17) paragraph [0077] - paragraph [0079]; figures 1a,1d,2a, 2b,7a paragraph [0109] - paragraph [0110] paragraph [0130] paragraph [0167] - paragraph [0168] paragraph [0180] - paragraph [0181] paragraph [0187] - paragraph [0188] -----	1-26
X	US 2010/306179 A1 (LIM KENG [US]) 2 December 2010 (2010-12-02) paragraph [0017] - paragraph [0021] paragraph [0110] paragraph [0178] - paragraph [0179] paragraph [0343] - paragraph [0379] paragraph [0444] - paragraph [0476] ----- -/--	1-26

[X] Further documents are listed in the continuation of Box C. [X] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
9 June 2016	16/06/2016

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Rey, Salvador

1

Form PCT/ISA/210 (second sheet) (April 2005)

IPR2025-00068
CrowdStrike EX1002 Page 186

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2016/012533

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2010/153693 A1 (STALL JONATHON MICHAEL [US] ET AL) 17 June 2010 (2010-06-17) paragraph [0003]; figure 1 paragraph [0025]	1-26
A	US 2012/167063 A1 (DETWILER STEPHEN CAIN [US] ET AL) 28 June 2012 (2012-06-28) the whole document	1-26

1

Form PCT/ISA/210 (continuation of second sheet) (April 2005)

IPR2025-00068
CrowdStrike EX1002 Page 187

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2016/012533

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2014108635 A1	17-04-2014	US 2008225722 A1	18-09-2008
		US 2010095018 A1	15-04-2010
		US 2014108635 A1	17-04-2014
US 2010306179 A1	02-12-2010	US 2008059474 A1	06-03-2008
		US 2008060051 A1	06-03-2008
		US 2008065700 A1	13-03-2008
		US 2008066149 A1	13-03-2008
		US 2008066150 A1	13-03-2008
		US 2008071728 A1	20-03-2008
		US 2008091682 A1	17-04-2008
		US 2010306179 A1	02-12-2010
		US 2012017000 A1	19-01-2012
		US 2012311665 A1	06-12-2012
		US 2013086261 A1	04-04-2013
		US 2014020054 A1	16-01-2014
		US 2014143830 A1	22-05-2014
		US 2014208381 A1	24-07-2014
		US 2014310423 A1	16-10-2014
		US 2014379673 A1	25-12-2014
		US 2015089584 A1	26-03-2015
		US 2015195307 A1	09-07-2015
		US 2015324602 A1	12-11-2015
		US 2016028776 A1	28-01-2016
		US 2016092694 A1	31-03-2016
		US 2016154965 A1	02-06-2016
US 2010153693 A1	17-06-2010	NONE	
US 2012167063 A1	28-06-2012	CA 2819691 A1	21-06-2012
		CN 103597447 A	19-02-2014
		EP 2652608 A2	23-10-2013
		JP 2014507023 A	20-03-2014
		KR 20140019776 A	17-02-2014
		US 2012167063 A1	28-06-2012
		WO 2012082936 A2	21-06-2012

PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

To:

see form PCT/ISA/220

PCT

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

(PCT Rule 43*bis*.1)

Date of mailing
(day/month/year) see form PCT/ISA/210 (second sheet)

Applicant's or agent's file reference
see form PCT/ISA/220

FOR FURTHER ACTION
See paragraph 2 below

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/US2016/012533	07.01.2016	07.01.2015

International Patent Classification (IPC) or both national classification and IPC
INV. H04L29/06 G06F9/445 G06F21/55 G06F9/45 G06F9/30

Applicant
COUNTERTACK, INC.

1. This opinion contains indications relating to the following items:

- ☒ Box No. I Basis of the opinion
- ☐ Box No. II Priority
- ☐ Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- ☐ Box No. IV Lack of unity of invention
- ☒ Box No. V Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step and industrial applicability; citations and explanations supporting such statement
- ☐ Box No. VI Certain documents cited
- ☐ Box No. VII Certain defects in the international application
- ☒ Box No. VIII Certain observations on the international application

2. **FURTHER ACTION**

If a demand for international preliminary examination is made, this opinion will usually be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notifed the International Bureau under Rule 66.1*bis*(b) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

Name and mailing address of the ISA:	Date of completion of this opinion	Authorized Officer
European Patent Office D-80298 Munich Tel. +49 89 2399 - 0 Fax: +49 89 2399 - 4465	see form PCT/ISA/210	Rey, Salvador Telephone No. +49 89 2399-0

Form PCT/ISA/237 (Cover Sheet) (January 2015)

Box No. I Basis of the opinion

1. With regard to the **language**, this opinion has been established on the basis of:

   ☒ the international application in the language in which it was filed.

   ☐ a translation of the international application into , which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1 (b)).

2. ☐ This opinion has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43*bis*.1(a))

3. ☐ With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, this opinion has been established on the basis of a sequence listing:

   a. ☐ forming part of the international application as filed:

      ☐ in the form of an Annex C/ST.25 text file.

      ☐ on paper or in the form of an image file.

   b. ☐ furnished together with the international application under PCT Rule 13*ter*.1(a) for the purposes of international search only in the form of an Annex C/ST.25 text file.

   c. ☐ furnished subsequent to the international filing date for the purposes of international search only:

      ☐ in the form of an Annex C/ST.25 text file (Rule 13*ter*.1(a)).

      ☐ on paper or in the form of an image file (Rule 13*ter*.1(b) and Administrative Instructions, Section 713).

4. ☐ In addition, in the case that more than one version or copy of a sequence listing has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that forming part of the application as filed or does not go beyond the application as filed, as appropriate, were furnished.

5. Additional comments:

IPR2025-00068
CrowdStrike EX1002 Page 190

Box No. V Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes:	Claims	5, 21
	No:	Claims	1-4, 6-20, 22-26
Inventive step (IS)	Yes:	Claims	
	No:	Claims	1-26
Industrial applicability (IA)	Yes:	Claims	1-26
	No:	Claims	

2. Citations and explanations

see separate sheet

Box No. VIII Certain observations on the international application

The following observations on the clarity of the claims, description, and drawings or on the question whether the claims are fully supported by the description, are made:

see separate sheet

Re Item V

Reasoned statement with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1 Reference is made to the following documents:

D1 US 2014/108635 A1 (KHEMANI PRAKASH [US] ET AL) 17 April 2014 (2014-04-17)

2 The present application does not meet the criteria of Article 33(1) PCT, because the subject-matter of claims 1 and 14 is not new in the sense of Article 33(2) PCT.

2.1 D1 discloses the following features of claim 1 (references between parentheses):

A computer implemented method of monitoring a collector computer system, the collector computer system comprising one or more processors (fig. 1d, 2b, par. 0077-0079, monitoring service including data collection, analysis and reporting; monitoring service including monitoring agents; monitoring agent including software and/or hardware for performing collection activities on an appliance; fig. 7a, par. 0187-0188, configure policies corresponding to plurality of appliances) and memory storing an interpreter and compiled instructions for execution by the one or more processors (fig. 2B, par. 0109-110, policy engine in appliance provides a configuration mechanism to allow a user to define or configure a caching policy; policy engine comprises functions or operations), said method comprising:
receiving machine interpretable code that is configured for interpretation by the interpreter, wherein the machine interpretable code is not directly executable by the one or more processors (par. 0180, a policy being interpreted at run-time on a policy engine, or being compiled before its execution) and the machine interpretable code includes: information identifying a first set of one or more monitoring targets within the collector computer system, a method for monitoring the first set of one or more monitoring targets, and predefined reporting criteria (par. 0130 the appliance inspects and intercepts attacks; par. 0180-0181, policies directing behaviour of the appliance including monitoring agents; policy comprising a rule evaluated at run-time with respect to objects, methods and operators);
interpreting the machine interpretable code with the interpreter to obtain the first set of one or more monitoring targets, the method for monitoring the first set of one or more monitoring targets, and the predefined reporting criteria (par. 0180, policy interpreted at run-time);

IPR2025-00068
CrowdStrike EX1002 Page 192

monitoring, using the one or more processors, at least a subset of the first set of one or more monitoring targets for candidate activity that satisfies the predefined reporting criteria by executing compiled instructions that correspond to the method for monitoring the first set of one or more monitoring targets; obtaining candidate event information that is associated with the candidate activity; and reporting the candidate event information to a computer system that is distinct from the collector computer system (par. 0077, agent of the monitoring service performs data collection, aggregation and reporting).

3 The objection above applies *mutatis mutandis* to corresponding independent system claims 10 and 12, and independent non-transitory computer readable storage medium claims 11 and 13.

4 The subject-matter of claim 14 is also not new as it is further disclosed in D1, fig. 7a, par. 0187-0188, configuration interface to configure policies corresponding to plurality of appliances, thus distributing the policies for these appliances from the device on which they are configured.

5 The objection above applies *mutatis mutandis* to corresponding independent system claims 23 and 25, and independent non-transitory computer readable storage medium claims 24 and 26.

6 Dependent claims 2-9 and 15-22 do not appear to contain any additional features which, in combination with the features of any claim to which they refer, meet the requirements of the PCT in respect of novelty and/or inventive step, as these are considered to further specify alternatives and implementation details which are either well known and thus obvious to the skilled person or disclosed in the prior art and which cannot be considered to involve an inventive step. See relevant passages of the International Search Report. In particular,

6.1 Claims 2 and 18: D1 also discloses object-oriented expressions for use in a policy engine using syntax of script languages, par. 0167-0168.

6.2 Claims 3 and 19: D1 also discloses the monitoring service performing monitoring of network infrastructure elements such as an appliance or network connection, par. 0079.

6.3 Claim 5 and 21: D1 also discloses the following features of claim 5 (references between parentheses):

The method of any of claims 1-4 (see point 2.1), wherein the receiving, the interpreting, the monitoring, and the obtaining are performed while the collector computer system is in a first state, the method further including: while

the collector computer system is in a second state that is distinct from the first state (no technical constraint is determined by this definition, since the state is determined by the actions performed and not inversely):
having at disposal~~receiving~~ machine executable code that is configured for execution by the one or more processors and that is not configured for interpretation by the interpreter (par. 0180, policy compiled before its execution, in opposition of being interpreted at run-time), wherein the machine executable code includes information identifying a second set of one or more monitoring targets, and second predefined reporting criteria;
monitoring using the one or more processors, the second set of the one or more monitoring targets for additional candidate activity that satisfies the second predefined reporting criteria by executing the machine executable code;
obtaining additional candidate event information that is associated with the additional candidate activity; and
reporting the additional candidate event information to the computer system that is distinct from the collector computer system (see point 2.1).

6.3.1 The subject-matter of claim 5 differs from D1 in that it further defines the policy being compiled prior to being received.

6.3.2 The difference above is considered as the obvious solution to the problem of how to execute a policy in compiled format in the absence of a local compiler in the appliance. Thus, the skilled person would arrive to the subject-matter of claim 5 when starting from D1 trying to solve the above mentioned problem without exercising inventive skill.

6.4 The subject-matter of claim 9 is also disclosed in D1, see fig. 2a, policy engine located in kernel space.

Re Item VIII

Certain observations on the international application

7 The application does not meet the requirements of Article 6 PCT, because claim 1 is not clear.

7.1 The imprecise statements in the description on paragraphs 0019 and 0047, indicating "incorporated by reference in its entirety" of prior applications, furthermore with a filing date earlier than twelve months of the current

application, imply that the subject-matter for which protection is sought may be different to that defined by the claims, thereby resulting in lack of clarity (Article 6 PCT) when used to interpret them.

Electronic Acknowledgement Receipt	
EFS ID:	26606908
Application Number:	14823916
International Application Number:	
Confirmation Number:	5143
Title of Invention:	System and Method for Identifying Unauthorized Activities on a Computer System using a Data Structure Model
First Named Inventor/Applicant Name:	Alen Capalik
Customer Number:	24341
Filer:	Tae-Woong Koo/Lamesha Robertson
Filer Authorized By:	Tae-Woong Koo
Attorney Docket Number:	067292-5005-US01
Receipt Date:	10-AUG-2016
Filing Date:	11-AUG-2015
Time Stamp:	17:18:52
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		067292_5005US01_IDS.pdf	231546 41e51d53f6d636f51e344e0815050b16d9ad794b	yes	5

	Multipart Description/PDF files in .zip description				
	Document Description		Start	End	
	Transmittal Letter		1	4	
	Information Disclosure Statement (IDS) Form (SB08)		5	5	
Warnings:					
Information:					
2	Non Patent Literature	Capalik_OA_14_542_376_22_Jun_2016.pdf	465911 5cfec1880cc1843014c7bfe419cbddadec12ddca	no	13
Warnings:					
Information:					
3	Non Patent Literature	CounterTack_ISR_WO_2016_012533_16_Jun_2016.pdf	399849 ad9a6fbc020276b46eb5aaef5b970cfcf6b77acf	no	11
Warnings:					
Information:					
		Total Files Size (in bytes):	1097306		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

<u>New Applications Under 35 U.S.C. 111</u>
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

<u>National Stage of an International Application under 35 U.S.C. 371</u>
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

<u>New International Application Filed with the USPTO as a Receiving Office</u>
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Electronically filed August 10, 2016

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application of:	Capalik et al	Confirmation No.:	5143
Serial No.:	14/823,916	Art Unit:	2453
Filed:	August 11, 2015	Examiner:	Nguyen, Thu Ha T.
For:	System and Method for Identifying Unauthorized Activities on a Computer System using a Data Structure Model	Attorney Docket No.:	067292-5005US01

INFORMATION DISCLOSURE STATEMENT

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

In accordance with the duty of disclosure provisions of 37 C.F.R. §1.56, there is hereby provided certain information which the Examiner may consider material to the examination of the subject U.S. patent application. It is requested that the Examiner make this information of record if it is deemed material to the examination of the application.

1. Enclosures accompanying this Information Disclosure Statement are:

1a. ☒ A list of all patents, publications, applications, or other information submitted for consideration by the office.

1b. A legible copy of:

☐ Each foreign patent;

☐ Each publication or that portion which caused it to be listed on the PTO-1449;

☐ For each cited pending U.S. application, the application specification including the claims, and any drawing of the application, or portion of the application which caused it to be listed on the PTO-1449 including any claims directed to that portion;

☒ all other information or portion which caused it to be listed on the PTO-1449.

1c. ☒ An English language copy of search report(s) from a counterpart foreign application or PCT International Search Report.

1d. ☐ Explanations of relevancy (ATTACHMENT 1(d), hereto) or English language abstracts of the non-English language publications.

IPR2025-00068
CrowdStrike EX1002 Page 198

2. ☒ This Information Disclosure Statement is filed under 37 C.F.R. §1.97(b):

☐ Within three months of the filing date of a national application other than a continued prosecution application under §1.53(d);

☐ Within three months of the date of entry of the national stage as set forth in §1.491 in an international application;

☒ Before the mailing of the first Office action on the merits;

☐ Before the mailing of a first Office action after the filing of a request for continued examination under §1.114.

3. ☐ This Information Disclosure Statement is filed under 37 C.F.R. §1.97(c) after the period specified in 37 C.F.R. §1.97(b), but before the mailing date of any of a final action under 37 C.F.R. §1.113, a notice of allowance under 37 C.F.R. §1.311 or an action that otherwise closes prosecution in the application.

(Check either Item 3a, 3b or 3c)

3a. ☐ The Certification Statement in Item 5 below is applicable. Accordingly, no fee is required.

3b. ☐ The $180.00 (large entity) fee set forth in 37 C.F.R. §1.17(p) in accordance with 37 C.F.R. §1.97(c) is to be charged to Morgan, Lewis & Bockius LLP Deposit Account No. 50-0310 (order no.).

3c. ☐ The $90.00 (small entity) fee set forth in 37 C.F.R. §1.17(p) in accordance with 37 C.F.R. §1.97(c) is to be charged to Morgan, Lewis & Bockius LLP Deposit Account No. 50-0310 (order no.).

(Items 3b or 3c to be checked if any reference known for more than 3 months)

4. ☐ This Information Disclosure Statement is filed under 37 C.F.R. §1.97(d) after the period specified in 37 C.F.R. §1.97(c), but on or before the date of payment of the issue fee.

(Check Item 4a, and 4b or 4c)

4a. ☐ The Certification Statement in Item 5 below is applicable.

4b. ☐ The $180.00 (large entity) fee set forth in 37 C.F.R. §1.17(p) in accordance with 37 C.F.R. §1.97(c) is to be charged to Morgan, Lewis & Bockius LLP Deposit Account No. 50-0310 (order no.).

4c. ☐ The $90.00 (small entity) fee set forth in 37 C.F.R. §1.17(p) in accordance with 37 C.F.R. §1.97(c) is to be charged to Morgan, Lewis & Bockius LLP Deposit Account No. 50-0310 (order no.).

5. ☐ Certification Statement (applicable if Item 3a or Item 4a is checked)

(Check either Item 5a, 5b, 5c or 5d)

5a. ☐ In accordance with 37 C.F.R. §1.97(e)(1), it is certified that each item of information contained in this information disclosure statement was first cited in a communication from a foreign patent office in a counterpart foreign application

IPR2025-00068
CrowdStrike EX1002 Page 199

not more than three months prior to the filing of this Information Disclosure Statement.

5b. ☐ In accordance with 37 C.F.R. §1.97(e)(2), it is certified that no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 C.F.R. §1.56(c) more than three months prior to the filing of this information disclosure statement.

5c. ☐ Each item of information contained in this information disclosure statement was cited in a communication from a foreign patent office in a counterpart application, and the communication was not **received** by any individual designated in 37 C.F.R. §1.56(c) more than thirty days prior to the filing of this information disclosure statement.

5d. ☐ Pursuant to 37 C.F.R. §1.704(d), each item of information contained in this information disclosure statement was cited in a communication from a foreign patent office in a counterpart application, and the communication was not **received** by any individual designated in 37 C.F.R. §1.56(c) more than thirty days prior to the filing of this information disclosure statement.

6. ☒ Copies of each cited U.S. patent and each U.S. patent application publication are not enclosed pursuant to the USPTO OG Notice dated 05 August 2003 waiving the requirement under 37 C.F.R. 1.98(a)(2)(i) for U.S. patent applications filed after June 30, 2003.

7. ☒ This application is a continuation application under 37 C.F.R. §1.53(b) or (d).

(Check appropriate Items 7a, 7b and/or 7c)

7a. ☐ A Petition to Withdraw from issue under 37 C.F.R. §1.313(b)(5) is concurrently filed herewith.

7b. ☐ Copies of publications listed on Form PTO-1449 from prior application Serial No. , filed on , of which this application claims priority under 35 U.S.C. §120, are not being submitted pursuant to 37 C.F.R. §1.98(d).

7c. ☒ Copies of the publications listed on the attached Form PTO-1449 that were not previously cited in prior application Serial No. 13/163,590, filed on June 17, 2011, are provided herewith.

8. ☐ This is a Supplemental Information Disclosure Statement. (Check Item 8a)

8a. ☐ This Supplemental Information Disclosure Statement under 37 C.F.R. §1.97(f) supplements the Information Disclosure Statement filed on . A bona fide attempt was made to comply with 37 C.F.R. §1.98, but inadvertent omissions were made. These omissions have been corrected herein. Accordingly, additional time is requested so that this Supplemental Information Disclosure Statement can be considered as if properly filed on .

9. ☐ In accordance with 37 C.F.R. §1.98, a concise explanation of what is presently understood to be the relevance of each non-English language publication is:

IPR2025-00068
CrowdStrike EX1002 Page 200

(Check Item 9a, 9b, or 9c)

9a. ☐ satisfied because all non-English language publications were cited on the enclosed English language copy of the PCT International Search Report or the search report from a counterpart foreign application indicating the degree of relevance found by the foreign office.

9b. ☐ set forth in the application.

9c. ☐ enclosed as an attachment hereto.

10. ☒ The Commissioner is authorized to charge any additional fee required or credit any overpayment for this Information Disclosure Statement and/or Petition to Morgan, Lewis & Bockius LLP Deposit Account No. 50-0310 (order no. 067292-5005US01).

11. ☒ No admission is made that the information cited in this Statement is, or is considered to be, material to patentability nor a representation that a search has been made (other than a search report of a foreign counterpart application or PCT International Search Report if submitted herewith). 37 C.F.R. §§1.97(g) and (h).

Respectfully submitted,

Date: August 10, 2016

59,649

Tae-Woong Koo (Reg. No.)
MORGAN, LEWIS & BOCKIUS LLP
1400 Page Mill Road
Palo Alto, CA 94304
(650) 843-4000

IPR2025-00068
CrowdStrike EX1002 Page 201

INFORMATION DISCLOSURE CITATION IN A PATENT PTO 1449				Electronically filed	*February 5, 2016*
				Application Number	*14/823,916*
				Filing Date	*August 11, 2015*
				First Named Inventor	*Alen Capalik*
				Group Art Unit	*2431*
				Examiner Name	*To be assigned*
Sheet	1	of	1	Attorney Docket Number	*067292-5005-US01*

U.S. PATENT DOCUMENTS

Examiner Initials	Cite No.	Document Number Number - Kind Code[1]	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pgs, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	A1	8,776,050 B2	07-08-2014	Plouffe et al.	
	A2	8,943,506 B2	01-27-2015	Tang et al.	
	A3	8,949,826 B2	02-03-2015	Fitzgerald et al.	

FOREIGN PATENT DOCUMENTS

Examiner Initials	Cite No.	Foreign Patent Document Country Code[2] - Number[3] - Kind Code[4] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pgs, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T Yes

OTHER NON PATENT LITERATURE DOCUMENTS

Examiner Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published
	C1	Capalik, Certificate of Grant, AU2011271157, 07JAN2016, 1 pg.
	C2	NeuralIQ Inc., Office Action, AU 2008242296, 05APR2012, 2 pgs
	C3	NeuralIQ Inc., Examination Report, AU2011271157, 13MAR2015, 4 pgs.

Examiner Signature		Date Considered	

DB2/ 28134257.1

Electronic Acknowledgement Receipt	
EFS ID:	24828444
Application Number:	14823916
International Application Number:	
Confirmation Number:	5143
Title of Invention:	System and Method for Identifying Unauthorized Activities on a Computer System using a Data Structure Model
First Named Inventor/Applicant Name:	Alen Capalik
Customer Number:	24341
Filer:	Tae-Woong Koo/Ramona J Zaya
Filer Authorized By:	Tae-Woong Koo
Attorney Docket Number:	067292-5005-US01
Receipt Date:	05-FEB-2016
Filing Date:	11-AUG-2015
Time Stamp:	17:43:30
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		067292-5005-US01-IDS.pdf	228900 cf16e1ba9340c5f93b66275f50091773ac55972f	yes	5

	Multipart Description/PDF files in .zip description				
	Document Description		Start	End	
	Transmittal Letter		1	4	
	Information Disclosure Statement (IDS) Form (SB08)		5	5	
Warnings:					
Information:					
2	Non Patent Literature	Capalik_Certificate-of-Grant-AU2011271157_07JAN2016.pdf	1287781 62fa701ca94e7bb36aa27c203a80bae82c4e3e99	no	1
Warnings:					
Information:					
3	Non Patent Literature	Neuraliq_Examination-Rpt-No2-AU2011271157_13MAR2015.pdf	370242 504be39b47be7a9f9178ae3e51b3d42b43d5e0e3	no	4
Warnings:					
Information:					
4	Non Patent Literature	NeurallQInc-OA-AU2008242296-05APR2012-2pgs.pdf	53428 f58388dd75c0be4e25e49e499d748235dc522465	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	1940351		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Electronically filed February 5, 2016

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application of:	Alen Capalik et al.	Confirmation No.:	5143
Serial No.:	14/823,916	Art Unit:	2431
Filed:	August 11, 2015	Examiner:	To be assigned
For:	System and Method for Identifying Unauthorized Activities on a Computer System using a Data Structure Model	Attorney Docket No.:	067292-5005-US01

INFORMATION DISCLOSURE STATEMENT

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

In accordance with the duty of disclosure provisions of 37 C.F.R. §1.56, there is hereby provided certain information which the Examiner may consider material to the examination of the subject U.S. patent application. It is requested that the Examiner make this information of record if it is deemed material to the examination of the application.

1. Enclosures accompanying this Information Disclosure Statement are:

1a. ☒ A list of all patents, publications, applications, or other information submitted for consideration by the office.

1b. A legible copy of:

☐ Each foreign patent;

☐ Each publication or that portion which caused it to be listed on the PTO-1449;

☐ For each cited pending U.S. application, the application specification including the claims, and any drawing of the application, or portion of the application which caused it to be listed on the PTO-1449 including any claims directed to that portion;

☒ all other information or portion which caused it to be listed on the PTO-1449.

1c. ☐ An English language copy of search report(s) from a counterpart foreign application or PCT International Search Report.

1d. ☐ Explanations of relevancy (ATTACHMENT 1(d), hereto) or English language abstracts of the non-English language publications.

IPR2025-00068
CrowdStrike EX1002 Page 205

2. ☒ This Information Disclosure Statement is filed under 37 C.F.R. §1.97(b):

☐ Within three months of the filing date of a national application other than a continued prosecution application under §1.53(d);

☐ Within three months of the date of entry of the national stage as set forth in §1.491 in an international application;

☒ Before the mailing of the first Office action on the merits;

☐ Before the mailing of a first Office action after the filing of a request for continued examination under §1.114.

3. ☐ This Information Disclosure Statement is filed under 37 C.F.R. §1.97(c) after the period specified in 37 C.F.R. §1.97(b), but before the mailing date of any of a final action under 37 C.F.R. §1.113, a notice of allowance under 37 C.F.R. §1.311 or an action that otherwise closes prosecution in the application.

(Check either Item 3a, 3b or 3c)

3a. ☐ The Certification Statement in Item 5 below is applicable. Accordingly, no fee is required.

3b. ☐ The $180.00 (large entity) fee set forth in 37 C.F.R. §1.17(p) in accordance with 37 C.F.R. §1.97(c) is to be charged to Morgan, Lewis & Bockius LLP Deposit Account No. 50-0310 (order no.).

3c. ☐ The $90.00 (small entity) fee set forth in 37 C.F.R. §1.17(p) in accordance with 37 C.F.R. §1.97(c) is to be charged to Morgan, Lewis & Bockius LLP Deposit Account No. 50-0310 (order no.).

(Items 3b or 3c to be checked if any reference known for more than 3 months)

4. ☐ This Information Disclosure Statement is filed under 37 C.F.R. §1.97(d) after the period specified in 37 C.F.R. §1.97(c), but on or before the date of payment of the issue fee.

(Check Item 4a, and 4b or 4c)

4a. ☐ The Certification Statement in Item 5 below is applicable.

4b. ☐ The $180.00 (large entity) fee set forth in 37 C.F.R. §1.17(p) in accordance with 37 C.F.R. §1.97(c) is to be charged to Morgan, Lewis & Bockius LLP Deposit Account No. 50-0310 (order no.).

4c. ☐ The $90.00 (small entity) fee set forth in 37 C.F.R. §1.17(p) in accordance with 37 C.F.R. §1.97(c) is to be charged to Morgan, Lewis & Bockius LLP Deposit Account No. 50-0310 (order no.).

5. ☐ Certification Statement (applicable if Item 3a or Item 4a is checked)

(Check either Item 5a, 5b, 5c or 5d)

5a. ☐ In accordance with 37 C.F.R. §1.97(e)(1), it is certified that each item of information contained in this information disclosure statement was first cited in a communication from a foreign patent office in a counterpart foreign application

IPR2025-00068
CrowdStrike EX1002 Page 206

not more than three months prior to the filing of this Information Disclosure Statement.

5b. ☐ In accordance with 37 C.F.R. §1.97(e)(2), it is certified that no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 C.F.R. §1.56(c) more than three months prior to the filing of this information disclosure statement.

5c. ☐ Each item of information contained in this information disclosure statement was cited in a communication from a foreign patent office in a counterpart application, and the communication was not **received** by any individual designated in 37 C.F.R. §1.56(c) more than thirty days prior to the filing of this information disclosure statement.

5d. ☐ Pursuant to 37 C.F.R. §1.704(d), each item of information contained in this information disclosure statement was cited in a communication from a foreign patent office in a counterpart application, and the communication was not **received** by any individual designated in 37 C.F.R. §1.56(c) more than thirty days prior to the filing of this information disclosure statement.

6. ☒ Copies of each cited U.S. patent and each U.S. patent application publication are not enclosed pursuant to the USPTO OG Notice dated 05 August 2003 waiving the requirement under 37 C.F.R. 1.98(a)(2)(i) for U.S. patent applications filed after June 30, 2003.

7. ☐ This application is a continuation application under 37 C.F.R. §1.53(b) or (d).

(Check appropriate Items 7a, 7b and/or 7c)

7a. ☐ A Petition to Withdraw from issue under 37 C.F.R. §1.313(b)(5) is concurrently filed herewith.

7b. ☐ Copies of publications listed on Form PTO-1449 from prior application Serial No. , filed on , of which this application claims priority under 35 U.S.C. §120, are not being submitted pursuant to 37 C.F.R. §1.98(d).

7c. ☐ Copies of the publications listed on the attached Form PTO-1449 that were not previously cited in prior application Serial No. , filed on , are provided herewith.

8. ☐ This is a Supplemental Information Disclosure Statement. (Check Item 8a)

8a. ☐ This Supplemental Information Disclosure Statement under 37 C.F.R. §1.97(f) supplements the Information Disclosure Statement filed on . A bona fide attempt was made to comply with 37 C.F.R. §1.98, but inadvertent omissions were made. These omissions have been corrected herein. Accordingly, additional time is requested so that this Supplemental Information Disclosure Statement can be considered as if properly filed on .

9. ☐ In accordance with 37 C.F.R. §1.98, a concise explanation of what is presently understood to be the relevance of each non-English language publication is:

IPR2025-00068
CrowdStrike EX1002 Page 207

(Check Item 9a, 9b, or 9c)

9a. ☐ satisfied because all non-English language publications were cited on the enclosed English language copy of the PCT International Search Report or the search report from a counterpart foreign application indicating the degree of relevance found by the foreign office.

9b. ☐ set forth in the application.

9c. ☐ enclosed as an attachment hereto.

10. ☒ The Commissioner is authorized to charge any additional fee required or credit any overpayment for this Information Disclosure Statement and/or Petition to Morgan, Lewis & Bockius LLP Deposit Account No. 50-0310 (order no. 067292-5005-US01).

11. ☒ No admission is made that the information cited in this Statement is, or is considered to be, material to patentability nor a representation that a search has been made (other than a search report of a foreign counterpart application or PCT International Search Report if submitted herewith). 37 C.F.R. §§1.97(g) and (h).

Respectfully submitted,

Date: February 5, 2016



59,649
Tae-Woong Koo (Reg. No.)

MORGAN, LEWIS & BOCKIUS LLP
2 Palo Alto Square
3000 El Camino Real, Suite 700
Palo Alto, CA 94306
(650) 843-4000

IPR2025-00068
CrowdStrike EX1002 Page 208

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
14/823,916	08/11/2015	Alen Capalik	067292-5005-US01

CONFIRMATION NO. 5143

24341
MORGAN, LEWIS & BOCKIUS LLP (PA)
2 PALO ALTO SQUARE
3000 EL CAMINO REAL, SUITE 700
PALO ALTO, CA 94306

PUBLICATION NOTICE

OC000000079654626

Title: System and Method for Identifying Unauthorized Activities on a Computer System using a Data Structure Model

Publication No.US-2015-0381638-A1
Publication Date:12/31/2015

NOTICE OF PUBLICATION OF APPLICATION

The above-identified application will be electronically published as a patent application publication pursuant to 37 CFR 1.211, et seq. The patent application publication number and publication date are set forth above.

The publication may be accessed through the USPTO's publically available Searchable Databases via the Internet at www.uspto.gov. The direct link to access the publication is currently http://www.uspto.gov/patft/.

The publication process established by the Office does not provide for mailing a copy of the publication to applicant. A copy of the publication may be obtained from the Office upon payment of the appropriate fee set forth in 37 CFR 1.19(a)(1). Orders for copies of patent application publications are handled by the USPTO's Office of Public Records. The Office of Public Records can be reached by telephone at (703) 308-9726 or (800) 972-6382, by facsimile at (703) 305-8759, by mail addressed to the United States Patent and Trademark Office, Office of Public Records, Alexandria, VA 22313-1450 or via the Internet.

In addition, information on the status of the application, including the mailing date of Office actions and the dates of receipt of correspondence filed in the Office, may also be accessed via the Internet through the Patent Electronic Business Center at www.uspto.gov using the public side of the Patent Application Information and Retrieval (PAIR) system. The direct link to access this status information is currently http://pair.uspto.gov/. Prior to publication, such status information is confidential and may only be obtained by applicant using the private side of PAIR.

Further assistance in electronically accessing the publication, or about PAIR, is available by calling the Patent Electronic Business Center at 1-866-217-9197.

Office of Data Managment, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

IPR2025-00068
CrowdStrike EX1002 Page 209

INFORMATION DISCLOSURE CITATION IN A PATENT PTO 1449				Electronically filed	*December 10, 2015*
				Application Number	*14/823,916*
				Filing Date	*August 11, 2015*
				First Named Inventor	*Alen Capalik*
				Group Art Unit	*2431*
				Examiner Name	*To be assigned*
Sheet	1	of	5	Attorney Docket Number	*067292-5005-US01*

U.S. PATENT DOCUMENTS					
Examiner Initials	Cite No.	Document Number Number - Kind Code[1]	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pgs, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	A1	2001/0011254 A1	08-02-2001	Clark	
	A2	2002/0099752 A1	07-25-2002	Markos et al.	
	A3	2002/0166063 A1	11-07-2002	Lachman, III et al.	
	A4	2002/0194437 A1	12-19-2002	Kapoor et al.	
	A5	2003/0023656 A1	01-30-2003	Hutchison et al.	
	A6	2003/0120935 A1	06-26-2003	Teal et al.	
	A7	2004/0025052 A1	02-05-2004	Dickenson	
	A8	2004/0153672 A1	08-05-2004	Watt et al.	
	A9	2004/0177269 A1	09-09-2004	Belnet et al.	
	A10	2004/0225877 A1	11-11-2004	Huang	
	A11	2005/0229250 A1	10-13-2005	Ring et al.	
	A12	2006/0018466 A1	01-26-2006	Adelstein et al.	
	A13	2006/0031673 A1	02-09-2006	Beck et al.	
	A14	2006/0136720 A1	06-22-2006	Armstrong et al.	
	A15	2006/0242703 A1	10-26-2006	Abeni	
	A16	2006/0288414 A1	12-21-2006	Kuroda	
	A17	2006/0294592 A1	12-28-2006	Polyakov et al.	
	A18	2007/0002689 A1	01-04-2007	Mateescu et al.	
	A19	2007/0101431 A1	05-03-2007	Clift et al.	
	A20	2007/0180450 A1	08-02-2007	Croft et al.	
	A21	2007/0180529 A1	08-02-2007	Costea et al.	
	A22	2007/0240221 A1	10-11-2007	Tuvell et al.	
	A23	2007/0250930 A1	10-25-2007	Aziz et al.	
	A24	2008/0005782 A1	01-03-2008	Aziz	
	A25	2008/0016571 A1	01-17-2008	Chang	
	A26	2008/0127114 A1	05-29-2008	Vasudevan	

Examiner Signature		Date Considered	

INFORMATION DISCLOSURE CITATION IN A PATENT PTO 1449				Electronically filed	*December 10, 2015*
				Application Number	*14/823,916*
				Filing Date	*August 11, 2015*
				First Named Inventor	*Alen Capalik*
				Group Art Unit	*2431*
				Examiner Name	*To be assigned*
Sheet	2	of	5	Attorney Docket Number	*067292-5005-US01*

	A27	2008/0177994 A1	07-24-2008	Mayer	
	A28	2008/0222729 A1	09-11-2008	Chen et al.	
	A29	2008/0320594 A1	12-25-2008	Jiang	
	A30	2009/0307273 A1	12-10-2009	Johnson et al.	
	A31	2010/0042632 A1	02-18-2010	Johnson et al.	
	A32	2010/0095281 A1	04-15-2010	Raber	
	A33	2011/0060947 A1	03-10-2011	Song et al.	
	A34	2011/0179136 A1	07-21-2011	Twitchell	
	A35	2011/0239291 A1	09-29-2011	Sotka	
	A36	2012/0174186 A1	07-05-2012	Aziz et al.	
	A37	2012/0179904 A1	07-12-2012	Dunn et al.	
	A38	2012/0255012 A1	10-04-2012	Sallam	
	A39	2012/0255018 A1	10-04-2012	Sallam	
	A40	2012/0331553 A1	12-27-2012	Azizi et al.	
	A41	2013/0047257 A1	02-21-2013	Aziz	
	A42	2013/0238785 A1	09-12-2013	Hawk et al.	
	A43	2013/0254870 A1	09-26-2013	Sotka	
	A44	2013/0304903 A1	11-14-2013	Mick et al.	
	A45	2014/0026121 A1	01-23-2014	Jackson et al.	
	A46	2014/0096131 A1	04-03-2014	Sonneck et al.	
	A47	5,339,426	08-16-1994	Aoshima	
	A48	5,621,886	04-15-1997	Alpert et al.	
	A49	5,664,159	09-02-1997	Richter et al.	
	A50	5,740,413	04-14-1998	Alpert et al.	
	A51	6,009,274	12-28-1999	Fletcher et al.	
	A52	6,279,113 B1	08-21-2001	Vaidya	
	A53	6,343,280 B2	01-29-2002	Clark	
	A54	6,360,327 B1	03-19-2002	Hobson	
	A55	6,446,062 B1	09-03-2002	Levine et al.	
	A56	7,222,366 B2	05-22-2007	Bruton, III et al.	
	A57	7,392,543 B2	06-24-2008	Szor	

Examiner Signature		Date Considered	

INFORMATION DISCLOSURE CITATION IN A PATENT PTO 1449				Electronically filed	*December 10, 2015*
				Application Number	*14/823,916*
				Filing Date	*August 11, 2015*
				First Named Inventor	*Alen Capalik*
				Group Art Unit	*2431*
				Examiner Name	*To be assigned*
Sheet	3	of	5	Attorney Docket Number	*067292-5005-US01*

	A58	7,464,407 B2	12-09-2008	Nakae et al.	
	A59	7,581,219 B2	08-25-2009	Neiger et al	
	A60	7,596,654 B1	09-29-2009	Wong	
	A61	7,996,836 B1	08-09-2011	McCorkendale et al.	
	A62	8,539,582 B1	09-17-2013	Aziz et al	
	A63	8,365,180 B2	01-29-2013	Kawasaki et al.	
	A64	8,448,170 B2	05-21-2013	Wipfel et al.	
	A65	8,539,582 B1	09-17-2013	Aziz et al.	
	A66	8,572,613 B1	10-29-2013	Brandwine	
	A67	8,683,548 B1	03-25-2014	Curry et al.	

FOREIGN PATENT DOCUMENTS

Examiner Initials	Cite No.	Foreign Patent Document Country Code[2] - Number[3] - Kind Code[4] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pgs, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T Yes
	B1	JP 2005-316779	11-10-2005	Intelligent Cosmos Research Institute		
	B2	WO 2006/113781 A1	10-26-2006	University of Columbia		
	B3	WO 2007/027739	03-08-2007	Microsoft Corp.		

OTHER NON PATENT LITERATURE DOCUMENTS

Examiner Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published
	C1	Asrigo, Using VMM-Based Sensors to Monitor Honeypots, 14JUN2006, 11 pgs
	C2	Capalik, Final Office Action, US 11/788,795, 14AUG2014, 18 pgs
	C3	Capalik, Examiner's Answer, US 11/788,795, 31MAY2011, 19 pgs
	C4	Capalik, Notice of Allowance, US 11/788,743, 24OCT2012, 9 pgs
	C5	Capalik, Notice of Allowance, US 13/759,335, 09OCT2013, 10 pgs
	C6	Capalik,Notice of Allowance, US 13/163,590, 10APR2015, 5 pgs
	C7	Capalik, Final Office Action, US 13/163,590, 15AUG2014, 11 pgs
	C8	Capalik, Notice of Allowance, US 13/163,590, 01MAY2014, 5 pgs

Examiner Signature		Date Considered	

IPR2025-00068
CrowdStrike EX1002 Page 212

INFORMATION DISCLOSURE CITATION IN A PATENT PTO 1449				Electronically filed	*December 10, 2015*
				Application Number	*14/823,916*
				Filing Date	*August 11, 2015*
				First Named Inventor	*Alen Capalik*
				Group Art Unit	*2431*
				Examiner Name	*To be assigned*
Sheet	4	of	5	Attorney Docket Number	*067292-5005-US01*

	C9	Capalik, Office Action, US 13/163,590, 25OCT2013, 11 pgs
	C10	Capalik, Office Action, US 11/488,743, 04AUG2010, 22 pgs
	C11	Capalik, Office Action, US 11/488,743, 16FEB2010, 23 pgs
	C12	Capalik, Office Action, US 11/488,743, 18JAN2011, 23 pgs
	C13	Capalik, Office Action, US 11/488,743, 30JUL2009, 21 pgs
	C14	Capalik, Office Action, US 11/788,795, 01DEC2010, 19 pgs
	C15	Capalik, Office Action, US 11/788,795, 09JUN2010, 14 pgs
	C16	Capalik, Office Action, US 13/163,578, 01NOV2013, 15 pgs
	C17	Capalik, Office Action, US 13/759,335, 14JUN2013, 32 pgs
	C18	Capalik, Office Action, US 14/542,376, 23JUL2015, 10 pgs
	C19	CounterTack Inc., Certificate of Grant, EP08745858.4, 05AUG2015, 1 pg.
	C20	CounterTack Inc., Extended European Search Report, EP15174670.8, 11NOV2015, 4 pgS.
	C21	Dagon et al., "HoneyStat: Local Worm Detection Using Honeypots," Recent Advances in Intrusion Detection, Springer Berlin Heidelberg, 2004, 20 pgs.
	C22	Debug Register, Aus Lowlevel, 22MAR2010, 2 pgs
	C23	European Network of Affined Honeypots, D1.2: Attack Detection and Signature Generation, 11MAY2006
	C24	Anonymous, Wikipedia, "Honeypot (Computing)" http://en.wikipedia.org/wiki/Honeypot, 17JUL2006, 4 pgs
	C25	Anonymous, Wikipedia, "Intrusion-Detection System" http://en.wikipedia.org/wiki/Intrusion_detection_system, 17JUL2006, 3 pgs
	C26	ISR, PCT/US08/60336, 11AUG2008
	C27	Joshi, Detecting Past and Present Intrusions Through Vulnerability Specific Predicates, SOSP'05, Brighton, UK, 23-26OCT2005, 14 pgs
	C28	Krapf, XEN memory management, 30OCT2007, 5 pgs
	C29	Liang, Fast and Automated Generation of Attach Signatures: A Basis for Building Self-Protecting Servers, 7-11NOV2005
	C30	Litty, Hypervisor support for identifying covertly executing binaries, 31DEC2008, 16 pgs
	C31	NeuralIQ Inc., Decision to Grant a Patent, JP 2010-504185, 26JUL2013, 1 pg
	C32	Debug Register, Aus Lowlevel, 22MAR2010, 2 pgs
	C33	European Network of Affined Honeypots, D1.2: Attack Detection and Signature Generation, 11MAY2006
	C34	NeuralIQ Inc., Extended European Search Report, 08745858-4, 12JUN2014, 4 pgs
	C35	NeuralIQ Inc., International Search Report / Written Opinion, PCT/US2011/041119, 04OCT2011, 12 pgs

Examiner Signature		Date Considered	

INFORMATION DISCLOSURE CITATION IN A PATENT PTO 1449				Electronically filed	*December 10, 2015*
				Application Number	*14/823,916*
				Filing Date	*August 11, 2015*
				First Named Inventor	*Alen Capalik*
				Group Art Unit	*2431*
				Examiner Name	*To be assigned*
Sheet	5	of	5	Attorney Docket Number	*067292-5005-US01*

	C36	NeuralIQ Inc., International Search Report / Written Opinion, PCT/US2011/041122, 21SEP2011, 12 pgs
	C37	NeuralIQ Inc., Notice of Reasons for Rejection, JP 2010-504185, 15MAR2013, 4 pgs
	C38	NeuralIQ Inc., Office Action, CA 2,689,126, 15AUG2012, 3 pgs
	C39	NeuralIQ Inc., Office Action, CA 2,689,126, 23JAN2014, 3 pgs
	C40	NeuralIQ Inc., Office Action, CA 2,689,126, 06MAR2015, 3 pgs
	C41	NeuralIQ Inc., Patent Examination Report No. 1, AU 2011271157, 16DEC2013, 4 pgs
	C42	Provos, A Virtual Honeypot Framework, 21OCT2003, 11 pgs
	C43	Shibuya, A study for some experiences of the Operation of Highly Interactive Decoy System, 10AUG2004, 10 pgs
	C44	Tian, A Study of Intrusion Signature Based on Honeypot, Parallel and Distributed Computing, Applications and Technologies, PDCAT'2005, 08DEC2005, pp. 125-129
	C45	Zhang, Honeypot: a supplemented active defense system for network security, Parallel and Distributed Computing, Applications and Technologies, PDCAT'2003, 29AUG2003, pp. 231-235

Examiner Signature		Date Considered	

IPR2025-00068
CrowdStrike EX1002 Page 214

Electronic Acknowledgement Receipt	
EFS ID:	24313330
Application Number:	14823916
International Application Number:	
Confirmation Number:	5143
Title of Invention:	System and Method for Identifying Unauthorized Activities on a Computer System using a Data Structure Model
First Named Inventor/Applicant Name:	Alen Capalik
Customer Number:	24341
Filer:	Tae-Woong Koo/Ramona J Zaya
Filer Authorized By:	Tae-Woong Koo
Attorney Docket Number:	067292-5005-US01
Receipt Date:	10-DEC-2015
Filing Date:	11-AUG-2015
Time Stamp:	14:40:32
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Non Patent Literature	Cert2Grant-EP08745858-4-05AUG2015.pdf	25942 74534772d8276a7819778e371ca63b81ce0e827a	no	1
Warnings:					
Information:					

2	Non Patent Literature	NOA-13163590-01MAY2014.pdf	358028 6f3073bda604c5c9c0bdc21c5bda909279ef96ef	no	5
Warnings:					
Information:					
3	Non Patent Literature	NOA-13163590-10APR2015.pdf	358048 4ef134c042a4a863ee1576dcda29fda98e8b6c46	no	5
Warnings:					
Information:					
4	Non Patent Literature	OA-13163590-15AUG2015.pdf	355863 2652b87922061c4b32d159c1a466cb5b8f0d29b3	no	11
Warnings:					
Information:					
5	Non Patent Literature	OA-13163590-25OCT2013.pdf	363018 618fd29a5a1e1de5b1ed43d23ca2ac857a9c1d51	no	11
Warnings:					
Information:					
6	Non Patent Literature	OA-14542376-23JUL2015.pdf	365002 f58558f12c3476a73c493ba0eed27438d4cae767	no	10
Warnings:					
Information:					
7		067292-5005-US01-IDS.pdf	512012 6bc3974c46a29c86ebdeae5e6038c5f28bd71283	yes	9

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Transmittal Letter	1	4
	Information Disclosure Statement (IDS) Form (SB08)	5	9
Warnings:			
Information:			
	Total Files Size (in bytes):	2337913	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Electronically filed December 10, 2015

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application of:	Alen Capalik et al.	Confirmation No.:	5143
Serial No.:	14/823,916	Art Unit:	2431
Filed:	August 11, 2015	Examiner:	To be assigned
For:	System and Method for Identifying Unauthorized Activities on a Computer System using a Data Structure Model	Attorney Docket No.:	067292-5005-US01

INFORMATION DISCLOSURE STATEMENT

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

In accordance with the duty of disclosure provisions of 37 C.F.R. §1.56, there is hereby provided certain information which the Examiner may consider material to the examination of the subject U.S. patent application. It is requested that the Examiner make this information of record if it is deemed material to the examination of the application.

1. Enclosures accompanying this Information Disclosure Statement are:

1a. ☒ A list of all patents, publications, applications, or other information submitted for consideration by the office.

1b. A legible copy of:

☒ Each foreign patent;

☒ Each publication or that portion which caused it to be listed on the PTO-1449;

☐ For each cited pending U.S. application, the application specification including the claims, and any drawing of the application, or portion of the application which caused it to be listed on the PTO-1449 including any claims directed to that portion;

☒ all other information or portion which caused it to be listed on the PTO-1449.

1c. ☒ An English language copy of search report(s) from a counterpart foreign application or PCT International Search Report.

1d. ☐ Explanations of relevancy (ATTACHMENT 1(d), hereto) or English language abstracts of the non-English language publications.

IPR2025-00068
CrowdStrike EX1002 Page 218

2. ☒ This Information Disclosure Statement is filed under 37 C.F.R. §1.97(b):

☐ Within three months of the filing date of a national application other than a continued prosecution application under §1.53(d);

☐ Within three months of the date of entry of the national stage as set forth in §1.491 in an international application;

☒ Before the mailing of the first Office action on the merits;

☐ Before the mailing of a first Office action after the filing of a request for continued examination under §1.114.

3. ☐ This Information Disclosure Statement is filed under 37 C.F.R. §1.97(c) after the period specified in 37 C.F.R. §1.97(b), but before the mailing date of any of a final action under 37 C.F.R. §1.113, a notice of allowance under 37 C.F.R. §1.311 or an action that otherwise closes prosecution in the application.

(Check either Item 3a, 3b or 3c)

3a. ☐ The Certification Statement in Item 5 below is applicable. Accordingly, no fee is required.

3b. ☐ The $180.00 (large entity) fee set forth in 37 C.F.R. §1.17(p) in accordance with 37 C.F.R. §1.97(c) is to be charged to Morgan, Lewis & Bockius LLP Deposit Account No. 50-0310 (order no.).

3c. ☐ The $90.00 (small entity) fee set forth in 37 C.F.R. §1.17(p) in accordance with 37 C.F.R. §1.97(c) is to be charged to Morgan, Lewis & Bockius LLP Deposit Account No. 50-0310 (order no.).

(Items 3b or 3c to be checked if any reference known for more than 3 months)

4. ☐ This Information Disclosure Statement is filed under 37 C.F.R. §1.97(d) after the period specified in 37 C.F.R. §1.97(c), but on or before the date of payment of the issue fee.

(Check Item 4a, and 4b or 4c)

4a. ☐ The Certification Statement in Item 5 below is applicable.

4b. ☐ The $180.00 (large entity) fee set forth in 37 C.F.R. §1.17(p) in accordance with 37 C.F.R. §1.97(c) is to be charged to Morgan, Lewis & Bockius LLP Deposit Account No. 50-0310 (order no.).

4c. ☐ The $90.00 (small entity) fee set forth in 37 C.F.R. §1.17(p) in accordance with 37 C.F.R. §1.97(c) is to be charged to Morgan, Lewis & Bockius LLP Deposit Account No. 50-0310 (order no.).

5. ☐ Certification Statement (applicable if Item 3a or Item 4a is checked)

(Check either Item 5a, 5b, 5c or 5d)

5a. ☐ In accordance with 37 C.F.R. §1.97(e)(1), it is certified that each item of information contained in this information disclosure statement was first cited in a communication from a foreign patent office in a counterpart foreign application

IPR2025-00068
CrowdStrike EX1002 Page 219

not more than three months prior to the filing of this Information Disclosure Statement.

5b. ☐ In accordance with 37 C.F.R. §1.97(e)(2), it is certified that no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 C.F.R. §1.56(c) more than three months prior to the filing of this information disclosure statement.

5c. ☐ Each item of information contained in this information disclosure statement was cited in a communication from a foreign patent office in a counterpart application, and the communication was not **received** by any individual designated in 37 C.F.R. §1.56(c) more than thirty days prior to the filing of this information disclosure statement.

5d. ☐ Pursuant to 37 C.F.R. §1.704(d), each item of information contained in this information disclosure statement was cited in a communication from a foreign patent office in a counterpart application, and the communication was not **received** by any individual designated in 37 C.F.R. §1.56(c) more than thirty days prior to the filing of this information disclosure statement.

6. ☒ Copies of each cited U.S. patent and each U.S. patent application publication are not enclosed pursuant to the USPTO OG Notice dated 05 August 2003 waiving the requirement under 37 C.F.R. 1.98(a)(2)(i) for U.S. patent applications filed after June 30, 2003.

7. ☒ This application is a continuation application under 37 C.F.R. §1.53(b) or (d).

(Check appropriate Items 7a, 7b and/or 7c)

7a. ☐ A Petition to Withdraw from issue under 37 C.F.R. §1.313(b)(5) is concurrently filed herewith.

7b. ☒ Copies of publications listed on Form PTO-1449 from prior application Serial No. 13/163,590 , filed on June 17, 2011, of which this application claims priority under 35 U.S.C. §120, are not being submitted pursuant to 37 C.F.R. §1.98(d).

7c. ☒ Copies of the publications listed on the attached Form PTO-1449 that were not previously cited in prior application Serial No. 13/163,590 , filed on June 17, 2011, are provided herewith.

8. ☐ This is a Supplemental Information Disclosure Statement. (Check Item 8a)

8a. ☐ This Supplemental Information Disclosure Statement under 37 C.F.R. §1.97(f) supplements the Information Disclosure Statement filed on . A bona fide attempt was made to comply with 37 C.F.R. §1.98, but inadvertent omissions were made. These omissions have been corrected herein. Accordingly, additional time is requested so that this Supplemental Information Disclosure Statement can be considered as if properly filed on .

9. ☐ In accordance with 37 C.F.R. §1.98, a concise explanation of what is presently understood to be the relevance of each non-English language publication is:

(Check Item 9a, 9b, or 9c)

9a. ☐ satisfied because all non-English language publications were cited on the enclosed English language copy of the PCT International Search Report or the search report from a counterpart foreign application indicating the degree of relevance found by the foreign office.

9b. ☐ set forth in the application.

9c. ☐ enclosed as an attachment hereto.

10. ☒ The Commissioner is authorized to charge any additional fee required or credit any overpayment for this Information Disclosure Statement and/or Petition to Morgan, Lewis & Bockius LLP Deposit Account No. 50-0310 (order no. 067292-5005-US01).

11. ☒ No admission is made that the information cited in this Statement is, or is considered to be, material to patentability nor a representation that a search has been made (other than a search report of a foreign counterpart application or PCT International Search Report if submitted herewith). 37 C.F.R. §§1.97(g) and (h).

Respectfully submitted,

Date: December 10, 2015

59,649
Tae-Woong Koo (Reg. No.)
MORGAN, LEWIS & BOCKIUS LLP
2 Palo Alto Square
3000 El Camino Real, Suite 700
Palo Alto, CA 94306
(650) 843-4000

IPR2025-00068
CrowdStrike EX1002 Page 221

Electronically filed December 10, 2015

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application of:	Alen Capalik et al.	Confirmation No.:	5143
Serial No.:	14/823,916	Art Unit:	2431
Filed:	August 11, 2015	Examiner:	To be assigned
For:	System and Method for Identifying Unauthorized Activities on a Computer System using a Data Structure Model	Attorney Docket No.:	067292-5005-US01

PRELIMINARY AMENDMENT

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This preliminary amendment is for the application identified above. Please enter this amendment prior to examination on the merits.

IPR2025-00068
CrowdStrike EX1002 Page 222

IN THE CLAIMS

Please rewrite the pending claims as follows:

1. (Original) A computer implemented method of identifying unauthorized activities on a computer system attached to a computer network, wherein the system comprises:

one or more processors; and

memory storing:

a virtual machine; and

a virtual machine monitor supervising the virtual machine, the method comprising, at the virtual machine monitor:

monitoring activity on the virtual machine;

identifying a plurality of activities being performed at the virtual machine, wherein each of the activities includes an activity source, an activity target, and an association between the activity source and the activity target;

storing in the memory the activity sources, activity targets, and associations; and

transmitting one or more of the activity sources, activity targets, and associations to prevent future attacks.

2. (Original) The method of claim 1, wherein the monitoring further comprises monitoring all activity on the virtual machine, and all activity on the virtual machine is assumed to be unauthorized.

3. (Original) The method of claim 1, further comprising:

creating, from the stored information, a fingerprint indicative of the activity on the virtual machine.

4. (Original) The method of claim 1, wherein the activities comprise two or more of: a file initiating an execution of an instruction, an instruction reading a file, an instruction writing to a file, and receiving data through the network.

5. (Original) The method of claim 1, wherein a respective activity target comprises one of: a file, a user, an instruction, a thread, data stream, and network socket connections.

6. (Original) The method of claim 1, wherein a respective activity source comprises one of: a file, a user, an instruction, a thread, data stream, and network socket connections.

IPR2025-00068
CrowdStrike EX1002 Page 223

7. (Original) The method of claim 1, further comprising:

graphically displaying at least a subset of the stored activities.

8. (Original) The method of claim 7, wherein the displaying includes visually distinguishing at least a subset of the associations.

9. (Original) The method of claim 1, wherein an activity target of a first activity of the plurality of activities is an activity source of a second activity of the plurality of activities.

10. (Original) The method of claim 1, further comprising:

identifying a respective association between a first activity source and a first activity target as unauthorized, wherein the first activity target, when associated as a second activity source with a second activity target, causes unauthorized activities on the second activity target.

11. (Original) The method of claim 10, further comprising:

tracking a transfer of malicious associations over time.

12. (Original) The method of claim 1, further comprising:

identifying activity sources that are affected by unauthorized activities.

13. (Original) The method of claim 12, wherein the identifying activity sources that are affected by unauthorized activities includes identifying activity sources that request to access a portion of memory that is set as non-executable.

14. (Original) The method of claim 12, wherein:

instructions executed by the one or more processors have respective privilege levels;

respective activity sources have respective privilege levels; and

the identifying activity sources that are affected by unauthorized activities includes identifying activity sources that request to execute underprivileged instructions.

15. (Original) The method of claim 12, wherein the identifying activity sources that are affected by unauthorized activities includes identifying data stream incoming from outside the computer system.

16. (Original) The method of claim 1, further comprising:

IPR2025-00068
CrowdStrike EX1002 Page 224

determining an activity status for the stored events, the activity status comprising one of:

a complete status, representing that a source of unauthorized activities is identified, and each activity target in the stored activities is associated with the source through one or more associations; and

an incomplete status, which represents that the source of unauthorized activities is not identified, or at least one activity target in the stored activities is not associated with the source through one or more associations.

17. (Original) The method of claim 1, further comprising:

determining an activity level representing a frequency of unauthorized activities on the virtual machine during a predefined time interval.

18. (Original) The method of claim 1, further comprising:

identifying a respective activity as unauthorized based on a determination that the respective activity is associated with an unauthorized activity that is distinct from the respective activity.

19. (Currently amended) A system, comprising:

one or more processors; and

memory storing:

a virtual machine;

a virtual machine monitor supervising the virtual machine; and

one or more programs, the one or more programs including instructions for:

monitoring activity on the virtual machine;

identifying a plurality of activities being performed at the virtual machine, where each of the activities includes an activity source, an activity target, and an association between the activity source and the activity target;

storing in the memory the activity sources, activity targets, and associations; and

transmitting one or more of the activity source, activity targets, and associations to prevent future attacks. ~~the fingerprint to prevent future attacks that comprise the same or similar activities as indicated by the fingerprint.~~

IPR2025-00068
CrowdStrike EX1002 Page 225

20. (Original) A computer readable storage medium, including one or more programs for execution by one or more processors of a computer system, the one or more programs including instructions for:

monitoring activity on the virtual machine;

identifying a plurality of activities being performed at the virtual machine, where each of the activities includes an activity source, an activity target, and an association between the activity source and the activity target;

storing in the memory the activity sources, activity targets, and associations; and

transmitting one or more of the activity sources, activity targets, and associations to prevent future attacks.

IPR2025-00068
CrowdStrike EX1002 Page 226

REMARKS

Claim 19 has been amended. Support for the claim amendments can be found at least in paragraphs [0010]-[0011], [0071], [0074], and [0103]-[0104] of the specification as originally filed. No new matter has been added.

Although no fee is believed to be due at this time, the Commissioner is hereby authorized to charge required fees or credit any overpayments to Morgan, Lewis & Bockius LLP Deposit Account No. 50-0310 (order no. 067292-5005-US01).

Respectfully submitted,

Date: December 10, 2015

/ Tae-Woong Koo / 59,649

Tae-Woong Koo (Reg. No.)

MORGAN, LEWIS & BOCKIUS LLP
2 Palo Alto Square
3000 El Camino Real, Suite 700
Palo Alto, CA 94306
(650) 843-4000

IPR2025-00068
CrowdStrike EX1002 Page 227

Electronically filed December 10, 2015

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application of:	Alen Capalik et al.	Confirmation No.:	5143
Serial No.:	14/823,916	Art Unit:	2431
Filed:	August 11, 2015	Examiner:	To be assigned
For:	System and Method for Identifying Unauthorized Activities on a Computer System using a Data Structure Model	Attorney Docket No.:	067292-5005-US01

RESPONSE TO THE INFORMATIONAL NOTICE TO APPLICANT

Mail Stop: MISSING PARTS
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

In response to the Informational Notice to Applicant mailed September 22, 2015 for the above-identified application, enclosed are copies of the executed declaration by the co-inventors. $70 surcharge has been already paid on September 11, 2015, in response to the Notice to File Missing Parts of Nonprovisional Application. Although no fee is believed to be due at this time, the Commissioner is hereby authorized to charge required fees or credit any overpayments to Morgan, Lewis & Bockius LLP Deposit Account No. 50-0310 (order no. 067292-5005-US01).

An Application Data Sheet was submitted with the application and no changes need to be made.

Respectfully submitted,

Date: December 10, 2015

/ Tae-Woong Koo / 59,649

Tae-Woong Koo (Reg. No.)
MORGAN, LEWIS & BOCKIUS LLP
2 Palo Alto Square
3000 El Camino Real, Suite 700
Palo Alto, CA 94306
(650) 843-4000

IPR2025-00068
CrowdStrike EX1002 Page 228

067292-5005 US01
DMD/TWK

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
14/823,916	08/11/2015	Alen Capalik	067292-5005-US01

CONFIRMATION NO. 5143

24341
MORGAN, LEWIS & BOCKIUS LLP (PA)
2 PALO ALTO SQUARE
3000 EL CAMINO REAL, SUITE 700
PALO ALTO, CA 94306

INFORMAL NOTICE

OC000000077545612

Date Mailed: 09/22/2015

INFORMATIONAL NOTICE TO APPLICANT

Applicant is notified that the above-identified application contains the deficiencies noted below. No period for reply is set forth in this notice for correction of these deficiencies. However, if a deficiency relates to the inventor's oath or declaration, the applicant must file an oath or declaration in compliance with 37 CFR 1.63, or a substitute statement in compliance with 37 CFR 1.64, executed by or with respect to each actual inventor no later than the expiration of the time period set in the "Notice of Allowability" to avoid abandonment. See 37 CFR 1.53(f).

The item(s) indicated below are also required and should be submitted with any reply to this notice to avoid further processing delays.

- A properly executed inventor's oath or declaration has not been received for the following inventor(s):
  Alen Capalik
  David Andrews
  Ben Becker

Questions about the contents of this notice and the requirements it sets forth should be directed to the Office of Data Management, Application Assistance Unit, at **(571) 272-4000** or **(571) 272-4200** or **1-888-786-0101**.

/dnguyen/

PREVIOUSLY DOCKETED
File Oath/Decl.
Due 26 Oct 2015

RECEIVED DOCKETING
SEP 23 2015
MORGAN LEWIS
PALO ALTO OFFICE

IPR2025-00068
CrowdStrike EX1002 Page 229

DECLARATION (37 CFR 1.63) FOR UTILITY OR DESIGN APPLICATION USING AN APPLICATION DATA SHEET (37 CFR 1.76)

Title of Invention	**SYSTEM AND METHOD FOR IDENTIFYING UNAUTHORIZED ACTIVITES ON A COMPUTER SYSTEM USING A DATA STRUCTURE MODEL**

As the below named inventor, I hereby declare that:

This declaration is directed to:

☐ The attached application, or

☒ United States application or PCT international application number 14/823,916 filed on August 11, 2015

The above-identified application was made or authorized to be made by me.

I believe that I am the original and first inventor or an original joint inventor of a claimed invention in the application.

I hereby state that I have reviewed and understand the contents of the above identified application, including the claims.

I acknowledge the duty to disclose information known to me to be material to patentability as defined by 37 CFR 1.56.

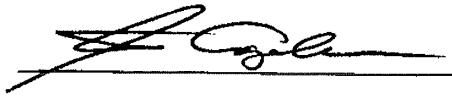
I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

WARNING:

Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.

LEGAL NAME OF INVENTOR

Inventor: **Alen CAPALIK** Date: 12/10/2015

Signature: 

LEGAL NAME OF INVENTOR

Inventor: **David ANDREWS** Date: _____

Signature: _____

LEGAL NAME OF INVENTOR

Inventor: **Ben BECKER** Date: _____

Signature: _____

DECLARATION (37 CFR 1.63) FOR UTILITY OR DESIGN APPLICATION USING AN APPLICATION DATA SHEET (37 CFR 1.76)

Title of Invention	SYSTEM AND METHOD FOR IDENTIFYING UNAUTHORIZED ACTIVITES ON A COMPUTER SYSTEM USING A DATA STRUCTURE MODEL

As the below named inventor, I hereby declare that:

This declaration is directed to:

- ☐ The attached application, or
- ☒ United States application or PCT international application number 14/823,916 filed on August 11, 2015

The above-identified application was made or authorized to be made by me.

I believe that I am the original and first inventor or an original joint inventor of a claimed invention in the application.

I hereby state that I have reviewed and understand the contents of the above identified application, including the claims.

I acknowledge the duty to disclose information known to me to be material to patentability as defined by 37 CFR 1.56.

I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

WARNING:

Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.

LEGAL NAME OF INVENTOR

Inventor: Alen CAPALIK Date: _____

Signature: _____

LEGAL NAME OF INVENTOR

Inventor: David ANDREWS Date: 8/18/2015

Signature: 

LEGAL NAME OF INVENTOR

Inventor: Ben BECKER Date: _____

Signature: _____

DECLARATION (37 CFR 1.63) FOR UTILITY OR DESIGN APPLICATION USING AN APPLICATION DATA SHEET (37 CFR 1.76)

Title of Invention	SYSTEM AND METHOD FOR IDENTIFYING UNAUTHORIZED ACTIVITES ON A COMPUTER SYSTEM USING A DATA STRUCTURE MODEL

As the below named inventor, I hereby declare that:

This declaration is directed to:

- ☐ The attached application, or
- ☒ United States application or PCT international application number 14/823,916 filed on August 11, 2015

The above-identified application was made or authorized to be made by me.

I believe that I am the original and first inventor or an original joint inventor of a claimed invention in the application.

I hereby state that I have reviewed and understand the contents of the above identified application, including the claims.

I acknowledge the duty to disclose information known to me to be material to patentability as defined by 37 CFR 1.56.

I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

WARNING:

Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.

LEGAL NAME OF INVENTOR

Inventor: Alen CAPALIK Date: _____

Signature: _____

LEGAL NAME OF INVENTOR

Inventor: David ANDREWS Date: _____

Signature: _____

LEGAL NAME OF INVENTOR

Inventor: Ben BECKER Date: 8/23/15

Signature: _____

DD2/26194309.1

Electronic Acknowledgement Receipt	
EFS ID:	24330059
Application Number:	14823916
International Application Number:	
Confirmation Number:	5143
Title of Invention:	System and Method for Identifying Unauthorized Activities on a Computer System using a Data Structure Model
First Named Inventor/Applicant Name:	Alen Capalik
Customer Number:	24341
Filer:	Tae-Woong Koo/Karen Zielen
Filer Authorized By:	Tae-Woong Koo
Attorney Docket Number:	067292-5005-US01
Receipt Date:	10-DEC-2015
Filing Date:	11-AUG-2015
Time Stamp:	20:27:02
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		067292-5005-US01_Preliminary_Amendment.pdf	187675 0176bebca8c6765052c4326bd923f206f74e8133	yes	6

	Multipart Description/PDF files in .zip description				
	Document Description		**Start**	**End**	
	Preliminary Amendment		1	1	
	Claims		2	5	
	Applicant Arguments/Remarks Made in an Amendment		6	6	
Warnings:					
Information:					
2		067292-5005-US01_Response_Information_Notice.pdf	307250 c3d8a1a86540dfb5547d48bddbc38175246fb397	yes	8
	Multipart Description/PDF files in .zip description				
	Document Description		**Start**	**End**	
	Applicant Response to Pre-Exam Formalities Notice		1	2	
	Oath or Declaration filed		3	8	
Warnings:					
Information:					
		Total Files Size (in bytes):	494925		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/SB/06 (09-11)
Approved for use through 1/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 14/823,916	Filing Date 08/11/2015	☐ To be Mailed

ENTITY: ☐ LARGE ☒ SMALL ☐ MICRO

APPLICATION AS FILED – PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	RATE ($)	FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	

APPLICATION AS AMENDED – PART II

AMENDMENT

12/10/2015	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	* 20	Minus	** 20	= 0	X $40 =	0
Independent (37 CFR 1.16(h))	* 3	Minus	***3	= 0	X $210 =	0
☐ Application Size Fee (37 CFR 1.16(s))						
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
					TOTAL ADD'L FEE	0

AMENDMENT

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	*	Minus	**	=	X $ =	
Independent (37 CFR 1.16(h))	*	Minus	***	=	X $ =	
☐ Application Size Fee (37 CFR 1.16(s))						
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
					TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.

** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".

*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".

The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

LIE
/PAMELA YOUNG/

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
14/823,916	08/11/2015	2143	800	067292-5005-US01	20	3

CONFIRMATION NO. 5143

UPDATED FILING RECEIPT

24341
MORGAN, LEWIS & BOCKIUS LLP (PA)
2 PALO ALTO SQUARE
3000 EL CAMINO REAL, SUITE 700
PALO ALTO, CA 94306

OC000000077545611

Date Mailed: 09/22/2015

Receipt is acknowledged of this non-provisional patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please submit a written request for a Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections**

Inventor(s)

Alen Capalik, Pacific Palisades, CA;
David Andrews, Los Angeles, CA;
Ben Becker, Santa Monica, CA;

Applicant(s)

COUNTERTACK INC., Santa Monica, CA;

Power of Attorney: None

Domestic Priority data as claimed by applicant

This application is a CON of 13/163,590 06/17/2011 PAT 9106697
which claims benefit of 61/358,367 06/24/2010

Foreign Applications for which priority is claimed (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see http://www.uspto.gov for more information.) - None.
Foreign application information must be provided in an Application Data Sheet in order to constitute a claim to foreign priority. See 37 CFR 1.55 and 1.76.

If Required, Foreign Filing License Granted: 09/18/2015

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 14/823,916**

Projected Publication Date: 12/31/2015

Non-Publication Request: No

Early Publication Request: No
**** SMALL ENTITY ****

IPR2025-00068
CrowdStrike EX1002 Page 239

Title

System and Method for Identifying Unauthorized Activities on a Computer System using a Data Structure Model

Preliminary Class

715

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications: No

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at http://www.uspto.gov/web/offices/pac/doc/general/index.html.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, http://www.stopfakes.gov. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4258).

IPR2025-00068
CrowdStrike EX1002 Page 240

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign AssetsControl, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

SelectUSA

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The U.S. offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to promote and facilitate business investment. SelectUSA provides information assistance to the international investor community; serves as an ombudsman for existing and potential investors; advocates on behalf of U.S. cities, states, and regions competing for global investment; and counsels U.S. economic development organizations on investment attraction best practices. To learn more about why the United States is the best country in the world to develop technology, manufacture products, deliver services, and grow your business, visit http://www.SelectUSA.gov or call +1-202-482-6800.

IPR2025-00068
CrowdStrike EX1002 Page 241

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number: 14/823,916

APPLICATION AS FILED - PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY FEE($)
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	70		N/A	
SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	300		N/A	
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	360		N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	20 minus 20 =	*	x 40 =	0.00	OR		
INDEPENDENT CLAIMS (37 CFR 1.16(h))	3 minus 3 =	*	x 210 =	0.00			
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			0.00			
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				0.00			
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	730		TOTAL	

APPLICATION AS AMENDED - PART II

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY ADDITIONAL FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE($)
AMENDMENT A	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY ADDITIONAL FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE($)
AMENDMENT B	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".
The "Highest Number Previously Paid For" (Total or Independent) is the highest found in the appropriate box in column 1.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
14/823,916	08/11/2015	Alen Capalik	067292-5005-US01

CONFIRMATION NO. 5143

24341
MORGAN, LEWIS & BOCKIUS LLP (PA)
2 PALO ALTO SQUARE
3000 EL CAMINO REAL, SUITE 700
PALO ALTO, CA 94306

INFORMAL NOTICE

OC000000077545612

Date Mailed: 09/22/2015

INFORMATIONAL NOTICE TO APPLICANT

Applicant is notified that the above-identified application contains the deficiencies noted below. No period for reply is set forth in this notice for correction of these deficiencies. However, if a deficiency relates to the inventor's oath or declaration, the applicant must file an oath or declaration in compliance with 37 CFR 1.63, or a substitute statement in compliance with 37 CFR 1.64, executed by or with respect to each actual inventor no later than the expiration of the time period set in the "Notice of Allowability" to avoid abandonment. See 37 CFR 1.53(f).

The item(s) indicated below are also required and should be submitted with any reply to this notice to avoid further processing delays.

- A properly executed inventor's oath or declaration has not been received for the following inventor(s):
  Alen Capalik
  David Andrews
  Ben Becker

Questions about the contents of this notice and the requirements it sets forth should be directed to the Office of Data Management, Application Assistance Unit, at **(571) 272-4000** or **(571) 272-4200** or **1-888-786-0101**.

/dnguyen/

Electronically filed September 11, 2015

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application of:	Alen Capalik	Confirmation No.:	5143
Serial No.:	14/823,916	Art Unit:	2143
Filed:	August 11, 2015	Examiner:	To be assigned
For:	System and Method for Identifying Unauthorized Activities on a Computer System using a Data Structure Model	Attorney Docket No:	067292-5005-US01

RESPONSE TO THE NOTICE TO FILE MISSING PARTS OF NONPROVISIONAL APPLICATION

Mail Stop: MISSING PARTS
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

In response to the Notice to File Missing Parts mailed August 26, 2015, enclosed is the Notice to File Missing Parts of Nonprovisional Application. The fee for the late oath or declaration surcharge is estimated to be $70. The Commissioner is hereby authorized to charge the required fees or credit any overpayments to Morgan, Lewis & Bockius LLP Deposit Account No. 50-0310 (order no. 067292-5005-US01).

An Application Data Sheet was submitted with the application and no changes need to be made.

Applicants note that an oath/declaration is also due. The oath/declaration will be submitted at a later date.

Also enclosed please find a Fee Transmittal Form setting forth the calculation for the statutory basic filing, search and examination fees, together with the excess claim fees due in this matter. The fees calculated for the statutory basic filing, search and examination fees together with the excess claim fees and application size fee (if applicable) are estimated to be $730. The

IPR2025-00068
CrowdStrike EX1002 Page 244

Commissioner is hereby authorized to charge the required fees or credit any overpayments to Morgan, Lewis & Bockius LLP Deposit Account No. 50-0310 (order no. 067292-5005-US01).

Respectfully submitted,

Date: September 11, 2015

59,649

Tae-Woong Koo (Reg. No.)
MORGAN, LEWIS & BOCKIUS LLP
2 Palo Alto Square
3000 El Camino Real, Suite 700
Palo Alto, CA 94306
(650) 843-4000

IPR2025-00068
CrowdStrike EX1002 Page 245

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
14/823,916	08/11/2015	Alen Capalik	067292-5005-US01

CONFIRMATION NO. 5143

24341
MORGAN, LEWIS & BOCKIUS LLP (PA)
2 PALO ALTO SQUARE
3000 EL CAMINO REAL, SUITE 700
PALO ALTO, CA 94306

FORMALITIES LETTER

OC000000077078036

Date Mailed: 08/26/2015

NOTICE TO FILE MISSING PARTS OF NONPROVISIONAL APPLICATION

FILED UNDER 37 CFR 1.53(b)

Filing Date Granted

Items Required To Avoid Abandonment:

An application number and filing date have been accorded to this application. The item(s) indicated below, however, are missing. Applicant is given **TWO MONTHS** from the date of this Notice within which to file all required items below to avoid abandonment. Extensions of time may be obtained by filing a petition accompanied by the extension fee under the provisions of 37 CFR 1.136(a).

- The statutory basic filing fee is missing.
- The application search fee must be submitted.
- The application examination fee must be submitted.
- Surcharge as set forth in 37 CFR 1.16(f) must be submitted.
  The surcharge is due for any one of:
  - late submission of the basic filing fee, search fee, or examination fee,
  - late submission of inventor's oath or declaration,
  - filing an application that does not contain at least one claim on filing, or
  - submission of an application filed by reference to a previously filed application.

SUMMARY OF FEES DUE:

The fee(s) required within **TWO MONTHS** from the date of this Notice to avoid abandonment is/are itemized below. Small entity discount is in effect. If applicant is qualified for micro entity status, an acceptable Certification of Micro Entity Status must be submitted to establish micro entity status. (See 37 CFR 1.29 and forms PTO/SB/15A and 15B.)

- $ **70** basic filing fee.
- $ **70** surcharge.
- $ **300** search fee.
- $ **360** examination fee.
- $(**0**) previous unapplied payment amount.
- $ **800** TOTAL FEE BALANCE DUE.

Items Required To Avoid Processing Delays:

Applicant is notified that the above-identified application contains the deficiencies noted below. No period for reply is set forth in this notice for correction of these deficiencies. However, if a deficiency relates to the inventor's

IPR2025-00068
CrowdStrike EX1002 Page 246

UTILITY PATENT APPLICATION FEE TRANSMITTAL *(Only for new nonprovisional applications under 37 CFR § 1.53(b))*	Attorney Docket No.	067292-5005-US01
	First Inventor	Alen Capalik
	Title	System and Method for Identifying Unauthorized Activities on a Computer System using a Data Structure Model
	Electronically filed	September 11, 2015

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

BASIC FILING, SEARCH AND EXAMINATION FEES

Application Type	Filing Fees	Search Fees	Examination Fees	Fees Paid ($)
Utility	$ 70	$ 300	$ 360	$ 730

EXCESS CLAIM FEES

Type	No. Filed	Less	Extra	Extra Rate ($)	Fee ($)
Total Claims	20	- 20		$ 80 each	0
Independent	3	- 3		$ 420 each	0
			Surcharge for late oath filing		70

APPLICATION SIZE FEE (Specification and Drawings)

Total Sheets	Extra Sheets	No. of each add'l 50 or fraction thereof	Fee ($)
50 x .75- 100	/ 50	(round up to whole no.) x $400	0

Sub Total	800
Applicant qualifies for the 50% Reduction for Independent Inventor, Nonprofit Organization or Small Business Concern	
TOTAL FILING FEE	**800**

Please charge the total filing fee and any other additional fees to Morgan, Lewis & Bockius LLP Deposit Account 50-0310 (order no. 067292-5005-US01).

Respectfully submitted,

Date: September 11, 2015

59,649
Tae-Woong Koo (Reg. No.)

MORGAN, LEWIS & BOCKIUS LLP
2 Palo Alto Square
3000 El Camino Real, Suite 700
Palo Alto, California 94306
(650) 843-4000

IPR2025-00068
CrowdStrike EX1002 Page 247

Electronic Patent Application Fee Transmittal

Application Number:	14823916
Filing Date:	11-Aug-2015
Title of Invention:	System and Method for Identifying Unauthorized Activities on a Computer System using a Data Structure Model
First Named Inventor/Applicant Name:	Alen Capalik
Filer:	Tae-Woong Koo
Attorney Docket Number:	067292-5005-US01

Filed as Small Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Utility filing Fee (Electronic filing)	4011	1	70	70
Utility Search Fee	2111	1	300	300
Utility Examination Fee	2311	1	360	360
Pages:				
Claims:				
Miscellaneous-Filing:				
Late Filing Fee for Oath or Declaration	2051	1	70	70
Petition:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
		Total in USD ($)		**800**

Electronic Acknowledgement Receipt	
EFS ID:	23473011
Application Number:	14823916
International Application Number:	
Confirmation Number:	5143
Title of Invention:	System and Method for Identifying Unauthorized Activities on a Computer System using a Data Structure Model
First Named Inventor/Applicant Name:	Alen Capalik
Customer Number:	24341
Filer:	Tae-Woong Koo
Filer Authorized By:	
Attorney Docket Number:	067292-5005-US01
Receipt Date:	11-SEP-2015
Filing Date:	11-AUG-2015
Time Stamp:	18:24:50
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$800
RAM confirmation Number	5525
Deposit Account	500310
Authorized User	KOO, TAE-WOONG
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Applicant Response to Pre-Exam Formalities Notice	67292_5005US01_RES.pdf	163789 1340c008be607e730247a1b4e6314db10b98b382	no	4
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	37057 1795341bab7156f57cb4366f44583dce10a67d23	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	200846		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number: 14/823,916

APPLICATION AS FILED - PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY FEE($)
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	70		N/A	
SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	300		N/A	
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	360		N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	20 minus 20 =	*	x 40 =	0.00	OR		
INDEPENDENT CLAIMS (37 CFR 1.16(h))	3 minus 3 =	*	x 210 =	0.00			
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			0.00			
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				0.00			
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	730		TOTAL	

APPLICATION AS AMENDED - PART II

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY ADDITIONAL FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE($)
AMENDMENT A	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY ADDITIONAL FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE($)
AMENDMENT B	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".
The "Highest Number Previously Paid For" (Total or Independent) is the highest found in the appropriate box in column 1.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
14/823,916	08/11/2015	Alen Capalik	067292-5005-US01

CONFIRMATION NO. 5143

24341
MORGAN, LEWIS & BOCKIUS LLP (PA)
2 PALO ALTO SQUARE
3000 EL CAMINO REAL, SUITE 700
PALO ALTO, CA 94306

FORMALITIES LETTER

OC000000077078036

Date Mailed: 08/26/2015

NOTICE TO FILE MISSING PARTS OF NONPROVISIONAL APPLICATION

FILED UNDER 37 CFR 1.53(b)

Filing Date Granted

Items Required To Avoid Abandonment:

An application number and filing date have been accorded to this application. The item(s) indicated below, however, are missing. Applicant is given **TWO MONTHS** from the date of this Notice within which to file all required items below to avoid abandonment. Extensions of time may be obtained by filing a petition accompanied by the extension fee under the provisions of 37 CFR 1.136(a).

- The statutory basic filing fee is missing.
- The application search fee must be submitted.
- The application examination fee must be submitted.
- Surcharge as set forth in 37 CFR 1.16(f) must be submitted.
  The surcharge is due for any one of:
  - late submission of the basic filing fee, search fee, or examination fee,
  - late submission of inventor's oath or declaration,
  - filing an application that does not contain at least one claim on filing, or
  - submission of an application filed by reference to a previously filed application.

SUMMARY OF FEES DUE:

The fee(s) required within **TWO MONTHS** from the date of this Notice to avoid abandonment is/are itemized below. Small entity discount is in effect. If applicant is qualified for micro entity status, an acceptable Certification of Micro Entity Status must be submitted to establish micro entity status. (See 37 CFR 1.29 and forms PTO/SB/15A and 15B.)

- $ **70** basic filing fee.
- $ **70** surcharge.
- $ **300** search fee.
- $ **360** examination fee.
- $(**0**) previous unapplied payment amount.
- $ **800** TOTAL FEE BALANCE DUE.

Items Required To Avoid Processing Delays:

Applicant is notified that the above-identified application contains the deficiencies noted below. No period for reply is set forth in this notice for correction of these deficiencies. However, if a deficiency relates to the inventor's

oath or declaration, the applicant must file an oath or declaration in compliance with 37 CFR 1.63, or a substitute statement in compliance with 37 CFR 1.64, executed by or with respect to each actual inventor no later than the expiration of the time period set in the "Notice of Allowability" to avoid abandonment. See 37 CFR 1.53(f).

- A properly executed inventor's oath or declaration has not been received for the following inventor(s):
  Alen Capalik
  David Andrews
  Ben Becker

Replies must be received in the USPTO within the set time period or must include a proper Certificate of Mailing or Transmission under 37 CFR 1.8 with a mailing or transmission date within the set time period. For more information and a suggested format, see Form PTO/SB/92 and MPEP 512.

Replies should be mailed to:

Mail Stop Missing Parts
Commissioner for Patents
P.O. Box 1450
Alexandria VA 22313-1450

Registered users of EFS-Web may alternatively submit their reply to this notice via EFS-Web, including a copy of this Notice and selecting the document description "Applicant response to Pre-Exam Formalities Notice". https://sportal.uspto.gov/authenticate/AuthenticateUserLocalEPF.html

For more information about EFS-Web please call the USPTO Electronic Business Center at 1-866-217-9197 or visit our website at http://www.uspto.gov/ebc.

If you are not using EFS-Web to submit your reply, you must include a copy of this notice.

Questions about the contents of this notice and the requirements it sets forth should be directed to the Office of Data Management, Application Assistance Unit, at **(571) 272-4000** or **(571) 272-4200** or **1-888-786-0101**.

/nhassani/

IPR2025-00068
CrowdStrike EX1002 Page 254

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
14/823,916	08/11/2015	2143	0.00	067292-5005-US01	20	3

CONFIRMATION NO. 5143

24341
MORGAN, LEWIS & BOCKIUS LLP (PA)
2 PALO ALTO SQUARE
3000 EL CAMINO REAL, SUITE 700
PALO ALTO, CA 94306

FILING RECEIPT



Date Mailed: 08/26/2015

Receipt is acknowledged of this non-provisional patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please submit a written request for a Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections**

Inventor(s)

Alen Capalik, Pacific Palisades, CA;
David Andrews, Los Angeles, CA;
Ben Becker, Santa Monica, CA;

Applicant(s)

COUNTERTACK INC., Santa Monica, CA;

Power of Attorney: None

Domestic Priority data as claimed by applicant

This application is a CON of 13/163,590 06/17/2011 PAT 9106697
which claims benefit of 61/358,367 06/24/2010

Foreign Applications for which priority is claimed (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see http://www.uspto.gov for more information.) - None.
Foreign application information must be provided in an Application Data Sheet in order to constitute a claim to foreign priority. See 37 CFR 1.55 and 1.76.

Projected Publication Date: To Be Determined - pending completion of Missing Parts

Non-Publication Request: No

Early Publication Request: No
** **SMALL ENTITY** **

IPR2025-00068
CrowdStrike EX1002 Page 255

Title

System and Method for Identifying Unauthorized Activities on a Computer System using a Data Structure Model

Preliminary Class

715

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications: No

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at http://www.uspto.gov/web/offices/pac/doc/general/index.html.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, http://www.stopfakes.gov. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4258).

IPR2025-00068
CrowdStrike EX1002 Page 256

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign AssetsControl, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

SelectUSA

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The U.S. offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to promote and facilitate business investment. SelectUSA provides information assistance to the international investor community; serves as an ombudsman for existing and potential investors; advocates on behalf of U.S. cities, states, and regions competing for global investment; and counsels U.S. economic development organizations on investment attraction best practices. To learn more about why the United States is the best country in the world to develop technology, manufacture products, deliver services, and grow your business, visit http://www.SelectUSA.gov or call +1-202-482-6800.

UTILITY PATENT APPLICATION TRANSMITTAL *(Only for new nonprovisional applications under 37 CFR § 1.53(b))*	Attorney Docket No.	067292-5005-US01
	First Inventor	Alen Capalik
	Title	System and Method for Identifying Unauthorized Activities on a Computer System using a Data Structure Model
	Electronically filed	August 11, 2015

APPLICATION ELEMENTS
See MPEP Chapter 600 concerning utility patent application contents.

Address to: **Commissioner for Patents**
P.O. Box 1450
Alexandria, VA 22313-1450

1. ☐ Fee Transmittal Form *(with duplicate for fee processing)*
2. ☒ Applicant claims Small Entity status, see 37 C.F.R. § 1.27
3. ☒ Specification [Total Pages 33]
4. ☒ Drawing(s) *(35 USC § 113)* [Total Sheets 17]
5. ☐ Oath or Declaration [Total Pages]
   a. ☐ Newly executed *(original or copy)*
   b. ☐ Copy from a prior application *(37 CFR § 1.63(d))*
6. ☒ Application Data Sheet, see 37 C.F.R. § 1.76
7. ☐ CD-ROM or CD-R in duplicate, large table or Computer Program *(Appendix)*
   ☐ Landscape Table on CD
8. ☐ Nucleotide and/or Amino Acid Sequence Submission *(if applicable, all necessary)*
   a. ☐ Computer Readable Form (CRF)
   b. ☐ Specification Sequence Listing on
      i. ☐ CD-ROM or CD-R (2 copies); or
      ii. ☐ Paper
   c. ☐ Statement verifying identity of above copies

ACCOMPANYING APPLICATION PARTS

9. ☐ Assignment Papers *(cover sheet & document(s))*
   Name of Assignee:
10. ☐ 37 CFR § 3.73(c) Statement
    a. ☐ Power of Attorney
11. ☐ English Translation Document *(if applicable)*
12. ☐ Information Disclosure Statement and PTO-1449
    a. ☐ Copies of citations attached
13. ☐ Preliminary Amendment
14. ☐ Return Receipt Postcard *(MPEP 503)*
15. ☐ Certified Copy of Priority Document(s) *(if foreign priority is claimed)*
16. ☐ Non-Publication Request under 35 U.S.C. § 122 (b)(2)(B)(i)
17. ☐ Other:

Note: (1) Benefit claims under 37 CFR 1.78 and foreign priority claims under 1.55 MUST be included in an Application Data Sheet (ADS).
(2) For applications filed under 35 U.S.C. 111, the application must contain an ADS specifying the applicant if the applicant is an assignee, person to whom the inventor is under an obligation to assign, or person who otherwise shows sufficient proprietary interest in the matter. See 37 CFR 1.46(b).

19. CORRESPONDENCE ADDRESS: Customer Number 24341

Signature		Date	August 11, 2015
Name (Print/Type)	Tae-Woong Koo	Registration No. (Attorney/Agent)	59,649

DB2/ 26194854.1

System and Method for Identifying Unauthorized Activities on a Computer System using a Data Structure Model

RELATED APPLICATIONS

[0001] This application is a continuation application of U.S. Patent Application Serial No. 13/163,590, filed June 17, 2011, entitled "System and Method for Identifying Unauthorized Activities on a Computer System Using a Data Structure Model," which claims priority to U.S. Provisional Patent Application Serial No. 61/358, 367, filed on June 24, 2010, entitled "System and Method for Identifying Unauthorized Activities on a Computer System Using a Data Structure Model," both of which are incorporated by reference herein in their entireties.

[0002] This relates to U.S. Patent Application No. 13/163,578, entitled "System and Method for Sampling Forensic Data of Unauthorized Activities Using Executability States" filed June 17, 2011, which claims priority to U.S. Provisional Patent Application Serial No. 61/358,363 filed on June 24, 2010, entitled "System and Method for Sampling Forensic Data of Unauthorized Activities Using Executability States," and U.S. Provisional Patent Application Serial No. 61/358, 367, filed on June 24, 2010, entitled "System and Method for Identifying Unauthorized Activities on a Computer System Using a Data Structure Model," all of which are incorporated by reference herein in their entireties.

[0003] This application relates to U.S. Patent Application No. 11/788,795, entitled "System and Method for Analyzing Unauthorized Intrusion into a Computer Network," filed on April 20, 2007, which is a continuation-in-part of U.S. Patent Application No. 11/488,743, entitled "Decoy Network Technology With Automatic Signature Generation for Intrusion Detection and Intrusion Prevention Systems," filed on July 17, 2006, which claims priority to U.S. Provisional Patent Application Serial No. 60/802,543, filed May 22, 2006, all of which are incorporated herein by reference in their entireties.

TECHNICAL FIELD

[0004] This invention relates generally to systems and methods for protecting computer networks, including but not limited to systems and methods for analyzing

IPR2025-00068
CrowdStrike EX1002 Page 259

malicious activities on a computer system in order to better protect the computer system from future malicious activity.

BACKGROUND

[0005] An increasing number of computers are connected to computer networks (e.g., the Internet). Networked computers provide a significant benefit of accessing and sharing data over the networks. However, these networked computers are also vulnerable to attacks, unwanted intrusions, and unauthorized access.

[0006] Certain existing network security systems have been developed to protect computers from attacks, unwanted intrusions, unauthorized access, and other malicious activities. Such network security systems typically include a firewall to prevent unauthorized access to the network or its computers. Exemplary network security systems also include intrusion detection systems (IDS) and intrusion prevention systems (IPS) that typically contain a library of malware fingerprints (e.g., fingerprints of malware payloads and other unauthorized activities). By using the malware fingerprints, the IDS or the IPS can detect attempts to access computer systems without authorization. When a connection is attempted to a network port, the IDS or IPS examines the low-level IP data packets and compares them to its library of fingerprints for a match. When a match is identified, the IDS or IPS provides notification of the match and/or prevents further access. Therefore, the malware fingerprints play a critical role in network security.

[0007] A critical threat to computer networks is the so-called zero-day attack that exploits security vulnerabilities previously unknown to software developers or system operators. Because the security vulnerabilities are unknown to the software developers or system operators, often the fingerprints of such zero-day attacks are unavailable for comparison. Until the fingerprints are identified, attacks exploiting the same security vulnerabilities continue without detection by the network security systems. However, identifying the fingerprints of malicious activities in the middle of numerous other non-malicious processes is not a trivial task.

[0008] Because network security systems depend on the malware fingerprints, there is a great need for efficient methods of identifying fingerprint data for previously unknown types of malicious and/or unauthorized activities.

IPR2025-00068
CrowdStrike EX1002 Page 260

SUMMARY

[0009] A number of embodiments that address the limitations and disadvantages described above are presented in more detail below. These embodiments provide computer-implemented methods and systems for generating fingerprint data for zero-day unauthorized activities.

[0010] As described in more detail below, some embodiments involve a computer-implemented method performed at a computer system having one or more processors and memory storing one or more programs for execution by the one or more processors. The method includes monitoring activity on the virtual machine. A plurality of activities performed at a virtual machine is identified. Each of the activities includes an activity source, an activity target, and an association between the activity source and the activity target. The activity sources, activity targets, and associations are stored in the memory. A fingerprint indicative of the activity on the virtual machine is created from the stored activities. The fingerprint is transmitted to one or more other computer systems on the network to prevent future attacks that comprise the same or similar activities as indicated by the fingerprint. In some embodiments, the fingerprint is transmitted to identify the attack on other affected systems.

[0011] In accordance with some embodiments, the system includes one or more processors, and memory. The memory stores a virtual machine, a virtual machine monitor supervising the virtual machine, and one or more programs. The virtual machine, the virtual machine monitor, and the one or more programs are configured for execution by the one or more processors. The one or more programs include instructions for monitoring activity on the virtual machine, and instructions for identifying a plurality of activities being performed at the virtual machine. Each of the activities includes an activity source, an activity target, and an association between the activity source and the activity target. The one or more programs furthermore include instructions for storing the activity sources, activity targets, and associations in the memory. The one or more programs also include instructions for creating a fingerprint indicative of the activity on the virtual machine from the stored activities. Finally, the one or more programs include instructions for transmitting the fingerprint to one or more other computer systems on the network to prevent future attacks that comprise the same or similar activities as indicated by the fingerprint. In some embodiments, the one or

IPR2025-00068
CrowdStrike EX1002 Page 261

more programs include instructions for displaying at least a subset of the activities (e.g., action sources, action targets, and actions).

[0012] In accordance with some embodiments, a computer readable storage medium stores one or more programs configured for execution by one or more processors of a computer. The one or more programs include instructions for performing the method described above.

[0013] These embodiments identify unauthorized activities by monitoring and identifying associations between activity sources and activity targets without using pre-determined fingerprints. The data collected by these embodiments can be used to generate fingerprint data in response to the zero-day attacks.

BRIEF DESCRIPTION OF THE DRAWINGS

[0014] For a better understanding of the aforementioned aspects of the invention as well as additional aspects and embodiments thereof, reference should be made to the Description of Embodiments below, in conjunction with the following drawings in which like reference numerals refer to corresponding parts throughout the figures.

[0015] Figure 1 is a high-level block diagram illustrating an exemplary distributed computer system in accordance with some embodiments.

[0016] Figure 2 is a block diagram illustrating a decoy network device, in accordance with some embodiments.

[0017] Figures 3A-3D are exemplary network diagrams illustrating unauthorized activities on a network socket, in accordance with some embodiments.

[0018] Figures 4A-4D are exemplary network diagrams illustrating unauthorized activities on files in a computer system, in accordance with some embodiments.

[0019] Figure 4E is an exemplary network diagram illustrating unauthorized activities on a computer system, in accordance with some embodiments.

[0020] Figure 5A illustrates an exemplary data structure of unauthorized activity data, in accordance with some embodiments.

[0021] Figure 5B illustrates an exemplary data structure of fingerprint, in accordance with some embodiments.

IPR2025-00068
CrowdStrike EX1002 Page 262

[0022] Figure 5C illustrates another exemplary data structure of fingerprint, in accordance with some embodiments.

[0023] Figures 6A-6C are flowcharts representing a method of identifying unauthorized activities on a computer system, in accordance with some embodiments.

DESCRIPTION OF EMBODIMENTS

[0024] Embodiments of various systems and methods for identifying unauthorized activities are described below. Reference will be made to certain embodiments of the invention, examples of which are illustrated in the accompanying drawings. While the invention will be described in conjunction with the embodiments, it should be understood that these particular embodiments are not intended to limit the invention. Instead, the invention is intended to cover alternatives, modifications and equivalents that are within the spirit and scope of the invention as defined by the appended claims. Moreover, in the following description, numerous specific details are set forth to provide a thorough understanding of the present invention. However, it will be apparent to one of ordinary skill in the art that the invention may be practiced without these particular details. In other instances, methods, procedures, components, and networks that are well-known to those of ordinary skill in the art are not described in detail to avoid obscuring aspects of the present invention.

[0025] Figure 1 illustrates an exemplary distributed computer system 100, according to some embodiments. The system 100 includes a decoy computer network 102, a communications network 148, and protected computer network 104. Various embodiments of the decoy computer network 102 and protected computer network 104 implement the unauthorized activity identifying methods described in this document.

[0026] In some embodiments, the systems on the decoy computer network 102 and the protected computer network 104 can be accessed by client computers 101. The client computers 101 can be any of a number of computing devices (e.g., Internet kiosk, personal digital assistant, cell phone, gaming device, desktop computer, laptop computer, handheld computer, or combinations thereof) used to enable the activities described below. The client computer(s) 101 is also referred to herein as client(s). The clients 101 are connected to the decoy network device 106 and the protected network device 136 (e.g., 136-1, 136-2, and 136-n) via the communications network 148.

IPR2025-00068
CrowdStrike EX1002 Page 263

[0027] The protected network devices 136-1 through 136-n are accessible from the network 148 by one or more authorized users using the clients 101 (e.g., the protected network devices can be servers providing services for webpages, emails, file downloading and sharing, web applications, etc.). Typically, the protected computer network 104 includes a firewall/router 198 to protect the protected network devices 136 and route network traffic to and from the protected network devices 136. Alternatively, the firewall/router 198 can protect both the decoy computer network 102 and the protected computer network 104, as illustrated in Figure 1.

[0028] In some embodiments, the protected computer network 104 also includes an IDS/IPS system 142 (intrusion detection and prevention system). The IDS/IPS system 142 includes, or has access to, a fingerprint library. The fingerprint library includes fingerprints of unauthorized activities. The IDS/IPS system 142 identifies unauthorized activities based on the fingerprints stored in the fingerprint library, and provides notification to a user or a system administrator, and/or prevents unauthorized activities matching the stored fingerprints by modifying the protected network devices 136 and/or the firewall/router 198. Suitable IDS/IPS systems 142 include Cisco Systems' IPS 4200 Series, Juniper's IDP 200, and Enterasys' Dragon IDS Network Sensor.

[0029] As explained above, in some embodiments, the IDS/IPS system 142 is coupled to the firewall/router 198 such that the IDS/IPS system can reconfigure the firewall/router 198 to protect the protected network devices 136 in the protected computer network 104 from future attacks. In some embodiments, the IDS/IPS and the firewall are located in a single combined device.

[0030] The decoy computer network 102 includes one or more decoy network device(s) 106. The decoy network device 106 is a decoy system that is monitored to collect fingerprint data of unauthorized activities. In some embodiments, the decoy network device 106 is intentionally kept vulnerable to unauthorized or malicious activities (e.g., known security weaknesses may be intentionally left unfixed or other security components (e.g., firewalls) are intentionally not installed). In other embodiments, the decoy network device 106 includes security devices and software applications like other protected network devices (e.g., the decoy network device 106 may be protected by the firewall/router 198 and any other security measures included in the protected network devices 136). The purpose of the decoy network device 106 is to

IPR2025-00068
CrowdStrike EX1002 Page 264

allow attackers to attack the decoy network device 106, so that the pattern of the attack can be monitored and analyzed to generate a fingerprint. This fingerprint of the attack can be used to prevent similar attacks on the decoy network device 106 and/or other computers (e.g., protected network devices 136).

[0031] Attackers can initiate attacker activities over the communications network(s) 148 on both the decoy computer network 102 and the protected computer network 104. Ideally, the firewall/router 198 or security software on the protected network devices 136 will protect the protected network devices 136 from at least some of the attacker activity(s), whereas the decoy network device 106 is typically exposed to the attacker activity(s) in order to attract the attacks.

[0032] Although Figure 1 illustrates the decoy computer network 102 and the protected computer network 104 as separate networks, in some embodiments, they are part of a same network. For example, in some embodiments, the protected computer network 104 includes the decoy computer network 102. In other embodiments, the decoy computer network 102 and the protected computer network 104 are the same network. Although the methods described herein are described with respect to monitoring the decoy network device 106, persons having ordinary skill in the art would recognize that similar methods may be used for monitoring one or more non-decoy systems, such as the protected network device 136.

[0033] Figure 2 is a block diagram illustrating the decoy network device 106 in accordance with some embodiments. The decoy network device 106 typically includes one or more processing units (CPUs) 202, one or more network or other communications interfaces 204, memory 206, and one or more communication buses 208 for interconnecting these components. In some embodiments, the communication buses 208 include circuitry (sometimes called a chipset) that interconnects and controls communications between system components. In some other embodiments, the decoy network device 106 includes a user interface (not shown) (e.g., a user interface having a display device, a keyboard, and a mouse or other pointing device), but when implemented as a server, the decoy network device 106 is more typically controlled from and accessed by various client systems (e.g., the client 101 in Figure 1; and more typically, a client connected through a secure private network).

IPR2025-00068
CrowdStrike EX1002 Page 265

[0034] The memory 206 of the decoy network device 106 includes high-speed random access memory, such as DRAM, SRAM, DDR RAM or other random access solid state memory devices; and may include non-volatile memory, such as one or more magnetic disk storage devices, optical disk storage devices, flash memory devices, or other non-volatile solid state storage devices. The memory 206 may optionally include one or more storage devices remotely located from the CPU(s) 202. The memory 206, or alternately the non-volatile memory device(s) within the memory 206, comprises a computer readable storage medium. The memory 206 or the computer readable storage medium of the memory 206 stores one or more of the following programs:

- the network communication module (or instructions) 212 that is used for connecting the decoy network device 106 to computer networks (e.g., communication network(s) 148, decoy computer network 102, and protected computer network 104), and/or other computers (e.g., the client 101) via the one or more communications interfaces 204 and one or more communications networks 148, such as the Internet, a wireless network (e.g., Wi-Fi, WiMAX, 3G, 4G, etc.), any local area network (LAN), wide area network (WAN), metropolitan area network, or a combination of such networks;
- the host operating system 110 (also called Hypervisor OS) that includes procedures for handling various basic system services and for performing hardware dependent tasks;
- database server 128, which stores data (e.g., unauthorized activity data 502 and/or fingerprint 580);
- fingerprint generation engine 130, which generates the fingerprint data 580 from the unauthorized activity data 502); and
- visualization interface 132, which prepares data (e.g., the fingerprint or unauthorized activities on the computer system) for display (e.g., on a GUI of a client 101).

[0035] The fingerprint 580, as described below with reference to Figures 5B and 5C, include data indicative of unauthorized activities on the decoy network device 106. Such fingerprint 580 can be used (e.g., by the IDS/IPS system 142) to detect and prevent unauthorized activities on protected network devices 136.

IPR2025-00068
CrowdStrike EX1002 Page 266

[0036] In some embodiments, the host operating system (e.g., the host OS 110) includes one or more of the following:

- a virtual machine monitor 214 (also called a hypervisor);
- virtual machines 216, including virtual machine 1 (113-1) and (optional) virtual machine 2 (113-2); and
- normal hypervisor OS user processes (e.g., 114-1 and 114-2), such as administrative utilities, network tools (e.g., netcat and ifconfig), shell processes (e.g., ssh and bash), package management utilities (e.g., dpg and apt), drivers, filesystem utilities, and programming environments (e.g., python and lua).

[0037] The virtual machine monitor 214 includes a hypervisor kernel 116 that resides in physical memory and provides the basic services to the virtual machine monitor 214. In some embodiments, the hypervisor kernel 116 is a part of the hypervisor operating system 110 (e.g., a kernel of the hypervisor operating system 110). In such embodiments, the hypervisor kernel 116 is a part of the operating system that activates the hardware directly or interfaces with another software layer that, in turn, drives the hardware.

[0038] The hypervisor kernel 116 includes a hypervisor virtual machine kernel module 118 that supports virtualization of a "guest" decoy operating system 112. The hypervisor kernel 116 also includes an introspection module 120 interposed between the virtual machine monitor 214 and decoy operating system(s) 112. The introspection module 120 performs introspection (e.g., monitoring) into the physical memory segments assigned to each of the virtualized decoy operating system 112.

[0039] Because no software is installed in the virtualized decoy operating system 112, it is more difficult for the virtualized decoy operating system 112 (or an attacker who has gained access to the virtualized decoy operating system 112) to detect that its memory is being monitored.

[0040] The introspection module is configured to examine the memory assigned to virtualized decoy operating systems 112 in order to acquire low-level data about the interaction between the decoy operating systems 112 and attack activity. The introspection module examines the memory of virtualized decoy operating systems 112 by means of three functional components: a code region selector 222, a trace instrumentor 224, and a trace analyzer 226. Regular expressions (also known as 'regex') are used

IPR2025-00068
CrowdStrike EX1002 Page 267

throughout the process to identify, describe, and profile the contents of the memory segments of the virtualized decoy operating systems 112. The code selector 222 identifies regions of code in memory that are of interest for further introspection. Regions of interest may include, but are not limited to, system calls, the arguments of system calls, the returns of system calls, device and memory input-output, driver information, library calls, branching information, instruction pointer jumps, and raw network information. The instrumentor 224 copies the memory traces of interest identified by the code selector and then profiles them. The trace analyzer 226 takes the profiled traces and uses them to build a simulation of the states in the virtualized decoy operating system 112 over time. In this manner, the introspection module examines the contents of the memory segments of the virtualized decoy operating systems 112 in an instrumented context that generates and retrieves forensic data (or fingerprint). In some embodiments, the trace analyzer 226 is located outside the introspection module 120 (e.g., in the fingerprint generation engine 130).

[0041] In some embodiments, the trace instrumentor 224 is configured to perform operations in accordance with one or more user-defined conditions. The one or more user-defined conditions may specify when one or more memory traces should be generated. Respective user-defined conditions may be rule-based or pattern-based, and may be based on system states or independent of system states. In some embodiments, the trace analyzer 226 is configured to perform operations in accordance with one or more user-defined conditions. The one or more user-defined conditions may specify what portions of the profiled traces to analyze. This allows the user to easily find traces of interest, without having to go through the entire set of traces.

[0042] In some embodiments, the introspection module 120 is configured to pause the execution of the virtualized decoy operating system 112, copy the content of memory at prescribed locations, and return execution control to the virtualized decoy operating system 112. In some embodiments, the introspection module 120 pauses the execution of the virtualized decoy operating system 112 for preventing malicious or undesired execution from occurring in the virtualized decoy operating system 112.

[0043] An attacker may be able to detect that the decoy operating system 112 is a virtualized operating system, based on the time it takes to perform standardized tasks. However, since the introspection module 120 runs completely outside the virtualized decoy operating system 112, it is difficult for an attacker accessing the decoy operating

IPR2025-00068
CrowdStrike EX1002 Page 268

system 112 to determine whether the decoy operating system 112 is being monitored. In other words, the attacker may suspect that the virtual machine monitor 214 exists, but the attacker may not determine whether the virtual machine monitor 214 includes the introspection module 120. As explained above, the introspection module 120 monitors and introspects into the memory segments of the virtualized decoy operating systems 112. The introspection module 120 introspects and gathers information on any virtualized operating system supported by the hypervisor operating system 110.

[0044] The virtual machines 216 are one or more software applications emulating one or more physical machines (e.g., computer systems). In some embodiments, at least one virtual machine (e.g., the virtual machine 1 (113-1)) includes a decoy operating system 112-1, which in turn optionally includes one or more programs (e.g., 220-1 and 220-2). The virtualized decoy operating systems 112 access the physical memory assigned to them by the virtual machine monitor 214 (or the hypervisor kernel 116).

[0045] These virtualized operating systems 112 act as decoy operating systems to attract attacker activity. For example, the decoy operating system 112 can be one of WINDOWS, SUN MICROSYSTEMS, SOLARIS, or any version of LINUX known to persons skilled in the art, as well as any combination of the aforementioned. The decoy network device 106 may include any number of virtualized decoy operating systems 112 or any number of virtual machines 113.

[0046] Each of the above identified modules, components, and applications in Figure 2 corresponds to a set of instructions for performing one or more functions described herein. These modules (i.e., sets of instructions) need not be implemented as separate software programs, procedures or modules, and thus various subsets of these modules may be combined or otherwise re-arranged in various embodiments. In some embodiments, the memory 206 may store a subset of the modules and data structures identified above. Furthermore, the memory 206 may store additional modules and data structures not described above.

[0047] Notwithstanding the discrete blocks in Figures 1 and 2, these figures are intended to be a functional description of some embodiments rather than a structural description of functional elements in the embodiments. One of ordinary skill in the art will recognize that an actual implementation might have the functional elements grouped or split among various components. In practice, and as recognized by those of ordinary

IPR2025-00068
CrowdStrike EX1002 Page 269

skill in the art, items shown separately could be combined and some items could be separated. For example, in some embodiments, the fingerprint generation engine 130 and the virtualized decoy OS 112 are part of or stored within the decoy network device 106. In other embodiments, the fingerprint generation engine 130 and the virtualized decoy OS 112 are implemented using separate computer systems. In some embodiments, the fingerprint generation engine 130 includes the database server 128. In some embodiments, the database server 128 is a remote database server located outside the decoy network device 106.

[0048] The actual number of servers used to implement the decoy network device 106 and how features are allocated among them will vary from one implementation to another, and may depend in part on the amount of data traffic that the system must handle during peak usage periods as well as during average usage periods, and may also depend on the amount of data processed by the decoy network device 106. Moreover, one or more of the blocks in Figures 1 and 2 may be implemented on one or more servers designed to provide the described functionality. For example, the decoy network device 106 may be implemented on two distinct computing devices: a monitor device and an analyzer device. The monitor device includes the virtual machine monitor 214, the virtual machines 216, and processes and modules therein. The analyzer device includes the database server 128, the fingerprint generation engine 130, and optionally the visualization interface 132. In such configuration, the monitor device collects unauthorized activity data, and the analyzer device analyzes the unauthorized activity data to generate fingerprints.

[0049] When in use, attackers typically search for vulnerable computers connected to the shared communication network(s), and attempt to perform unauthorized activities on such vulnerable computers through the shared communication network(s).

[0050] Attacker activity may be directed at the decoy computer network 102 through one or more ports of each of the virtualized decoy operating system 112 that are left open as a gateway for the attacker activity. For example, the decoy network 102 can be configured to respond to connection attempts made at network addresses that do not exist on the protected network 104 (e.g., through a connection from the firewall/router 198 to the decoy network device 106 as illustrated in Figure 1). Connections to these non-existent network addresses are assumed to be unauthorized and routed to one of the decoy operating systems 112, since no production hardware (e.g., protected network

IPR2025-00068
CrowdStrike EX1002 Page 270

device 136) exists on the protected network 104 at these addresses. In particular, the decoy operating systems 112 are not configured to provide any user service, and therefore, no ordinary (i.e., authorized and/or non-malicious) user would attempt to access to the virtual machine.

[0051] The decoy operating systems 112 (in the form of a virtualized operating system) may be configured to respond to any such non-existent network address. In a typical attack, the attacker activity scans for an open port, ostensibly in an attempt to make a network connection and then access one or more computing devices on the protected computer network 104. When the attacker activity scans for open ports at non-existent network addresses, however, the attacker is presented with a virtualized decoy operating system 112 instead.

[0052] When the attacker connects to a virtualized decoy operating system 112 through an open port, the attacker sees a fully-functional standard operating system fingerprint. Since the decoy network device 106 can be configured to present any operating system as a fully-functional virtualized decoy operating system 112, responses to connection requests from attacker activity are guaranteed to be authentic for the operating system running on that decoy. For example, an FTP port access request for WINDOWS may return a specific character sequence that differs from an FTP response for LINUX. Similarly, an FTP access request to a WINDOWS port may return a response "> ftp: connect: Connection refused." This character sequence may be slightly different from that generated by LINUX. Further, different versions of WINDOWS may respond with slightly different, version-specific character sequences. Since attackers often use these sequences to identify what type of operating system is at a particular network address and the version (or range of possible versions) for that operating system, the fact that virtualized decoy operating systems 112 generate authentic responses makes them realistic decoys and encourages intruders to attempt unauthorized access to them. The instigator of the attack is thus lured into accessing the decoy 112, which is overseen by the hypervisor operating system 110 running on the hardware-based, decoy network device 106. Attacker activity may then initiate previously unknown attacks for the observed operating system. When the attacker activity proceeds to interact with the decoy operating system 112, the attacker provides the decoy operating system 112 with the data used to obtain control of the decoy operating system 112. These data are recorded and analyzed by the introspection module without the knowledge of the attacker.

IPR2025-00068
CrowdStrike EX1002 Page 271

[0053] All scans by the attacker activity receive real-world operating system and service information, leading the instigator of the attack activity to believe that there is a potentially vulnerable system responding. The attacker is thus lured into communicating with the decoy network device 106 and its virtualized decoy operating systems 112 and services. Since the decoy network device 106 includes real hardware, the attacker is essentially attacking an actual physical system and, therefore, cannot tell that the system is actually an instrumented honeypot that monitors the attacker activity from the introspection module. When an attacker connects to a network port and begins interacting with a virtualized decoy operating system 112, the introspection module monitors and captures information from the connection, including port numbers, data streams, file uploads, keystrokes, ASCII or binary files, malicious payloads, memory manipulation attempts, and any other data transfers or malicious attempts.

[0054] In some embodiments, the introspection module monitors all activity (e.g., system calls, library calls, kernel calls, etc.) on virtualized decoy operating systems 112. In other embodiments, the introspection module, instead of monitoring all activity on virtualized decoy operating systems 112, monitors activity on virtualized decoy operating system 112 based on a monitoring priority (e.g., key system calls and kernel calls). The monitoring priority may be set based on the type of unauthorized activities. For example, in some embodiments, incoming network packets are given high priorities, and therefore, the incoming network packets are thoroughly monitored and analyzed. In some other embodiments, system calls are given high priorities. In yet other embodiments, a virtualized decoy operating system (e.g., 112-1) on a virtual machine 1 (e.g., 113-1) is given a high priority than other virtualized decoy operating system, when the virtual machine 1 is experiencing a high frequency of unauthorized activities. Also a combination of the factors stated above can be used to determine the monitoring priority. In some embodiments, the monitoring priority is user-configurable.

[0055] In use, the introspection module captures (through the introspection) raw attack information. The raw attack information is then communicated to and stored on the database server 128 as forensic data 236 for later analysis. The fingerprint generation engine 130 or the trace analyzer 226 then uses this raw forensic information 236 to generate a signature of the attack. In some embodiments, the fingerprint generation engine 130 or the trace analyzer 226 uses the raw attack information to generate a signature of the attack without storing the raw attack information (i.e.,

IPR2025-00068
CrowdStrike EX1002 Page 272

unauthorized activity data) in a database server (e.g., database server 128) first. In some embodiments, the fingerprint generation engine 130 or the trace analyzer 226 uses the raw attack information to generate a signature of the attack without storing the raw attack information in persistent data storage (e.g., database server 128) at all. It should be appreciated that although the signature of the attack may be used to generate an attack signature suitable for use in security applications (e.g., IPS, AV, etc.), the signature of the attack is distinct from the attack signature. The signature (also called a fingerprint) may be used for providing detailed forensic analysis of the character and nature of the attack and its impact on the target operating system, which can be used as the basis for generating triggers. Such triggers may be used to deny malicious system or library calls on the decoy operating system 112.

[0056] In some embodiments, the entire process from attack detection through fingerprint generation occurs automatically, *i.e.,* without any human intervention, at a timescale ranging from nearly immediate to several minutes. The IDS/IPS system 142 uses the attack signature to identify and prevent subsequent attacks.

[0057] In one or more embodiments, the signature may be sent from the fingerprint generation engine 130 to the intrusion detection and/or prevention (IDS/IPS) signature library 134 through a second network connection 140, which is used by the fingerprint generation engine 130 to directly interact with the IDS/IPS system 142.

[0058] After collecting unauthorized activity data, the introspection module 120 may easily clean the virtualized decoy operating system 112 at any time by removing the running system image of the compromised virtualized decoy operating system and replacing it with a pre-attack system image. Thus the introspection module 120 can cleanse or reset the virtualized decoy operating system 112 of any malicious software or payload, removing the possibility that attacker(s) can use that virtualized decoy operating system 112 for further attacks on other networks. In this manner, the attack can be thwarted, and the operating system does not become a tool of the attacker(s). This procedure may also be automated, i.e., may occur without further human intervention.

[0059] Figures 3A-3D and 4A-4E illustrate exemplary network diagrams representing unauthorized activity on a computer system (e.g., the virtual machine 113-1), in accordance with various embodiments. Although Figures 3A-3D and 4A-4E illustrate

IPR2025-00068
CrowdStrike EX1002 Page 273

unauthorized activities on the virtual machine 113-1, analogous methods can be used to represent and analyze unauthorized activities on non-virtualized computer systems.

[0060] Figure 3A-3D illustrate exemplary network diagrams 300 representing unauthorized activities on a network socket (e.g., the virtual machine 113-1), in accordance with some embodiments. In Figure 3A, a data packet stream 304 at a socket 306 of the virtual machine 113-1 is detected by the virtual machine 113-1 and monitored by the virtual machine monitor 214. When the virtual machine 113-1 is a decoy system, the virtual machine 113-1 typically does not actively send and receive packet streams over the network (because the purpose of the decoy system is to wait for a potential attack from an attacker), and any incoming packet stream 304 of data is treated as an unauthorized activity (e.g., an attempt by a hacker to probe a security system of the virtual machine 113-1). In some embodiments, any request to access a computer that does not exist on the protected computer network is treated as an unauthorized activity, and such request is routed to one of the decoy systems (e.g., a virtual machine 113-1 on the decoy network device 106), which is monitored for additional unauthorized activities. In some embodiments, an attacker 302 who sends the packet stream 304 to the socket 306 is identified (e.g., by the Internet Protocol (IP) address).

[0061] Once the packet stream 304 and the socket 306 are identified as affected by unauthorized activities, related unauthorized activities are identified. Figure 3B shows that the packet stream 304 received by the socket 306 is directed to a process A 308, and the process A 308 is treated as affected by unauthorized activities. In turn, in Figure 3C, the process A 308 accesses a file X 310 and a file Y 312, and both the file X 310 and the file Y 312 are treated as affected by unauthorized activities. Thereafter, the file X 310 initiates a process B 314, and the process B is treated as affected by unauthorized activities.

[0062] By analyzing these activities, the fingerprint of the unauthorized activities can be identified (e.g., the unauthorized activities start with the packet stream 304; the unauthorized activities send the packet stream 304 into the computer system 398 through the socket 306; the packet stream 304 is directed to the process A 308; etc.). By using this information, the security of the protected network devices 136 can be improved (e.g., the socket 306 can be closed; the process A 308 can be modified to not respond to data similar to the packet stream 304; etc.).

IPR2025-00068
CrowdStrike EX1002 Page 274

[0063] Figures 4A-4D illustrate exemplary network diagrams 400 representing unauthorized activities on files in a computer system (e.g., the virtual machine 113-1), in accordance with some embodiments. In Figure 4A, unauthorized activities on the file X 310 and the file Y 312 in the virtual machine 113-1 are detected. For example, the unauthorized activity may be detected by using checksum values of the file X 310 and the file Y 312 (e.g., a different checksum value can indicate that a corresponding file has been modified by an unauthorized process). Alternatively, the unauthorized activity may be detected by monitoring data execution prevention (DEP) exceptions associated with the file X 310 and the file Y 312, generated by the one or more processors (e.g., 202 in Figure 2); or by a manual selection from a system administrator (e.g., based on a file corruption or an erratic behavior).

[0064] Figure 4B shows that the process A 308 accesses both the file X 310 and the file Y 312, and the process A 308 is treated as affected by unauthorized activities. Also in Figure 4B, the file X 310 initiates the process B 314, and the process B is treated as affected by unauthorized activities.

[0065] In Figure 4C, data from the socket 306 is directed to the process A 308, and the socket 306 is treated as affected by unauthorized activities. Figure 4D shows that the socket 306 receives the packet stream 304, and the packet stream 304 is treated as affected by unauthorized activities. In some embodiments, the attacker 302 who sends the packet stream 304 to the socket 306 is identified (e.g., by the IP address).

[0066] Figure 4E illustrates an exemplary network diagram 420 representing unauthorized activities on a computer system (e.g., the virtual machine 113-1), in accordance with some embodiments. In Figure 4E, multiple packets of data streams (e.g., 304-1 and 304-2) are detected, and all activity on the computer system 498 are monitored and recorded. When the type of associations is identified (e.g., malignant, benign, etc., as described in more detail below with reference to a type 516 in Figure 5A), at least a subset of the associations can be visually distinguished (e.g., a respective bold arrow representing a malignant association; a regular arrow representing a benign association; alternatively, any other graphical scheme can be used to visually distinguish the subset of the associations, such as color, font, shape, icons, etc.). It is also noted that certain objects drawn with dashed lines (e.g., files, processes, etc.) may have been identified as affected by unauthorized activities, but their associations with other objects may not have been identified.

IPR2025-00068
CrowdStrike EX1002 Page 275

[0067] Figure 5A is a block diagram illustrating exemplary data structures of unauthorized activity data 502 and unauthorized activity entries 505 in the unauthorized activity data 502, in accordance with some embodiments. Unauthorized activity data 502 includes unauthorized activity entries 505. In some embodiments, the unauthorized activity entries are grouped into one or more sets (e.g., 504) based on time (e.g., time when the entries are recorded or time window of recorded activity), association types (e.g., malicious associations v. benign associations), source types, target types, and other characteristics of the unauthorized activities.

[0068] The unauthorized activity data 502 shown in Figure 5A is grouped based on time (e.g., when the entries are recorded). Each set optionally includes one or more of the following set variables 503:

- status 506, which indicates whether the unauthorized activity data 502 is complete or incomplete; the set (e.g., 504-1) is determined to be complete if associations for all objects (e.g., activity sources and activity targets) affected by unauthorized activities are identified; the set (e.g., 504-1) is determined to be incomplete if an association for any object affected by unauthorized activities is not identified;
- frequency 508, which indicates a number of unauthorized activities on the computer system (e.g., virtual machine 113) during a predefined time interval (e.g., one second, five seconds, one minute, five minutes, one hour, five hours, one day, two days, etc.); in some embodiments, the frequency 508 is a relative frequency measured by a number of computer processes affected by unauthorized activities and a total number of computer processes running on the computer system; for example, if the computer system (e.g., virtual machine 113) runs fifty total processes including ten processes affected by unauthorized activities, the frequency 508 is 20% (= 10 / 50); and
- a global time stamp 510, which represents the time when the data in the set (e.g., 504-1) was collected.

[0069] Each set 504 in the unauthorized activity data 502 in Figure 5A also includes one or more unauthorized activity entries 505 (e.g., 505-1, 505-2, 505-3, 505-4, and 505-5). Each unauthorized activity entry 505 includes one or more of the following:

- an activity source 512, which calls, accesses, or executes the activity target 514; the activity source 512 may be one of the following: access to a particular file,

IPR2025-00068
CrowdStrike EX1002 Page 276

access from a particular user, an Internet Protocol address, an instruction, a message, data stream, a hardware component, and a network port; for example, when an instruction A accesses a file X, the instruction A is the activity source, and the file X is the activity target 514;

- an activity target 514, which is called, accessed, or executed by the activity source 512. The activity target 514 may be one of the following: a file, an Internet Protocol address, an instruction, a message, data stream, a hardware component, and a network port; and
- an action 515, which represents an event or operation occurring between the activity source 512 and the activity target 514. The action 515 is typically one of: calling, executing, modifying, or accessing operation, such as system calls and library calls.
- An (optional) association type 516, which when identified, represents the type of association between the activity source 512 and the activity target 514; the association type may be one of the following:
    - malignant, which represents that the activity source 512 has modified the activity target 514 to perform unauthorized activities;
    - benign, which represents that the activity source 512 has interacted with the activity target 514 but has not modified the activity target 514 to perform unauthorized activities (e.g., the instruction A reads the file X, but does not modify the file X); and
    - remission, which represents that the activity source 512 is determined to be no longer active in propagating unauthorized activity; for example, the activity source 514 may be modified to remove malicious data and/or to stop unauthorized activities (e.g., by the IDS/IPS system 142);
- (optional) probability 518, which when identified, represents a probability that the corresponding association is malignant; and
- (optional) time stamp 520, which when identified, represents the time when the activity source 512 associates with the activity target 514 (e.g., when the activity source 512 calls, accesses, or executes the activity target 514).

IPR2025-00068
CrowdStrike EX1002 Page 277

[0070] Figures 5B illustrates an exemplary data structure of fingerprint 580, in accordance with some embodiments. In Figure 5B, the fingerprint 580-1 includes one or more of the following: an (optional) status 506, an activity source 512, an activity target 514, an (optional) association type 516, and an (optional) time stamp 520, all of which are described above.

[0071] The fingerprint 580-1 can be used to prevent future attacks on the computer system or other computer systems, by modifying the activity targets 514 (e.g., increasing privileges, changing the file/instruction name, changing the file/instruction structure, moving the file/instruction to a different location, blocking a particular port, encrypting the file, etc.) to protect the activity targets 514 or blocking the same or similar (e.g., at least partially matching) pattern or sequence of activities (e.g., if the fingerprint of the unauthorized activities starts with sending packets A, B, and C in order, blocking the receipt of the packet C after receiving the packets A and B).

[0072] In some embodiments, the fingerprint 580 consists of respective pairs of activity sources and activity targets, when the association type for a respective pair is malignant. This reduces the size of the fingerprint 580.

[0073] Figures 5C illustrates another exemplary data structure of fingerprint 580, in accordance with some embodiments. In Figure 5C, the fingerprint 580-2 includes the following, or a subset or superset thereof:

- (one or more) activity sources 512, as described above;
- a reference value 522, which is used to identify a particular activity source 512; for example, the reference value 522 can be a file size, a checksum value, one or more portions of the file, instruction, or data packet;
- an (optional) method 524, which is used to indicate how the reference value 522 is used to identify a corresponding activity source 512, or how the activity source is processed to obtain a measured value which can be compared with the reference value 522 to identify the activity source 512. For example, the method can be "checksum," which requires determining a checksum value of the activity source 512, or "match," which requires matching the reference value with the activity source 512. The method 524 is typically omitted when a default method is used to identify the source 512.

IPR2025-00068
CrowdStrike EX1002 Page 278

[0074] The fingerprint 580-2 can be used to prevent future attacks on the computer system or other computer systems, by blocking activity sources that match a pattern of unauthorized activities (e.g., the reference value 522). For example, if the fingerprint of the activity source includes a data stream with a repeated character of a predefined length (e.g., a 2KB long string of a repeated character), the IDS/IPS can block such data stream by using the reference value 522.

[0075] In some embodiments, the fingerprint 580-2 includes activity targets 514 in lieu of, or in addition to, the activity sources 512.

[0076] In some embodiments, the fingerprint 580 includes one or more of: system calls, arguments of system calls, returns of system calls, device and memory input-output, driver information, library calls, branching information, instruction pointer jumps, and raw network information collected from a respective virtual machine 113 or a respective decoy operating system 112 (not shown).

[0077] Figures 6A-6C are flowcharts representing a method 600 of identifying unauthorized activities on a computer system (e.g., the virtual machine 113-1) attached to a computer network, in accordance with some embodiments. The computer-implemented method 600 is performed at a decoy network device (e.g., 106 in Figure 1B) having one or more processors and memory storing a virtual machine and a virtual machine monitor supervising the virtual machine. The memory also stores one or more programs for execution by the one or more processors to perform the method. Typically, the one or more programs executed by the one or more processors to perform the method are executed at the virtual machine monitor.

[0078] The decoy network device monitors (602) activity on the virtual machine. In some embodiments, the decoy network device monitors a predefined set of activity on the virtual machine. In some embodiments, the decoy network device monitors all activity related to incoming data stream on the virtual machine, based on an assumption that all incoming data stream on the virtual machine is unauthorized (e.g., Figures 3A-3D). In some embodiments, the decoy network device monitors activity based on the monitoring priority.

[0079] In some embodiments, the monitoring further includes monitoring all activity on the virtual machine, and all activity on the virtual machine is assumed (603) to be unauthorized, because the virtual machine is not configured to provide user services

IPR2025-00068
CrowdStrike EX1002 Page 279

(e.g., email, web, or file services, etc.) and no authorized user would need to access the virtual machine. In some embodiments, all incoming data packet on the virtual machine is assumed to be unauthorized.

[0080] The decoy network device identifies (604) a plurality of activities being performed at the virtual machine. Each of the activities includes an activity source, an activity target, and an association between the activity source and the activity target. For example, the activity between the file X 310 and the process B 314 in Figure 3D includes the file X 310 as an activity source, the process B 314 as an activity target, and the association represented by the arrow from the file X 310 to the process B 314.

[0081] In some embodiments, a respective activity target comprises (606) one of: a file, a user, an instruction (such as computer processes or system calls), a thread (e.g., a thread of processes), data stream (e.g., network packets), and network socket connections (or sockets). In some embodiments, the respective activity target is an Internet Protocol address.

[0082] In some embodiments, a respective activity source comprises (608) one of: a file, a user, an instruction (such as computer processes or system calls), a thread (e.g., a thread of processes), data stream (e.g., network packets), and network socket connections (or sockets). In some embodiments, the respective activity source is an Internet Protocol address.

[0083] In some embodiments, the decoy network device identifies (610) a respective association between a first activity source and a first activity target as unauthorized. The first activity target, when associated as a second activity source with a second activity target, causes unauthorized activities on the second activity target. For example, we turn to illustrations in Figures 3B-3C. Data from the socket 306 modifies the process A 308 so that the process A 308 performs unauthorized activities (Figure 3B). Therefore, the socket 306 is an activity source in relation to the process A 308, which is an activity target in relation to the socket 306. Then, as shown in Figure 3C, the process A 308 modifies the file X 310, performing unauthorized activities (e.g., corrupting data or writing a malicious code). The process A 308, as an activity source to the file X 310, causes unauthorized activities on the file X 310. By identifying that the process A 308 performed unauthorized activities, the process A 308 is determined to be affected by the

IPR2025-00068
CrowdStrike EX1002 Page 280

unauthorized activities, and the association between the socket 306 and the process A 308 is determined to be malicious (i.e., unauthorized).

[0084] In some embodiments, the decoy network device tracks (612) a transfer of malicious associations over time. For example, as shown in Figure 5A, the decoy network device stores propagation of unauthorized activities (or malicious associations) as a function of time. This allows time-based analysis of the unauthorized activities, and preventing unauthorized activities based on time or sequence-based filters.

[0085] In some embodiments, the decoy network device identifies (614) activity sources that are affected by unauthorized activities. In some embodiments, the identifying activity sources that are affected by unauthorized activities includes (616) identifying activity sources that request to access a portion of memory that is set as non-executable. This can be achieved by data execution prevention (DEP) mechanisms. For example, microprocessors manufactured by Intel Corporation (Santa Clara, CA) allow setting one or more portions of the memory as non-executable (e.g., using a non-executable bit in respective page table entries), and generate an exception when there is an attempt to execute an instruction that is set as non-executable. Similarly, operating systems sold by Microsoft Corporation (Redmond, WA) has an analogous function implemented in the operating system (e.g., Windows XP, Windows 7, etc.).

[0086] In some embodiments, instructions executed by the one or more processors have (618) respective privilege levels. Respective activity sources have respective privilege levels, and the identifying activity sources that are affected by unauthorized activities includes identifying activity sources that request to execute unprivileged instructions. For example, low level processes (or fundamental OS processes) typically require a fundamental privilege level (e.g., privilege levels 0, 1, and 2 in a microprocessor architecture provided by Intel Corporation), and most applications run at a different privilege level (e.g., privilege level 3 in Intel Architecture). An application running at the privilege level 3 is unprivileged to run a privilege level 0 process. When the privilege level 3 application attempts to run a privilege level 0 process, such activity is identified as an unauthorized activity.

[0087] In some embodiments, the identifying activity sources that are affected by unauthorized activities includes (620) receiving a selection of one or more activity sources from a system administrator. For example, a system administrator may suspect

IPR2025-00068
CrowdStrike EX1002 Page 281

that a certain file or process is affected by unauthorized activities, and select the file or process as affected. The decoy network device monitors activity sources and activity targets associated with the selected file or process, thereby identifying additional unauthorized activities.

[0088] In some embodiments, the identifying activity sources that are affected by unauthorized activities includes (622) identifying a data stream incoming from outside the computer system. As discussed above, all incoming data stream on a decoy system is assumed to be affected by unauthorized activities.

[0089] The decoy network device stores (624) the activity sources, activity targets, and associations in the memory. For example, the decoy network device 106 stores unauthorized activity data 502 (e.g., as illustrated in Figure 5A) in memory 206 (as shown in Figure 2) or in the database server 128 (as shown in Figure 2).

[0090] In some embodiments, the decoy network device graphically displays (626) at least a subset of the stored activities. For example, the graphical representation can be an activity diagram as shown in Figures 3A-3D and 4A-4E.

[0091] In some embodiments, the displaying includes (628) visually distinguishing at least a subset of the associations (e.g., in Figure 4E, certain associations are visually distinguished with bold lines. Alternatively, certain associations are visually distinguished with any other visual indications, such as color, shape, icons, etc.). In some embodiments, the visually distinguishing includes visually distinguishing at least a subset of the associations based on the associated probability.

[0092] In some embodiments, the subset of activities includes (630) a first activity and a second activity, and the activity target of the first activity is the activity source of the second activity. For example, Figure 3C illustrates the first activity between the socket 306 and the process A 308 and the second activity between the process A 308 and the file X 310. The process A 308 is the activity target of the first activity and the activity source of the second activity. In other words, the first activity and the second activity are connected through the process A 308. In Figure 3C, both the first activity and the second activity are graphically illustrated.

[0093] In some embodiments, the decoy network device determines (632) an activity status for the stored events. The activity status includes one of: a complete status and an incomplete status. The complete status represents that a source of

IPR2025-00068
CrowdStrike EX1002 Page 282

unauthorized activities is identified, and each activity target in the stored activities is associated with the source through one or more associations (e.g., in Figure 4D, each activity is associated with the source, packet stream 304 through one or more associations). The incomplete status represents that the source of unauthorized activities is not identified, or at least one activity target in the stored activities is not associated with the source through one or more associations (e.g., in Figure 4A, the source is not identified, and activities are not associated with the source).

[0094] In some embodiments, the decoy network device determines (634) an activity level representing a frequency of unauthorized activities on the virtual machine during a predefined time interval (e.g., frequency 508 in Figure 5A).

[0095] In some embodiments, the decoy network device determines a probability of a respective association (or a probability/confidence of an unauthorized association). The probability represents likelihood that the association is malignant (or benign). For example, if the process A 308 reads the file Y 312 (in Figure 4B), the file Y 312 is not modified, and the association is not malignant. The probability for the association between the process A 308 and the file Y 312 is 0%. However, if the process A 308 writes to (or modifies) the file X 310 (in Figure 4B), the association can be malignant. If we know that the process A 308 is affected by the unauthorized activities, the probability for the association between the process A 308 and the file X 310 is 100%. If we do not know that the process A 308 is affected by the unauthorized activities, the probability for the association between the process A 308 and the file X 310 is a predefined number (e.g., 50%). If the file X 310, in turn, calls the process B 314, the association between the file X 310 and the process B 314 can be assigned a probability based on a predefined rule (e.g., 25% = 50% of the probability associated with the file X 310, which is 50%).

[0096] In some embodiments, the probability is used to adjust monitoring priority for the introspection module. For example, if the association between the process A 308 and the file Y 312 has 0% probability, the association between the process A 308 and the file X 310 has 50% probability, and the association between the file X 310 and the process B 314 has 25% probability, the monitoring priority would be placed in the order of the process A 308 (which can be 100% affected by unauthorized activities), the file X 310 with a 50% probability association, the process B 314 with a 25% probability association, and the file Y 312 with a 0% probability association.

IPR2025-00068
CrowdStrike EX1002 Page 283

[0097] The decoy network device creates (636) a fingerprint indicative of the activity on the virtual machine from the stored activities. For example, the fingerprint can be fingerprint 580-1 in Figure 5B, fingerprint 580-2 in Figure 5C, or any other fingerprint described herein. The fingerprint 580-1 can be created directly from the stored activities (e.g., unauthorized activity data 502). The fingerprint 580-2 can be created by analyzing unauthorized activity data 502 (in particular the activity sources 512) or collecting additional data associated with the activity sources 512 (e.g., calculating a checksum value of an activity source 512, etc.).

[0098] In some embodiments, the fingerprint includes (638) files that are affected by unauthorized activities on the virtual machine. For example, the activity source 512 in the fingerprint 580-1 can be a file or file information (e.g., file name, location, size, checksum value, etc.).

[0099] In some embodiments, the fingerprint includes (640) processes that are affected by the unauthorized activities on the virtual machine. For example, the activity source 512 in the fingerprint 580-1 can be a process or process information (e.g., process name, size, privilege level, related processes, etc.).

[00100] In some embodiments, the fingerprint includes one or more of: system calls' arguments and returns, device and memory input-output, driver calls' arguments and returns, library calls' arguments and returns, branching information, instruction pointer jumps, and raw network information collected from a respective virtual machine 113 or a respective decoy operating system 112.

[00101] In some embodiments, the fingerprint includes one or more of: port numbers, data streams, file uploads, file downloads, keystrokes, ASCII or binary files, malicious payloads, operating system configuration changes (e.g., new or updated registry keys in windows) and memory manipulation attempts.

[00102] In some embodiments, the activities comprise (642) two or more of: a file initiating an execution of an instruction, an instruction reading a file, an instruction writing to a file, and receiving data through the network.

[00103] The decoy network device transmits (644) the fingerprint to one or more protected network devices 136 to prevent future attacks that comprise the same or similar activities as indicated by the fingerprint. In some embodiments, the decoy network

IPR2025-00068
CrowdStrike EX1002 Page 284

device transmits the fingerprint to the IDS/IPS system 142 to prevent future attacks that comprise the same or similar activities on one or more protected network devices 136.

[00104] In some embodiments, one or more other computer systems (e.g., protected network devices 136) on the network are modified (646) to prevent future attacks that comprise the same or similar activities as indicated by the fingerprint (e.g., in Figure 1A, the IDS/IPS system modifies at least one of the protected network device(s) 136 to prevent future attacks that comprise the same or similar activities).

[00105] The foregoing description, for purpose of explanation, has been described with reference to specific embodiments. However, the illustrative discussions above are not intended to be exhaustive or to limit the invention to the precise forms disclosed. Many modifications and variations are possible in view of the above teachings. The embodiments were chosen and described in order to best explain the principles of the invention and its practical applications, to thereby enable others skilled in the art to best utilize the invention and various embodiments with various modifications as are suited to the particular use contemplated.

[00106] For example, although the activity source 512 and the activity target 514 are described with respect to processes, threads, files, addresses, instructions, messages, hardware components, etc., persons skilled in the art would recognize that similar methods can be used with respect to other types of activity sources and activity targets. In some embodiments, the analysis engine is configured to maintain several layers of network diagrams, where each layer uses the layer beneath it as input and providing more generalized representations of the unauthorized activity as output. For example, a low-level layer might consist of a process reading from a file and subsequently writing many new files. In some cases, the analysis engine might identify this low level pattern as a representation of a file archive being unpacked, and generate a higher-level layer that includes an unpacking process. This exemplary generalization allows the system to identify common elements of attacks, identify classes of attack that have not been seen before (e.g., zero-day attacks), and generate higher-quality signatures. A layer including the level of detail appropriate to the context may be selected for analysis.

[00107] Moreover, the methods described herein need not be restricted to analysis of a single virtualized operating system but, rather, are able to follow a chain of unauthorized activity across multiple virtualized operating systems. This is important in

IPR2025-00068
CrowdStrike EX1002 Page 285

identifying and thwarting advanced threats that involve multiple attackers spread across multiple systems and that evolve over long periods of time.

[00108] Furthermore, although the methods are described with respect to security application, it should be appreciated that similar methods can be used generally for monitoring behavior of a computer system that follows a source event. For example, similar methods can be used for tracking a user behavior on a system, and/or profiling application behavior for performance improvement or debugging purposes.

IPR2025-00068
CrowdStrike EX1002 Page 286

What is claimed is:

1. A computer implemented method of identifying unauthorized activities on a computer system attached to a computer network, wherein the system comprises:

one or more processors; and

memory storing:

a virtual machine; and

a virtual machine monitor supervising the virtual machine, the method comprising, at the virtual machine monitor:

monitoring activity on the virtual machine;

identifying a plurality of activities being performed at the virtual machine, wherein each of the activities includes an activity source, an activity target, and an association between the activity source and the activity target;

storing in the memory the activity sources, activity targets, and associations; and

transmitting one or more of the activity sources, activity targets, and associations to prevent future attacks.

2. The method of claim 1, wherein the monitoring further comprises monitoring all activity on the virtual machine, and all activity on the virtual machine is assumed to be unauthorized.

3. The method of claim 1, further comprising:

creating, from the stored information, a fingerprint indicative of the activity on the virtual machine.

4. The method of claim 1, wherein the activities comprise two or more of: a file initiating an execution of an instruction, an instruction reading a file, an instruction writing to a file, and receiving data through the network.

5. The method of claim 1, wherein a respective activity target comprises one of: a file, a user, an instruction, a thread, data stream, and network socket connections.

6. The method of claim 1, wherein a respective activity source comprises one of: a file, a user, an instruction, a thread, data stream, and network socket connections.

7. The method of claim 1, further comprising:

IPR2025-00068
CrowdStrike EX1002 Page 287

graphically displaying at least a subset of the stored activities.

8. The method of claim 7, wherein the displaying includes visually distinguishing at least a subset of the associations.

9. The method of claim 1, wherein an activity target of a first activity of the plurality of activities is an activity source of a second activity of the plurality of activities.

10. The method of claim 1, further comprising:

identifying a respective association between a first activity source and a first activity target as unauthorized, wherein the first activity target, when associated as a second activity source with a second activity target, causes unauthorized activities on the second activity target.

11. The method of claim 10, further comprising:

tracking a transfer of malicious associations over time.

12. The method of claim 1, further comprising:

identifying activity sources that are affected by unauthorized activities.

13. The method of claim 12, wherein the identifying activity sources that are affected by unauthorized activities includes identifying activity sources that request to access a portion of memory that is set as non-executable.

14. The method of claim 12, wherein:

instructions executed by the one or more processors have respective privilege levels;

respective activity sources have respective privilege levels; and

the identifying activity sources that are affected by unauthorized activities includes identifying activity sources that request to execute underprivileged instructions.

15. The method of claim 12, wherein the identifying activity sources that are affected by unauthorized activities includes identifying data stream incoming from outside the computer system.

16. The method of claim 1, further comprising:

IPR2025-00068
CrowdStrike EX1002 Page 288

determining an activity status for the stored events, the activity status comprising one of:

a complete status, representing that a source of unauthorized activities is identified, and each activity target in the stored activities is associated with the source through one or more associations; and

an incomplete status, which represents that the source of unauthorized activities is not identified, or at least one activity target in the stored activities is not associated with the source through one or more associations.

17. The method of claim 1, further comprising:

determining an activity level representing a frequency of unauthorized activities on the virtual machine during a predefined time interval.

18. The method of claim 1, further comprising:

identifying a respective activity as unauthorized based on a determination that the respective activity is associated with an unauthorized activity that is distinct from the respective activity.

19. A system, comprising:

one or more processors; and

memory storing:

a virtual machine;

a virtual machine monitor supervising the virtual machine; and

one or more programs, the one or more programs including instructions for:

monitoring activity on the virtual machine;

identifying a plurality of activities being performed at the virtual machine, where each of the activities includes an activity source, an activity target, and an association between the activity source and the activity target;

storing in the memory the activity sources, activity targets, and associations; and

transmitting the fingerprint to prevent future attacks that comprise the same or similar activities as indicated by the fingerprint.

IPR2025-00068
CrowdStrike EX1002 Page 289

20. A computer readable storage medium, including one or more programs for execution by one or more processors of a computer system, the one or more programs including instructions for:

monitoring activity on the virtual machine;

identifying a plurality of activities being performed at the virtual machine, where each of the activities includes an activity source, an activity target, and an association between the activity source and the activity target;

storing in the memory the activity sources, activity targets, and associations; and

transmitting one or more of the activity sources, activity targets, and associations to prevent future attacks.

IPR2025-00068
CrowdStrike EX1002 Page 290

ABSTRACT OF THE DISCLOSURE

A computer implemented method includes monitoring activity on the virtual machine. A plurality of activities being performed at the virtual machine is identified. Each of the activities includes an activity source, an activity target, and an association between the activity source and the activity target. The activity information is stored in the memory. The one or more of the activity sources, activity targets, and associations are transmitted to prevent future attacks.

IPR2025-00068
CrowdStrike EX1002 Page 291

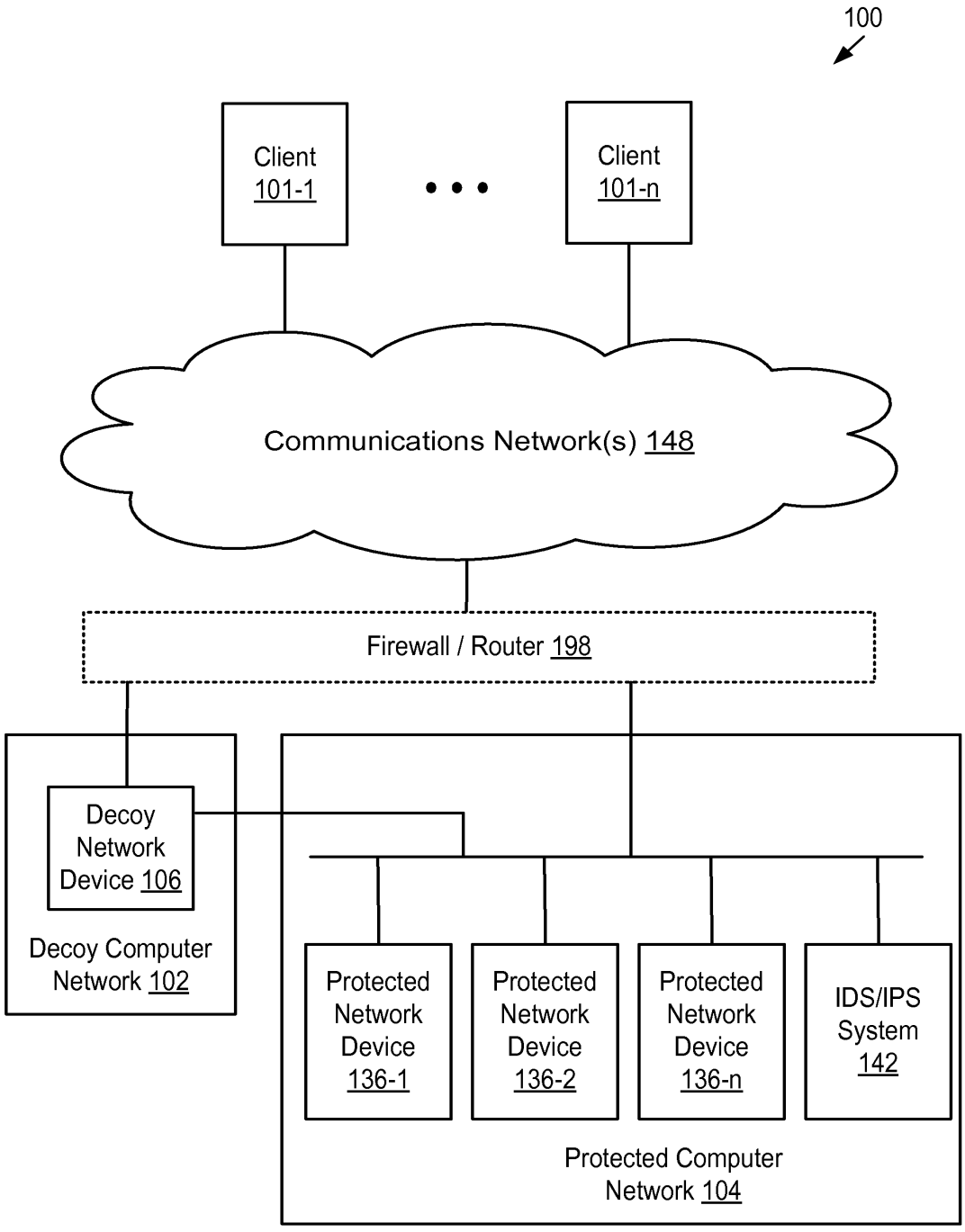

100
Client 101-1
Client 101-n
Communications Network(s) 148
Firewall / Router 198
Decoy Network Device 106
Decoy Computer Network 102
Protected Network Device 136-1
Protected Network Device 136-2
Protected Network Device 136-n
IDS/IPS System 142
Protected Computer Network 104

Figure 1

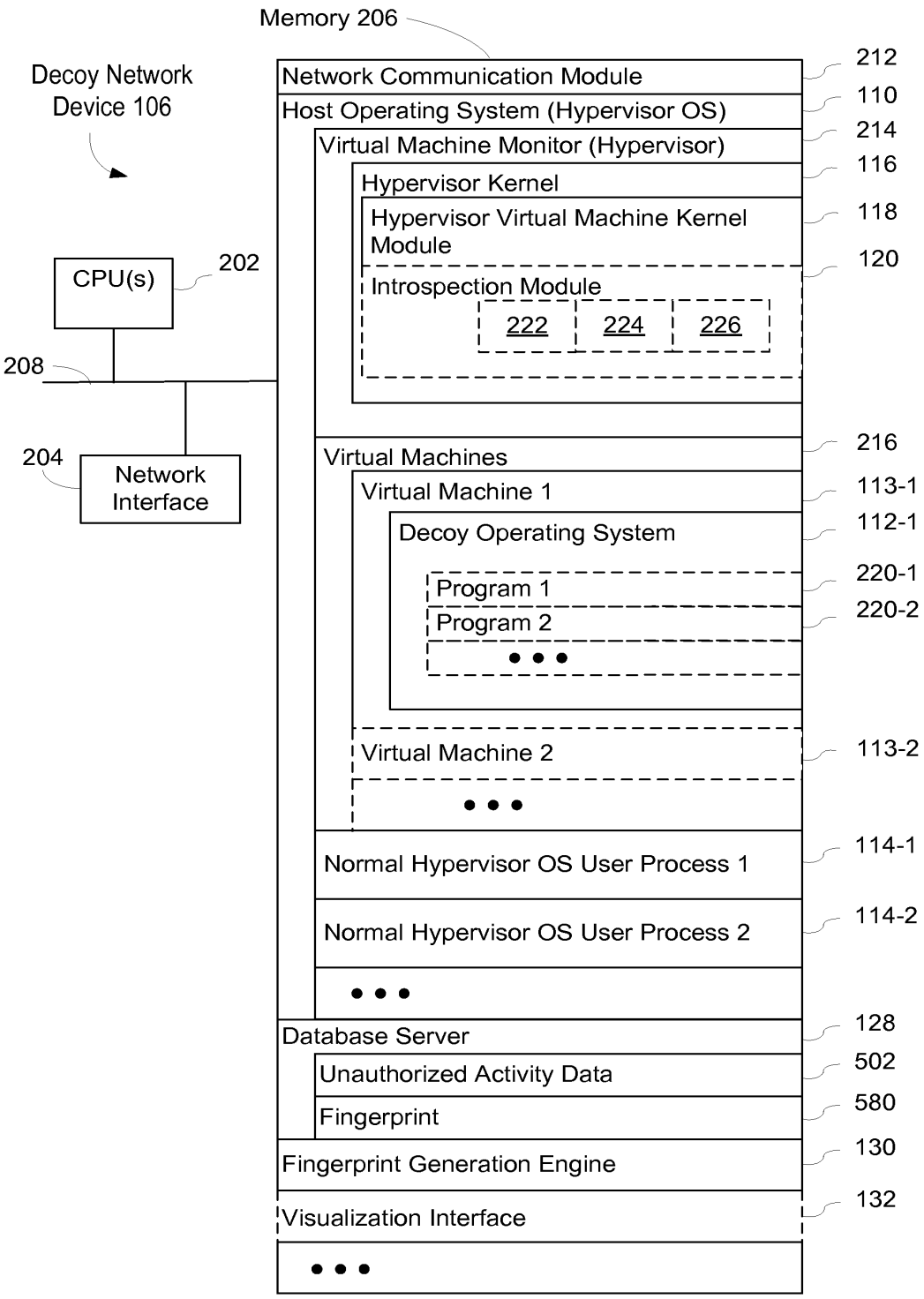

Memory 206
Decoy Network Device 106
Network Communication Module
212
Host Operating System (Hypervisor OS)
110
Virtual Machine Monitor (Hypervisor)
214
Hypervisor Kernel
116
Hypervisor Virtual Machine Kernel Module
118
Introspection Module
120
222
224
226
CPU(s)
202
208
204
Network Interface
Virtual Machines
216
Virtual Machine 1
113-1
Decoy Operating System
112-1
Program 1
220-1
Program 2
220-2
Virtual Machine 2
113-2
Normal Hypervisor OS User Process 1
114-1
Normal Hypervisor OS User Process 2
114-2
Database Server
128
Unauthorized Activity Data
502
Fingerprint
580
Fingerprint Generation Engine
130
Visualization Interface
132

Figure 2

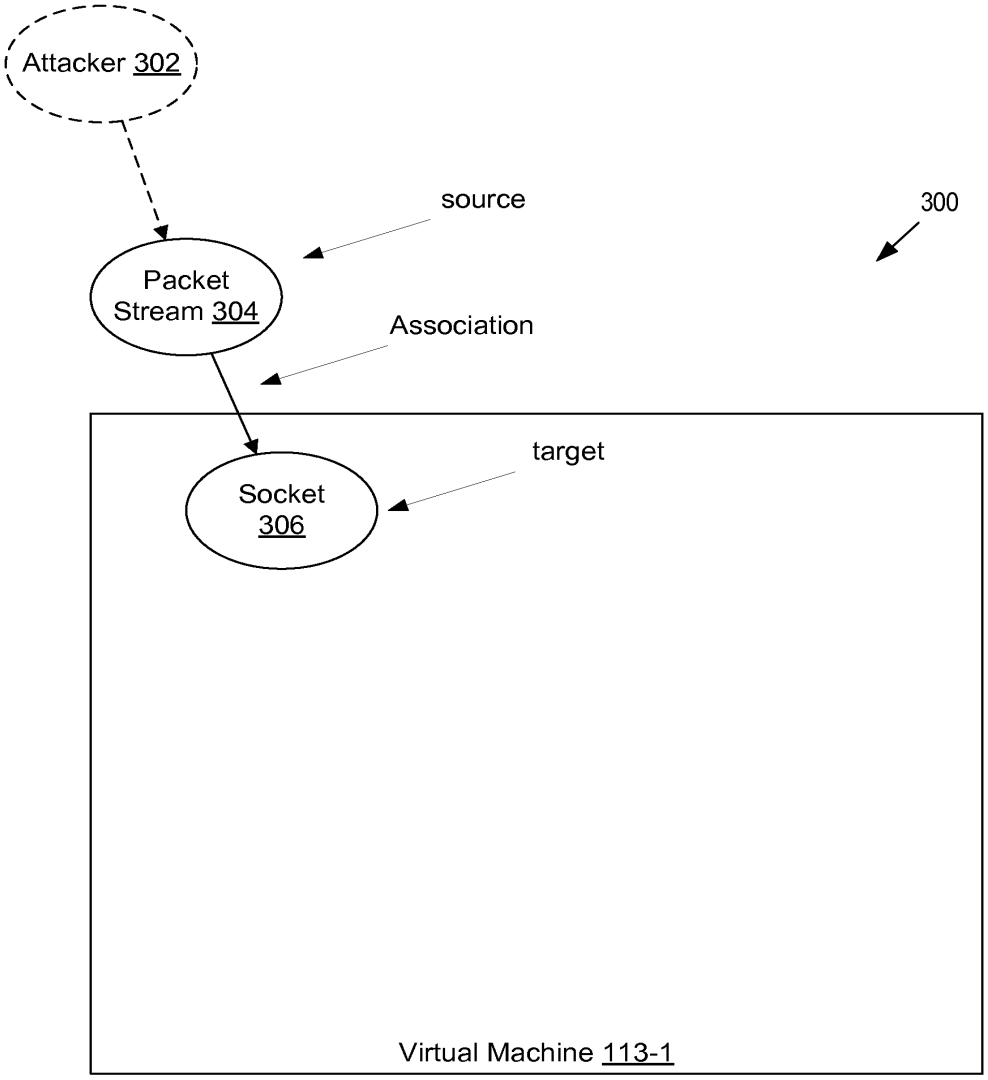

Attacker 302
source
300
Packet Stream 304
Association
target
Socket 306
Virtual Machine 113-1

Figure 3A

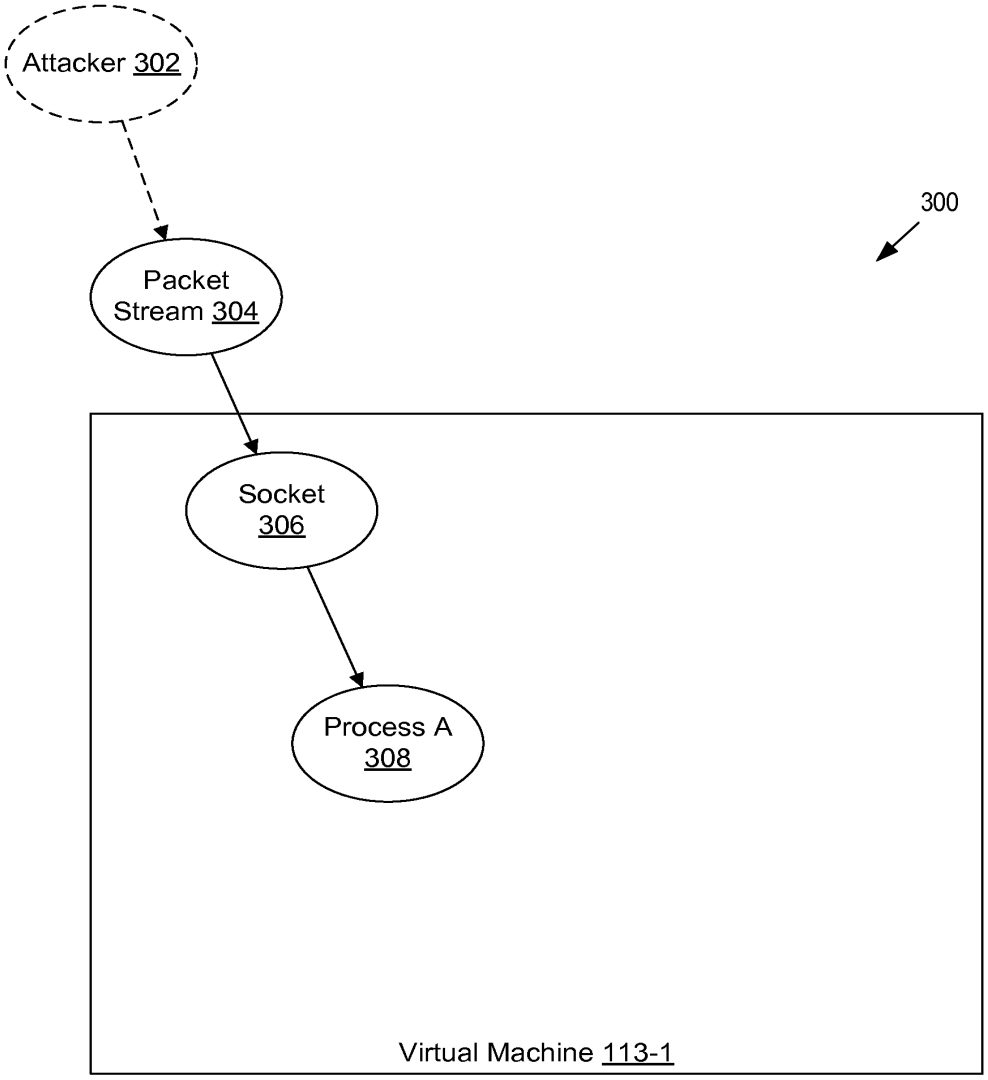

Attacker 302
300
Packet Stream 304
Socket 306
Process A 308
Virtual Machine 113-1

Figure 3B

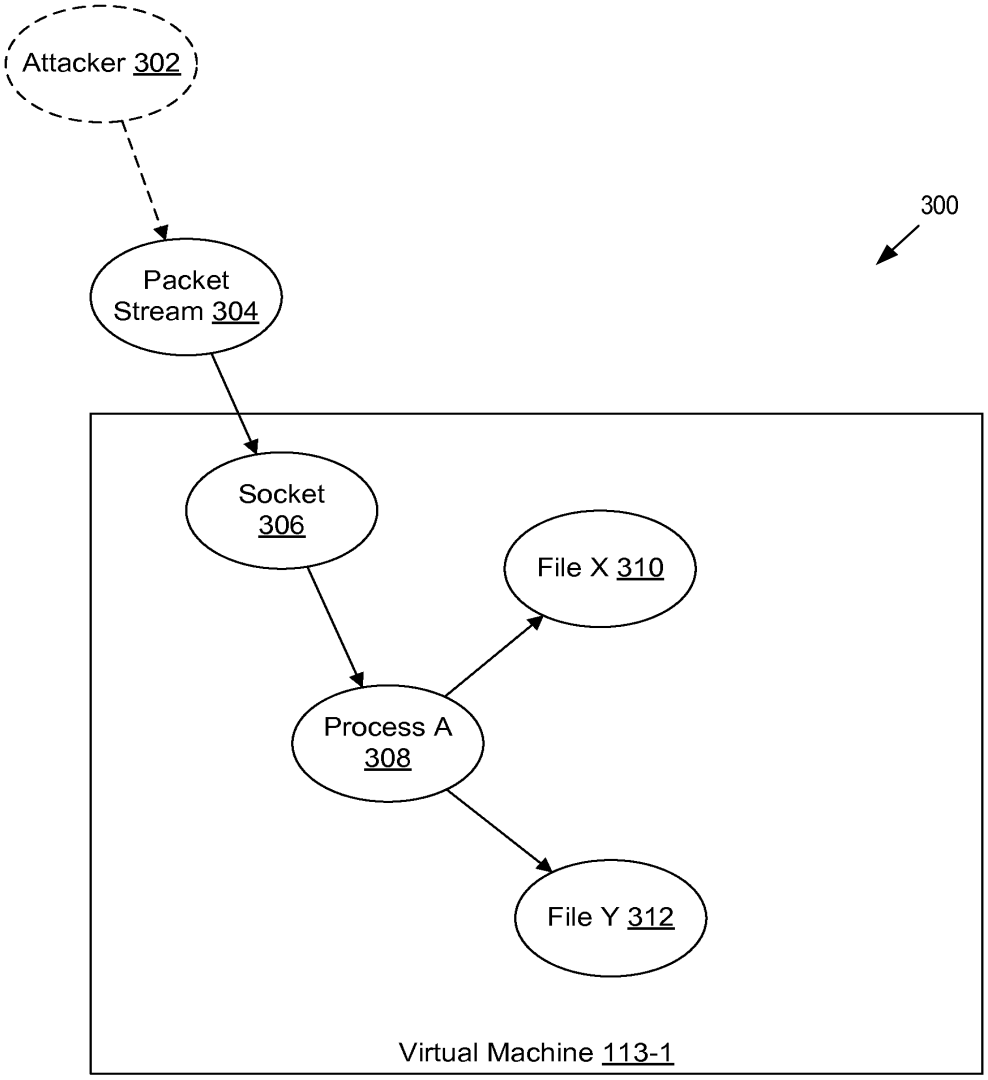

Attacker 302
300
Packet Stream 304
Socket 306
File X 310
Process A 308
File Y 312
Virtual Machine 113-1

Figure 3C

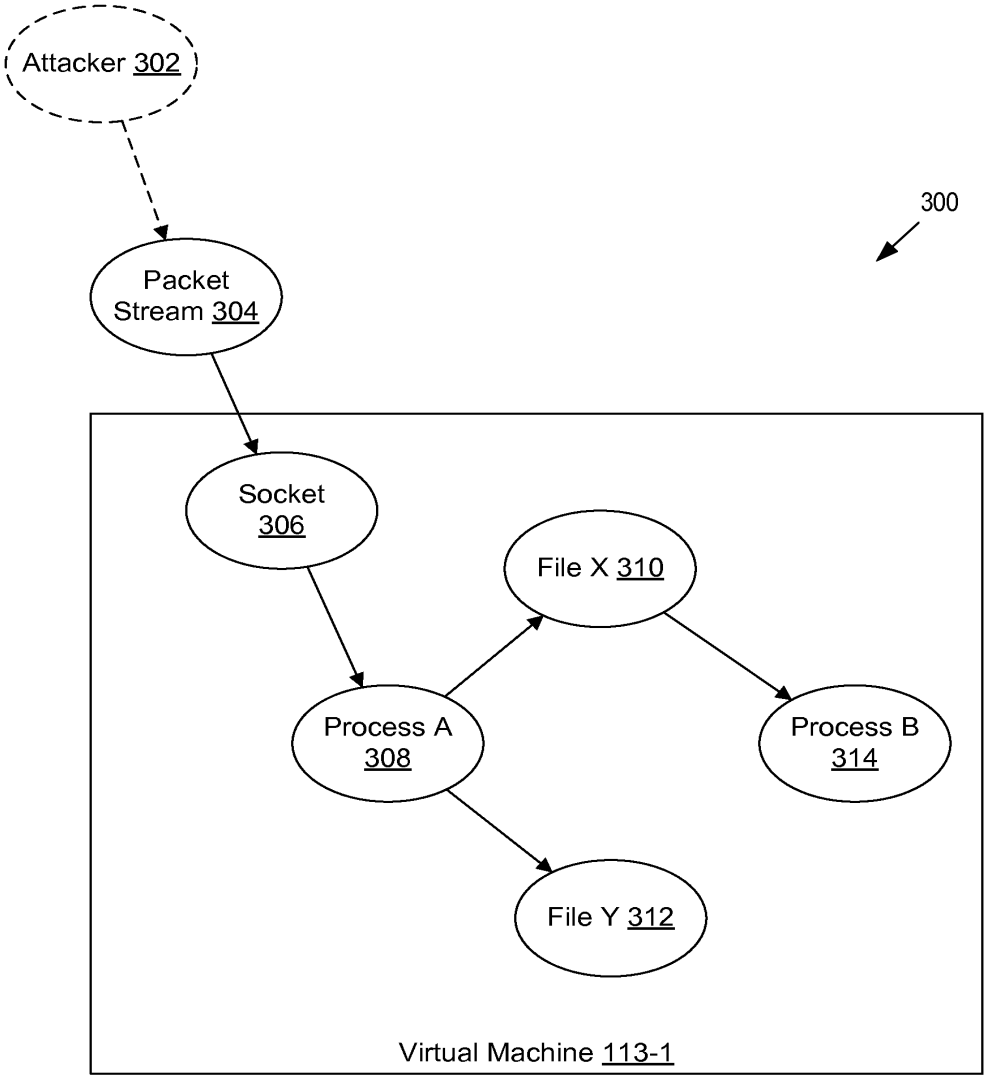

Attacker 302
300
Packet Stream 304
Socket 306
File X 310
Process A 308
Process B 314
File Y 312
Virtual Machine 113-1

Figure 3D

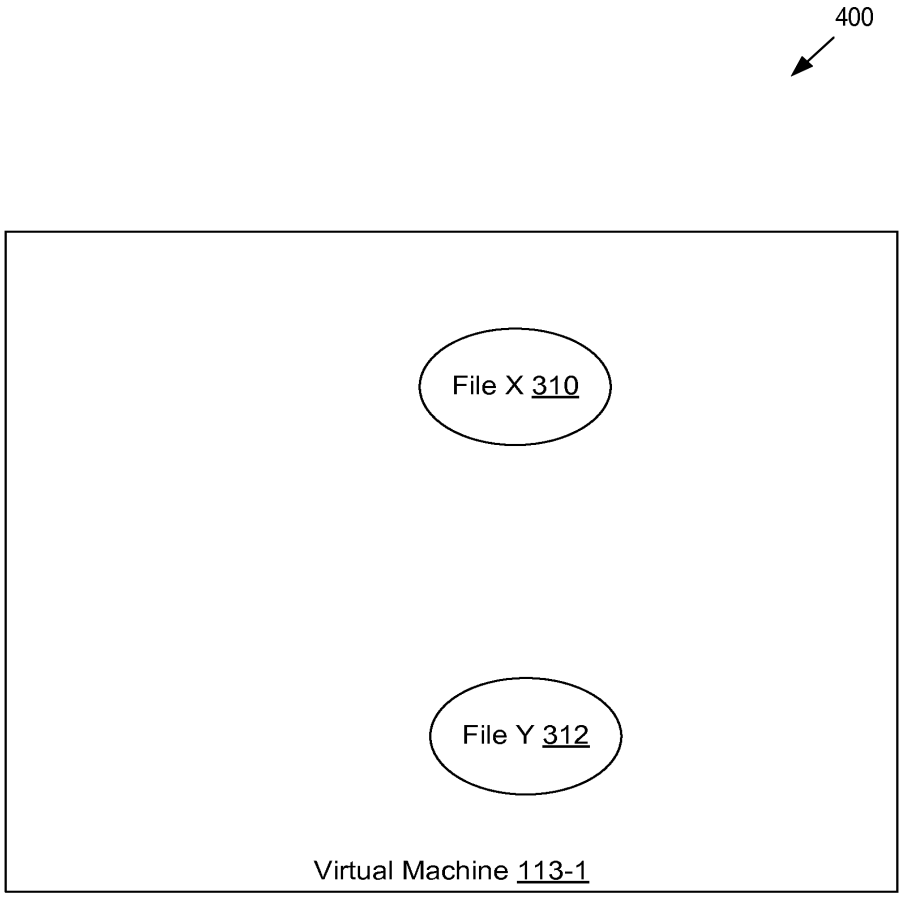


Figure 4A

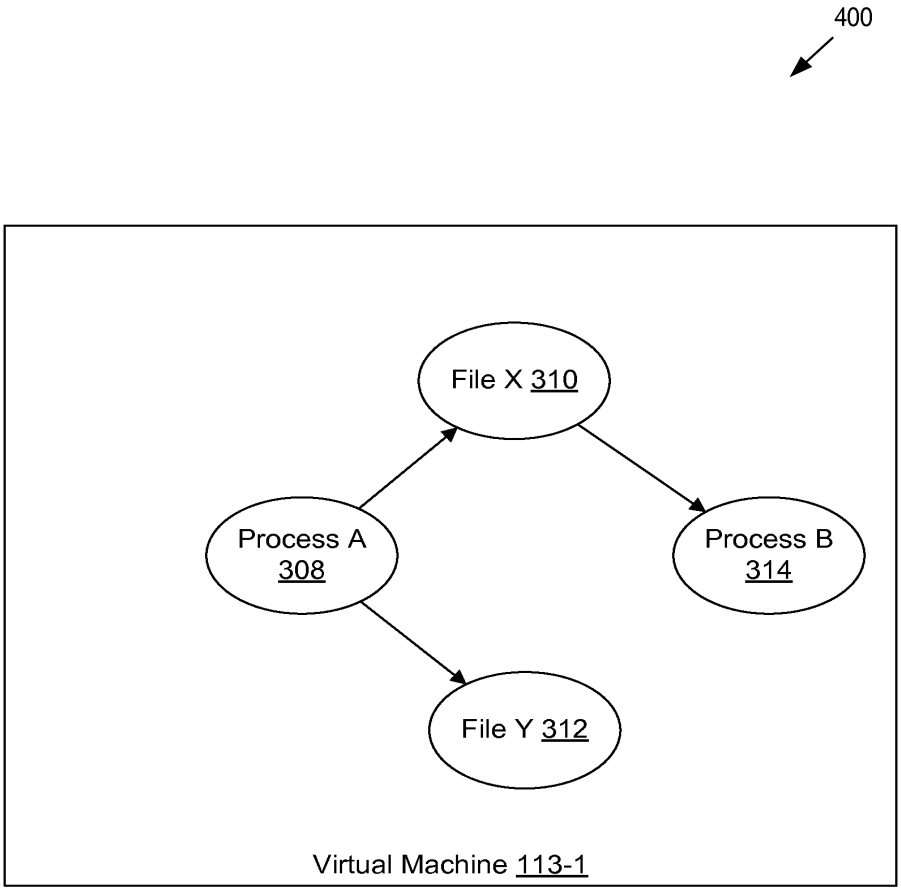

400
File X 310
Process A
308
Process B
314
File Y 312
Virtual Machine 113-1

Figure 4B

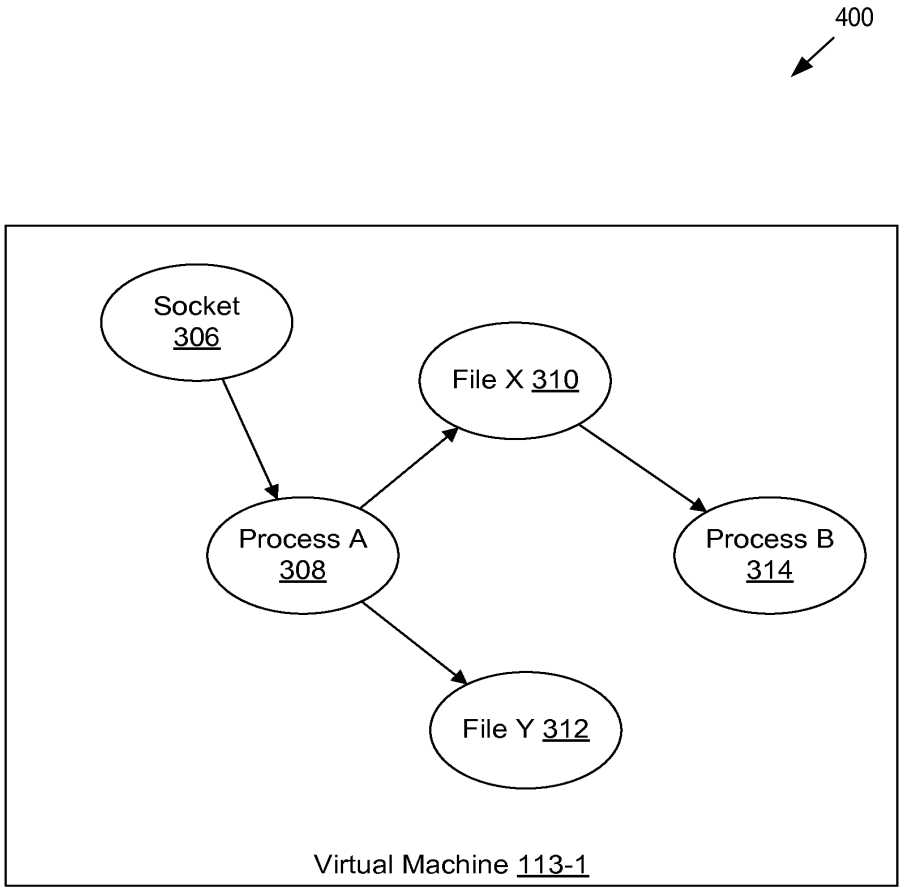

400
Socket
306
File X 310
Process A
308
Process B
314
File Y 312
Virtual Machine 113-1

Figure 4C

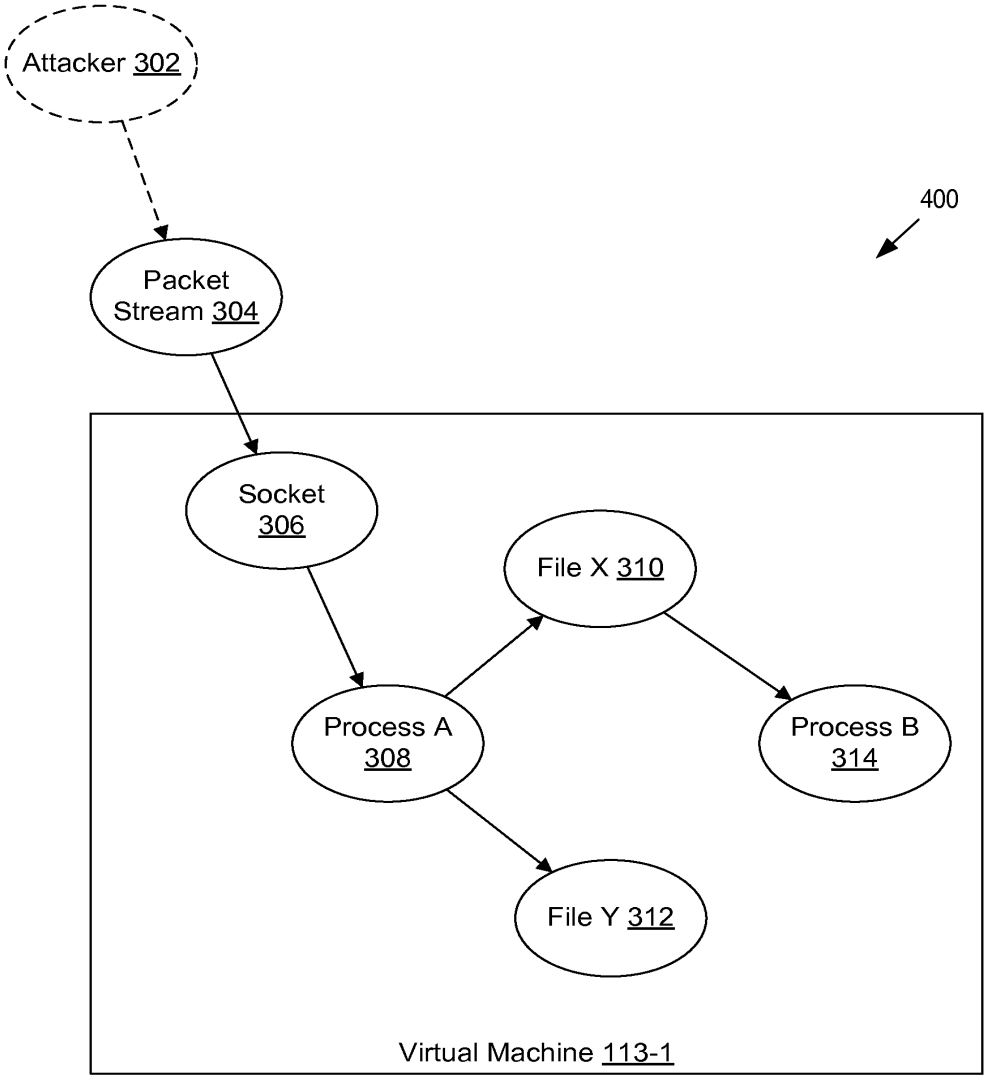

Attacker 302
400
Packet Stream 304
Socket 306
File X 310
Process A 308
Process B 314
File Y 312
Virtual Machine 113-1

Figure 4D

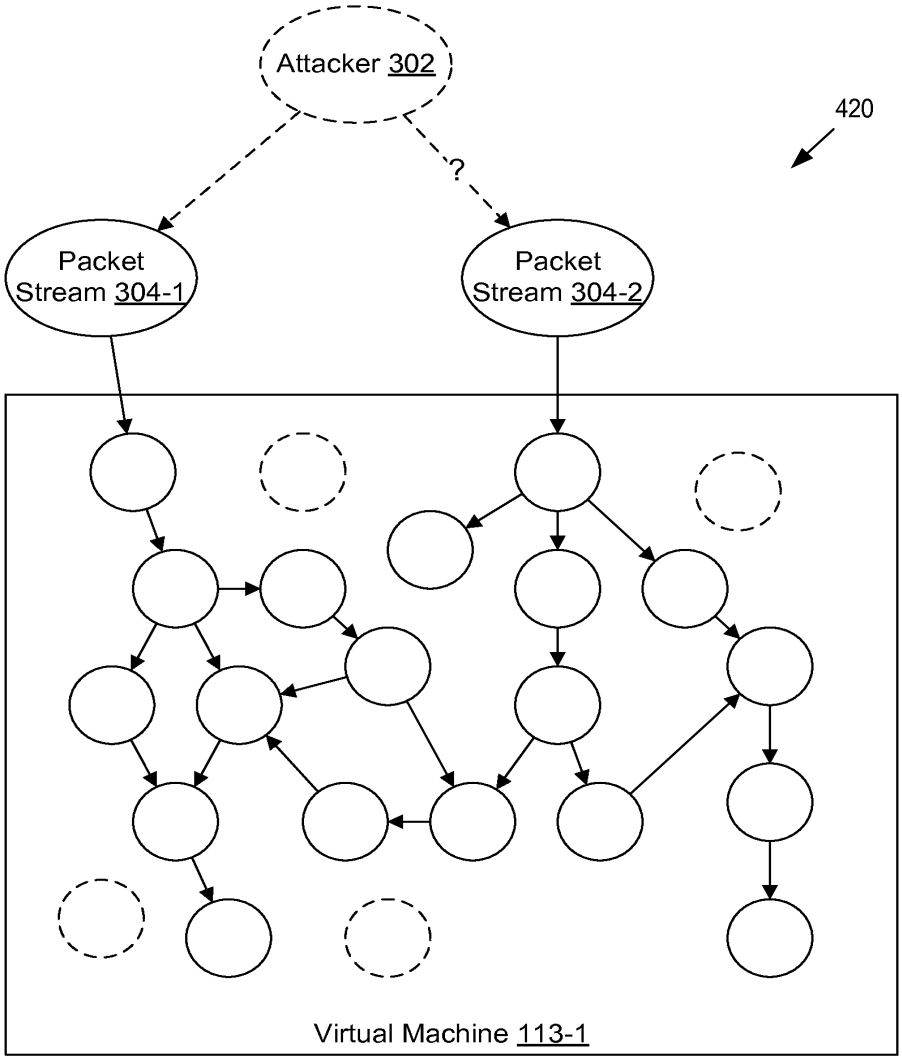

Attacker 302
420
?
Packet Stream 304-1
Packet Stream 304-2
Virtual Machine 113-1

Figure 4E

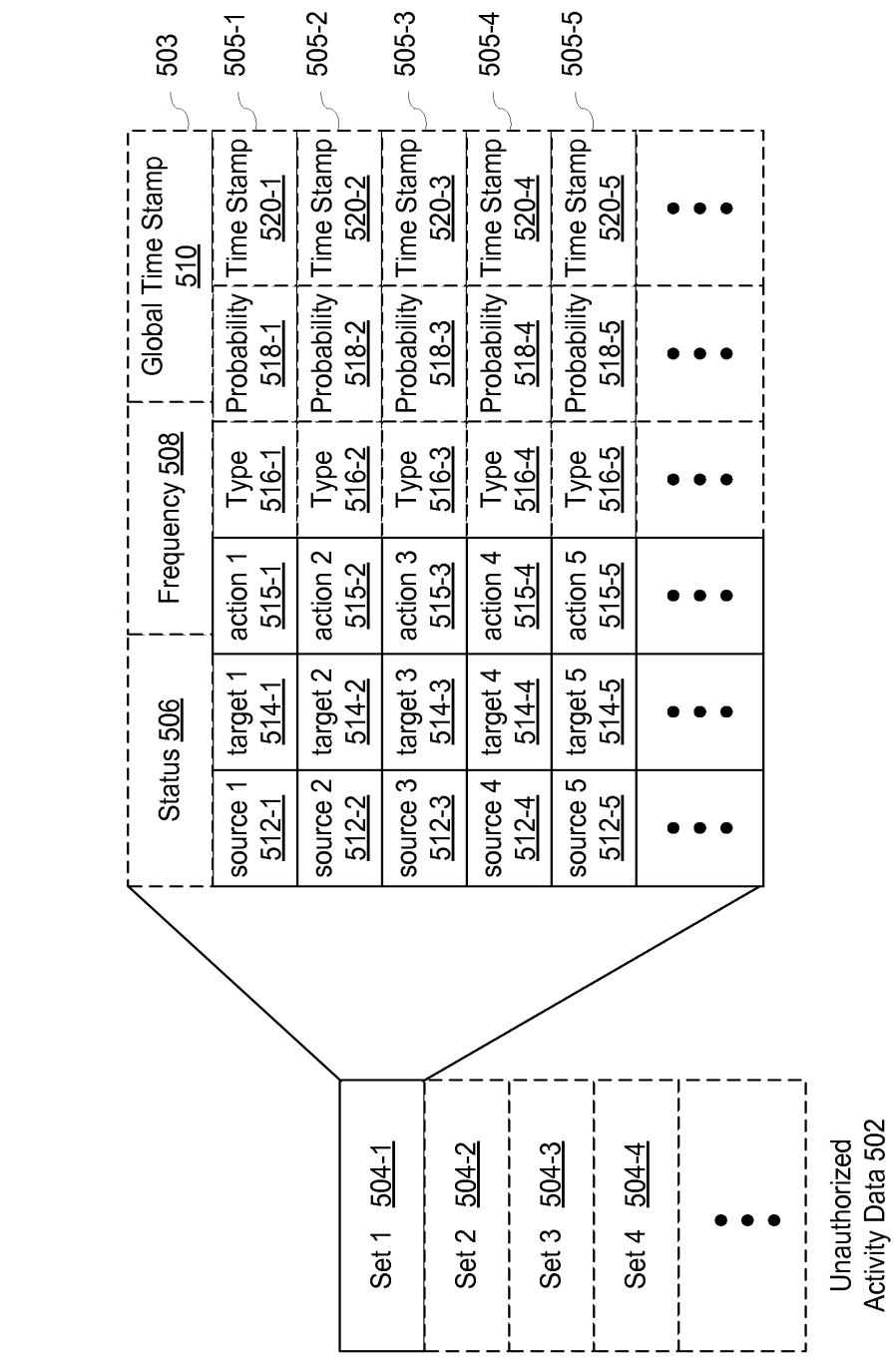

503
505-1
505-2
505-3
505-4
505-5
Status 506
Frequency 508
Global Time Stamp 510
source 1 512-1
target 1 514-1
action 1 515-1
Type 516-1
Probability 518-1
Time Stamp 520-1
source 2 512-2
target 2 514-2
action 2 515-2
Type 516-2
Probability 518-2
Time Stamp 520-2
source 3 512-3
target 3 514-3
action 3 515-3
Type 516-3
Probability 518-3
Time Stamp 520-3
source 4 512-4
target 4 514-4
action 4 515-4
Type 516-4
Probability 518-4
Time Stamp 520-4
source 5 512-5
target 5 514-5
action 5 515-5
Type 516-5
Probability 518-5
Time Stamp 520-5
Set 1 504-1
Set 2 504-2
Set 3 504-3
Set 4 504-4
Unauthorized Activity Data 502

Figure 5A

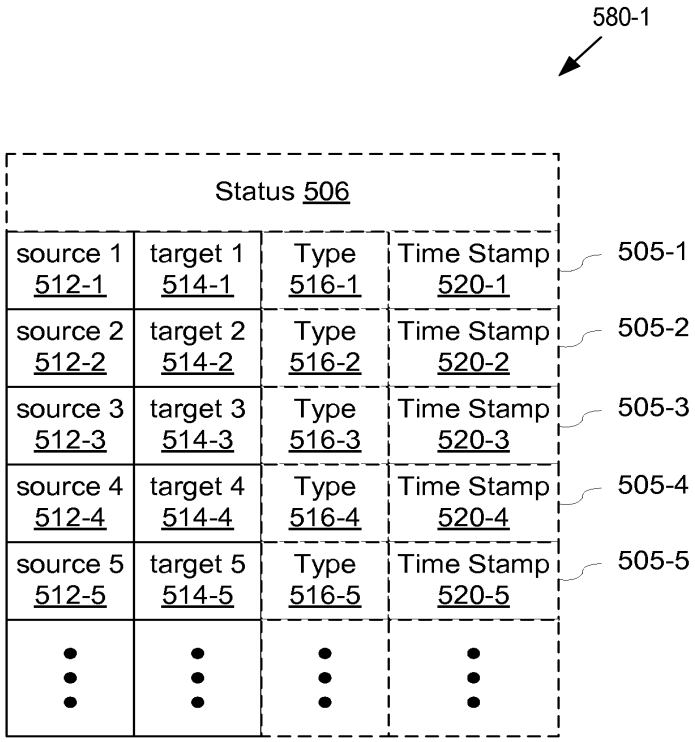

580-1
Status 506
source 1 512-1
target 1 514-1
Type 516-1
Time Stamp 520-1
505-1
source 2 512-2
target 2 514-2
Type 516-2
Time Stamp 520-2
505-2
source 3 512-3
target 3 514-3
Type 516-3
Time Stamp 520-3
505-3
source 4 512-4
target 4 514-4
Type 516-4
Time Stamp 520-4
505-4
source 5 512-5
target 5 514-5
Type 516-5
Time Stamp 520-5
505-5

Figure 5B

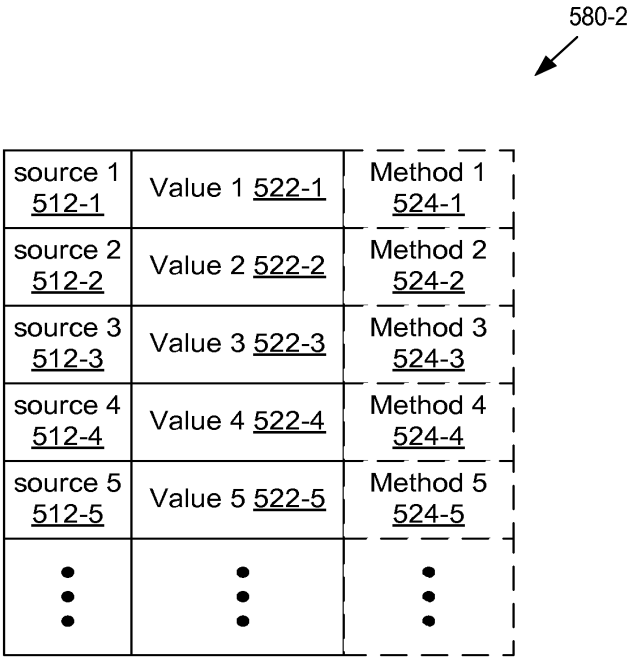

580-2
source 1 512-1
Value 1 522-1
Method 1 524-1
source 2 512-2
Value 2 522-2
Method 2 524-2
source 3 512-3
Value 3 522-3
Method 3 524-3
source 4 512-4
Value 4 522-4
Method 4 524-4
source 5 512-5
Value 5 522-5
Method 5 524-5

Figure 5C

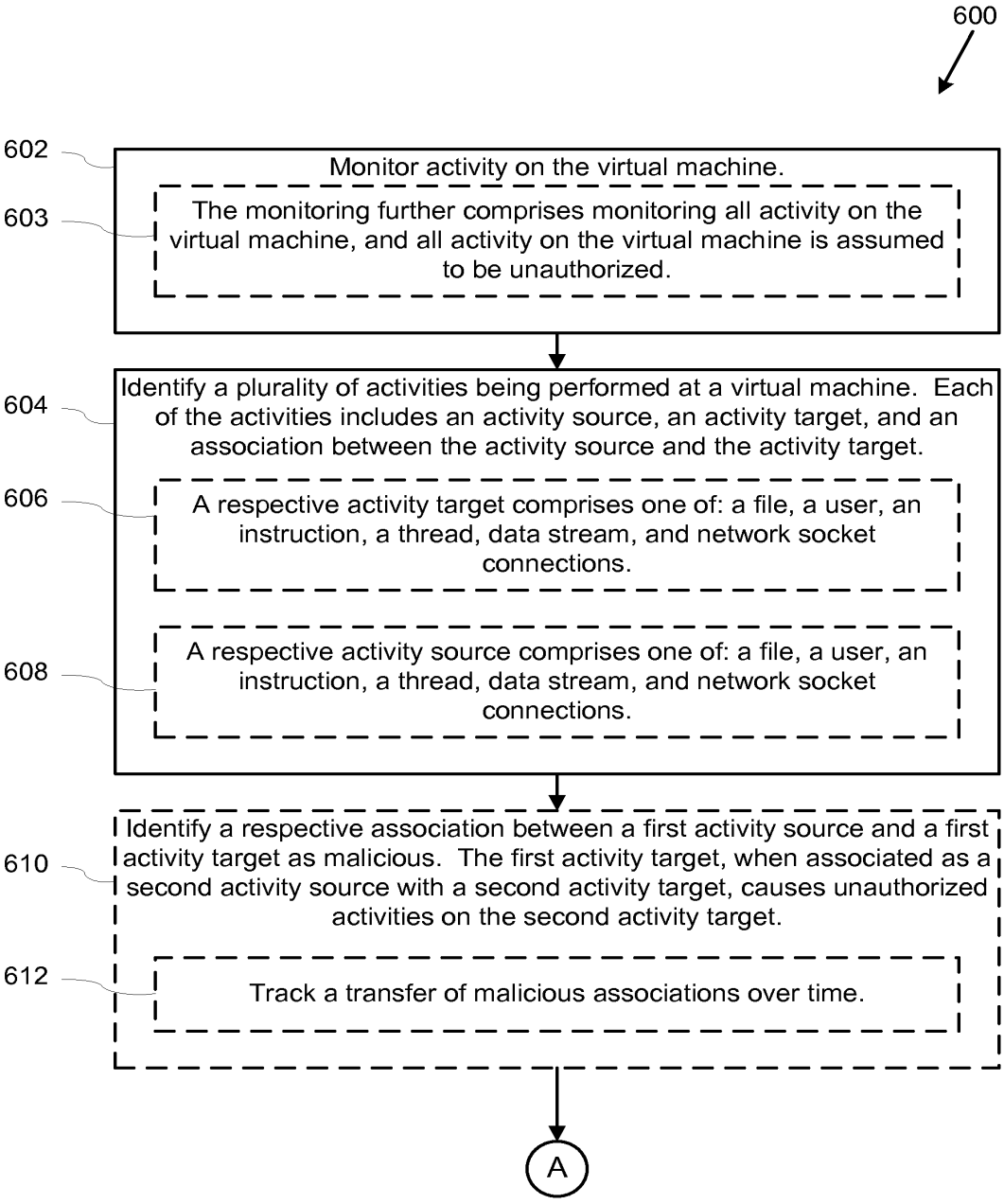

600
602
Monitor activity on the virtual machine.
603
The monitoring further comprises monitoring all activity on the virtual machine, and all activity on the virtual machine is assumed to be unauthorized.
604
Identify a plurality of activities being performed at a virtual machine. Each of the activities includes an activity source, an activity target, and an association between the activity source and the activity target.
606
A respective activity target comprises one of: a file, a user, an instruction, a thread, data stream, and network socket connections.
608
A respective activity source comprises one of: a file, a user, an instruction, a thread, data stream, and network socket connections.
610
Identify a respective association between a first activity source and a first activity target as malicious. The first activity target, when associated as a second activity source with a second activity target, causes unauthorized activities on the second activity target.
612
Track a transfer of malicious associations over time.
A

Figure 6A

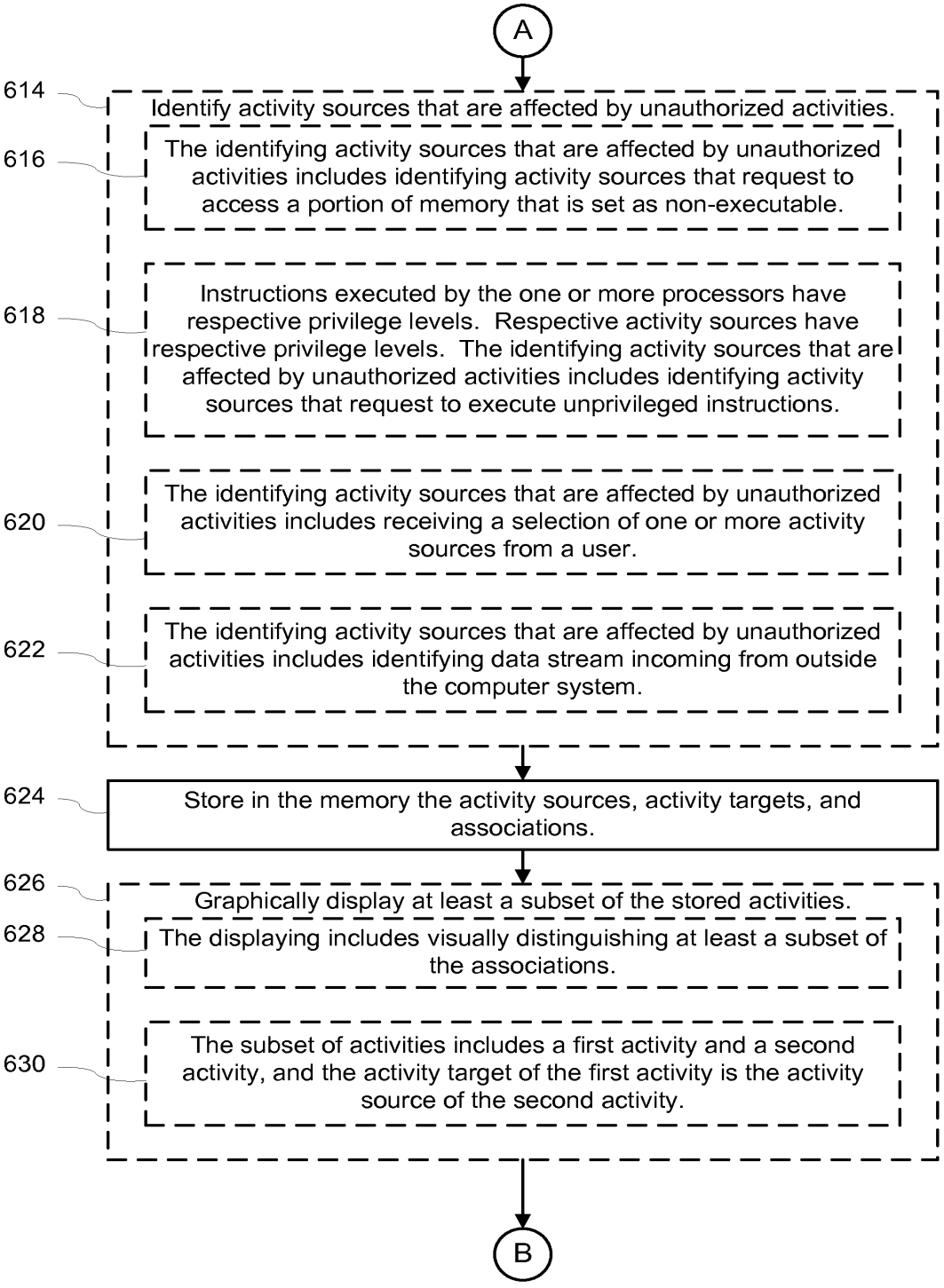

A
614
Identify activity sources that are affected by unauthorized activities.
616
The identifying activity sources that are affected by unauthorized activities includes identifying activity sources that request to access a portion of memory that is set as non-executable.
618
Instructions executed by the one or more processors have respective privilege levels. Respective activity sources have respective privilege levels. The identifying activity sources that are affected by unauthorized activities includes identifying activity sources that request to execute unprivileged instructions.
620
The identifying activity sources that are affected by unauthorized activities includes receiving a selection of one or more activity sources from a user.
622
The identifying activity sources that are affected by unauthorized activities includes identifying data stream incoming from outside the computer system.
624
Store in the memory the activity sources, activity targets, and associations.
626
Graphically display at least a subset of the stored activities.
628
The displaying includes visually distinguishing at least a subset of the associations.
630
The subset of activities includes a first activity and a second activity, and the activity target of the first activity is the activity source of the second activity.
B

Figure 6B

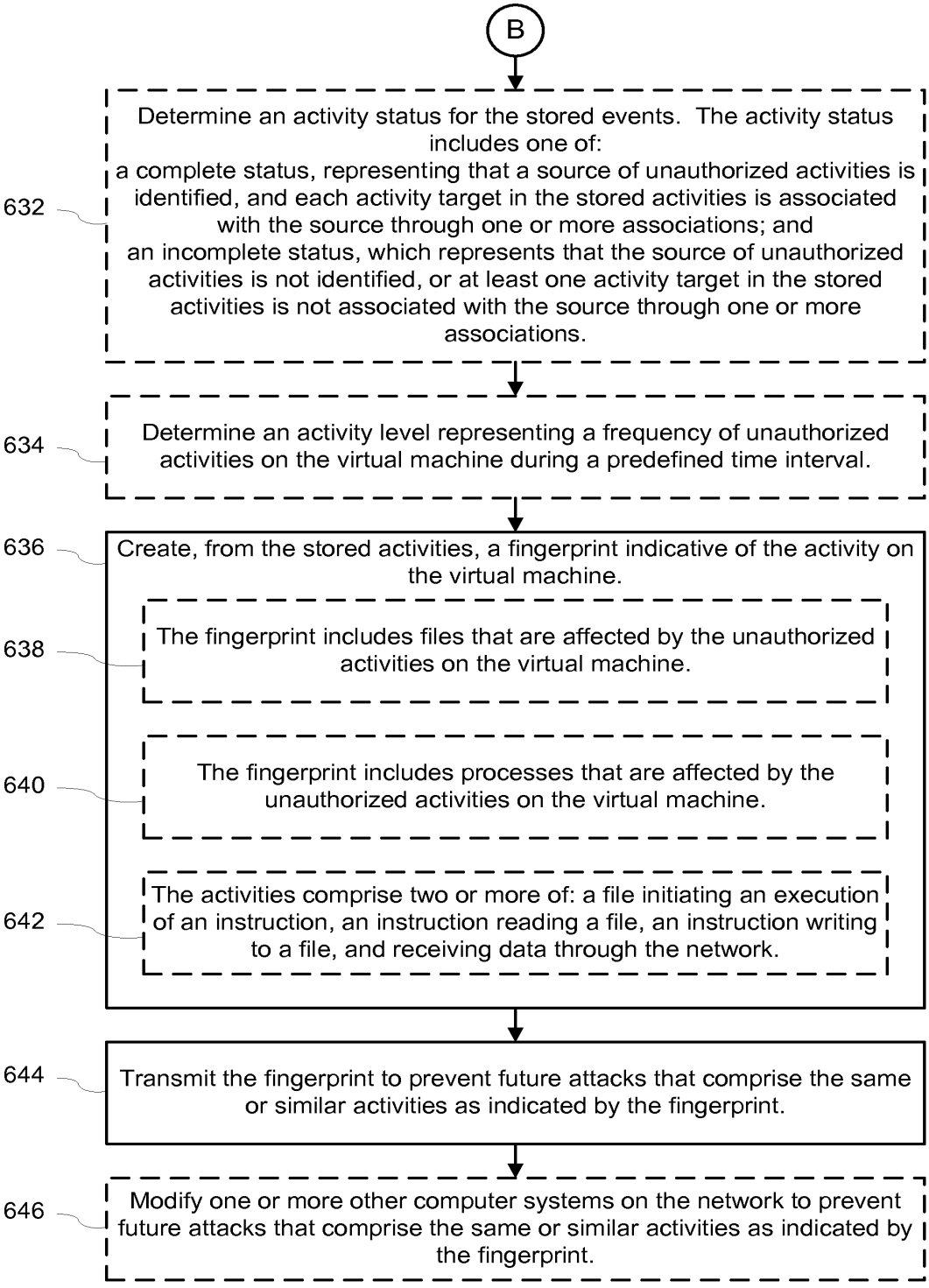

B
Determine an activity status for the stored events. The activity status includes one of:
a complete status, representing that a source of unauthorized activities is identified, and each activity target in the stored activities is associated with the source through one or more associations; and
an incomplete status, which represents that the source of unauthorized activities is not identified, or at least one activity target in the stored activities is not associated with the source through one or more associations.
632
Determine an activity level representing a frequency of unauthorized activities on the virtual machine during a predefined time interval.
634
Create, from the stored activities, a fingerprint indicative of the activity on the virtual machine.
636
The fingerprint includes files that are affected by the unauthorized activities on the virtual machine.
638
The fingerprint includes processes that are affected by the unauthorized activities on the virtual machine.
640
The activities comprise two or more of: a file initiating an execution of an instruction, an instruction reading a file, an instruction writing to a file, and receiving data through the network.
642
Transmit the fingerprint to prevent future attacks that comprise the same or similar activities as indicated by the fingerprint.
644
Modify one or more other computer systems on the network to prevent future attacks that comprise the same or similar activities as indicated by the fingerprint.
646

Figure 6C

PTO/AIA/14 (11-13)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	067292-5005-US01
	Application Number	
Title of Invention	System and Method for Identifying Unauthorized Activities on a Computer System using a Data Structure Model	

The application data sheet is part of the provisional or nonprovisional application for which it is being submitted. The following form contains the bibliographic data arranged in a format specified by the United States Patent and Trademark Office as outlined in 37 CFR 1.76.
This document may be completed electronically and submitted to the Office in electronic format using the Electronic Filing System (EFS) or the document may be printed and included in a paper filed application.

Secrecy Order 37 CFR 5.2

☐ Portions or all of the application associated with this Application Data Sheet may fall under a Secrecy Order pursuant to 37 CFR 5.2 (Paper filers only. Applications that fall under Secrecy Order may not be filed electronically.)

Inventor Information:

Inventor 1 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	Alen		Capalik	

Residence Information (Select One) ◉ US Residency ○ Non US Residency ○ Active US Military Service

City	Pacific Palisades	State/Province	CA	Country of Residence i	US

Mailing Address of Inventor:

Address 1	1639 11TH STREET		
Address 2			
City	SANTA MONICA	State/Province	CA
Postal Code	90404	Country i	US

Inventor 2 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	David		Andrews	

Residence Information (Select One) ◉ US Residency ○ Non US Residency ○ Active US Military Service

City	Los Angeles	State/Province	CA	Country of Residence i	US

Mailing Address of Inventor:

Address 1	1639 11TH STREET		
Address 2			
City	SANTA MONICA	State/Province	CA
Postal Code	90404	Country i	US

Inventor 3 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	Ben		Becker	

Residence Information (Select One) ◉ US Residency ○ Non US Residency ○ Active US Military Service

PTO/AIA/14 (11-13)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	067292-5005-US01
	Application Number	
Title of Invention	System and Method for Identifying Unauthorized Activities on a Computer System using a Data Structure Model	

City	Santa Monica	State/Province	CA	Country of Residence i	US

Mailing Address of Inventor:

Address 1	1639 11TH STREET		
Address 2			
City	SANTA MONICA	State/Province	CA
Postal Code	90404	Country i	US

All Inventors Must Be Listed - Additional Inventor Information blocks may be generated within this form by selecting the **Add** button. Add

Correspondence Information:

Enter either Customer Number or complete the Correspondence Information section below.
For further information see 37 CFR 1.33(a).

☐ **An Address is being provided for the correspondence Information of this application.**

Customer Number	24341		
Email Address		Add Email	Remove Email

Application Information:

Title of the Invention	System and Method for Identifying Unauthorized Activities on a Computer System using a Data Structure Model		
Attorney Docket Number	067292-5005-US01	Small Entity Status Claimed	☒
Application Type	Nonprovisional		
Subject Matter	Utility		
Total Number of Drawing Sheets (if any)	17	Suggested Figure for Publication (if any)	

Publication Information:

☐ Request Early Publication (Fee required at time of Request 37 CFR 1.219)

☐ **Request Not to Publish.** I hereby request that the attached application not be published under 35 U.S.C. 122(b) and certify that the invention disclosed in the attached application **has not and will not** be the subject of an application filed in another country, or under a multilateral international agreement, that requires publication at eighteen months after filing.

Representative Information:

Representative information should be provided for all practitioners having a power of attorney in the application. Providing this information in the Application Data Sheet does not constitute a power of attorney in the application (see 37 CFR 1.32).
Either enter Customer Number or complete the Representative Name section below. If both sections are completed the customer Number will be used for the Representative Information during processing.

Please Select One:	◉ Customer Number	○ US Patent Practitioner	○ Limited Recognition (37 CFR 11.9)

PTO/AIA/14 (11-13)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	067292-5005-US01
	Application Number	
Title of Invention	System and Method for Identifying Unauthorized Activities on a Computer System using a Data Structure Model	

Customer Number	24341

Domestic Benefit/National Stage Information:

This section allows for the applicant to either claim benefit under 35 U.S.C. 119(e), 120, 121, or 365(c) or indicate National Stage entry from a PCT application. Providing this information in the application data sheet constitutes the specific reference required by 35 U.S.C. 119(e) or 120, and 37 CFR 1.78.
When referring to the current application, please leave the application number blank.

Prior Application Status	Pending		Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
	Continuation of	13/163590	2011-06-17
Prior Application Status	Expired		Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
13/163590	Claims benefit of provisional	61/358367	2010-06-24

Additional Domestic Benefit/National Stage Data may be generated within this form by selecting the **Add** button. Add

Foreign Priority Information:

This section allows for the applicant to claim priority to a foreign application. Providing this information in the application data sheet constitutes the claim for priority as required by 35 U.S.C. 119(b) and 37 CFR 1.55(d). When priority is claimed to a foreign application that is eligible for retrieval under the priority document exchange program (PDX) [i] the information will be used by the Office to automatically attempt retrieval pursuant to 37 CFR 1.55(h)(1) and (2). Under the PDX program, applicant bears the ultimate responsibility for ensuring that a copy of the foreign application is received by the Office from the participating foreign intellectual property office, or a certified copy of the foreign priority application is filed, within the time period specified in 37 CFR 1.55(g)(1).

Remove

Application Number	Country [i]	Filing Date (YYYY-MM-DD)	Access Code [i] (if applicable)

Additional Foreign Priority Data may be generated within this form by selecting the **Add** button. Add

PTO/AIA/14 (11-13)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	067292-5005-US01
	Application Number	
Title of Invention	System and Method for Identifying Unauthorized Activities on a Computer System using a Data Structure Model	

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications

☐ This application (1) claims priority to or the benefit of an application filed before March 16, 2013 and (2) also contains, or contained at any time, a claim to a claimed invention that has an effective filing date on or after March 16, 2013.
NOTE: By providing this statement under 37 CFR 1.55 or 1.78, this application, with a filing date on or after March 16, 2013, will be examined under the first inventor to file provisions of the AIA.

Authorization to Permit Access:

☐ Authorization to Permit Access to the Instant Application by the Participating Offices

If checked, the undersigned hereby grants the USPTO authority to provide the European Patent Office (EPO), the Japan Patent Office (JPO), the Korean Intellectual Property Office (KIPO), the World Intellectual Property Office (WIPO), and any other intellectual property offices in which a foreign application claiming priority to the instant patent application is filed access to the instant patent application. See 37 CFR 1.14(c) and (h). This box should not be checked if the applicant does not wish the EPO, JPO, KIPO, WIPO, or other intellectual property office in which a foreign application claiming priority to the instant patent application is filed to have access to the instant patent application.

In accordance with 37 CFR 1.14(h)(3), access will be provided to a copy of the instant patent application with respect to: 1) the instant patent application-as-filed; 2) any foreign application to which the instant patent application claims priority under 35 U.S.C. 119(a)-(d) if a copy of the foreign application that satisfies the certified copy requirement of 37 CFR 1.55 has been filed in the instant patent application; and 3) any U.S. application-as-filed from which benefit is sought in the instant patent application.

In accordance with 37 CFR 1.14(c), access may be provided to information concerning the date of filing this Authorization.

Applicant Information:

Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

PTO/AIA/14 (11-13)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	067292-5005-US01
	Application Number	
Title of Invention	System and Method for Identifying Unauthorized Activities on a Computer System using a Data Structure Model	

Applicant 1 Remove

If the applicant is the inventor (or the remaining joint inventor or inventors under 37 CFR 1.45), this section should not be completed. The information to be provided in this section is the name and address of the legal representative who is the applicant under 37 CFR 1.43; or the name and address of the assignee, person to whom the inventor is under an obligation to assign the invention, or person who otherwise shows sufficient proprietary interest in the matter who is the applicant under 37 CFR 1.46. If the applicant is an applicant under 37 CFR 1.46 (assignee, person to whom the inventor is obligated to assign, or person who otherwise shows sufficient proprietary interest) together with one or more joint inventors, then the joint inventor or inventors who are also the applicant should be identified in this section.

Clear

(•) Assignee	( ) Legal Representative under 35 U.S.C. 117	( ) Joint Inventor
( ) Person to whom the inventor is obligated to assign.	( ) Person who shows sufficient proprietary interest	

If applicant is the legal representative, indicate the authority to file the patent application, the inventor is:

Name of the Deceased or Legally Incapacitated Inventor :

If the Applicant is an Organization check here. [X]

Organization Name	COUNTERTACK INC.		
Mailing Address Information:			
Address 1	1639 11th Street		
Address 2			
City	Santa Monica	**State/Province**	CA
Country [i]	US	Postal Code	90404
Phone Number		Fax Number	
Email Address			

Additional Applicant Data may be generated within this form by selecting the Add button. Add

Assignee Information including Non-Applicant Assignee Information:

Providing assignment information in this section does not subsitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

Assignee 1

Complete this section if assignee information, including non-applicant assignee information, is desired to be included on the patent application publication . An assignee-applicant identified in the "Applicant Information" section will appear on the patent application publication as an applicant. For an assignee-applicant, complete this section only if identification as an assignee is also desired on the patent application publication.

Remove

If the Assignee or Non-Applicant Assignee is an Organization check here. [ ]

PTO/AIA/14 (11-13)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	067292-5005-US01
	Application Number	
Title of Invention	System and Method for Identifying Unauthorized Activities on a Computer System using a Data Structure Model	

Prefix	**Given Name**	Middle Name	**Family Name**	Suffix

Mailing Address Information For Assignee including Non-Applicant Assignee:

Address 1			
Address 2			
City		**State/Province**	
Country i		Postal Code	
Phone Number		Fax Number	
Email Address			

Additional Assignee or Non-Applicant Assignee Data may be generated within this form by selecting the Add button. Add

Signature:

Remove

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications

Signature	/ Tae-Woong Koo /			Date (YYYY-MM-DD)	2015-08-11
First Name	Tae-Woong	Last Name	Koo	Registration Number	59649

Additional Signature may be generated within this form by selecting the Add button. Add

This collection of information is required by 37 CFR 1.76. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 23 minutes to complete, including gathering, preparing, and submitting the completed application data sheet form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Acknowledgement Receipt

EFS ID:	23181043
Application Number:	14823916
International Application Number:	
Confirmation Number:	5143
Title of Invention:	System and Method for Identifying Unauthorized Activities on a Computer System using a Data Structure Model
First Named Inventor/Applicant Name:	Alen Capalik
Customer Number:	24341
Filer:	Tae-Woong Koo
Filer Authorized By:	
Attorney Docket Number:	067292-5005-US01
Receipt Date:	11-AUG-2015
Filing Date:	
Time Stamp:	19:24:41
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		067292_5005US_Trans_Appln_Drwgs.pdf	860365 d4d7b06c1767b162a9bcd72f793ffc6d6f72e663	yes	51

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Transmittal of New Application	1	1
	Specification	2	29
	Claims	30	33
	Abstract	34	34
	Drawings-only black and white line drawings	35	51
Warnings:			
Information:			

2	Application Data Sheet	067292_5005_US01_ADS.pdf	1265400 feb3f2e6cdf7fbf95aaaf15202004cafa0680117	no	7
Warnings:					
Information:					
		Total Files Size (in bytes):	2125765		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.