**FAX**

European Patent Office
80298 Munich

April 27, 2020

Change of Representative

Our Ref.: SGR 001

We herewith take over representation of the patent applications mentioned in the enclosed list.

All future correspondence should be addressed to

Betten & Resch Patent- und Rechtsanwälte PartGmbH
Maximiliansplatz 14
80333 München
Tel +49 89 2424170
Fax +49 89 2607896

The former representative has already laid down representation or will do so shortly.

Finally, the Office is respectfully requested to take note of our ref. no. for each case and accordingly update its records.

Dirk C. Sieckmann

Enclosure: List (1 page)

Patentanwälte
European Patent Attorneys
European Trademark Attorneys
European Design Attorneys

Franz-Josef Schöninger
Dipl.-Phys.

Dr. Alexander Esslinger
Dipl.-Phys.

Dirk C. Sieckmann, LL.M.
Dipl.-Ing.

Dr. René Günther
Dipl.-Phys.

Prof. Dr. Christoph von Praun
Dipl.-Inf.

Märkte Širava, LL.M.
Dipl.-Inf.

Attila Scharfenecker
Dipl.-Phys.

Rechtsanwälte
Fachanwälte für Gewerblichen
Rechtsschutz

Alexandra Parr

Philip Reichel, LL.M.

European Patent Attorneys

Dr. Sebastian Stier
Dipl.-Phys.

Kimio Takahashi
Japanese Patent Attorney
M. Eng.

European Trademark Attorney
European Design Attorney

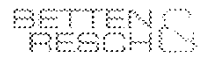
Dott. Isabella Peiker-Giannotti
Consulente in Marchi

BETTEN & RESCH
Patent- und Rechtsanwälte
PartGmbH
AG München PR 1377

Maximiliansplatz 14
80333 München
Deutschland

T +49(0)89-242417-0
F +49(0)89-2607896

mail@bettenresch.com
www.bettenresch.com



EP Application No.	EP Publication No.	Title	Our Ref.
06755686.0	1899884	METHODS AND APPARATUS FOR DEALING WITH MALWARE	SGR 140 WO/EP
13167436.8	2629232	METHODS AND APPARATUS FOR DEALING WITH MALWARE	SGR 140 WO/EP DIV1
13167434.3	2629231	METHODS AND APPARATUS FOR DEALING WITH MALWARE	SGR 140 WO/EP DIV2
16161075.3	3067801	SYSTEMS AND METHODS FOR AUTOMATIC SYNCHRONIZATION OF RECENTLY MODIFIED DATA	SGR 139 EP DIV1
14161847.0	2750071	METHODS AND APPARATUS FOR DEALING WITH MALWARE	SGR 137 EP DIV2
14850450.9	3053046	NETWORK INTRUSION DETECTION	SGR 138 WO/EP
17185908.5	3282670	MAINTAINING DATA SECURITY IN A NETWORK DEVICE	SGR 136 EP
14161844.7	2750070	METHODS AND APPARATUS FOR DEALING WITH MALWARE	SGR 137 EP DIV1



European Patent Office
80298 MUNICH
GERMANY

Questions about this communication ?

Contact Customer Services at www.epo.org/contact



Betten & Resch
Patent- und Rechtsanwälte PartGmbH
Maximiliansplatz 14
80333 München
ALLEMAGNE

Date
24.04.20

Reference	Application No./Patent No. 13167436.8 - 1213 / 2629232
Applicant/Proprietor Webroot Inc.	

Communication of amended entries concerning the representative (R. 143(1)(h) EPC)

As requested, for the above-mentioned European patent application / European patent the entries concerning the representative have been amended as follows:

Betten & Resch
Patent- und Rechtsanwälte PartGmbH
Maximiliansplatz 14
80333 München
DE

The amendment will be recorded in the Register of European Patents.

Important note for EPO deposit account holders

If you would like to have fee refunds credited to a deposit account held with the EPO, you should ensure that you provide clear and up-to-date refund instructions to this effect, using one of the permitted electronic means of filing (see Arrangements for deposit accounts).

For the Examining Division





Letter accompanying subsequently filed items

Representative:

Grünecker Patent- und Rechtsanwälte PartG mbB
72
Leopoldstrasse 4
80802 München
Germany

Phone: +49 89 21 23 50
Fax: +49 89 22 02 87
E-mail: info@grunecker.de

80298 Munich
Germany
Tel. +49(0)89 2399-0 | Fax -4465

P.O. Box 5818
2280 HV Rijswijk
Netherlands
Tel. +31(0)70 340-2040 | Fax -3016

10958 Berlin
Germany
Tel. +49(0)30 25901-0 | Fax -840

The document(s) listed below is (are) subsequently filed documents pertaining to the following application:

Application number

06755686.0

Applicant's or representative's reference

EP106738-EH

	Description of document	Original file name	Assigned file name
1	Document concerning representation	EP106738-EH.pdf	FREP-1.pdf

	Payment	
1	Method of payment	Not specified

Signatures

Place: **Munich**

Date: **20 April 2020**

Signed by: **Michael Heise 38571**

Association: **Grünecker Patent- und Rechtsanwälte PartG mbB**

Representative name: **Michael Heise**

Capacity: **(Representative)**

EP106738-EH

European Patent Office
Bob-van-Benthem-Platz 1
80469 München

Ihr Zeichen / Your Ref.

Unser Zeichen / Our Ref.

Datum / Date

April 20, 2020

We herewith withdraw from representation of the following European patent applications of Webroot Inc.:

13 745 954.1	EP106737
06 755 686.0	EP106738
13 167 436.8	EP106738I
13 167 434.3	EP106738II
14 161 844.7	EP106743I
14 161 847.0	EP106743II
14 850 450.9	EP109630
05 807 741.3	EP119684

Please direct any further correspondence to:

Betten & Resch Patent- und Rechtsanwälte PartGmbH
Attn: Dirk C. Sieckmann
Maximiliansplatz 14, 80333 Munich
Telephone: +49 89 24 24 170
Fax: +49 89 26 07 896
E-Mail: d.sieckmann@bettenpat.com

M. Heise

Grünecker Patent- und Rechtsanwälte PartG mbB

Leopoldstr. 4 Tel. +49 (0) 89 21 23 50
80802 München Fax +49 (0) 89 22 02 87
Germany Mail info@grunecker.de

Amtsgericht: München
Partnerschaftsregister:
PR 1397

Deutsche Bank München
SWIFT / BIC-code: DEUT DE MM
IBAN: DE 47 7007 0010 0175 173400

¹ auch/also: Mediator ² auch/also: Agente de la Propiedad Industrial (España) ³ auch/also: Consulente in Brevetti (Italia)

⁴ European Patent Attorney and UK Chartered Patent Attorney ⁵ Professor an der Fachhochschule für angewandtes Management

⁶ auch/also: Attorney-at-Law, New York ⁷ in Kooperation/in cooperation

MÜNCHEN

Patentanwälte European Patent Attorneys

Thomas Schuster
Dr. Klara Goldbach
Martin Aulenanger, LL.M., MM¹
Dr. Heike Vogelsang-Wenke
Reinhard Knauer
Dietmar Kuhl
Dr. Franz-Josef Zimmer
Bettina K. Reichelt
Dr. Anton K. Pfau
Dr. Udo Weigelt, LL.M.
Rainer Bertram
Jens C. Koch, M.S. (U of PA)
Bernd Rothaemel
Thomas W. Laubenthal, LL.M.
Dr. Andreas Kayser
Dr. Jens Hammer
Dr. Thomas Eickelkamp
Dr. Peter Miltényi²
Dr. Moritz Hoffe, LL.M.
Gero Maatz-Jansen
Michael Heise
Christian Meisinger
Dr. Martin Ahr
Dr. Wolfgang Neubeck
Steven M. Zeman, Ph.D.
André Nickel
Felix Kahr
Dr. Alexander Stumvoll, LL.M.
Dr. Stefano Marchini³
Dr. Thomas Kronberger
Yilin Jin
Dr. Georg Seisenberger
Dr. Olivia Nemethova, LL.M.
Dr. Rainer Plaggenborg
Victor Lopes Aguiar
Dr. Sabine Koch
Wolfram Thomas
Dr. Markus Grammel
Dr. Jegannath Korukottu⁴
Matthias Knapp

Rechtsanwälte Attorneys-at-Law

Dr. Ulrich Blumenröder, LL.M.
Prof. Dr. Maximilian Kinkeldey, LL.M.⁵
Dr. Karsten Brandt
Anja Franke, LL.M.
Ute Stephani
Dr. Bernd Alekotte, LL.M.⁶
Dr. Elvira Bertram, LL.M.
Babett Ertle
Christine Neuhierl
Sabine Brandstätter
Cornelia Schmitt
Petra Lübke
Dr. Holger Gauss
Dr. Nicolás Schmitz
Marina Schlumberger
Kirsten Hammerstingl
Sebastian Clotten, LL.M.
Jennifer Rosenhäger, LL.M.
Mark Peters, LL.M.
Dr. Nicola Busch
Julia Bittner, LL.M.
Sebastian Ochs
Philipp Strommer
Jan Rether
Karin Lochner
Swetlana Frese
Jantje Agena, LL.M.

BERLIN

Patentanwälte European Patent Attorneys

Dr. Patrick P. Erk, M.S. (MIT)
Tino Rumpold

KÖLN

Patentanwälte European Patent Attorneys

Dr. Martin Dropmann
Dr. Martin Bierbaum

PARIS⁷

Conseil en Propriété Industrielle
European Patent Attorney
Dr. Wolfgang Neubeck

OF COUNSEL

Patentanwälte European Patent Attorneys

Gottfried Kiltzsch
Rechtsanwälte
Attorneys-at-Law
Dr. Helmut Eichmann
Gerhard Barth



**Beschwerdekammern
Boards of Appeal
Chambres de recours**

Boards of Appeal of the
European Patent Office
Richard-Reitzner-Allee 8
85540 Haar
GERMANY
Tel. +49 (0)89 2399-0
Fax +49 (0)89 2399-4465

Appeal number:

T3292/19-3.5.06

Order

1. In accordance with the business distribution scheme of the Technical Boards of Appeal, the following shall hear the above appeal:

Chairman: M. Müller

technically qualified member: A. Teale

as legally qualified member: B. Müller

In the case of an extended Board:

technically qualified member: _____

as legally qualified member: _____

2. The rapporteur shall be: A. Teale

3. The additional rapporteur shall be: _____

4. Back to the Registry for further action.

Munich, 16.01.20

The Chairman: Martin Müller





**Beschwerdekammern
Boards of Appeal
Chambres de recours**

Boards of Appeal of the
European Patent Office
Richard-Reitzner-Allee 8
85540 Haar
GERMANY
Tel. +49 (0)89 2399-0
Fax +49 (0)89 2399-4465



Grünecker Patent- und Rechtsanwälte
PartG mbB
Leopoldstraße 4
80802 München
ALLEMAGNE

Datum/Date
07.01.20

Zeichen/Reference/Référence EP1067381EHmf1	APPR	Anmeldung Nr./Application No./Demande n°/Patent Nr./Patent No./Brevet n° 13167436.8 / 2629232
Anmelder/Applicant/Demandeur/Patentinhaber/Proprietor/Titulaire Webroot Inc.		

File number: **T3292/19-3.5.06**

Commencement of proceedings before the Board of Appeal

The letter dated 04.10.19 filed by the applicant
against the decision of the European Patent Office of 25.07.19
has been referred to Board of Appeal 3506.

The reference number is mentioned above.

Any further communications should be addressed to the Boards of Appeal of the European
Patent Office and should quote this reference number.

The Registrar L. Stridde
Tel.: 089 / 2399 - 3561



Annex:
Registered letter

GRÜNECKER

PATENT- UND RECHTSANWÄLTE

Grünecker PartG mbB Leopoldstr. 4 80802 München Germany

European Patent Office
Bob-van-Benthem-Platz 1
80469 München

Ihr Zeichen / Your Ref.

Unser Zeichen / Our Ref.

Datum / Date

EP1067381-EHswa

December 4, 2019

European Patent Application No. 13 167 436.8
Applicant: WEBROOT INC.

Further to the appeal filed on October 4, 2019, against the decision of July 25, 2019, herewith submitted is a statement setting out the grounds of appeal.

The Main Request and the Auxiliary Requests subject to the decision under appeal and as identified in the decision are maintained.

It is accordingly requested to set the decision aside and to grant a European patent on basis of either the Main Request or one of the Auxiliary Requests on file. As a further Auxiliary Request, oral proceedings in front of the Board of Appeal are requested.

I. Main Request

The Main Request has been refused for reasons of non-compliance with Articles 76(1), 84, 83 and 56 EPC. These objections and findings from the Examining Division are considered to be incorrect, for the following reasons.

Article 76(1) EPC

As reasoned under **section 1** of the decision, the step of searching the database of claim 1 of the Main Request is considered to be not directly and unambiguously derivable from the parent application as originally filed. This is incorrect, for the reasons as also submitted during the oral proceedings before

Grünecker Patent- und Rechtsanwälte PartG mbB

Leopoldstr. 4 Tel. +49 (0) 89 21 23 50
80802 München Fax +49 (0) 89 22 02 87
Germany Mail info@gruenecker.de PR 1387

Amtesgericht: München Deutscher Bank München
Partnerschaftsregister: SWIFT / BIC-code: DEUT DE MM
IBAN: DE 47 7007 0010 0175 173400

¹ auch/also: Mediator ² auch/also: Agente de la Propriété Industrielle (Espagne) ³ auch/also: Consulente in Brevetti (Italia)

⁴ European Patent Attorney and UK Chartered Patent Attorney ⁵ Professor an der Fachhochschule für angewandtes Management

⁶ auch/also: Attorneys-at-Law New York City ⁷ in Kooperation/In cooperation

MÜNCHEN

Patentanwälte
European Patent Attorneys
Thomas Schuster
Dr. Klara Goldbach
Martin Aufenanger, LL.M., MM.
Dr. Helke Vogelbein-Wenke
Reinhard Knauer
Dietmar Kuhl
Dr. Franz-Josef Zimmer
Bettina K. Helchelt
Dr. Anton K. Pfau
Dr. Udo Weigelt, LL.M.
Rainer Bertram
Jens C. Koch, M.S. (U of PA)
Bernd Hothaemel
Thomas W. Laubenthal, LL.M.
Dr. Andreas Kayser
Dr. Jens Hammer
Dr. Thomas Cickelkamp
Dr. Peter Millényi
Dr. Moritz Hölff, LL.M.
Gero Maatz-Jensen
Michael Helgo
Christian Melinger
Dr. Martin Ahr
Dr. Wolfgang Neubeck
Steven M. Zeman, Ph.D.
André Nickel
Felix Kair
Dr. Alexander Sturmvoß, LL.M.
Dr. Stefano Marchini
Dr. Thomas Kronberger
Yilin Jin
Dr. Georg Seisenberger
Dr. Oliver Nemethovs, LL.M.
Dr. Rainer Pluggenberg
Victor Lopes Aguiar
Dr. Sabino Koch
Wolfram Thomas
Dr. Markus Grammel
Dr. Jagannath Korukottu

Rechtsanwälte

Attorneys-at-Law
Dr. Ulrich Blumenröder, LL.M.
Prof. Dr. Maximilian Kinkeldey, LL.M.
Dr. Karsten Brandt
Anja Franke, LL.M.
Ute Stephani
Dr. Bernd Allekotte, LL.M.
Dr. Elvira Bertram, LL.M.
Babett Erle
Christine Naehler
Sabine Brandstätter
Cornelia Schmitt
Petra Lübke
Dr. Holger Geuss
Dr. Nicola Schmitz
Marina Schlumberger
Kirsten Hammerstingl
Sebastian Clatten, LL.M.
Jennifer Rosenhäger, LL.M.
Mark Peters, LL.M.
Dr. Nicola Busch
Julia Bittner, LL.M.
Sebastian Ochs
Philipp Strommer
Jan Hether
Karin Lochner
Svetlana Fresco

BERLIN

Patentanwälte
European Patent Attorneys
Dr. Patrick P. Erk, M.S. (MIT)
Ino Humpold

KÖLN

Patentanwälte
European Patent Attorneys
Dr. Martin Drogmann
Dr. Martin Blerbaum

PARIS⁷

Conseil en Propriété Industrielle
European Patent Attorney
Dr. Wolfgang Naubeck

OF COUNSEL

Patentanwälte
European Patent Attorneys
Gottfried Klitzsch

Rechtsanwälte

Attorneys-at-Law
Dr. Holmut Eichmann
Gerhard Barth

the Examining Division and as summarized in the decision and in the official minutes of the oral proceedings.

Specifically, this searching step is unambiguously derivable from the embodiment disclosed in the description as originally filed on page 36, line 15 through page 39, line 2. As part of this disclosure, it is disclosed on page 37, lines 15 to 25, that the database can be searched for computers having the same or a similar combination of security products as a specific computer. It is also disclosed on page 37 that the database is provided of details of processes that run by every computer of the system. On the first paragraph of page 38, a specific example is then provided for this embodiment in which "the database knows that a computer" had a specific combination of security products (combination of A to G) but was unable to detect a particular malware process P. According to this example of the embodiment, the user of a computer having the same particular combination of security products will be provided with information that his computer is vulnerable to the particular malware process P so that the user can take respective actions such as download and install software to remove the risk. This example is then again summarized by the last paragraph on page 38, repeating the example from above. Here, it is expressly summarized that the database is provided with information relating to all the security products and that this database is then searched for events or processes marked as bad, that occurred on computers with that particular mix of security products, and that were not locally detected. This summary in the last paragraph of page 38 thereby unambiguously repeats what is already disclosed by pages 36 and 37 and the specific example on page 38.

Consequently, it is directly and unambiguously disclosed that the database is searched to identify processes marked as being bad / being malware that occurred on computers having the same particular combination of security products as a first computer and that were not locally detected, as almost literally disclosed by the last paragraph on page 38, and also by the example given at the beginning of page 38 as originally filed.

The Examining Division states that the example on top of page 38 would not disclose searching the database. This position is to be rejected, already because any database storing information will be searched for that information. The literal wording "the database knows that a computer..." in lines 1 and 2 of page 38 thereby unambiguously and necessarily implies a searching of that database, because that is the only way a database can "know." However, the feature of searching the database is also literally disclosed on

page 37, lines 15 to 19, as well as on page 38, lines 25 to 30, both sections consistently and explicitly disclosing the searching of the database for the purpose claimed.

The Examining Division further argues that the last paragraph on page 38 would not disclose the searching for (events or) processes marked as bad, but only for "events for processes" marked as being bad. Even though this complies with the literal wording of page 38, line 28, it is respectfully submitted that a person skilled in the art directly and unambiguously understands that this is a mere typographical error in that the "events for processes" is meant to be "events or processes." This is also consistent with the marking of events or processes as bad as is disclosed elsewhere in the description (for example, as disclosed on page 23, lines 14 to 16, or on page 18, lines 21 to 25, of the parent application as originally filed), as well in light of the remainder of the specific embodiment of pages 36 to 39, consistently referring to processes as being malware/bad (as also disclosed elsewhere in the description, for example on page 39, lines 29 to 33 as filed).

For these reasons, the step of searching the database as included in claim 1 of the Main Request is directly and unambiguously derivable from the application as originally filed and complies with the requirements of Article 76(1) and 123(2) EPC. The same applies to the respective feature in corresponding apparatus claim 3 of the Main Request.

Clarity / Sufficiency of Disclosure

The Examining Division argues under section 2, specifically **items 2.1 and 2.3** of the decision under appeal, that the feature of searching the database to identify any processes marked as being malware that occurred on computers having the same particular combination of security products as the first remote computer and that were not locally detected, would be both unclear and insufficiently disclosed, contrary to the requirements of Articles 84 and 83 EPC. This presumption and conclusion from the Examining Division is incorrect, at least for the following reasons.

The Examining Division's clarity and insufficient disclosure objections against the feature of identifying a process marked as being malware in the searching step of claim 1 seems to be based on the central argument of the Examining Division that the "origin of the marking of processes as being malware is undefined" (see line 1 of item 2.1 of the decision). The Examining Division argues in the decision and during the oral proceedings that because the particular combination of security products of the first remote computer could not locally detect the process, it would be unclear and insufficiently disclosed how

the process can then "otherwise" be marked as malware. This position of the Examining Division has to be rejected as clearly unreasonable and against the common understanding of a skilled person within the field of the present invention. Certainly, it occurs repeatedly nowadays and at the priority date of the present application that security products on remote computers cannot identify a certain malicious process as being malware. This, for example, becomes eventually known when the computer becomes infected with a virus i.e. the malware process and behaves abnormally, which means that the malware was obviously not locally detected by the security products on that computer. Once the virus is identified, it will also be known that the particular security products on that remote computer were obviously unable to detect that malware process. Thus, it can be reported to the central database that the particular combination of security products was unable to detect the malware process, i.e., a process being marked as bad/malware. Since this particular malware process will not be on every other remote computer in the system but potentially could arrive at any computer, it is the idea of the claimed invention to inform those other remote computers that have the same combination of security products of this potential vulnerability, namely that their combination of security products is unable to detect the specific malware process.

It cannot be seen how this teaching is unclear to a skilled person, nor that it is necessary to understand "who, when or how the process is being marked as malware" as questioned under **item 2.1** of the decision under appeal. Of course, a malware process will be identified as a malware process, at last when it behaves maliciously on a computer. Naturally, another obvious situation to identify a process as malware is that another combination of security products, or another version of a specific security product, identifies the process as being malware, so that then the process will be marked as being bad. Since the specific combination of security products, as well as the processes running on the plurality of remote computers are reported to the database, the database can also identify other computers having the same combination of security products as one specific ("first") remote computer when that remote computer was infected by a malicious process, but that first remote computer was unable to identify that malicious process. It is, however, neither unclear nor essential for the understanding of the claimed invention how, by whom or when a specific process was detected as being malware and, accordingly, marked as malware (which is a common feature and even the application discloses several means to identify processes as being malware).

Under item 2.2 of the decision, the Examining Division further argues that the database receives "only" the information about the security products loaded on the computers and the details of processes run by said computers. Based on this presumption that only these two kinds of information are received by the database, the Examining Division concludes that it is unclear and insufficiently disclosed which process can be considered to be "a process not locally detected". This understanding is also incorrect for the following reasons. Firstly, it is incorrect that claim 1 requires that only the information about the security products and the details of processes run by the computers is received by the database. Instead, claim 1 positively defines that the database receives the information on the security products loaded or available on the other remote computers, as well as the details of the processes run by the plurality of computers.

In addition, claim 1 defines that the database is searched to identify those processes marked as being malware that did occur on computers having the same combination of security products as a first remote computer and that was not locally detected. This clearly defines that processes are to be marked as malware and it is further expressly defined that these processes marked as being malware "occurred on computers". Thus, it is clear to a skilled person that this feature can be implemented in that upon occurrence of a detected malware process on a computer of the system, respective information is provided to the database informing the database of the particular process being malware. This is both clear and sufficiently enabled for a person skilled in the art to implement the features claimed by claim 1, specifically, with regard to the processes being marked as malware that occur on computers. In addition, claim 1 defines that these malware processes not only occurred on computers, but it is expressly defined that these processes occurred on computers having the same particular combination of security products that were not able to locally detect the process as malware. Thus, if a malware process occurred on some computer, not only the information that the particular process is malware is provided to the database, but also that the combination of security products of that computer was unable to locally detect the process as being malware (otherwise and logically, the computer would not have allowed the process to occur). Thus, it is clear to a skilled person without undue burden that upon the occurrence of a malware process on a particular computer, information is provided to the database of that particular malware process, as well as the combination of security products on that affected computer that was unable to detect the process as malware (so that the database can then be searched for processes as defined by the searching step of claim 1.) Based on

the features of claim 1, this understanding is readily and apparent to a skilled person and is complete for the skilled person to carry out the claimed invention.

For these reasons, the subject matter of the claims of the Main Request complies with the requirements of Articles 84 and 83 EPC, contrary to the findings under section 2 of the decision under appeal.

Moreover, it is noted that the Examiner's objections under section 2 are in contradiction to the Examining Division's arguments under Article 56 EPC, wherein the Examining Division argues that the very features considered to be unclear and insufficiently disclosed would allegedly be already known from document D1. If, however, already known from document D1, these features cannot be insufficiently enabled for a skilled person to carry out that feature of the claimed invention.

Inventive Step

Under **section 3** of the decision under appeal, the Examining Division confirms that the "search of the database is performed in a different way," but disregards this conceptual difference due to the objections under Articles 76, 84 and 83 EPC. As discussed above, since these objections are unjustified, the distinctions have to be considered for assessing the requirements of Article 56 EPC and, in fact, lead to the presence of an inventive step, as will be discussed below. For completeness, it is also noted that the feature analysis of claim 1 with regard to document D1 under section 3 of the decision is also incorrect, as will also be discussed below.

Secondly, the Examining Division argues that the feature of providing information to the user would be a mere presentation of information and, therefore, cannot lead to an inventive step. This understanding, however, is respectfully rejected, because the feature of providing information to the user of the first remote computer as defined in claim 1 is not a mere presentation of information, but, in fact, has a technical effect on the claimed system.

Specifically, claim 1 not only presents information to a user, but additionally provides for a technical effect, which is to "increase the computer's effective security" as literally stated on description page 39, line 2. This increased security is achieved by the novel manner how the database can identify processes that are malware which the particular remote computer could not identify locally as malware. This identification of potential malware is

novel over the malware detection process of D1. Even if the result of the malware detection is only presented to the user the system security is nonetheless improved, because the user, (i.e. the users of the multiple computers of the system!), can be expected to take respective actions or measures once she/he becomes aware of a potential malware. Even if one particular user would not react to such information, as soon as some users do, the security of the system has been improved. This, together with the different approach in identifying potential malware compared to the cited prior art leads to an inventive step as further discussed below.

In addition, the following arguments show that the claimed subject matter and, specifically, their differences over closest prior art document D1 lead to the presence of an inventive step within the meaning of Article 56 EPC, contrary to the conclusion under section 3 of the decision.

As discussed in **section 3** of the decision, paragraphs [0025] and [0030] of D1 would be the closest available prior art to the claimed invention. However, this teaching of D1 is conceptually different than the claimed invention according to claims 1 and 3.

According to D1, a policy organizing server 32 receives status information from various computers indicating the malware scanning products used, the scanner engine versions and the virus definition data versions (see [0025] of D1). This status information is used by server 32 only to be able to determine whether each computer within the network runs out-of-date malware products and out-of-date malware definition data and which computers run the most up-to-date versions. The reason and motivation for this determination in D1 is to eventually instruct those computers that are out-of-date to perform an updating of its malware definition data. Specifically, if the server of D1 receives messages from computers concerning a particular malware and if all messages originate from up-to-date computers only, the server instructs all other computers that are out-of-date to update their malware definition data.

While this solution of D1 certainly also provides a concept of improving malware protection of remote computers, the claimed invention according to new claims 1 and 3 does not use or implement such a suggested concept of a forced updating of out-of-date computers.

Instead, the claimed invention suggests a conceptually different concept that does not require that all computers must update to the same up-to-date malware definition data.

According to new claim 1, remote computers provide not only information of all or selected security products on the remote computer, but also details of processes that run on the remote computer. In addition – since this information is stored in the database – remote computers having the same particular combination of security products as a specific (i.e. first) one of the remote computers can be identified. This is already different and non-obvious from D1, because the out-of-date computers (that are eventually forced to be updated) have a different particular combination of security products than the up-to-date computers that sent the malware messages concerning a malware process to the server 32 in D1.

As a further distinction—instead of forcing a specific out-of-date computer to change/update its “security products” to the different up-to-date security products if a particular malware was detected by other computers with such different i.e. up-to-date security products, as in D1—the claimed invention then identifies those processes that are malware and occurred on computers having the same particular combination of security products but were not locally detected. Thus, instead of forcing an updating of the out-of-date security products of a first remote computer to those of other up-to-date computers as suggested by D1, the user of the first remote computer is provided with the information of identified processes that are marked as malware but were not locally detected by other computers having the same combination of security products as the first computer.

These are two alternative, incompatible solutions for increasing the protection of local computers from malware. The solution of D1 (changing the settings of security products to that of other computers with different security products that have detected a malware process) neither implies nor suggests the alternative solution of the claimed invention (informing a computer of non-detected malware processes that were not detected by other computers with the same security products).

Consequently, the claimed subject matter does not arise from the available prior art in an obvious manner without applying hindsight knowledge from the present application, but involves an inventive step within the meaning of Article 56 EPC.

Summary

In view of the above, all grounds for the refusal against the Main Request are unjustified, and the claims of the Main Request comply with the requirements of the EPC.

II. Auxiliary Request 1

Auxiliary Request 1 subject to the decision under appeal is maintained.

Auxiliary Request 1 has been rejected, because the amendment to the Main Request of adding the feature that the details (of processes run by each of the remote computers) comprise whether or not a process has been detected as malware, would not be directly and unambiguously derivable from the application as originally filed. This conclusion of the Examining Division is incorrect.

The feature and amendment can be unambiguously derivable from the passages identified by footnotes in the marked-up copy of Auxiliary Request 1 dated May 31, 2019. Specifically, page 37, lines 21 to 24, discloses that the database is provided with details of processes run by every computer and, thus, knows whether or not a process has been detected by each computer. Within the context of the claimed invention and the technical purpose of the malware detection mechanisms disclosed, it is directly and unambiguously derivable for a skilled person that this detection referred to on page 37, lines 21 to 24, within the context of that embodiment can only mean that the process is detected as being malware. Moreover, this passage, in combination with the disclosure on page 38 of the description, clearly and unambiguously discloses that the database is provided with information of whether a particular malware process was detected by a (combination of security products on) a remote computer, because exactly that information is searched for in the database.

Therefore, the feature added to Auxiliary Request 1 (compared to the Main Request) is directly and unambiguously derivable from the application as filed, contrary to the findings under **item 4.1** of the decision.

Otherwise, the same arguments apply to Auxiliary Request 1 as those provided above with regard to the Main Request.

In addition, the added clarification further addresses the objection under Articles 84 and 83 EPC raised with regard to the Main Request and emphasizes the inventive technical contribution of the claimed invention over the available prior art.

III. Auxiliary Request 2

Auxiliary Request 2 subject to the decision under appeal is maintained.

Auxiliary Request 2 has been rejected by the decision for the reason that the added amendments to the providing step of claim 1 (and, accordingly, to the feature of providing information to the user of corresponding claim 3) would be an undisclosed generalization of the disclosure given in the description, specifically on page 38, lines 15 to 23.

This objection is considered to be unjustified. As correctly noted, this amendment is based on and derivable from description page 38, lines 15 to 23, as originally filed. The Examining Division merely states in the decision that this passage would disclose a "specific example" that would not allow for the alleged generalization in the amended feature, without providing further explanations or reasons in this respect. However, page 38, lines 15 to 23, concerns the "simple example" (see line 1 of page 38) that illustrates the embodiment by referring to an example. The specifically mentioned Sobig virus is thereby clearly understood by a skilled person as an example of a general malware process referred to in the description of this embodiment of the present invention. It is also readily apparent that the specific example or type of malware process is entirely unessential for the claimed invention, so that the type of malware process being a Sobig virus is non-essential for the disclosed invention.

Consequently, the amendments added to Auxiliary Request 2 (as compared to the Main Request) are not an undisclosed generalization, because no essential features are omitted from the disclosure given on page 38 as identified above.

Otherwise, the same arguments provided above with regard to the Main Request also apply to Auxiliary Request 2.

The added features of providing information to the user when the security products expose the remote computer to a risk of being infected and offering software to download and install to remove the risk further emphasizes on the technical effect of increasing the system security as discussed above with regard to the requirements of Article 56 EPC of the Main Request.

IV. Auxiliary Request 3

Auxiliary Request 3 subject to the decision under appeal is maintained.

Since Auxiliary Request 3 is an exact combination of Auxiliary Requests 1 and 2, the same arguments as provided above apply to Auxiliary Request 3.

As a further Auxiliary Request, oral proceedings before the Board of Appeal are requested.



M. Heise

European Patent Office
Bob-van-Benthen-Platz 1
80469 München

EPO - Munich
101
04. Dez. 2019

Ihr Zeichen / Your Ref.

Unser Zeichen / Our Ref.

Datum / Date

EP106738I-EHswa

December 4, 2019

European Patent Application No. 13 167 436.8
Applicant: WEBROOT INC.

Further to the appeal filed on October 4, 2019, against the decision of July 25, 2019, herewith submitted is a statement setting out the grounds of appeal.

The Main Request and the Auxiliary Requests subject to the decision under appeal and as identified in the decision are maintained.

It is accordingly requested to set the decision aside and to grant a European patent on basis of either the Main Request or one of the Auxiliary Requests on file. As a further Auxiliary Request, oral proceedings in front of the Board of Appeal are requested.

I. Main Request

The Main Request has been refused for reasons of non-compliance with Articles 76(1), 84, 83 and 56 EPC. These objections and findings from the Examining Division are considered to be incorrect, for the following reasons.

Article 76(1) EPC

As reasoned under **section 1** of the decision, the step of searching the database of claim 1 of the Main Request is considered to be not directly and unambiguously derivable from the parent application as originally filed. This is incorrect, for the reasons as also submitted during the oral proceedings before

MÜNCHEN

Patentanwälte
European Patent Attorneys
Thomas Schuster
Dr. Klara Goldbach
Martin Aufenanger, LL.M., MM.¹
Dr. Heike Vogelsang-Wenke
Reinhard Knauer
Dietmar Kuhl
Dr. Franz-Josef Zimmer
Bettina K. Reichelt
Dr. Anton K. Pfau
Dr. Udo Weigelt, LL.M.
Rainer Bertram
Jens C. Koch, M.S. (U of PA)
Bernd Rothaemel
Thomas W. Laubenthal, LL.M.
Dr. Andreas Kayser
Dr. Jens Hammer
Dr. Thomas Eickelkamp
Dr. Peter Miltényi²
Dr. Moritz Höffe, LL.M.
Gero Maatz-Jansen
Michael Heise
Christian Meisinger
Dr. Martin Ahr
Dr. Wolfgang Neubeck
Steven M. Zeman, Ph.D.
André Nickel
Felix Kahr
Dr. Alexander Stumvoll, LL.M.
Dr. Stefano Marchini³
Dr. Thomas Kronberger
Yilin Jin
Dr. Georg Seisenberger
Dr. Olivia Nemethova, LL.M.
Dr. Rainer Plaggenborg
Victor Lopes Aguiar
Dr. Sabine Koch
Wolfram Thomas
Dr. Markus Grammel
Dr. Jegannath Korukottu⁴

Rechtsanwälte **Attorneys-at-Law**

Dr. Ulrich Blumenröder, LL.M.
Prof. Dr. Maximilian Kinkeldey, LL.M.⁵
Dr. Karsten Brandt
Anja Franke, LL.M.
Ute Stephani
Dr. Bernd Allekotte, LL.M.⁶
Dr. Elvira Bertram, LL.M.
Babett Ertle
Christine Neuhierl
Sabine Brandstätter
Cornelia Schmitt
Petra Lübke
Dr. Holger Gauss
Dr. Nicolás Schmitz
Marina Schlumberger
Kirsten Hammerstingl
Sebastian Clotten, LL.M.
Jennifer Rosenhäger, LL.M.
Mark Peters, LL.M.
Dr. Nicola Busch
Julia Bittner, LL.M.
Sebastian Ochs
Philipp Strommer
Jan Rether
Karin Lochner
Swetlana Frese

BERLIN

Patentanwälte
European Patent Attorneys
Dr. Patrick P. Erk, M.S. (MIT)
Tino Rumpold

KÖLN

Patentanwälte
European Patent Attorneys
Dr. Martin Drophmann
Dr. Martin Bierbaum

PARIS⁷

Conseil en Propriété Industrielle
European Patent Attorney
Dr. Wolfgang Neubeck

OF COUNSEL

Patentanwälte
European Patent Attorneys
Gottfried Klitzsch

Rechtsanwälte
Attorneys-at-Law
Dr. Helmut Eichmann
Gerhard Barth

Grünecker Patent- und Rechtsanwälte PartG mbB

Leopoldstr. 4 Tel. +49 (0) 89 21 23 50
80802 München Fax +49 (0) 89 22 02 87
Germany Mail info@grunecker.de

Amtsgericht: München
Partnerschaftsregister:
PR 1397

Deutsche Bank München
SWIFT / BIC-code: DEUT DE MM
IBAN: DE 47 7007 0010 0175 173400

¹ auch/also: Mediator ² auch/also: Agente de la Propiedad Industrial (España) ³ auch/also: Consulente in Brevetti (Italia)

⁴ European Patent Attorney and UK Chartered Patent Attorney ⁵ Professor an der Fachhochschule für angewandtes Management

⁶ auch/also: Attorney-at-Law, New York ⁷ in Kooperation/in cooperation

the Examining Division and as summarized in the decision and in the official minutes of the oral proceedings.

Specifically, this searching step is unambiguously derivable from the embodiment disclosed in the description as originally filed on page 36, line 15 through page 39, line 2. As part of this disclosure, it is disclosed on page 37, lines 15 to 25, that the database can be searched for computers having the same or a similar combination of security products as a specific computer. It is also disclosed on page 37 that the database is provided of details of processes that run by every computer of the system. On the first paragraph of page 38, a specific example is then provided for this embodiment in which "the database knows that a computer" had a specific combination of security products (combination of A to G) but was unable to detect a particular malware process P. According to this example of the embodiment, the user of a computer having the same particular combination of security products will be provided with information that his computer is vulnerable to the particular malware process P so that the user can take respective actions such as download and install software to remove the risk. This example is then again summarized by the last paragraph on page 38, repeating the example from above. Here, it is expressly summarized that the database is provided with information relating to all the security products and that this database is then searched for events or processes marked as bad, that occurred on computers with that particular mix of security products, and that were not locally detected. This summary in the last paragraph of page 38 thereby unambiguously repeats what is already disclosed by pages 36 and 37 and the specific example on page 38.

Consequently, it is directly and unambiguously disclosed that the database is searched to identify processes marked as being bad / being malware that occurred on computers having the same particular combination of security products as a first computer and that were not locally detected, as almost literally disclosed by the last paragraph on page 38, and also by the example given at the beginning of page 38 as originally filed.

The Examining Division states that the example on top of page 38 would not disclose searching the database. This position is to be rejected, already because any database storing information will be searched for that information. The literal wording "the database knows that a computer..." in lines 1 and 2 of page 38 thereby unambiguously and necessarily implies a searching of that database, because that is the only way a database can "know." However, the feature of searching the database is also literally disclosed on

page 37, lines 15 to 19, as well as on page 38, lines 25 to 30, both sections consistently and explicitly disclosing the searching of the database for the purpose claimed.

The Examining Division further argues that the last paragraph on page 38 would not disclose the searching for (events or) processes marked as bad, but only for “events for processes” marked as being bad. Even though this complies with the literal wording of page 38, line 28, it is respectfully submitted that a person skilled in the art directly and unambiguously understands that this is a mere typographical error in that the “events for processes” is meant to be “events or processes.” This is also consistent with the marking of events or processes as bad as is disclosed elsewhere in the description (for example, as disclosed on page 23, lines 14 to 16, or on page 18, lines 21 to 25, of the parent application as originally filed), as well in light of the remainder of the specific embodiment of pages 36 to 39, consistently referring to processes as being malware/bad (as also disclosed elsewhere in the description, for example on page 39, lines 29 to 33 as filed).

For these reasons, the step of searching the database as included in claim 1 of the Main Request is directly and unambiguously derivable from the application as originally filed and complies with the requirements of Article 76(1) and 123(2) EPC. The same applies to the respective feature in corresponding apparatus claim 3 of the Main Request.

Clarity / Sufficiency of Disclosure

The Examining Division argues under section 2, specifically **items 2.1** and **2.3** of the decision under appeal, that the feature of searching the database to identify any processes marked as being malware that occurred on computers having the same particular combination of security products as the first remote computer and that were not locally detected, would be both unclear and insufficiently disclosed, contrary to the requirements of Articles 84 and 83 EPC. This presumption and conclusion from the Examining Division is incorrect, at least for the following reasons.

The Examining Division’s clarity and insufficient disclosure objections against the feature of identifying a process marked as being malware in the searching step of claim 1 seems to be based on the central argument of the Examining Division that the “origin of the marking of processes as being malware is undefined” (see line 1 of item 2.1 of the decision). The Examining Division argues in the decision and during the oral proceedings that because the particular combination of security products of the first remote computer could not locally detect the process, it would be unclear and insufficiently disclosed how

the process can then “otherwise” be marked as malware. This position of the Examining Division has to be rejected as clearly unreasonable and against the common understanding of a skilled person within the field of the present invention. Certainly, it occurs repeatedly nowadays and at the priority date of the present application that security products on remote computers cannot identify a certain malicious process as being malware. This, for example, becomes eventually known when the computer becomes infected with a virus i.e. the malware process and behaves abnormally, which means that the malware was obviously not locally detected by the security products on that computer. Once the virus is identified, it will also be known that the particular security products on that remote computer were obviously unable to detect that malware process. Thus, it can be reported to the central database that the particular combination of security products was unable to detect the malware process, i.e., a process being marked as bad/malware. Since this particular malware process will not be on every other remote computer in the system but potentially could arrive at any computer, it is the idea of the claimed invention to inform those other remote computers that have the same combination of security products of this potential vulnerability, namely that their combination of security products is unable to detect the specific malware process.

It cannot be seen how this teaching is unclear to a skilled person, nor that it is necessary to understand “who, when or how the process is being marked as malware” as questioned under **item 2.1** of the decision under appeal. Of course, a malware process will be identified as a malware process, at last when it behaves maliciously on a computer. Naturally, another obvious situation to identify a process as malware is that another combination of security products, or another version of a specific security product, identifies the process as being malware, so that then the process will be marked as being bad. Since the specific combination of security products, as well as the processes running on the plurality of remote computers are reported to the database, the database can also identify other computers having the same combination of security products as one specific (“first”) remote computer when that remote computer was infected by a malicious process, but that first remote computer was unable to identify that malicious process. It is, however, neither unclear nor essential for the understanding of the claimed invention how, by whom or when a specific process was detected as being malware and, accordingly, marked as malware (which is a common feature and even the application discloses several means to identify processes as being malware).

Under **item 2.2** of the decision, the Examining Division further argues that the database receives “only” the information about the security products loaded on the computers and the details of processes run by said computers. Based on this presumption that only these two kinds of information are received by the database, the Examining Division concludes that it is unclear and insufficiently disclosed which process can be considered to be “a process not locally detected”. This understanding is also incorrect for the following reasons. Firstly, it is incorrect that claim 1 requires that only the information about the security products and the details of processes run by the computers is received by the database. Instead, claim 1 positively defines that the database receives the information on the security products loaded or available on the other remote computers, as well as the details of the processes run by the plurality of computers.

In addition, claim 1 defines that the database is searched to identify those processes marked as being malware that did occur on computers having the same combination of security products as a first remote computer and that was not locally detected. This clearly defines that processes are to be marked as malware and it is further expressly defined that these processes marked as being malware “occurred on computers”. Thus, it is clear to a skilled person that this feature can be implemented in that upon occurrence of a detected malware process on a computer of the system, respective information is provided to the database informing the database of the particular process being malware. This is both clear and sufficiently enabled for a person skilled in the art to implement the features claimed by claim 1, specifically, with regard to the processes being marked as malware that occur on computers. In addition, claim 1 defines that these malware processes not only occurred on computers, but it is expressly defined that these processes occurred on computers having the same particular combination of security products that were not able to locally detect the process as malware. Thus, if a malware process occurred on some computer, not only the information that the particular process is malware is provided to the database, but also that the combination of security products of that computer was unable to locally detect the process as being malware (otherwise and logically, the computer would not have allowed the process to occur). Thus, it is clear to a skilled person without undue burden that upon the occurrence of a malware process on a particular computer, information is provided to the database of that particular malware process, as well as the combination of security products on that affected computer that was unable to detect the process as malware (so that the database can then be searched for processes as defined by the searching step of claim 1.) Based on

the features of claim 1, this understanding is readily and apparent to a skilled person and is complete for the skilled person to carry out the claimed invention.

For these reasons, the subject matter of the claims of the Main Request complies with the requirements of Articles 84 and 83 EPC, contrary to the findings under section 2 of the decision under appeal.

Moreover, it is noted that the Examiner's objections under section 2 are in contradiction to the Examining Division's arguments under Article 56 EPC, wherein the Examining Division argues that the very features considered to be unclear and insufficiently disclosed would allegedly be already known from document D1. If, however, already known from document D1, these features cannot be insufficiently enabled for a skilled person to carry out that feature of the claimed invention.

Inventive Step

Under **section 3** of the decision under appeal, the Examining Division confirms that the "search of the database is performed in a different way," but disregards this conceptual difference due to the objections under Articles 76, 84 and 83 EPC. As discussed above, since these objections are unjustified, the distinctions have to be considered for assessing the requirements of Article 56 EPC and, in fact, lead to the presence of an inventive step, as will be discussed below. For completeness, it is also noted that the feature analysis of claim 1 with regard to document D1 under section 3 of the decision is also incorrect, as will also be discussed below.

Secondly, the Examining Division argues that the feature of providing information to the user would be a mere presentation of information and, therefore, cannot lead to an inventive step. This understanding, however, is respectfully rejected, because the feature of providing information to the user of the first remote computer as defined in claim 1 is not a mere presentation of information, but, in fact, has a technical effect on the claimed system.

Specifically, claim 1 not only presents information to a user, but additionally provides for a technical effect, which is to "increase the computer's effective security" as literally stated on description page 39, line 2. This increased security is achieved by the novel manner how the database can identify processes that are malware which the particular remote computer could not identify locally as malware. This identification of potential malware is

novel over the malware detection process of D1. Even if the result of the malware detection is only presented to the user the system security is nonetheless improved, because the user, (i.e. the users of the multiple computers of the system!), can be expected to take respective actions or measures once she/he becomes aware of a potential malware. Even if one particular user would not react to such information, as soon as some users do, the security of the system has been improved. This, together with the different approach in identifying potential malware compared to the cited prior art leads to an inventive step as further discussed below.

In addition, the following arguments show that the claimed subject matter and, specifically, their differences over closest prior art document D1 lead to the presence of an inventive step within the meaning of Article 56 EPC, contrary to the conclusion under section 3 of the decision.

As discussed in **section 3** of the decision, paragraphs [0025] and [0030] of D1 would be the closest available prior art to the claimed invention. However, this teaching of D1 is conceptually different than the claimed invention according to claims 1 and 3.

According to D1, a policy organizing server 32 receives status information from various computers indicating the malware scanning products used, the scanner engine versions and the virus definition data versions (see [0025] of D1). This status information is used by server 32 only to be able to determine whether each computer within the network runs out-of-date malware products and out-of-date malware definition data and which computers run the most up-to-date versions. The reason and motivation for this determination in D1 is to eventually instruct those computers that are out-of-date to perform an updating of its malware definition data. Specifically, if the server of D1 receives messages from computers concerning a particular malware and if all messages originate from up-to-date computers only, the server instructs all other computers that are out-of-date to update their malware definition data.

While this solution of D1 certainly also provides a concept of improving malware protection of remote computers, the claimed invention according to new claims 1 and 3 does not use or implement such a suggested concept of a forced updating of out-of-date computers.

Instead, the claimed invention suggests a conceptually different concept that does not require that all computers must update to the same up-to-date malware definition data.

According to new claim 1, remote computers provide not only information of all or selected security products on the remote computer, but also details of processes that run on the remote computer. In addition – since this information is stored in the database – remote computers having the same particular combination of security products as a specific (i.e. first) one of the remote computers can be identified. This is already different and non-obvious from D1, because the out-of-date computers (that are eventually forced to be updated) have a different particular combination of security products than the up-to-date computers that sent the malware messages concerning a malware process to the server 32 in D1.

As a further distinction—instead of forcing a specific out-of-date computer to change/update its “security products” to the different up-to-date security products if a particular malware was detected by other computers with such different i.e. up-to-date security products, as in D1—the claimed invention then identifies those processes that are malware and occurred on computers having the same particular combination of security products but were not locally detected. Thus, instead of forcing an updating of the out-of-date security products of a first remote computer to those of other up-to-date computers as suggested by D1, the user of the first remote computer is provided with the information of identified processes that are marked as malware but were not locally detected by other computers having the same combination of security products as the first computer.

These are two alternative, incompatible solutions for increasing the protection of local computers from malware. The solution of D1 (changing the settings of security products to that of other computers with different security products that have detected a malware process) neither implies nor suggests the alternative solution of the claimed invention (informing a computer of non-detected malware processes that were not detected by other computers with the same security products).

Consequently, the claimed subject matter does not arise from the available prior art in an obvious manner without applying hindsight knowledge from the present application, but involves an inventive step within the meaning of Article 56 EPC.

Summary

In view of the above, all grounds for the refusal against the Main Request are unjustified, and the claims of the Main Request comply with the requirements of the EPC.

II. Auxiliary Request 1

Auxiliary Request 1 subject to the decision under appeal is maintained.

Auxiliary Request 1 has been rejected, because the amendment to the Main Request of adding the feature that the details (of processes run by each of the remote computers) comprise whether or not a process has been detected as malware, would not be directly and unambiguously derivable from the application as originally filed. This conclusion of the Examining Division is incorrect.

The feature and amendment can be unambiguously derivable from the passages identified by footnotes in the marked-up copy of Auxiliary Request 1 dated May 31, 2019. Specifically, page 37, lines 21 to 24, discloses that the database is provided with details of processes run by every computer and, thus, knows whether or not a process has been detected by each computer. Within the context of the claimed invention and the technical purpose of the malware detection mechanisms disclosed, it is directly and unambiguously derivable for a skilled person that this detection referred to on page 37, lines 21 to 24, within the context of that embodiment can only mean that the process is detected as being malware. Moreover, this passage, in combination with the disclosure on page 38 of the description, clearly and unambiguously discloses that the database is provided with information of whether a particular malware process was detected by a (combination of security products on) a remote computer, because exactly that information is searched for in the database.

Therefore, the feature added to Auxiliary Request 1 (compared to the Main Request) is directly and unambiguously derivable from the application as filed, contrary to the findings under **item 4.1** of the decision.

Otherwise, the same arguments apply to Auxiliary Request 1 as those provided above with regard to the Main Request.

In addition, the added clarification further addresses the objection under Articles 84 and 83 EPC raised with regard to the Main Request and emphasizes the inventive technical contribution of the claimed invention over the available prior art.

III. Auxiliary Request 2

Auxiliary Request 2 subject to the decision under appeal is maintained.

Auxiliary Request 2 has been rejected by the decision for the reason that the added amendments to the providing step of claim 1 (and, accordingly, to the feature of providing information to the user of corresponding claim 3) would be an undisclosed generalization of the disclosure given in the description, specifically on page 38, lines 15 to 23.

This objection is considered to be unjustified. As correctly noted, this amendment is based on and derivable from description page 38, lines 15 to 23, as originally filed. The Examining Division merely states in the decision that this passage would disclose a "specific example" that would not allow for the alleged generalization in the amended feature, without providing further explanations or reasons in this respect. However, page 38, lines 15 to 23, concerns the "simple example" (see line 1 of page 38) that illustrates the embodiment by referring to an example. The specifically mentioned Sobig virus is thereby clearly understood by a skilled person as an example of a general malware process referred to in the description of this embodiment of the present invention. It is also readily apparent that the specific example or type of malware process is entirely unessential for the claimed invention, so that the type of malware process being a Sobig virus is non-essential for the disclosed invention.

Consequently, the amendments added to Auxiliary Request 2 (as compared to the Main Request) are not an undisclosed generalization, because no essential features are omitted from the disclosure given on page 38 as identified above.

Otherwise, the same arguments provided above with regard to the Main Request also apply to Auxiliary Request 2.

The added features of providing information to the user when the security products expose the remote computer to a risk of being infected and offering software to download and install to remove the risk further emphasizes on the technical effect of increasing the system security as discussed above with regard to the requirements of Article 56 EPC of the Main Request.

IV. Auxiliary Request 3

Auxiliary Request 3 subject to the decision under appeal is maintained.

Since Auxiliary Request 3 is an exact combination of Auxiliary Requests 1 and 2, the same arguments as provided above apply to Auxiliary Request 3.

As a further Auxiliary Request, oral proceedings before the Board of Appeal are requested.



M. Heise



Acknowledgement of receipt

We hereby acknowledge receipt of the following subsequently filed document(s):

Submission number	7924437	
Application number	EP13167436.8	
Date of receipt	04 October 2019	
Receiving Office	European Patent Office, The Hague	
Your reference	EP106738I-EH	
Applicant	All applicants as on file	
Documents submitted	package-data.xml epf1038.pdf (2 p.)	ep-sfd-request.xml APPEAL.pdf\EP106738IEH.pdf (1 p.)
Submitted by	CN=Michael Heise 38571	
Method of submission	Online	
Date and time receipt generated	04 October 2019, 13:39 (CEST)	
Message Digest	3D:B1:9D:E7:DB:D5:A7:CB:67:A9:7C:DA:77:D3:6C:B9:47:E7:FD:87	

Correction by the EPO of errors in debit instructions filed by eOLF

Errors in debit instructions filed by eOLF that are caused by the editing of Form 1038E entries or the continued use of outdated software (all forms) may be corrected automatically by the EPO, leaving the payment date unchanged (see decision T 152/82, OJ EPO 1984, 301 and point 6.3 ff ADA, Supplement to OJ EPO 10/2007).

/European Patent Office/



Letter accompanying subsequently filed items

Representative:

Grünecker Patent- und Rechtsanwälte PartG mbB
Association 72 / Zusammenschluss 72
Leopoldstraße 4
80802 München
Germany

Phone: +49 (0) 89 21 23 50

Fax: +49 (0) 89 22 02 87

E-mail: info@grunecker.de

80298 Munich

Germany

Tel. +49(0)89 2399-0 | Fax -4465

P.O. Box 5818

2280 HV Rijswijk

Netherlands

Tel. +31(0)70 340-2040 | Fax -3016

10958 Berlin

Germany

Tel. +49(0)30 25901-0 | Fax -840

The document(s) listed below is (are) subsequently filed documents pertaining to the following application:

Application number

13167436.8

Applicant's or representative's reference

EP106738I-EH

	Description of document	Original file name	Assigned file name
1	Notice of appeal	EP106738IEH.pdf	APPEAL.pdf

	Fees	Factor applied	Fee schedule	Amount to be paid
15-1	011 Appeal fee for an appeal filed by an entity other than those referred to in Rule 6(4) and (5) EPC	1	2 255.00	2 255.00
	Total:		EUR	2 255.00

	Payment	
1	Method of payment	Debit from deposit account
	Currency:	EUR
	The European Patent Office is hereby authorised, to debit from the deposit account with the EPO any fees and costs indicated on the fees page.	
	Deposit account number:	28000437
	Account holder:	Grünecker Patent- und Rechtsanwälte PartG mbB
2	Refund/Reimbursement	
	Reimbursement (if any) to be made to EPO deposit account:	28000437
	Account holder:	Grünecker Patent- und Rechtsanwälte PartG mbB

Signatures

Place:

Munich

Date:

04 October 2019

Signed by:

Michael Heise 38571

Association:

Grünecker Patent- und Rechtsanwälte PartG mbB

Representative name:

Michael Heise

EP106738I-EH

Capacity:

(Representative)

EP106738I-EH

European Patent Office

**Bob-van-Benthem-Platz 1
80469 München**

Ihr Zeichen / Your Ref.

Unser Zeichen / Our Ref.

Datum / Date

EP1067381-EHswa

October 4, 2019

European Patent Application No. 13 167 436.8

**Applicant: Webroot Inc.
385 Interlocken Crescent
Broomfield, CO 80021 / US**

In the name and on behalf of the above-identified applicant,

Notice of Appeal

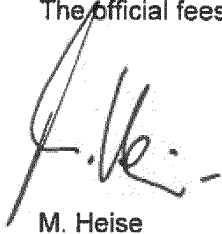
is herewith filed against the decision dated July 25, 2019.

It is requested that

- 1. the above-mentioned decision be set aside, and**
- 2. a European patent be granted on the basis of the claims, description and drawings on file.**

Auxiliary oral proceedings are requested.

The official fees will be paid via online fee payment.


M. Heise

Grünecker Patent- und Rechtsanwälte PartG mbB

Leopoldstr. 4 Tel. +49 (0) 89 21 23 50
80802 München Fax +49 (0) 89 22 02 87
Germany Mail info@grunecker.de

Amtsgericht: München
Partnerschaftsregister:
PR 1397

Deutsche Bank München
SWIFT / BIC-code: DEUT DE 33
IBAN: DE47 7007 0010 0175 173400

¹ auch/also: Mediator ² auch/also: Agente de la Propriété Industrielle (España) ³ auch/also: Consulente in Brevetti (Italia)

⁴ European Patent Attorney and UK Chartered Patent Attorney ⁵ Professor an der Fachhochschule für angewandtes Management

⁶ auch/also: Attorney-at-Law, New York ⁷ in Kooperation/in cooperation

MÜNCHEN

Patentanwälte
European Patent Attorneys
Thomas Schuster
Dr. Klara Goldbach
Martin Aulenanger, LL.M., MM.¹
Dr. Heike Vogelsang-Wenke
Reinhard Krauer
Dietmar Kuhl
Dr. Franz-Josef Zimmer
Bettina K. Reichelt
Dr. Anton K. Pfau
Dr. Udo Weigelt, LL.M.
Rainer Bertram
Jens C. Koch, M.S. (J of PA)
Bernd Rothaemel
Thomas W. Laubenthal, LL.M.
Dr. Andreas Koyser
Dr. Jens Hammer
Dr. Thomas Eickelkamp
Dr. Peter Miltényi ²
Dr. Moritz Höfle, LL.M.
Gero Maatz-Jansen
Michael Heise
Christian Meisinger
Dr. Martin Ahr
Dr. Wolfgang Neubeck
Staven M. Zeman, Ph.D.
André Nickel
Felix Kahr
Dr. Alexander Stumvoll, LL.M.
Dr. Stefano Marchini ³
Dr. Thomas Kronberger
Yilin Jin
Dr. Georg Seisenberger
Dr. Olivia Nemethova, LL.M.
Dr. Rainer Plaggenborg
Victor Lopes Aguiar
Dr. Sabine Koch
Wolfram Thomas
Dr. Markus Grammel
Dr. Jegannath Korukottu ⁴

Rechtsanwälte
Attorneys-at-Law
Dr. Ulrich Blumenröder, LL.M.
Prof. Dr. Maximilian Kinkeldey, LL.M. ⁵
Dr. Karsten Brandt
Anja Franke, LL.M.
Ute Stephani
Dr. Bernd Allekotta, LL.M. ⁶
Dr. Elvira Bertram, LL.M.
Babett Ertle
Christiane Neuhierl
Sabine Brandstätter
Cornelia Schmitt
Petra Lübke
Dr. Holger Gauss
Dr. Nicolás Schmitz
Marina Schlumberger
Kirsten Hammerstingl
Sebastian Clotten, LL.M.
Jennifer Rosenhäger, LL.M.
Mark Peters, LL.M.
Dr. Nicola Busch
Julia Bittner, LL.M.
Sebastian Ochs
Philipp Strommer
Jan Rother
Karin Lochner
Swetlana Frese

BERLIN

Patentanwälte
European Patent Attorneys
Dr. Patrick P. Erk, M.S. (Mit)
Tino Rumpold

KÖLN

Patentanwälte
European Patent Attorneys
Dr. Martin Drogmann

PARIS ⁷

Conseil en Propriété Industrielle
European Patent Attorney
Dr. Wolfgang Neubeck

OF COUNSEL

Patentanwälte
European Patent Attorneys
Gottfried Kitzsch

Rechtsanwälte
Attorneys-at-Law
Dr. Helmut Eichmann
Gerhard Barth



Bericht van ontvangst/Handtekening Retour
Advice of receipt

CN 07

Stempel van
kantoor van
terugzending

Stamp of the office
returning the advice

Designated operator of the Netherlands
Op kantoor van verzending in te vullen / To complete at office of posting

Kantoor van verzending Office of posting	Datum Date 25/7/2019
Geadresseerde Addressee Grünecker Patent- und Rechtsanwälte PartG mbB Leopoldstraße 4 80802 München ALLEMAGNE	

Aard van de zending / Nature of the item

Aangetekend nr.: Registered No. of item RD 431325232 nl	☐ Evt. bedrag en valuta Waarde- aangifte/Verzekerd Vervoer Opt. insured amount and currency
--	--

Op plaats van bestemming in te vullen / To sign on place of destination

Naam, datum en handtekening Name, date and signature 29.7.19 <i>Ligendui</i>

* Afhankelijk van de voorschriften in het land van bestemming wordt het bericht getekend door de geadresseerde of zijn gemachtigde of door de postmedewerker

AD EPA RETOUR tel: (070)3403060 23-08-2019
--

Priority/By Airmail Mailroom 5

Terugzenden aan (in te vullen door de afz.) / Return to

Naam of firma Name Europäisches Patentamt European Patent Office Office Européen des Brevets Patentlaan 2	Postcode en plaats Niederlande 2288 EE Rijswijk (ZH)
Straat en huisnummer Street and No. HH-004 #Y338H6B#35#0702# RETOUR - Ongeldig/incomplete adres PATENTLAAN 2 2288 EE RIJSWIJK ZH	



Designated operator of the Netherlands

Op kantoor van verzending in te vullen / To complete at office of posting

Kantoor van verzending
Office of posting

Datum	
Date	

25.7.2019

Geadress
Addressee

**Grünecker Patent- und Rechtsanwälte
PartG mbB
Leopoldstraße 4
80802 München
ALLEMAGNE**

Aard van de zending / Nature of the item

Aangetekend nr.:
Registered No. of item

Evt. bedrag en valuta Waarde-aangifte/Verzekerd Vervoer
Opt. insured amount and currency

RD 4213252 L6 NL

Op plaats van bestemming in te vullen / To sign on place of destination

Naam, datum en handtekening
Name, date and signature

29.7.19 Nicotiana

* Afhankelijk van de voorschriften in het land van bestemming wordt het bericht getekend door de geadresseerde of zijn gemachtigde of door de postmedewerker

Bericht van ontvangst/Handtekening Retour/
Advice of receipt

CN 07

EPA EPO OEB
tel: (070)3403060

~~Stempel van
kantoor van
terugzending~~

~~Stamp of the office
returning the advice~~

20-08-2019

~~RA.~~

Priority/By Airmail

Terugzenden aan (in te vullen door de afz.) / Return to

Naam of firma
Name

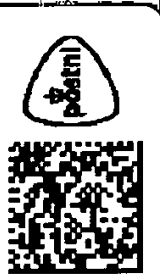


Europäisches Patentamt
European Patent Office

#Y338H6B#35#0702#

AN 2

U.S. DEPARTMENT OF JUSTICE

Land
Country

三

131 67436.8 - 1217



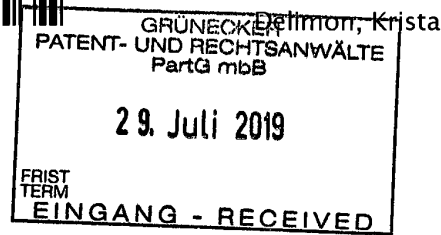
European Patent Office
80298 MUNICH
GERMANY

EPO - Munich
102
31. Juli 2019

Questions about this communication ?
Contact Customer Services at www.epo.org/contact



Grünecker Patent- und Rechtsanwälte
PartG mbB
Leopoldstraße 4
80802 München
ALLEMAGNE



Date
25.07.2019

Reference EP1067381EHmf	Application No./Patent No. 13167436.8 - 1217 / 2629232
Applicant/Proprietor Webroot Inc.	

EPA/EPO/OEB Formblatt/Form/Formulaire : 2007

Empfangsbescheinigung über den Zugang des vorstehend bezeichneten Schriftstücks
Acknowledgement of receipt of the document specified above
Récépissé du document spécifié ci-dessus

Unter Bezugnahme auf die Mitteilung im ABI EPA 7/2010, 377 wird gebeten, die Empfangsbescheinigung mit Empfangsdatum und Unterschrift zu versehen und **umgehend** an das EPA zurückzusenden:

With reference to the Notice in OJ EPO 7/2010, 377, you are requested to date and sign the acknowledgement of receipt and return it to the EPO **immediately**:

Conformément au communiqué paru au JO OEB 7/2010, 377, vous êtes prié d'indiquer sur le récépissé la date de réception du document, de signer le récépissé et de le renvoyer **sans délai** à l' OEB:

- **über die Online-Dienste des EPA** (als Anlage zu EPA Form 1038) / **through EPO Online Services** (as annex to EPO Form 1038) / **par les services en ligne de l'OEB** (en tant que pièce jointe au formulaire OEB 1038),
- **per Fax / by fax / par téléfax** (+49 (0) 89 2399-4465 or +31 (0) 70 340-3016)
- **oder per Post / or by post / ou par courrier.**

Empfangen am / Received on / Reçu le : 29. Juli 2019

Unterschrift / Signature:

Empfangsberechtigter/authorised recipient/
le destinataire ou la personne dûment mandatée

Rücksende-Adresse / Return address / Adresse de retour
(Umschlag / envelope / enveloppe ISO C4 / DL / C6/C5 / C6)

DEUTSCHLAND
80298 MÜNCHEN
Europäisches Patentamt

Rücksende-Adresse / Return address / Adresse de retour

EPA/EPO/OEB Form 2936 08.10



European Patent Office
80298 MUNICH
GERMANY

EPO - Munich
102
31. Juli 2019

Questions about this communication ?
Contact Customer Services at www.epo.org/contact



Grünecker Patent- und Rechtsanwälte
PartG mbB
Leopoldstraße 4
80802 München
ALLEMAGNE

GRÜNECKER, Krista
PATENT- UND RECHTSANWÄLTE
PartG mbB
29. Juli 2019
FRIST
TERM
EINGANG - RECEIVED

Date
25.07.2019

Reference EP1067381EHmf	Application No./Patent No. 13167436.8 - 1217 / 2629232
Applicant/Proprietor Webroot Inc.	

EPA/EPO/OEB Formblatt/Form/Formulaire : 2007

Empfangsbescheinigung über den Zugang des vorstehend bezeichneten Schriftstücks
Acknowledgement of receipt of the document specified above
Récépissé du document spécifié ci-dessus

Unter Bezugnahme auf die Mitteilung im ABI EPA 7/2010, 377 wird gebeten, die Empfangsbescheinigung mit Empfangsdatum und Unterschrift zu versehen und **umgehend** an das EPA zurückzusenden:

With reference to the Notice in OJ EPO 7/2010, 377, you are requested to date and sign the acknowledgement of receipt and return it to the EPO **immediately**:

Conformément au communiqué paru au JO OEB 7/2010, 377, vous êtes prié d'indiquer sur le récépissé la date de réception du document, de signer le récépissé et de le renvoyer **sans délai** à l' OEB:

- **über die Online-Dienste des EPA** (als Anlage zu EPA Form 1038) / **through EPO Online Services** (as annex to EPO Form 1038) / **par les services en ligne de l'OEB** (en tant que pièce jointe au formulaire OEB 1038),
- **per Fax / by fax / par téléfax** (+49 (0) 89 2399-4465 or +31 (0) 70 340-3016)
- **oder per Post / or by post / ou par courrier.**

Empfangen am / Received on: 29. Juli 2019
Unterschrift / Signature:
Empfangsberechtigter/authorised recipient/
le destinataire ou la personne dûment mandatée

Rücksende-Adresse / Return address / Adresse de retour
(Umschlag / envelope / enveloppe ISO C4 / DL / C6/C5 / C6)

DEUTSCHLAND
80298 MÜNCHEN
Europäisches Patentamt

Rücksende-Adresse / Return address / Adresse de retour

EPA/EPO/OEB Form 2936 08.10



European Patent Office
80298 MUNICH
GERMANY

Questions about this communication ?

Contact Customer Services at www.epo.org/contact



Delimon, Krista

Grünecker Patent- und Rechtsanwälte
PartG mbB
Leopoldstraße 4
80802 München
ALLEMAGNE

Date

25.07.2019

Reference
EP1067381EHmf

Application No./Patent No.
13167436.8 - 1217 / 2629232

Applicant/Proprietor
Webroot Inc.

EPA/EPO/OEB Formblatt/Form/Formulaire : 2007

Empfangsbescheinigung über den Zugang des vorstehend bezeichneten Schriftstücks
Acknowledgement of receipt of the document specified above
Récépissé du document spécifié ci-dessus

Unter Bezugnahme auf die Mitteilung im ABI EPA 7/2010, 377 wird gebeten, die Empfangsbescheinigung mit Empfangsdatum und Unterschrift zu versehen und **umgehend** an das EPA zurückzusenden:

With reference to the Notice in OJ EPO 7/2010, 377, you are requested to date and sign the acknowledgement of receipt and return it to the EPO **immediately**:

Conformément au communiqué paru au JO OEB 7/2010, 377, vous êtes prié d'indiquer sur le récépissé la date de réception du document, de signer le récépissé et de le renvoyer **sans délai** à l' OEB:

- **über die Online-Dienste des EPA** (als Anlage zu EPA Form 1038) / **through EPO Online Services** (as annex to EPO Form 1038) / **par les services en ligne de l'OEB** (en tant que pièce jointe au formulaire OEB 1038),
- **per Fax / by fax / par téléfax** (+49 (0) 89 2399-4465 or +31 (0) 70 340-3016)
- oder per Post / or by post / ou par courrier.

Empfangen am / Received on / Reçu le :

Unterschrift / Signature:

Empfangsberechtigter/authorised recipient/
le destinataire ou la personne dûment mandatée

Rücksende-Adresse / Return address / Adresse de retour
(Umschlag / envelope / enveloppe ISO C4 / DL / C6/C5 / C6)

DEUTSCHLAND
80298 MÜNCHEN
Europäisches Patentamt

Rücksende-Adresse / Return address / Adresse de retour

EP Application No.: 13 167 436.8
Applicant: WEBROOT INC.
Our Ref.: EP106738I-EH
Date: May 31, 2019

5

CLAIMS – Main Request

1. A method of determining the protection that a first remote computer of a plurality of remote computers has from malware, the method comprising:

receiving at a database (7) of a base computer (3) information of all or selected security
10 products loaded on or available at a point in time on said first remote computer (2);

receiving at the database (7) information of all or selected security products loaded on or
available at a point in time on other remote computers (2) of said plurality of remote
computers connected to the database (7);

receiving at the database (7) details of processes run by said plurality of remote
15 computers (2);

storing the information and the details in the database (7);

searching the database (7) to identify any processes marked as being malware that
occurred on computers (2) having the same particular combination of security products
as the first remote computer (2) and that were not locally detected; and

20 providing information to the user of said first remote computer (2) that said first remote
computer (2) may be susceptible to attack by said identified any processes marked as
being malware.
2. A method according to claim 1, wherein the information of all or selected security
products includes the name of the security products, versions, and loaded signature
25 files.
3. Apparatus for determining the protection that a first remote computer of a plurality of
remote computers has from malware, the apparatus comprising:

a database (7) of a base computer (3) adapted to:

receive information of all or selected security products loaded on or available at a
30 point in time on said first remote computer (2),

receive information of all or selected security products loaded on or available at a
point in time on other remote computers (2) of said plurality of remote computers
connected to the database (7),

receive details of processes run by said plurality of remote computers (2), and
store the information and the details in the database (7); and

the base computer (3) being adapted to:

5 search the database (7) to identify any processes marked as malware that occurred
on computers (2) having the same particular combination of security products as the
first remote computer (2) and that were not locally detected, and

provide information to the user of said first remote computer (2) that said first remote
computer (2) may be susceptible to attack by said identified any processes marked
as being malware.

- 10 4. Apparatus according to claim 3, wherein the information of all or selected security
products includes the name of the security products, versions, and loaded signature
files.
5. A computer program comprising program instructions for causing a computer to perform
the method of claim 1 or claim 2.

EP Application No.: 13 167 436.8
Applicant: WEBROOT INC.
Our Ref.: EP1067381-EH
Date: May 31, 2019

5

CLAIMS – Auxiliary Request 1

1. A method of determining the protection that a first remote computer of a plurality of remote computers has from malware, the method comprising:

receiving at a database (7) of a base computer (3) information of all or selected security products loaded on or available at a point in time on said first remote computer (2);

receiving at the database (7) information of all or selected security products loaded on or available at a point in time on other remote computers (2) of said plurality of remote computers connected to the database (7);

receiving at the database (7) details of processes run by each of said plurality of remote computers (2), said details comprise whether or not a process has been detected as malware;

storing the information and the details in the database (7);

searching the database (7) to identify any processes marked as being malware that occurred on computers (2) having the same particular combination of security products as the first remote computer (2) and that were not locally detected; and

providing information to the user of said first remote computer (2) that said first remote computer (2) may be susceptible to attack by said identified any processes marked as being malware.
2. A method according to claim 1, wherein the information of all or selected security products includes the name of the security products, versions, and loaded signature files.
3. Apparatus for determining the protection that a first remote computer of a plurality of remote computers has from malware, the apparatus comprising:

a database (7) of a base computer (3) adapted to:

receive information of all or selected security products loaded on or available at a point in time on said first remote computer (2),

receive information of all or selected security products loaded on or available at a point in time on other remote computers (2) of said plurality of remote computers connected to the database (7),

receive details of processes run by each of said plurality of remote computers (2),
said details comprise whether or not a process has been detected as malware, and
store the information and the details in the database (7); and

the base computer (3) being adapted to:

5 search the database (7) to identify any processes marked as malware that occurred
 on computers (2) having the same particular combination of security products as the
 first remote computer (2) and that were not locally detected, and
 provide information to the user of said first remote computer (2) that said first remote
 computer (2) may be susceptible to attack by said identified any processes marked
10 as being malware.

4. Apparatus according to claim 3, wherein the information of all or selected security
 products includes the name of the security products, versions, and loaded signature
 files.
5. A computer program comprising program instructions for causing a computer to perform
15 the method of claim 1 or claim 2.

EP Application No.: 13 167 436.8
Applicant: WEBROOT INC.
Our Ref.: EP106738I-EH
Date: May 31, 2019

5

CLAIMS – Auxiliary Request 2

1. A method of determining the protection that a first remote computer of a plurality of remote computers has from malware, the method comprising:

receiving at a database (7) of a base computer (3) information of all or selected security products loaded on or available at a point in time on said first remote computer (2);

receiving at the database (7) information of all or selected security products loaded on or available at a point in time on other remote computers (2) of said plurality of remote computers connected to the database (7);

receiving at the database (7) details of processes run by said plurality of remote computers (2);

storing the information and the details in the database (7);

searching the database (7) to identify any processes marked as being malware that occurred on computers (2) having the same particular combination of security products as the first remote computer (2) and that were not locally detected; and

providing information to the user of said first remote computer (2) that the security products on said first remote computer (2) expose the first remote computer to a risk of being infected by said identified any processes marked as being malware and offering the user software to download and install to remove the risk.
2. A method according to claim 1, wherein the information of all or selected security products includes the name of the security products, versions, and loaded signature files.
3. Apparatus for determining the protection that a first remote computer of a plurality of remote computers has from malware, the apparatus comprising:

a database (7) of a base computer (3) adapted to:

receive information of all or selected security products loaded on or available at a point in time on said first remote computer (2),

receive information of all or selected security products loaded on or available at a point in time on other remote computers (2) of said plurality of remote computers connected to the database (7),

receive details of processes run by said plurality of remote computers (2), and
store the information and the details in the database (7); and

the base computer (3) being adapted to:

5 search the database (7) to identify any processes marked as malware that occurred
on computers (2) having the same particular combination of security products as the
first remote computer (2) and that were not locally detected, and

provide information to the user of said first remote computer (2) that the security
products on said first remote computer (2) expose the first remote computer to a risk
of being infected by said identified any processes marked as being malware and
10 offer the user software to download and install to remove the risk.

4. Apparatus according to claim 3, wherein the information of all or selected security
products includes the name of the security products, versions, and loaded signature
files.
5. A computer program comprising program instructions for causing a computer to perform
15 the method of claim 1 or claim 2.

EP Application No.: 13 167 436.8
Applicant: WEBROOT INC.
Our Ref.: EP106738I-EH
Date: May 31, 2019

5

CLAIMS – Auxiliary Request 3

1. A method of determining the protection that a first remote computer of a plurality of remote computers has from malware, the method comprising:

receiving at a database (7) of a base computer (3) information of all or selected security products loaded on or available at a point in time on said first remote computer (2);

receiving at the database (7) information of all or selected security products loaded on or available at a point in time on other remote computers (2) of said plurality of remote computers connected to the database (7);

receiving at the database (7) details of processes run by each of said plurality of remote computers (2), said details comprise whether or not a process has been detected as malware;

storing the information and the details in the database (7);

searching the database (7) to identify any processes marked as being malware that occurred on computers (2) having the same particular combination of security products as the first remote computer (2) and that were not locally detected; and

providing information to the user of said first remote computer (2) that the security products on said first remote computer (2) expose the first remote computer to a risk of being infected by said identified any processes marked as being malware and offering the user software to download and install to remove the risk.
2. A method according to claim 1, wherein the information of all or selected security products includes the name of the security products, versions, and loaded signature files.
3. Apparatus for determining the protection that a first remote computer of a plurality of remote computers has from malware, the apparatus comprising:

a database (7) of a base computer (3) adapted to:

receive information of all or selected security products loaded on or available at a point in time on said first remote computer (2),

receive information of all or selected security products loaded on or available at a point in time on other remote computers (2) of said plurality of remote computers connected to the database (7),

5 receive details of processes run by each of said plurality of remote computers (2), said details comprise whether or not a process has been detected as malware, and store the information and the details in the database (7); and

the base computer (3) being adapted to:

10 search the database (7) to identify any processes marked as malware that occurred on computers (2) having the same particular combination of security products as the first remote computer (2) and that were not locally detected, and

provide information to the user of said first remote computer (2) that the security products on said first remote computer (2) expose the first remote computer to a risk of being infected by said identified any processes marked as being malware and offer the user software to download and install to remove the risk.

- 15 4. Apparatus according to claim 3, wherein the information of all or selected security products includes the name of the security products, versions, and loaded signature files.
5. A computer program comprising program instructions for causing a computer to perform the method of claim 1 or claim 2.

Application No.:

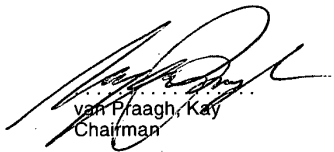
13 167 436.8

Decision of the Examining Division

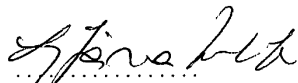
In the oral proceedings held on 02.07.2019, the examining division has decided:

The European patent application is refused on the basis of Article 97(2) EPC. The reasons for the decision are attached (Form(s) 2916).

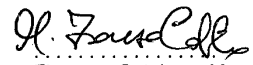
10-07-2019
Date



van Praagh, Kay
Chairman



Arbutina, Ljiljana
1st examiner



Fiorenzo Catalano, M
2nd examiner

Enclosure(s): Form 2916
main and three auxiliary requests filed on 31-05-2019



European Patent Office
Postbus 5818
2280 HV Rijswijk
NETHERLANDS
Tel: +31 70 340 2040
Fax: +31 70 340 3016



Grünecker Patent- und Rechtsanwälte
PartG mbB
Leopoldstraße 4
80802 München
ALLEMAGNE

Formalities Officer
Name: Delimon, Krista
Tel: +31 70 340 - 4446
or call
+31 (0)70 340 45 00

Substantive Examiner
Name: Arbutina, Ljiljana
Tel: +31 70 340 - 4522

Application No. 13 167 436.8 - 1217	Ref. EP1067381EHmf	Date 25.07.2019
Applicant Webroot Inc.		

Decision to refuse a European Patent application

The Examining Division - at the oral proceedings dated 02.07.2019 - has decided:

European Patent application No. 13 167 436.8 is refused.

Applicant/s:

Webroot Inc.
385 Interlocken Crescent
Broomfield, CO 80021
US

Title

Methods and apparatus for dealing with malware

The grounds for the decision are set out on the supplemental sheets annexed hereto.

Means of redress

This decision is open to appeal.

Attention is drawn to the attached text of Articles 106 to 108 EPC and Rules 97 and 98 EPC.

Examining Division:

Chairman: van Praagh, Kay
2nd Examiner: Fiorenzo Catalano, M
1st Examiner: Arbutina, Ljiljana



Delimon, Krista
Formalities Officer
Tel. No.: +31 70 340-4446

Branch at The Hague

Enclosure(s): 8 page/s reasons (Form 2916)
Form 2019
main and three auxiliary requests filed on 31-05-2019
to EPO postal service: 18.07.19

I. Summary of Facts and Submissions

- 1 European patent application No. 13 167 436.8 having the title "Methods and apparatus for dealing with malware" was filed on 13-05-2013 . It claims priority of GB 0513375 filed on 30-06-2005. The applicant is
Webroot Inc.
385 Interlocken Crescent
Broomfield, CO 80021
US.
- 2 The European search opinion cited the document

D1 US 2003/131256 A1 (ACKROYD ROBERT JOHN [GB]) 10 July
2003 (2003-07-10)

and raised objections under Articles 83 and 84 EPC.
- 3 In the response received on 18-03-2014 the applicant requested further examination on an amended set of claims 1-5 and provided arguments in support of the patentability of these claims. As a precaution, oral proceedings in a form of a video conference were requested.
- 4 In a communication under Article 94(3) EPC issued by the examining division on 26-04-2018, objections under Articles 76(1) and 56 EPC were raised.
- 5 In the response received on 04-09-2018 the applicant requested further examination on an amended set of claims 1-5 and provided arguments in support of the patentability of the claims.
- 6 On 05-02-2019 the examining division issued a summons to attend oral proceedings on 02-07-2019. In the annex to the summons, objections under Articles 76(1), 84, 83, and 56 EPC were raised.
- 7 In a response to the summons received on 31-05-2019 the applicant submitted the main and three auxiliary requests, and provided arguments in support of the patentability of the claims.
- 8 On 27-06-2019 the division informed the applicant that the date fixed for the oral proceedings was maintained. In the annex, a preliminary opinion of the division about the requests on file was communicated to the applicant.
- 9 On 02-07-2019, oral proceedings were held.
- 10 The decision is based on the following requests:

Main Request

Datum
Date 25.07.2019
Date

Blatt
Sheet 2
Feuille

Anmelde-Nr:
Application No: 13 167 436.8
Demande n°:

Description, Pages

1, 3, 5-43 as originally filed

2, 2a, 4, 4a received on 04-09-2018 with letter of 04-09-2018

Claims, Numbers

1-5 received on 31-05-2019 with letter of 31-05-2019

Drawings, Sheets

1/3-3/3 as originally filed

Auxiliary Request 1

Description, Pages

1, 3, 5-43 as originally filed

2, 2a, 4, 4a received on 04-09-2018 with letter of 04-09-2018

Claims, Numbers

1-5 received on 31-05-2019 with letter of 31-05-2019

Drawings, Sheets

1/3-3/3 as originally filed

Auxiliary Request 2

Description, Pages

1, 3, 5-43 as originally filed

2, 2a, 4, 4a received on 04-09-2018 with letter of 04-09-2018

Datum
Date 25.07.2019
Date

Blatt
Sheet 3
Feuille

Anmelde-Nr:
Application No: 13 167 436.8
Demande n°:

Claims, Numbers

1-5 received on 31-05-2019 with letter of 31-05-2019

Drawings, Sheets

1/3-3/3 as originally filed

Auxiliary Request 3

Description, Pages

1, 3, 5-43 as originally filed

2, 2a, 4, 4a received on 04-09-2018 with letter of 04-09-2018

Claims, Numbers

1-5 received on 31-05-2019 with letter of 31-05-2019

Drawings, Sheets

1/3-3/3 as originally filed

- 11 The claims under consideration are attached to this decision. As to the other application documents, reference is made to the file.

II. Reasons for the Decision

Main request

Amendments

1. The amendments of the main request introduce subject-matter which extends beyond the content of the earlier application as filed, contrary to Article 76(1) EPC, for the following reason:

The feature "searching the database to identify any processes marked as being malware that occurred on computers having the same particular combination of security products as the first remote computer and that were not locally detected" is not disclosed in the parent application, nor is it directly and unambiguously derivable therefrom.

The applicant identified two passages as being bases for this amendment, namely, page 38, lines 5-7 and lines 27-30. These passages recite

"if for example the database knows that a computer in the past has version A of anti-virus product B ..., but that a particular malware process P was not detected by this combination", and,

"the database ... is searched for events for processes marked as "bad" that occurred on computers with that particular mix of security products and that were not locally detected".

As can be seen, the first passage does not disclose searching the database, and the second passage discloses searching the database for events for processes marked as "bad". Therefore, none of the passages discloses the feature under consideration, nor is it directly and unambiguously derivable therefrom.

1.1. During the oral proceedings the applicant argued that, in the second passage indicated above, there was a typo, that the passage should read as *"events or processes"* instead *"events for processes"* and that "bad" means being malware. The division was not convinced by this argument.

Clarity / Sufficiency of Disclosure

2. The feature of claim 1

"searching the database to identify any processes marked as being malware that occurred on computers having the same particular combination of security products as the first remote computer and that were not locally detected"

renders claim 1, and the corresponding claims 3 and 5, unclear, contrary to the requirements of Article 84 EPC. Moreover, the application as filed does not disclose the invention in a manner sufficiently clear and complete for this feature to be carried out by a person skilled in the art, contrary to the requirements of Article 83 EPC. The reasons therefore are the following:

2.1. The origin of the marking of processes as being malware is undefined. It is unclear who, when, or how, marked the process as being malware; the information about a process being a malware is not provided to the database by any feature of the claim. This indicates that there are essential features missing in the claim (Article 84 EPC).

2.2. The feature requires to search for "any processes ... that were not locally detected". On one hand, this requirement is unclear; it is unclear which process can be considered to be "a process not locally detected" (Article 84 EPC). On the other hand, the database receives only the information about the security products loaded on a plurality of computers, and details of processes run by said computers; none of these appear to correspond to "a process not locally detected". Thus, a skilled person is confronted with the problem of performing the search of a database whereby an unclear condition for the search is given, and where the database itself does not appear to contain any information that relates to this unclear condition. The application does not give any teaching which would allow a skilled person to implement the required search. Therefore, the application does not disclose the invention in a manner sufficiently clear and complete for it to be carried out by a person skilled in the art, contrary to the requirements of Article 83 EPC.

2.3. During the oral proceedings, the applicant argued that the claimed subject-matter is based on the parent application, pages 36 to 38; that the first paragraph on page 38 gives a simple example explaining the invention. It is disclosed, lines 6-7, that "a particular malware process was not detected by this combination of programs at that point of time". The applicant argued that the database knows this because software administrators regularly keep track of such information: when a program is detected as being malware, they check for computers running this program and record this information. Thus, such information is in the database. It is not important how it gets there, the invention is in how it is used.

The division considers this to be a purely speculative interpretation, neither present nor hinted to by the application documents.

Inventive Step

3. The subject-matter of claim 1, as well as corresponding claims 3 and 5, is not inventive in the sense of Article 56 EPC over document D1, which discloses a method of determining the protection that a first remote computer has from malware, the method comprising:

receiving at a database of a base computer information of all or selected security products loaded on or available at a point in time on said first remote computer and on other remote computers (par.[0025], lines 10-15)

receiving at the database details of processes run by said remote computers (par. [0025], lines 6-10; in case of dynamic malware detection, the detection is done while the program is running),

storing the information and the details in the database (implicit);

searching the database to identify the remote computers having the particular combination of security products that does not locally detect a process marked as being malware (par.[0030], lines 9-13 and lines 18-22), and

updating the security products on the remote computers that may be susceptible to attack by said malware processes on the basis of said identifying (par.[0030], lines 18-22).

The subject-matter of independent claims 1, 3 and 5 differs from the teaching of D1

i) in that the information that the computer may be susceptible to attack is provided to the user, which, being presentation of information, cannot be considered as a basis of an inventive step, and

ii) the search of the database is performed in a different way; however, this subject-matter is not allowable for the reasons presented above in sections 1, 2.-2.2.

Therefore, the independent claims do not contain any features that could be considered as having inventive contribution over the prior art.

3.1. The additional features of dependent claims 2 and 4 consist merely in naming the information, and as such cannot be considered as involving inventive step in the sense of Article 56 EPC.

Auxiliary Request 1

Amendments

4. The first auxiliary request introduces subject-matter which extends beyond the content of the earlier application as filed, contrary to Article 76(1) EPC, for the reason presented above for the main request, in section 1. and additionally for the following reason:

4.1. The amendment

"receiving at the database details of processes run by each of said plurality of remote computers, said details comprise whether or not a process has been detected as malware"

is neither disclosed in the passages cited by the applicant, nor is it directly and unambiguously derivable therefrom.

The first passage indicated by the applicant recites

"The community database 7 in this embodiment is also provided by the agent software with details of processes run by every computer 2 and thus knows whether or not a process has been detected by each computer 2."

The second passage indicated by the applicant recites

"In a simple example, if for example the database knows that a computer in the past has version A of anti-virus product B with downloaded signature update C, and also has a firewall D with particular settings E, and perhaps anti-spyware software F with signature updates G, but that a particular malware process P was not detected by this combination of programs at that point in time"

The third passage indicated by the applicant recites:

"the database 7, when provided with information relating to all the security products, etc. on a particular computer at a particular time, is searched for events for processes marked as "bad" that occurred on computers with that particular mix of security products and that were not locally detected".

As can be seen, none of the passages disclose receiving details whether or not a process has been detected as malware, and neither is such subject-matter directly and unambiguously derivable therefrom.

During the oral proceedings, the applicant argued that it is obvious from the first of the passages cited here above that the process that is detected has to be malware. The division was not convinced.

Clarity / Sufficiency of Disclosure / Inventive Step

5. The above discussed feature is the only amendment of auxiliary request 1 with respect to the main request. Therefore, for the remaining features of auxiliary request 1, the arguments presented above for the main request apply.

Auxiliary request 2

Amendments

6. Auxiliary request 2 introduces subject-matter which extends beyond the content of the earlier application as filed, contrary to Article 76(1) EPC, for the reason presented above for the main request, in section 1., and additionally for the following reason:

6.1. The auxiliary request 2 has the following amendment of the last feature of claims 1 and 3:

"providing information ... that the security products ... expose the first remote computer to a risk of being infected ... and offering the user software to download and install to remove the risk".

This amended is based on, as indicated by the applicant, page 38, lines 15 - 23.

However, the indicated passage discloses a specific example, which does not give support for the generalization claimed in the amended feature.

Clarity / Sufficiency of Disclosure / Inventive Step

7. The above discussed feature is the only amendment of auxiliary request 2 with respect to the main request. Therefore, for the remaining features of auxiliary request 2, the arguments presented above for the main request apply. In particular, the part of the amendment reciting "offering the user software to download and install to remove the risk" is void of any technical character and as such does not overcome the inventive step objection presented for the main request.

7.1. During the oral proceedings, the applicant argued that the additional features of claim 1 were technical. The division could not share this opinion.

Auxiliary Request 3

8. The third auxiliary is a combination of auxiliary requests 1 and 2. Therefore, the reasons presented for auxiliary requests 1 and 2 apply also to the third auxiliary request.

III. Decision

For the reasons given in detail above, the application is refused under Article 97(2) EPC for lack of an inventive step in the sense of Article 56 EPC, and for infringing Articles 76(1), 83 and 84 EPC for all the requests on file.

Article 106
Decisions subject to appeal

- (1) An appeal shall lie from decisions of the Receiving Section, Examining Divisions, Opposition Divisions and the Legal Division. It shall have suspensive effect.
- (2) A decision which does not terminate proceedings as regards one of the parties can only be appealed together with the final decision, unless the decision allows a separate appeal.
- (3) The right to file an appeal against decisions relating to the apportionment or fixing of costs in opposition proceedings may be restricted in the Implementing Regulations.

Rule 97
Appeal against apportionment and fixing of costs

- (1) The apportionment of costs of opposition proceedings cannot be the sole subject of an appeal.
- (2) A decision fixing the amount of costs of opposition proceedings cannot be appealed unless the amount exceeds that of the fee for appeal.

Rule 98
Surrender or lapse of the patent

The decision of an Opposition Division may be appealed even if the European patent has been surrendered in all the designated Contracting States or has lapsed in all those States.

Article 107
Persons entitled to appeal and to be parties to appeal proceedings

Any party to proceedings adversely affected by a decision may appeal. Any other parties to the proceedings shall be parties to the appeal proceedings as of right.

Article 108
Time limit and form

Notice of appeal shall be filed, in accordance with the Implementing Regulations, at the European Patent Office within **two months** of notification of the decision. Notice of appeal shall not be deemed to have been filed until the fee for appeal has been paid. Within **four months** of notification of the decision, a statement setting out the grounds of appeal shall be filed in accordance with the Implementing Regulations.

Further information concerning the filing of an appeal

- (a) Notice of appeal can be filed in accordance with Rule 1 and Rule 2(1) EPC, by delivery by hand, by post, or by technical means of communication. The filing has to comply with the details and conditions and, where appropriate, any special formal or technical requirements laid down by the President of the European Patent Office (R. 99(3) EPC).
- (b) The addresses of the filing offices of the European Patent Office are as follows:

(i) European Patent Office D-80298 Munich Germany Fax: +49 89 2399-4465	(ii) European Patent Office Postbus 5818 NL-2280 HV Rijswijk (ZH) The Netherlands Fax: +31 70 340-3016	(iii) European Patent Office D-10958 Berlin Germany Fax: +49 30 259 01-840
--	--	---

- (c) The notice of appeal must contain the name and address of the appellant in accordance with the provisions of Rule 41(2)(c) EPC, an indication of the decision impugned, and a request defining the subject of the appeal. In the statement of grounds of appeal the appellant shall indicate the reasons for setting aside the decision impugned, or the extent to which it is to be amended, and the facts and evidence on which the appeal is based (R. 99(1) and (2) EPC). The notice of appeal and any subsequent submissions stating the grounds for appeal must be signed (R. 50(3) EPC).
- (d) The fee for appeal is laid down in the Rules relating to Fees. The schedule of fees and expenses of the EPO or a reference to the current version is regularly published in the Official Journal of the European Patent Office under the heading "Guidance for the payment of fees, expenses and prices". Fee information is also published on the EPO website under www.epo.org/fees.

Opening of the proceedings

The oral proceedings by means of video conference were opened at 15:15.

The chairman stated that the applicant was duly summoned by means of video conference and was represented by Mr M. Heise.

The chairman checked the current state of the file and found that the following set of claims submitted with letter dated 31-05-2019 were present on file:

- a main request (MR) with 5 claims;
- auxiliary requests 1, 2 and 3 (AR1, AR2 and AR3) with 5 claims each;

and the following application documents:

- description, pages 1-3, 5-43, as originally filed, and pages 2, 2a, 4, 4a filed with letter dated 04-09-2018;
- drawings, sheets 1/3-3/3, as originally filed.

The applicant confirmed the requests as on file.

The chairman asked the applicant if he had further requests or submissions, which the latter denied.

Main request

Regarding the main request, the chairman stated that the position of the division was as presented in the annex to the summons and in the preliminary opinion sent by telefax on 27-06-2019, namely that the main request on file not only contravened Articles 76(1), 84 and 83 EPC, but also lacked an inventive step in the sense of Article 56 EPC over the disclosure of document D1.

The chairman proposed to address first the objections under Articles 83 and 84 EPC.

The chairman referred to section 2 of the preliminary opinion and stated that the features of claim 1 related to "any processes marked as being malware" in combination with "*that were not locally detected*" of the searching step and "*said identified any processes marked as being malware*" of the providing step were objected to under Article 83 EPC.

The applicant provided pages 38-39 of the description of the parent application and in particular page 36, line 15, starting with "In another embodiment", and page 37, lines 21-24 for supporting the disclosure of "*the marked processes as malware*", since the passage discloses that the process running on the computer has been detected. Thus, it can be assumed that the DB knows if a particular computer has a particular

combination of security products and if a particular malware process, running on that computer, was not detected by this combination of security products on that computer.

The chairman asked how the DB knows that a malware process running on a computer was not detected.

The applicant replied that is a process P running on a computer is a malware and it is not identified as malware then the process P is not detected by the security programs, and since it is already known that process P is marked as malware, it can be determined that malware P is not detected on the computer where is running. The applicant further added that page 37, lines 11-13 disclose that the DB is provided with all the the information from many many millions of computers. Then the applicant provided the following example: if a malware process P is running on PC1 and the same ID process of P is identified on another computer, e.g. on PC2, having the same combination of security programs of PC1, then PC2 may be infected because process P is a malware process running on PC1 but not locally detected on PC1 by the same combination of security programs running on PC2.

The applicant further argued that providing all the information related to the malware processes into the DB is not part of the invention, the information are provided beforehand. The invention mainly relates to searching the DB to determine that a malware running on a second computer having the same combination of security programs of a first computer that did not detect the malware running on that first computer and to informing the user that the second computer might be at risk.

The chairman stated that the division would take into account the arguments provided by the applicant and then asked the applicant if he had further arguments regarding the objection under Articles 83 and 84 EPC, which the latter denied.

The proceedings were interrupted from 15:53 to 16:30 to deliberate on the allowability of the main request under Articles 83 and 84 EPC in view of the arguments presented by the applicant.

Upon reopening of the oral proceedings, the chairman stated that the examining division was still negatively minded with regard to Articles 83 and 84 EPC for claim 1 of the main request. In particular, it was stated that the division was not convinced by the applicant arguments, thus the objections of section 2 of the preliminary opinion related to the searching step were maintained.

The chairman stated that the subject-matter of claim 1 of the main request was then assessed in view of Article 76(1) and 56 EPC. In particular, reference to section 1 of the preliminary opinion was made, and in view of the arguments presented by the applicant, the objections under section 1-i) were dropped. The objections under

section 1-ii) were maintained, since page 38, lines 25-30 of the description of the parent application discloses *a searching step for events **for** processes marked as "bad"*. It was further added that there was no searching step disclosed in the example disclosed in page 38, lines 1-24.

The applicant replied that there was a spelling mistake in line 28, page 38, since it has to be read as *searched for events **or** processes marked as "bad"*. The division was not convinced by this argument.

The chairman then asked the applicant if he had further arguments regarding the objection under Article 76(1) EPC, which the latter denied.

The chairman then stated that the examining division was still negatively minded with regard to Article 56 EPC for claim 1 of the main request for the same reasoning based on the disclosure of D1 as in the annex to the summons.

The first examiner presented the following arguments regarding Article 56 EPC. The distinguishing features between claim 1 of the main request and the disclosure of D1 relates to the information provided to the user, which as such is considered matter of presentation of information, and thus it does not provide for any technical effect. Regarding the feature related to the receiving step, i.e. *the detail of processes run by said plurality of remote computers*, it was also considered part of the distinguishing features, since the objection under Article 76(1) EPC was dropped. It was further added that, since sending indication detection of malware falls under the scope of lines 14-15 of claim 1, it falls also under the scope of document D1, thus the distinguishing features related to the receiving step of *the details of processes* is considered implicitly disclosed in document D1.

The applicant remained of the same opinion previously presented and reiterates its arguments as follows. The applicant argued that *searching the database to identify any process marked as being malware that were not locally detected* was not disclosed in D1. The technical contribution for these distinguishing features is to identify possible attacks of computers, which is not disclosed and not obvious from D1.

The chairman then asked the applicant if he had new arguments, which the latter denied.

The chairman concluded that the main request was not allowable for lack of inventive step of the subject-matter of claim 1 (Article 56 EPC), and for infringing Articles 83, 84 and 76(1) EPC.

Auxiliary Request 1 (AR1)

The chairman admitted AR1 into the proceedings and then referred to sections 4 and 5 of the preliminary opinion of the examining division regarding the objections under Articles 83, 84, 76(1) and 56 EPC of auxiliary request 1.

The applicant provided the passage of in page 37, lines 21-24 stating that the only meaning that can be derived from this passage in the context of the application is that *weather or not a process has been detected as malware*.

The chairman stated that the subject-matter of claim 1 of AR1 was not allowable under Article 56 EPC for the same reasoning as provided for the main request, and asked the applicant to present the arguments related to the inventive step.

The applicant referred to the arguments provided during the written procedure.

The chairman then asked the applicant if he had new arguments, which the latter denied.

The chairman concluded that AR1 was not allowable for lack of inventive step of the subject-matter of claim 1 (Article 56 EPC) and for infringing Articles 83, 84 and 76(1) EPC.

Auxiliary Request 2 (AR2)

The chairman admitted AR2 into the proceedings and then referred to sections 6 and 7 of the preliminary opinion of the examining division regarding the objections under Articles 83, 84, 76(1) and 56 EPC of auxiliary request 2.

The chairman stated that the amendments of AR2 related to an unallowable generalization that contravened Article 76(1) EPC.

The chairman further added that regarding Articles 83, 84 and 56 EPC, the reasoning applied to the main request applies accordingly to AR2.

The applicant provided the passage in page 38, lines 19-23 as supporting passage for the disclosure of the objected amendment under Article 76(1) EPC.

The chairman then added that the term "*offering*" is void of any technical character and as such does not overcome the objection under Article 56 EPC presented for the main request.

The chairman then asked the applicant if he had new arguments, which the latter denied.

The chairman concluded that AR2 was not allowable for lack of inventive step of the subject-matter of claim 1 (Article 56 EPC) and for infringing Articles 83, 84 and 76(1) EPC.

Auxiliary Request 3 (AR3)

The chairman admitted AR3 into the proceedings and then referred to sections 8 of the preliminary opinion of the examining division regarding the objections under Articles 76(1), 83, 84 and 56 EPC of auxiliary request 3, for the same reasons as for auxiliary requests 1 and 2, since auxiliary request 3 is a combination of auxiliary requests 1 and 2.

The chairman then asked the applicant if he had further arguments regarding the objections under Articles 76(1), 83, 84 and 56 EPC for AR3, which the latter denied.

The chairman informed the applicant that the examining division has come to the conclusion that the subject-matter of claims 1-5 of AR3 does not satisfy the requirements of Articles 76(1), 83, 84 and 56 EPC.

The proceedings were interrupted from 16:53 to 16:58.

Closing of the proceedings

The chairman first stated that the main request and three auxiliary requests have been examined and then asked the applicant if he had further requests or submissions, which the latter denied.

The chairman announced formally the decision that the application was refused under Article 97(2) EPC as the subject-matter of the main request and auxiliary requests AR1-AR3 did not meet the requirements of Articles 83, 84, 76(1) and 56 EPC.

The chairman stated that the decision is appealable and that the written decision would be notified as soon as possible along with the minutes of the oral proceedings and an indication of the possibility of appeal.

The oral proceedings were closed at 17:00.

After deliberation of the examining division, the chairman announced the following **decision** :

"The European patent application is refused."

Regarding the reasons for the decision, the chairman referred to:

Article 97(2) EPC: the application does not meet the requirements of Article/s 83, 84, 76(1), 56 EPC.

The chairman **closed the proceedings** on 02.07.2019 at 17:00 hours.



signed:

van Praagh, Kay
.....
Chairman

signed:

Fiorenzo Catalano, M
.....
Minute Writer

Enclosure(s):

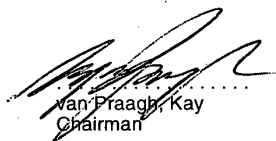
After deliberation of the examining division, the chairman announced the following **decision**:

"The European patent application is refused."

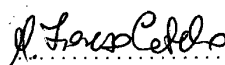
Regarding the reasons for the decision, the chairman referred to:

Article 97(2) EPC: the application does not meet the requirements of Article/s 83, 84, 76(1), 56 EPC.

The chairman **closed the proceedings** on 02.07.2019 at 17:00 hours.



van Praagh, Kay
Chairman



Fiorenzo Catalano, M
Minute Writer

Annex(es):

Application No. :

13 167 436.8

Minutes of the oral proceedings before the EXAMINING DIVISION

The proceedings were not public.

Proceedings opened on 02.07.2019 **at** 15:15 **hours**

Examining Division:

Chairman:	van Praagh, Kay
1st member:	Arbutina, Ljiljana
2nd member:	Fiorenzo Catalano, M
Minute writer:	Fiorenzo Catalano, M

Present as/for the applicant/s:

M. Heise

The identity of the person/s present and, where necessary, the authorisation to represent/authority to act were checked.

Essentials of the oral proceedings and relevant statements of the applicant/s:



European Patent Office
Postbus 5818
2280 HV Rijswijk
NETHERLANDS
Tel: +31 70 340 2040
Fax: +31 70 340 3016



Grünecker Patent- und Rechtsanwälte
PartG mbB
Leopoldstraße 4
80802 München
ALLEMAGNE

Formalities Officer
Name: Delimon, Krista
Tel: +31 70 340 - 4446
or call
+31 (0)70 340 45 00

Application No. 13 167 436.8 - 1217	Ref. EP1067381EHmf	Date 24.07.2019
Applicant Webroot Inc.		

Provision of a copy of the minutes in accordance with Rule 124(4) EPC

The attached copy of the minutes of the oral proceedings is sent to you in accordance with Rule 124(4) EPC.



Delimon, Krista
For the Examining Division
Tel. No.: +31 70 340 - 4446

Branch at The Hague

Enclosure(s): Copy of the minutes (Form 2009)

The amendments and the Applicant's arguments have been taken into careful consideration. The preliminary opinion of the Division is that none of the requests currently on file comply with the requirements of EPC, for the reasons presented below. Therefore, the date set for the oral proceedings is maintained.

The Examining Division further notes, after analyzing the application as a whole in the process of establishing the reasoning presented below, that at least some of the objections are such that there appears to be no way of overcoming them by amendments. Therefore, the application is expected to be refused at the end of the procedure.

The division finds it fair to inform the applicant about this preliminary opinion as a professional courtesy, in order for the applicant to take this into account in deciding on further course of action.

Finally, the Applicant is reminded that any further amendments will be admitted into the procedure at the Examining Division's discretion (Rule 137(3) EPC) during the oral proceedings.

The preliminary opinion of the examining division is as follows:

The examination is being carried out on the **following application documents**

Main Request

Description, Pages

1, 3, 5-43	as originally filed		
2, 2a, 4, 4a	received on	04-09-2018	with letter of 04-09-2018

Claims, Numbers

1-5	received on	31-05-2019	with letter of 31-05-2019
-----	-------------	------------	---------------------------

Drawings, Sheets

1/3-3/3	as originally filed
---------	---------------------

Auxiliary Request 1

Datum
Date **CODINGDATE**
Date

Blatt
Sheet 2
Feuille

Anmelde-Nr:
Application No: 13 167 436.8
Demande n°:

Description, Pages

1, 3, 5-43 as originally filed

2, 2a, 4, 4a received on 04-09-2018 with letter of 04-09-2018

Claims, Numbers

1-5 received on 31-05-2019 with letter of 31-05-2019

Drawings, Sheets

1/3-3/3 as originally filed

Auxiliary Request 2

Description, Pages

1, 3, 5-43 as originally filed

2, 2a, 4, 4a received on 04-09-2018 with letter of 04-09-2018

Claims, Numbers

1-5 received on 31-05-2019 with letter of 31-05-2019

Drawings, Sheets

1/3-3/3 as originally filed

Auxiliary Request 3

Description, Pages

1, 3, 5-43 as originally filed

2, 2a, 4, 4a received on 04-09-2018 with letter of 04-09-2018

Claims, Numbers

1-5 received on 31-05-2019 with letter of 31-05-2019

Drawings, Sheets

1/3-3/3 as originally filed

The letters of the applicant will be referred to as follows:

R1: the letter dated 04-09-2018

R2: the letter dated 31-05-2019

Main request

Amendments

1. The amendments of the main request do not solve the objections regarding Article 76(1) EPC from the summons. The applicant neither replied to the objections, nor identified in R2 any support for the new amendments. Instead, the applicant states that the new modifications "*are clarifications to address the objections under items 1.1 to 1.4 of the summons*", and that "*the claimed subject matter complies with the direct and unambiguous disclosure*" by referring to the previously submitted passages.

However, as reasoned in detail in items 1.1. to 1.4 of the summons, the examining division is of the opinion that the claimed subject-matter is not directly and unambiguously derivable from the identified passages.

Therefore, the main request introduces subject-matter which extends beyond the content of the earlier application as filed, contrary to Article 76(1) EPC, for the reasons presented in the summons, which are summarized here below:

- i) (referring to items 1.1 and 1.2) The division maintains that the passages indicated by the applicant do not disclose that the information is received at a database in three separate steps, and stored in an additional step, as recited by claim 1, neither is such subject-matter directly and unambiguously derivable therefrom.
- ii) (referring to items 1.3 and 1.4) The division maintains that the step of searching the database and the step of providing information to the user as recited in claim 1 are neither disclosed in the passages indicated by the applicant, nor are they directly and unambiguously derivable therefrom.

Should the applicant maintain the opinion that "the claimed subject matter complies with the direct and unambiguous disclosure", he is invited to provide further evidence. The applicant is reminded that, where the basis is not explicit, a short explanation of why Art.123(2) EPC is fulfilled should be given (see Guidelines H-III, 2.2).

Clarity / Sufficiency of Disclosure

2. The division maintains the opinion expressed in items 1.3 and 1.4 of the summons that the feature

"searching the database to identify any processes marked as being malware that occurred on computers having the same particular combination of security products as the first remote computer and that were not locally detected"

renders claim 1, and the corresponding claims 3 and 5, unclear, contrary to the requirements of Article 84 EPC, and that the application as filed does not disclose the invention in a manner sufficiently clear and complete for this feature to be carried out by a person skilled in the art, contrary to the requirements of Article 83 EPC.

2.1. Considering Article 84 EPC, in item 1.3 of the summons the division expressed the opinion that "the origin of the marking of processes as being malware is undefined."

The applicant replies in R2 as follows:

"With respect to item 1.3 of the summons, it is further noted that claim 1 defines that the database is searched to identify those processes that are marked as being malware "that occurred on computers" having the same particular combination of security products... Thus, the processes in the database to be searched and eventually identified have been marked as being malware and it is defined that they occurred on other computers. As such, it is not unclear that a database stores processes that did occur on other computers."

The division notes that that this does not answer the question regarding the origin of marking; it remains unclear who, when, or how, marked a process as being malware.

2.1.1. The division puts forward an additional clarity issue concerning the feature under consideration. The feature requires to identify "any processes ... that were not locally detected". This requirement is unclear; it is unclear which process can be considered to be "a process not locally detected".

2.2. Considering Article 83 EPC, the applicant replies in R2 as follows:

"Moreover, a person skilled in the art will be able to fully understand and implement the claimed invention and specifically this feature, because the application itself discloses possibilities to identify and mark processes as being malware. This is also not contradicted by the two receiving steps of claim 1, requiring that the database receives information of security products loaded on or available at the first remote computer as well as on the other remote computers. To the contrary, these features clarify that the database is connected to all remote computers and receives information from these computers, so that it is clear that the same database is able to also receive information about processes being marked as malware by these computers."

The division notes, first, that the applicant uses the terminology which is not allowable under Article 76(1) EPC: according to the description, page 38, lines 26-30, the search is done for processes marked "as bad", not "as malware". Second, there is no reply to a question how a skilled person would implement the searching for processes "that were not locally detected". And, third, the division does not see any relevance of the fact the database is able to receive some further information.

Inventive Step

3. The objection under Article 56 EPC presented in the summons is maintained.

3.1. For the sake of completeness, it is further noted that the additional subject matter of dependent claims 2 and 4 consists merely in naming the information, and as such cannot be considered as involving inventive step in the sense of Article 56 EPC.

3.2. The applicant's arguments in favour of inventive step presented in R1 were replied to in the summons, and the additional arguments presented in R2 were not convincing.

The applicant argues in R2 as follows:

"In addition, it has been noted that the Examining Division discusses under section 2 of the summons that the last paragraph of claim 1 could not lead to inventive subject matter, because it only defines features of presenting information to a user that are not considered to be technical. This presumption is considered to be incorrect for the claimed subject matter, because the claimed invention not only presents information to a user, but additionally and inherently provides a technical effect of increasing the computer's effective security (as also literally stated on page 39, line 2 of the original description). This increased security is achieved by the claimed subject matter by the novel manner of how the database can identify processes that are (potentially) malware that the particular (i.e. first) remote computer could not identify locally as malware. This identification of potential malware is novel over the malware detection

process of the cited prior art. By providing this identification of potential malware to the user, the system security is increased, because the risk of malware can now be detected by the system, despite not being detectable locally by the computer, so that once aware of the potential malware, the user can take respective actions or measures against the identified malware. The technical distinguishing features thereby particularly concern the manner of how the potential malware can be automatically detected."

The division cannot agree that providing information to the user has the the technical effect of "increasing the computer's effective security". The passage cited by the applicant reads "...allowing a new user or a user of a new computer to be able to increase the computer's effective security very quickly". As can be seen, whether the security will be increased or not depends entirely on the user. Considering "the novel manner of how the database can identify processes that are (potentially) malware", the division re-iterates the opinion that the feature related to identifying a particular process is drafted in unclear way, and is subject to a lack of sufficiency of disclosure, see reasoning above in items 2.1, 2.1.1 and 2.2. Due to the lack of clarity of this feature, the reasoning of the applicant can not be followed, i.e., the division does not see how or why the process identified by this feature would be "(potentially) malware that the particular (i.e. first) remote computer could not identify locally as malware".

Auxiliary Request 1

4. The first auxiliary request introduces subject-matter which extends beyond the content of the earlier application as filed, contrary to Article 76(1) EPC.

The amendment

"receiving at the database details of processes run by each of said plurality of remote computers, said details comprise whether or not a process has been detected as malware"

is neither disclosed in the passages cited by the applicant, nor is it directly and unambiguously derivable therefrom.

The first passage indicated by the applicant recites

"The community database 7 in this embodiment is also provided by the agent software with details of processes run by every computer 2 and thus knows whether or not a process has been detected by each computer 2."

The second passage indicated by the applicant recites

"In a simple example, if for example the database knows that a computer in the past has version A of anti-virus product B with downloaded signature update C, and also has a firewall D with particular settings E, and perhaps anti-spyware software F with signature updates G, but that a particular malware process P was not detected by this combination of programs at that point in time"

The third passage indicated by the applicant recites:

"the database 7, when provided with information relating to all the security products, etc. on a particular computer at a particular time, is searched for events for processes marked as "bad" that occurred on computers with that particular mix of security products and that were not locally detected".

As can be seen, none of the passages disclose receiving details whether or not a process has been detected as malware, and neither is such subject-matter directly and unambiguously derivable therefrom.

5. The above discussed feature is the only amendment of auxiliary request 1 with respect to the main request. Therefore, for the remaining features of auxiliary request 1, the arguments presented above for the main request apply.

Auxiliary request 2

6. Auxiliary request 2 introduces subject-matter which extends beyond the content of the earlier application as filed, contrary to Article 76(1) EPC, for the following reason:

Auxiliary request 2 is based on the main request, whereby the last feature of claims 1 and 3 is amended based on, as indicated in R2, page 38, lines 15 - 23.

However, the indicated passage discloses a specific example, which does not give support for the generalization claimed in the amended feature.

7. The above discussed feature is the only amendment of auxiliary request 2 with respect to the main request. Therefore, for the remaining features of auxiliary request 2, the arguments presented above for the main request apply. In particular, the part of the amendment reciting "offering the user software to download and install to remove the risk" is void of any technical character and as such does not overcome the inventive step objection presented for the main request.

Auxiliary Request 3

8. The third auxiliary is a combination of auxiliary requests 1 and 2. Therefore, the reasons presented for auxiliary requests 1 and 2 apply also to the third auxiliary request.



European Patent Office
80298 MUNICH
GERMANY

Questions about this communication ?
Contact Customer Services at www.epo.org/contact

Soliman, Ahmed



Grünecker Patent- und Rechtsanwälte
PartG mbB
Leopoldstraße 4
80802 München
ALLEMAGNE

FAXED ON 20.06.19

Date
27.06.2019

Reference EP1067381EHmf	Application No./Patent No. 13167436.8 - 1217 / 2629232
Applicant/Proprietor Webroot Inc.	

BRIEF COMMUNICATION

Oral Proceedings on 02.07.19 at 13:00 hours

- Subject: ☒ Your letter of 31.05.19
☐ Maintenance / Cancellation / postponement at the instigation of the division
☐ Consultation by telephone on.....(EPO Form 2036)
- Communication: 1. ☒ The date / time fixed for oral proceedings is maintained.
☒ The reasons are indicated on enclosed EPO Form 2906.
2. ☐ The above-mentioned oral proceedings will start at hours.
3. ☐ The summons to attend oral proceedings on the date indicated above is cancelled.
- 3.1 ☐ The reasons are indicated on enclosed EPO Form 2906.
☐ The procedure will be continued in writing.
☐ A new date will be set later.
☐ New summons will follow.
- 3.2 ☐ For administrative reasons the oral proceedings are postponed to a later date. New summons will follow.
- 3.3 ☐ The application is deemed to be withdrawn. The right to oral proceedings only persists as long as proceedings are pending.
4. ☐ The request for the oral proceedings to be held by videoconference:
- 4.1 ☐ is allowed.
- 4.2 ☐ is rejected.
- ☐ No videoconference studio is available on the date indicated above.
☐ See enclosed EPO Form 2906.

5. ☒ Please confirm receipt of this communication by return fax with date stamp and signature to the EPO central fax server in Munich: (+49) (0) 89 23 99 44 65.

Please take note.

For the Examining Division



Enclosure(s): ☒ EPO Form 2906
☐ EPO Form 2036

VERZEND CONTROLE RAPPORT

TIJD : 20/06/2019 15:53
 NAAM :
 FAX :
 TEL :
 SER NR: E71281A8J539713

DATUM, TIJD
 FAX NR./NAAM
 TIJDSDUUR
 PAGINA'S
 RESULT
 MODE

20/06 15:51
 0004989220287
 00:01:52
 08
 OK
 STANDAARD
 FCM



European Patent Office
 80298 MUNICH
 GERMANY

Questions about this communication ?
 Contact Customer Services at www.epo.org/contact

Sollman, Ahmed



Grünecker Patent- und Rechtsanwälte
 PartG mbB
 Leopoldstraße 4
 80802 München
 ALLEMAGNE

FAXED ON 20.06.19

Date
 27.06.2019

Reference EP1067381EHmf	Application No./Patent No. 13167436.8 - 1217 / 2629232
Applicant/Proprietor Webroot Inc.	

BRIEF COMMUNICATION

Oral Proceedings on 02.07.19 at 13:00 hours

Subject: ☒ Your letter of 31.05.19
☐ Maintenance / Cancellation / postponement at the instigation of the division
☐ Consultation by telephone on.....(EPO Form 2036)

Communication: 1. ☒ The date / time fixed for oral proceedings is maintained.
☒ The reasons are indicated on enclosed EPO Form 2906.
 2. ☐ The above-mentioned oral proceedings will start at hours.
 3. ☐ The summons to attend oral proceedings on the date indicated above is cancelled.
 3.1 ☐ The reasons are indicated on enclosed EPO Form 2906.
☐ The procedure will be continued in writing.
☐ A new date will be set later.

EP Application No.: 13 167 436.8
Applicant: WEBROOT INC.
Our Ref.: EP106738I-EH
Date: May 31, 2019

5

new CLAIMS – Auxiliary Request 1 – marked-up against new main request

1. A method of determining the protection that a first remote computer of a plurality of remote computers has from malware, the method comprising:
- 10 receiving at a database (7) of a base computer (3) information of all or selected security products loaded on or available at a point in time on said first remote computer (2);
- receiving at the database (7) information of all or selected security products loaded on or available at a point in time on other remote computers (2) of said plurality of remote computers connected to the database (7);
- 15 receiving at the database (7) details of processes run by each of said plurality of remote computers (2), said details comprise whether or not a process has been detected as malware¹;
- storing the information and the details in the database (7);
- searching the database (7) to identify any processes marked as being malware that occurred on computers (2) having the same particular combination of security products as the first remote computer (2) and that were not locally detected; and
- 20 providing information to the user of said first remote computer (2) that said first remote computer (2) may be susceptible to attack by said identified any processes marked as being malware.
2. A method according to claim 1, wherein the information of all or selected security products includes the name of the security products, versions, and loaded signature files.
- 25 3. Apparatus for determining the protection that a first remote computer of a plurality of remote computers has from malware, the apparatus comprising:

¹ Derivable from original parent:

- page 37, lines 21-24 ("database 7 ...is provided...with details of processes... and thus knows whether or not a process has been detected...") and
- page 38, lines 1-7 ("...database knows that a computer...has [security products].... but that a particular malware process P was not detected by this [computer's combination of security products]...") and
- page 38, lines 25-30 ("database 7...is searched for events [f]or processes marked... that occurred on computers with that...security products and that were not locally detected [on a particular computer relating to the security products].")

a database (7) of a base computer (3) adapted to:

receive information of all or selected security products loaded on or available at a point in time on said first remote computer (2),

5 receive information of all or selected security products loaded on or available at a point in time on other remote computers (2) of said plurality of remote computers connected to the database (7),

receive details of processes run by each of said plurality of remote computers (2), said details comprise whether or not a process has been detected as malware, and

store the information and the details in the database (7); and

10 the base computer (3) being adapted to:

search the database (7) to identify any processes marked as malware that occurred on computers (2) having the same particular combination of security products as the first remote computer (2) and that were not locally detected, and

15 provide information to the user of said first remote computer (2) that said first remote computer (2) may be susceptible to attack by said identified any processes marked as being malware.

4. Apparatus according to claim. 3, wherein the information of all or selected security products includes the name of the security products, versions, and loaded signature files.

20 5. A computer program comprising program instructions for causing a computer to perform the method of claim 1 or claim 2.

EP Application No.: 13 167 436.8
Applicant: WEBROOT INC.
Our Ref.: EP106738I-EH
Date: May 31, 2019

5

new CLAIMS – Auxiliary Request 3 – marked-up against new main request

(= combination of Auxiliary Requests 1 and 2)

1. A method of determining the protection that a first remote computer of a plurality of remote computers has from malware, the method comprising:
- 10 receiving at a database (7) of a base computer (3) information of all or selected security products loaded on or available at a point in time on said first remote computer (2);
- receiving at the database (7) information of all or selected security products loaded on or available at a point in time on other remote computers (2) of said plurality of remote computers connected to the database (7);
- 15 receiving at the database (7) details of processes run by each of said plurality of remote computers (2), said details comprise whether or not a process has been detected as malware¹;
- storing the information and the details in the database (7);
- searching the database (7) to identify any processes marked as being malware that
- 20 occurred on computers (2) having the same particular combination of security products as the first remote computer (2) and that were not locally detected; and
- providing information to the user of said first remote computer (2) that the security products on said first remote computer (2) expose the first remote computer to a risk of being infected~~may be susceptible to attack~~ by said identified any processes marked as
- 25 being malware and offering the user software to download and install to remove the risk².
2. A method according to claim 1, wherein the information of all or selected security products includes the name of the security products, versions, and loaded signature files.

¹ Derivable from original parent:

- page 37, lines 21-24 ("database 7 ...is provided...with details of processes... and thus knows whether or not a process has been detected...") and
- page 38, lines 1-7 ("...database knows that a computer...has [security products]... but that a particular malware process P was not detected by this [computer's combination of security products]...") and
- page 38, lines 25-30 ("database 7...is searched for events [f]or processes marked... that occurred on computers with that...security products and that were not locally detected [on a particular computer relating to the security products].")

² Derivable from page 38, lines 15-23

3. Apparatus for determining the protection that a first remote computer of a plurality of remote computers has from malware, the apparatus comprising:

a database (7) of a base computer (3) adapted to:

5 receive information of all or selected security products loaded on or available at a point in time on said first remote computer (2),

receive information of all or selected security products loaded on or available at a point in time on other remote computers (2) of said plurality of remote computers connected to the database (7),

10 receive details of processes run by each of said plurality of remote computers (2), said details comprise whether or not a process has been detected as malware, and

store the information and the details in the database (7); and

the base computer (3) being adapted to:

15 search the database (7) to identify any processes marked as malware that occurred on computers (2) having the same particular combination of security products as the first remote computer (2) and that were not locally detected, and

20 provide information to the user of said first remote computer (2) that the security products on said first remote computer (2) expose the first remote computer to a risk of being infected~~may be susceptible to attack~~ by said identified any processes marked as being malware and offer the user software to download and install to remove the risk.

4. Apparatus according to claim 3, wherein the information of all or selected security products includes the name of the security products, versions, and loaded signature files.

- 25 5. A computer program comprising program instructions for causing a computer to perform the method of claim 1 or claim 2.

EP Application No.: 13 167 436.8
Applicant: WEBROOT INC.
Our Ref.: EP106738I-EH
Date: May 31, 2019

5

NEW CLAIMS – Main Request – marked-up against previously submitted claims

1. A method of determining the protection that a first remote computer of a plurality of remote computers has from malware, the method comprising:

10 receiving at a database (7) of a base computer (3) information of all or selected security products loaded on or available at a point in time on said first remote computer (2);

receiving at the database (7) information of all or selected security products loaded on or available at a point in time on other remote computers (2) of said plurality of remote computers connected to the database (7) ~~and;~~

15 receiving at the database (7) details of processes run by said ~~other plurality of~~ remote computers (2); ~~and~~

storing the information and the details in the database (7);

searching the database (7) to identifying any processes marked as being malware that occurred on computers (2) having the same particular combination of security products as the first remote computer (2) and that were not locally detected; and

20 providing ~~the identified~~ information to the user of said first remote computer (2) that said first remote computer (2) may be susceptible to attack by said identified any processes marked as being malware ~~processes on the basis of said identifying~~.

2. A method according to claim 1, wherein the information of all or selected security products includes the name of the security products, versions, and loaded signature files.

25

3. Apparatus for determining the protection that a first remote computer of a plurality of remote computers has from malware, the apparatus comprising:

a database (7) of a base computer (3) ~~constructed and arranged~~ adapted to:

30 receive information of all or selected security products loaded on or available at a point in time on said first remote computer (2); ~~and~~

~~the database (7) being constructed and arranged to receive~~ information of all or selected security products loaded on or available at a point in time on other remote computers (2) of said plurality of remote computers connected to the database (7) ~~and;~~

receive details of processes run by said ~~other plurality of~~ remote computers (2), and
 to store the information and the details in the database (7); and
 the base computer (3) being ~~constructed and arranged~~ adapted to:
 search the database (7) to identify any processes marked as malware that occurred
 on computers (2) having the same particular combination of security products as the
 first remote computer (2) and that were not locally detected, and
 wherein the base computer (3) is ~~constructed and arranged to provide the identified~~
 information to the user of said first remote computer (2) that said first remote
 computer (2) may be susceptible to attack by said identified any processes marked
as being malware processes on the basis of said identifying.

4. Apparatus according to claim 3, wherein the information of all or selected security products includes the name of the security products, versions, and loaded signature files.
5. A computer program comprising program instructions for causing a computer to perform the method of claim 1 or claim 2.

EP Application No.: 13 167 436.8
Applicant: WEBROOT INC.
Our Ref.: EP106738I-EH
Date: May 31, 2019

5

new CLAIMS – Auxiliary Request 2 – marked-up against new main request

1. A method of determining the protection that a first remote computer of a plurality of remote computers has from malware, the method comprising:
- 10 receiving at a database (7) of a base computer (3) information of all or selected security products loaded on or available at a point in time on said first remote computer (2);
- receiving at the database (7) information of all or selected security products loaded on or available at a point in time on other remote computers (2) of said plurality of remote computers connected to the database (7);
- 15 receiving at the database (7) details of processes run by said plurality of remote computers (2);
- storing the information and the details in the database (7);
- searching the database (7) to identify any processes marked as being malware that occurred on computers (2) having the same particular combination of security products as the first remote computer (2) and that were not locally detected; and
- 20 providing information to the user of said first remote computer (2) that the security products on said first remote computer (2) expose the first remote computer to a risk of being infected~~may be susceptible to attack~~ by said identified any processes marked as being malware and offering the user software to download and install to remove the risk¹.
2. A method according to claim 1, wherein the information of all or selected security products includes the name of the security products, versions, and loaded signature files.
- 25 3. Apparatus for determining the protection that a first remote computer of a plurality of remote computers has from malware, the apparatus comprising:
- a database (7) of a base computer (3) adapted to:
- 30 receive information of all or selected security products loaded on or available at a point in time on said first remote computer (2),

¹ Derivable from page 38, lines 15-23

receive information of all or selected security products loaded on or available at a point in time on other remote computers (2) of said plurality of remote computers connected to the database (7),

receive details of processes run by said plurality of remote computers (2), and

5 store the information and the details in the database (7); and

the base computer (3) being adapted to:

search the database (7) to identify any processes marked as malware that occurred on computers (2) having the same particular combination of security products as the first remote computer (2) and that were not locally detected, and

10 provide information to the user of said first remote computer (2) that the security products on said first remote computer (2) expose the first remote computer to a risk of being infected~~may be susceptible to attack~~ by said identified any processes marked as being malware and offer the user software to download and install to remove the risk.

15 4. Apparatus according to claim 3, wherein the information of all or selected security products includes the name of the security products, versions, and loaded signature files.

5. A computer program comprising program instructions for causing a computer to perform the method of claim 1 or claim 2.

EP Application No.: 13 167 436.8
Applicant: WEBROOT INC.
Our Ref.: EP106738I-EH
Date: May 31, 2019

5

CLAIMS – Auxiliary Request 3

1. A method of determining the protection that a first remote computer of a plurality of remote computers has from malware, the method comprising:

receiving at a database (7) of a base computer (3) information of all or selected security
10 products loaded on or available at a point in time on said first remote computer (2);

receiving at the database (7) information of all or selected security products loaded on or
available at a point in time on other remote computers (2) of said plurality of remote
computers connected to the database (7);

receiving at the database (7) details of processes run by each of said plurality of remote
15 computers (2), said details comprise whether or not a process has been detected as
malware;

storing the information and the details in the database (7);

searching the database (7) to identify any processes marked as being malware that
occurred on computers (2) having the same particular combination of security products
20 as the first remote computer (2) and that were not locally detected; and

providing information to the user of said first remote computer (2) that the security
products on said first remote computer (2) expose the first remote computer to a risk of
being infected by said identified any processes marked as being malware and offering
the user software to download and install to remove the risk.
- 25 2. A method according to claim 1, wherein the information of all or selected security
products includes the name of the security products, versions, and loaded signature
files.
3. Apparatus for determining the protection that a first remote computer of a plurality of
remote computers has from malware, the apparatus comprising:
30 a database (7) of a base computer (3) adapted to:

receive information of all or selected security products loaded on or available at a
point in time on said first remote computer (2),

receive information of all or selected security products loaded on or available at a point in time on other remote computers (2) of said plurality of remote computers connected to the database (7),

5 receive details of processes run by each of said plurality of remote computers (2),
said details comprise whether or not a process has been detected as malware, and
store the information and the details in the database (7); and

the base computer (3) being adapted to:

10 search the database (7) to identify any processes marked as malware that occurred
on computers (2) having the same particular combination of security products as the
first remote computer (2) and that were not locally detected, and

provide information to the user of said first remote computer (2) that the security
products on said first remote computer (2) expose the first remote computer to a risk
of being infected by said identified any processes marked as being malware and
offer the user software to download and install to remove the risk.

15 4. Apparatus according to claim 3, wherein the information of all or selected security
products includes the name of the security products, versions, and loaded signature
files.

5. A computer program comprising program instructions for causing a computer to perform
the method of claim 1 or claim 2.

EP Application No.: 13 167 436.8
Applicant: WEBROOT INC.
Our Ref.: EP106738I-EH
Date: May 31, 2019

5

CLAIMS – Auxiliary Request 1

1. A method of determining the protection that a first remote computer of a plurality of remote computers has from malware, the method comprising:

receiving at a database (7) of a base computer (3) information of all or selected security products loaded on or available at a point in time on said first remote computer (2);

receiving at the database (7) information of all or selected security products loaded on or available at a point in time on other remote computers (2) of said plurality of remote computers connected to the database (7);

receiving at the database (7) details of processes run by each of said plurality of remote computers (2), said details comprise whether or not a process has been detected as malware;

storing the information and the details in the database (7);

searching the database (7) to identify any processes marked as being malware that occurred on computers (2) having the same particular combination of security products as the first remote computer (2) and that were not locally detected; and

providing information to the user of said first remote computer (2) that said first remote computer (2) may be susceptible to attack by said identified any processes marked as being malware.
2. A method according to claim 1, wherein the information of all or selected security products includes the name of the security products, versions, and loaded signature files.
3. Apparatus for determining the protection that a first remote computer of a plurality of remote computers has from malware, the apparatus comprising:

a database (7) of a base computer (3) adapted to:

receive information of all or selected security products loaded on or available at a point in time on said first remote computer (2),

receive information of all or selected security products loaded on or available at a point in time on other remote computers (2) of said plurality of remote computers connected to the database (7),

receive details of processes run by each of said plurality of remote computers (2),
said details comprise whether or not a process has been detected as malware, and
store the information and the details in the database (7); and

the base computer (3) being adapted to:

- 5 search the database (7) to identify any processes marked as malware that occurred
 on computers (2) having the same particular combination of security products as the
 first remote computer (2) and that were not locally detected, and
 provide information to the user of said first remote computer (2) that said first remote
10 computer (2) may be susceptible to attack by said identified any processes marked
 as being malware.
4. Apparatus according to claim 3, wherein the information of all or selected security
 products includes the name of the security products, versions, and loaded signature
 files.
5. A computer program comprising program instructions for causing a computer to perform
15 the method of claim 1 or claim 2.

EP Application No.: 13 167 436.8
Applicant: WEBROOT INC.
Our Ref.: EP106738I-EH
Date: May 31, 2019

5

CLAIMS – Main Request

1. A method of determining the protection that a first remote computer of a plurality of remote computers has from malware, the method comprising:

receiving at a database (7) of a base computer (3) information of all or selected security products loaded on or available at a point in time on said first remote computer (2);

receiving at the database (7) information of all or selected security products loaded on or available at a point in time on other remote computers (2) of said plurality of remote computers connected to the database (7);

receiving at the database (7) details of processes run by said plurality of remote computers (2);

storing the information and the details in the database (7);

searching the database (7) to identify any processes marked as being malware that occurred on computers (2) having the same particular combination of security products as the first remote computer (2) and that were not locally detected; and

providing information to the user of said first remote computer (2) that said first remote computer (2) may be susceptible to attack by said identified any processes marked as being malware.

2. A method according to claim 1, wherein the information of all or selected security products includes the name of the security products, versions, and loaded signature files.

3. Apparatus for determining the protection that a first remote computer of a plurality of remote computers has from malware, the apparatus comprising:

a database (7) of a base computer (3) adapted to:

receive information of all or selected security products loaded on or available at a point in time on said first remote computer (2),

receive information of all or selected security products loaded on or available at a point in time on other remote computers (2) of said plurality of remote computers connected to the database (7),

receive details of processes run by said plurality of remote computers (2), and
store the information and the details in the database (7); and

the base computer (3) being adapted to:

5 search the database (7) to identify any processes marked as malware that occurred
on computers (2) having the same particular combination of security products as the
first remote computer (2) and that were not locally detected, and

provide information to the user of said first remote computer (2) that said first remote
computer (2) may be susceptible to attack by said identified any processes marked
as being malware.

- 10 4. Apparatus according to claim 3, wherein the information of all or selected security
products includes the name of the security products, versions, and loaded signature
files.
5. A computer program comprising program instructions for causing a computer to perform
the method of claim 1 or claim 2.

EP Application No.: 13 167 436.8
Applicant: WEBROOT INC.
Our Ref.: EP106738I-EH
Date: May 31, 2019

5

CLAIMS – Auxiliary Request 2

1. A method of determining the protection that a first remote computer of a plurality of remote computers has from malware, the method comprising:

10 receiving at a database (7) of a base computer (3) information of all or selected security products loaded on or available at a point in time on said first remote computer (2);

receiving at the database (7) information of all or selected security products loaded on or available at a point in time on other remote computers (2) of said plurality of remote computers connected to the database (7);

15 receiving at the database (7) details of processes run by said plurality of remote computers (2);

storing the information and the details in the database (7);

searching the database (7) to identify any processes marked as being malware that occurred on computers (2) having the same particular combination of security products as the first remote computer (2) and that were not locally detected; and

20 providing information to the user of said first remote computer (2) that the security products on said first remote computer (2) expose the first remote computer to a risk of being infected by said identified any processes marked as being malware and offering the user software to download and install to remove the risk.
2. A method according to claim 1, wherein the information of all or selected security products includes the name of the security products, versions, and loaded signature files.
25
3. Apparatus for determining the protection that a first remote computer of a plurality of remote computers has from malware, the apparatus comprising:

a database (7) of a base computer (3) adapted to:

30 receive information of all or selected security products loaded on or available at a point in time on said first remote computer (2),

receive information of all or selected security products loaded on or available at a point in time on other remote computers (2) of said plurality of remote computers connected to the database (7),

receive details of processes run by said plurality of remote computers (2), and
store the information and the details in the database (7); and
the base computer (3) being adapted to:

- 5 search the database (7) to identify any processes marked as malware that occurred
on computers (2) having the same particular combination of security products as the
first remote computer (2) and that were not locally detected, and
- provide information to the user of said first remote computer (2) that the security
products on said first remote computer (2) expose the first remote computer to a risk
of being infected by said identified any processes marked as being malware and
10 offer the user software to download and install to remove the risk.
4. Apparatus according to claim 3, wherein the information of all or selected security
products includes the name of the security products, versions, and loaded signature
files.
5. A computer program comprising program instructions for causing a computer to perform
15 the method of claim 1 or claim 2.

Video Conference Details

System 1 (Polycom 1)

Brand of vico system: Polycom 7000 HDX
Name of vico studio: Grünecker Patent- und Rechtsanwälte -1

IP

Transmission speed: up to 2 Mbit/s (Standard 1 Mbit/s)
Standards H.323
Security Encryption AES FIPS 197,H235V3 und H.233/234f

Video dial-in numbers:

IP-Address (H.323) 217.9.115.202
Studio location: variable
Studio telephone number: +49 89 21235 -0
Studio fax number : +49 89 22 02 87

Names of contact for pre-vico test:

Grunecker IT Support +4989212351149, support@grunecker.de

System 2 (Polycom2)

Brand of vico system: Polycom 7000 HDX
Name of vico studio: Grünecker Patent- und Rechtsanwälte -2

IP

Transmission speed: up to 2 Mbit/s (Standard 1 Mbit/s)
Standards H.323
Security Encryption AES FIPS 197,H235V3 und H.233/234f

Video dial-in numbers:

IP-Address (H.323) 217.9.115.203
Studio location: variable
Studio telephone number: +49 89 21235 -0
Studio fax number : +49 89 220287

Names of contact for pre-vico test:

Grunecker IT Support +4989212351149, support@grunecker.de

System 3 (Polycom3)

Brand of vico system: Polycom Group 500
Name of vico studio: Grünecker Patent- und Rechtsanwälte -3

IP

Transmission speed: up to 2 Mbit/s (Standard 1 Mbit/s)
Standards H.323
Security Encryption AES FIPS 197,H235V3 und H.233/234f

Video dial-in numbers:

IP-Address (H.323) 217.9.115.204
Studio location: C.II.20
Studio telephone number: +49 89 21235 -1654
Studio fax number : (C.II.12) +49 89 21235 -2440

Names of contact for pre-vico test:

Grunecker IT Support +4989212351149, support@grunecker.de

Stand: 12.09.2017

European Patent Office

Bob-van-Bentham-Platz 1
80469 München

Ihr Zeichen / Your Ref.

Unser Zeichen / Our Ref.

Datum / Date

EP1067381-EHswa

May 31, 2019

European Patent Application No. 13 167 436.8
Applicant: WEBROOT INC.

In preparation of the oral proceedings:

Herewith submitted are:

- a new Main Request comprising new claims 1 to 5 to replace all claims on file;
- a First Auxiliary Request comprising new claims 1 to 5 to replace all claims on file;
- a Second Auxiliary Request comprising new claims 1 to 5 to replace all claims on file;
- a Third Auxiliary Request comprising new claims 1 to 5 to replace all claims on file.

Also enclosed are marked-up copies of all claim sets highlighting all claim amendments.

The claims have been amended in reply to the objections raised in the summons.

MÜNCHEN
Patentanwälte
European Patent Attorneys
Thomas Schuster
Dr. Klara Goldbach
Martin Aufenanger, LL.M., MM¹
Dr. Heike Vogelsang-Wenke
Reinhard Knauer
Dietmar Kuhl
Dr. Franz-Josef Zimmer
Bettina K. Reichelt
Dr. Anton K. Pfau
Dr. Udo Weigelt, LL.M.
Rainer Bertram
Jens C. Koch, M.S. (U of PA)
Bernd Rothaemel
Thomas W. Laubenthal, LL.M.
Dr. Andreas Kayser
Dr. Jens Hammer
Dr. Thomas Eickelkamp
Dr. Peter Miltényi²
Dr. Moritz Höffe, LL.M.
Gero Maatz-Jansen
Michael Heise
Christian Meisinger
Dr. Martin Ahr
Dr. Wolfgang Neubeck
Steven M. Zeman, Ph.D.
André Nickel
Felix Kahr
Dr. Alexander Stumvoll, LL.M.
Dr. Stefano Marchini³
Dr. Thomas Kronberger
Yilin Jin
Dr. Georg Seisenberger
Dr. Olivia Nemethova, LL.M.
Dr. Rainer Plaggenborg
Victor Lopes Aguiar
Dr. Sabine Koch
Wolfram Thomas
Dr. Markus Grammel
Dr. Jegannath Korukottu⁴

Rechtsanwälte
Attorneys-at-Law
Dr. Ulrich Blumenröder, LL.M.
Prof. Dr. Maximilian Kinkeldey, LL.M.⁵
Dr. Karsten Brandt
Anja Franke, LL.M.
Ute Stephani
Dr. Bernd Allekotte, LL.M.⁶
Dr. Elvira Bertram, LL.M.
Babett Ertle
Christine Neuhiel
Sabine Brandstätter
Cornelia Schmitt
Petra Lübke
Dr. Holger Gauss
Dr. Nicolás Schmitz
Marina Schlumberger
Kirsten Hammerstingl
Sebastian Clotten, LL.M.
Jennifer Rosenhäger, LL.M.
Mark Peters, LL.M.
Dr. Nicola Busch
Julia Bittner, LL.M.
Sebastian Ochs
Philipp Strommer
Jan Rether
Karin Lochner
Swetlana Frese

BERLIN
Patentanwälte
European Patent Attorneys
Dr. Patrick P. Erk, M.S. (MIT)
Tino Rumpold

KÖLN
Patentanwälte
European Patent Attorneys
Dr. Martin Dropmann

PARIS⁷
Conseil en Propriété Industrielle
European Patent Attorney
Dr. Wolfgang Neubeck

OF COUNSEL
Patentanwälte
European Patent Attorneys
Gottfried Klitzsch

Rechtsanwälte
Attorneys-at-Law
Dr. Helmut Eichmann
Gerhard Barth

Grünecker Patent- und Rechtsanwälte PartG mbB

Leopoldstr. 4
80802 München
Germany

Tel. +49 (0) 89 21 23 50
Fax +49 (0) 89 22 02 87
Mail info@grünecker.de

Amtsgericht: München
Partnerschaftsregister:
PR 1397

Deutsche Bank München
SWIFT / BIC-code: DEUT DE MM
IBAN: DE47 7007 0010 0175 173400

¹ auch/also: Mediator ² auch/also: Agente de la Propiedad Industrial (España) ³ auch/also: Consulente in Brevetti (Italia)

⁴ European Patent Attorney and UK Chartered Patent Attorney ⁵ Professor an der Fachhochschule für angewandtes Management

⁶ auch/also: Attorney-at-Law, New York ⁷ in Kooperation/in cooperation

The new claims of the Main Request are thereby based on the previously submitted claims with additional clarifications to address the objections under items 1.1 to 1.4 of the summons.

At least with these further amendments and clarifications, the claimed subject matter complies with the direct and unambiguous disclosure given by the application as originally filed on page 36, line 15 through page 39 line 2 as previously submitted and as discussed in the summons, as well as the corresponding summary section on original description page 11, line 5 through page 12, line 17.

With respect to item 1.3 of the summons, it is further noted that claim 1 defines that the database is searched to identify those processes that are marked as being malware "that occurred on computers" having the same particular combination of security products... Thus, the processes in the database to be searched and eventually identified have been marked as being malware and it is defined that they occurred on other computers. As such, it is not unclear that a database stores processes that did occur on other computers. Moreover, a person skilled in the art will be able to fully understand and implement the claimed invention and specifically this feature, because the application itself discloses possibilities to identify and mark processes as being malware. This is also not contradicted by the two receiving steps of claim 1, requiring that the database receives information of security products loaded on or available at the first remote computer as well as on the other remote computers. To the contrary, these features clarify that the database is connected to all remote computers and receives information from these computers, so that it is clear that the same database is able to also receive information about processes being marked as malware by these computers.

The independent claims of the First Auxiliary Request additionally define and clarify that the details of the processes that are provided to the database comprise whether or not a process has been detected as malware in order to further address these objections. This additional clarification is unambiguously derivable from the application as originally filed as indicated by the marked-up copy of the First Auxiliary Request.

With regard to the requirements of Article 56 EPC, the previously submitted arguments are respectfully maintained, which are fully applicable to the new claims as the objections under section 1 of the summons are considered to be overcome.

In addition, it has been noted that the Examining Division discusses under section 2 of the summons that the last paragraph of claim 1 could not lead to inventive subject matter, because it only defines features of presenting information to a user that are not considered to be technical. This presumption is considered to be incorrect for the claimed subject matter, because the claimed invention not only presents information to a user, but additionally and inherently provides a technical effect of increasing the computer's effective security (as also literally stated on page 39, line 2 of the original description). This increased security is achieved by the claimed subject matter by the novel manner of how the database can identify processes that are (potentially) malware that the particular (i.e. first) remote computer could not identify locally as malware. This identification of potential malware is novel over the malware detection process of the cited prior art. By providing this identification of potential malware to the user, the system security is increased, because the risk of malware can now be detected by the system, despite not being detectable locally by the computer, so that once aware of the potential malware, the user can take respective actions or measures against the identified malware. The technical distinguishing features thereby particularly concern the manner of how the potential malware can be automatically detected.

The independent claims of the Second Auxiliary Request additionally define that the user is not only provided with information that the security products of his computer is exposed to a risk of being infected, but also with an offer for software to remove the risk. This provision of respective software to download and install to remove the risk thereby goes beyond merely informing the user of the identified risk of locally unidentified malware.

The Third Auxiliary Request is a combination of Auxiliary Requests 1 and 2 and respectively addresses both objections, if necessary.



Michael Heise

Encl.

New claims forming the Main and Auxiliary Requests (clean and marked-up copies)



Bericht van ontvangst/Handtekening Retour
Advice of receipt

EXAM- 13167436.8

CN 07

Stempel van
kantoor van
terugzending

Stamp of the office
returning the advice

Designated operator of the Netherlands
Op kantoor van verzending in te vullen / To complete at office of posting

Kantoor van verzending Office of posting	Datum Date 05.02.2019
Geadresseerde van Addressee of the item Grünecker Patent- und Rechtsanwälte PartG mbB Leopoldstraße 4 80802 München ALLEMAGNE	

Aard van de zending / Nature of the item

Aangetekend nr.:
Registered No. of item

☐ Evt. bedrag en valuta Waarde-
aangifte/Verzekerd Vervoer
Opt. insured amount and currency

RD 425767752 NL

Op plaats van bestemming in te vullen / To sign on place of destination

Naam, datum en handtekening
Name, date and signature

08.02.19 *Lijenski*

* Afhankelijk van de voorschriften in het land van bestemming wordt het bericht getekend door de geadresseerde of zijn gemachtigde of door de postmedewerker

A.R.
EPA EPO OEB
tel: (070)3403060
06 -03- 2019

Priority/By Airmail Mailroom 5

Terugzenden aan (in te vullen door de afz.) / Return to

Naam of firma Name	Europeïsch Patentamt European Patent Office Office Européen des Brevets
Straat en huisnummer Street and No.	PB 5818 - Patentlaan 2
Postcode en plaats Postcode and place	
RH-012 #6621X0X#00#0000#	
POSTBUS 5818 2280 HV RIJSWIJK ZH	





European Patent Office
80298 MUNICH
GERMANY

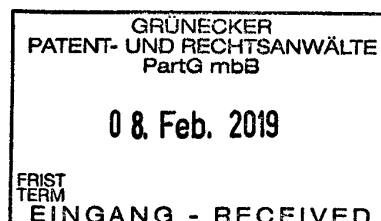
Questions about this communication ?
Contact Customer Services at www.epo.org/contact



Grünecker Patent- und Rechtsanwälte
PartG mbB
Leopoldstraße 4
80802 München
ALLEMAGNE

EPO - Munich
101

11. Feb. 2019



Date
05.02.2019

Reference EP1067381EHmf	Application No./Patent No. 13167436.8 - 1217 / 2629232 ✓
Applicant/Proprietor Webroot Inc.	

EPA/EPO/OEB Formblatt/Form/Formulaire : 2008 + 2906(5 pages)

Empfangsbescheinigung über den Zugang des vorstehend bezeichneten Schriftstücks
Acknowledgement of receipt of the document specified above
Récépissé du document spécifié ci-dessus

Unter Bezugnahme auf die Mitteilung im ABI EPA 7/2010, 377 wird gebeten, die Empfangsbescheinigung mit Empfangsdatum und Unterschrift zu versehen und **umgehend** an das EPA zurückzusenden:

With reference to the Notice in OJ EPO 7/2010, 377, you are requested to date and sign the acknowledgement of receipt and return it to the EPO **immediately**:

Conformément au communiqué paru au JO OEB 7/2010, 377, vous êtes prié d'indiquer sur le récépissé la date de réception du document, de signer le récépissé et de le renvoyer **sans délai** à l' OEB:

- **über die Online-Dienste des EPA** (als Anlage zu EPA Form 1038) / **through EPO Online Services** (as annex to EPO Form 1038) / **par les services en ligne de l'OEB** (en tant que pièce jointe au formulaire OEB 1038),
- **per Fax / by fax / par téléfax** (+49 (0) 89 2399-4465 or +31 (0) 70 340-3016)
- **oder per Post / or by post / ou par courrier.**

Empfangen am / Received on / Reçu le
GRÜNECKER PATENT- UND RECHTSANWÄLTE PartG mbB
08. Feb. 2019
Unterschrift / Signature: <i>FN Müller</i>
FRIST TERM EINGANG - RECEIVED

Empfangsberechtigter/authorised recipient/
le destinataire ou la personne dûment mandatée

Rücksende-Adresse / Return address / Adresse de retour
(Umschlag / envelope / enveloppe ISO C4 / DL / C6/C5 / C6)

DEUTSCHLAND
80298 MÜNCHEN
Europäisches Patentamt

Rücksende-Adresse / Return address / Adresse de retour

EPA/EPO/OEB Form 2936 08.10



European Patent Office
80298 MUNICH
GERMANY

Questions about this communication ?
Contact Customer Services at www.epo.org/contact



Grünecker Patent- und Rechtsanwälte
PartG mbB
Leopoldstraße 4
80802 München
ALLEMAGNE

Date
05.02.2019

Reference EP1067381EHmf	Application No./Patent No. 13167436.8 - 1217 / 2629232
Applicant/Proprietor Webroot Inc.	

EPA/EPO/OEB Formblatt/Form/Formulaire : 2008 + 2906(5 pages)

Empfangsbescheinigung über den Zugang des vorstehend bezeichneten Schriftstücks
Acknowledgement of receipt of the document specified above
Récépissé du document spécifié ci-dessus

Unter Bezugnahme auf die Mitteilung im ABI EPA 7/2010, 377 wird gebeten, die Empfangsbescheinigung mit Empfangsdatum und Unterschrift zu versehen und **umgehend** an das EPA zurückzusenden:

With reference to the Notice in OJ EPO 7/2010, 377, you are requested to date and sign the acknowledgement of receipt and return it to the EPO **immediately**:

Conformément au communiqué paru au JO OEB 7/2010, 377, vous êtes prié d'indiquer sur le récépissé la date de réception du document, de signer le récépissé et de le renvoyer **sans délai** à l' OEB:

- **über die Online-Dienste des EPA** (als Anlage zu EPA Form 1038) / **through EPO Online Services** (as annex to EPO Form 1038) / **par les services en ligne de l'OEB** (en tant que pièce jointe au formulaire OEB 1038),
- **per Fax / by fax / par téléfax** (+49 (0) 89 2399-4465 or +31 (0) 70 340-3016)
- oder per Post / or by post / ou par courrier.

Empfangen am / Received on / Reçu le :

Unterschrift / Signature:

Empfangsberechtigter/authorised recipient/
le destinataire ou la personne dûment mandatée

Rücksende-Adresse / Return address / Adresse de retour
(Umschlag / envelope / enveloppe ISO C4 / DL / C6/C5 / C6)

DEUTSCHLAND
80298 MÜNCHEN
Europäisches Patentamt

Rücksende-Adresse / Return address / Adresse de retour

Datum
Date 05.02.2019
Date

Blatt
Sheet 1
Feuille

Anmelde-Nr:
Application No: 13 167 436.8
Demande n°:

The examination is being carried out on the **following application documents**

Description, Pages

1, 3, 5-43	as originally filed			
2, 2a, 4, 4a	received on	04-09-2018	with letter of	04-09-2018

Claims, Numbers

1-5	received on	04-09-2018	with letter of	04-09-2018
-----	-------------	------------	----------------	------------

Drawings, Sheets

1/3-3/3	as originally filed
---------	---------------------

Reference is made to the following document; the numbering will be adhered to in the rest of the procedure.

D1	US 2003/131256 A1 (ACKROYD ROBERT JOHN [GB]) 10 July 2003 (2003-07-10)
----	---

Amendments

1. The set of claims filed with the letter of reply dated 04-09-2018 (referred to in the further communication as R2) introduce subject-matter which extends beyond the content of the earlier application as filed, contrary to Article 76(1) EPC, for the following reasons:

Claim 1 recites a method of determining the protection that a first remote computer has from malware, the method comprising:

- a) receiving at a database of a base computer information of all or selected security products loaded on or available at a point in time on said first remote computer;
- b) receiving at the database information of all or selected security products loaded on or available at a point in time on other remote computers connected to the database and details of processes run by said other remote computers, and storing the information in the database;
- c) searching the database identifying any processes marked as being malware that occurred on computers having the same particular combination of security products as the first remote computer and that were not locally detected; and

d) providing the identified information to the user of said first remote computer that said first remote computer may be susceptible to attack by said malware processes on the basis of said identifying.

1.1. The basis for amendments of step a) provided in R2 is the same as the basis provided for amendments of step b). Thus, step a) and step b) are amended based on the same passages from the description. However, these passages relate to all the remote computers. It is not disclosed in the application that one type of information is received from one remote computer, and other type of information from other remote computers, in two separate method steps, as claimed, nor is such subject-matter directly and unambiguously derivable therefrom.

1.2. The basis for amendment of step b), reciting "details of processes run by said other remote computers" is to be found, as indicated in R2, on page 37, lines 21-24. However, this passage does not disclose that "details of processes run by said other remote computers" are provided at the same point of time as the other information recited by step b), nor is such subject-matter directly and unambiguously derivable therefrom.

1.3. Considering step c), it appears to be grammatically incorrect ("searching the database identifying any processes marked as being malware..."), rendering the claimed subject-matter unclear in the sense of Article 84 EPC. For the purpose of further analysis, the wording of claim 3 will be used, namely "searching the database to identify any processes marked as being malware...".

The applicant identified in R2 two passages as being bases for this amendment, namely, page 38, lines 5-7 and lines 27-30. These passages recite

"if for example the database knows that a computer in the past has version A of anti-virus product B ..., but that a particular malware process P was not detected by this combination", and,

"the database ... is searched for events for processes marked as "bad" that occurred on computers with that particular mix of security products and that were not locally detected".

As can be seen, the first passage does not disclose searching the database, and the second passage discloses searching the database for events for processes marked as "bad". Therefore, none of the passages discloses the step c), nor is step c) directly and unambiguously derivable therefrom.

Additionally, the scope defined by this step is not clear, contrary to the requirements of Article 84 EPC, since the origin of the marking of processes as being malware is undefined.

Moreover, the amended step introduces subject-matter which is not compliant with the requirements of Article 83 EPC. The step, as far as it can be understood, is expressed in terms of results to be achieved, namely, searching a database for processes marked as being malware that occurred on computers ... and that were not locally detected. The database, on the other hand, receives information listed in steps a) and b), which does not include any information related to detecting malware processes locally. The application does not indicate any way which would allow a skilled person to implement the step c) on this database. Therefore, the application does not meet the requirements of Article 83 EPC considering this subject-matter.

1.4. The basis for the amendment "the identified information" in step d) is to be found, as indicated in R2, on page 38, line 12 or line 30.

First, it is noted that it is not clear which information is referred to by the term "the identified information", contrary to the requirements of Article 84 EPC. The clarity extends also to the passages identified by the applicant as being basis for this amendment: both passages recite "this information can be presented/fed back to the user", where the exact nature of the information remains unspecified. Due to the lack of clarity of the amendment, it cannot be considered as directly and unambiguously derivable from the parent application.

1.5. The same reasoning applies to corresponding independent claims 3 and 5.

Inventive Step

2. Due to the extent of issues concerning Articles 76(1), 83 and 84 EPC, it is not practicable to make a complete inventive step analysis of the present set of claims.

However, the division is of the opinion that the subject-matter of claim 1, as well as corresponding claims 3 and 5, is not inventive in the sense of Article 56 EPC over document D1, which discloses a method of determining the protection that a first remote computer has from malware, the method comprising:

receiving at a database of a base computer information of all or selected security products loaded on or available at a point in time on remote computers (par.[0025], lines 10-15) and information indicating detection of malware items by the malware scanners operating at said computers (par.[0025], lines 6-10), and storing the information in the database;

searching the database to identify the remote computers having the particular combination of security products that does not locally detect a process marked as being malware (par.[0030], lines 9-13 and lines 18-22), and

updating the security products on the remote computers that may be susceptible to attack by said malware processes on the basis of said identifying (par.[0030], lines 18-22).

The subject-matter of independent claims 1, 3 and 5 differs from the teaching of D1

i) in that the information that the computer may be susceptible to attack is provided to the user, which, being presentation of information, cannot be considered as a basis of an inventive step, and

ii) in the subject-matter which is not allowable for the reasons presented above in sections 1.1-1.4.

Therefore, the independent claims do not contain any features that could be considered as having inventive contribution over the prior art.

Applicant's Arguments

3. The arguments of the applicant presented in R2 are based mainly on distinguishing feature c), which, according to the applicant, is to be seen as an alternative solution to the same problem addressed by D1. However, as reasoned here above, sections 1.1 - 1.4, this feature is not compliant with Articles 76(1), 83, and 84 EPC and therefore cannot be considered as basis of an inventive step.

To summarize, the applicant argues in R2 as follows

"These are two alternative, incompatible solutions for increasing the protection of local computers from malware. The solution of D1 (changing the settings of security products to that of other computers with different security products that have detected a malware process) neither implies nor suggests the alternative solution of the claimed invention (informing a computer of non-detected malware processes that were not detected by other computers with the same security products)."

The division notes that, according to the claim, the information is provided to the user, not to the computer, as argued by the applicant. According to the application, page 38, lines 7-15, even when the information is provided to the computer, the only purpose is for it to be presented to the user. Therefore, irrespective of what the information is, and how it is obtained, its presentation to the user does not provide any technical effect, such that no technical problem solved by the present claim can be identified.

Therefore, the division cannot agree with the applicant that the present claim is an alternative solution to the solution of D1, since the present claim does not achieve a technical effect of increasing the protection of local computers from malware.

Closing Remarks

4.0. After having analyzed the application as a whole and the applicant's arguments in the process of establishing the reasoning presented above, the division is of the preliminary opinion that at least some of the objections are such that there appears to be no way of overcoming them by amendments, and, consequently, that the application should be refused under Article 97(2) EPC. Thus, for efficiency reasons, and as requested by the applicant in his letter dated 04-09-2018, the summons for oral proceedings are considered to be the most appropriate next procedural step.

4.1. In the case of further amendments submitted to the examining division, the applicant should be aware that any amendments will be allowed into the procedure at the examining division's discretion (Rule 137(3) EPC).

4.2. In order to facilitate the examination of the conformity of the amended application with the requirements of Article 123(2) EPC, the applicant is requested to clearly identify the amendments made, irrespective of whether they concern amendments by addition, replacement or deletion, and indicate the passages of the application as filed on which these amendments are based. Where the basis is not explicit, in particular when a different wording is used or features are taken only from drawing or generalized from a specific embodiment, a short explanation of why Art.123(2) EPC is fulfilled should be given (see Guidelines H-III, 2.2).

4.3. The subject-matter of the new claims should not diverge considerably from the claims already filed. The subject-matter of auxiliary requests should constitute a limitation in the direction of an intended invention and should not make use of different characteristics in order to branch out in different directions (T1273/04)

4.4. In case of amendments, the applicant is also invited to specify in an accompanying letter the **technical difference** between the independent claims and the prior art, what **technical problem** is solved by said difference, and why the proposed solution is **not obvious** to the skilled person.

4.5. Alternatively, the applicant may request a decision according to the state of the file (see GL C V 15 and E X 2.5) and withdraw the request for Oral Proceedings. The applicant should realise that filing further amendments or argumentation in response to the summons to oral proceedings may preclude the examining division from acceding to such a request.



European Patent Office
80298 MUNICH
GERMANY

Questions about this communication ?

Contact Customer Services at www.epo.org/contact



Grünecker Patent- und Rechtsanwälte
PartG mbB
Leopoldstraße 4
80802 München
ALLEMAGNE

Date

05.02.2019

Reference EP1067381EHmf	Application No./Patent No. 13167436.8 - 1217 / 2629232
Applicant/Proprietor Webroot Inc.	

Summons to attend oral proceedings pursuant to Rule 115(1) EPC

You are hereby summoned to attend oral proceedings arranged in connection with the above-mentioned European patent application.

The matters to be discussed are set out in the communication accompanying this summons (EPO Form 2906).

The oral proceedings, which will not be public, will take place before the Examining Division

on 02.07.19 at 13.00 hrs as a video-conference

No changes to the date of the oral proceedings can be made, except on serious grounds (see OJ EPO 2009, 68). If you do not appear as summoned, the oral proceedings may continue without you (R. 115(2) EPC, see also OJ EPO 2008, 471).

Your attention is drawn to Rule 4 EPC, regarding the language of the oral proceedings, and to Special edition No. 3 OJ EPO 2007, L.1, concerning the filing of authorisations for company employees and lawyers acting as representatives before the EPO.

The final date for making written submissions and/or amendments (R. 116 EPC) is 31.05.19.

In this respect, you are informed that the EPO video-conference studios employ IP technology (SIP or H.323, Videocoding CIF H.261, H.263, H.264, Audiocoding G.711, G.722, max. transmission rate 1024 Kbit/s). Your video-conference equipment should meet a minimum transmission rate of at least 256 Kbit/s, but at least 384 Kbit/s is preferred.

The European Patent Office provides the applicant or his representative with the opportunity to test the video conferencing system in advance of the oral proceedings. It is possible to check the connection in advance using the EPO test system. The SIP/H.323 address is EPOdemo@cvc.epo.org or 69072068@cvc.epo.org.

In case of questions concerning testing or connection to the EPO test system please contact Operators@epo.org.

Please supply the EPO as soon as possible with the following information concerning your videoconference studio:

- type and name of VICO equipment,
- telephone and fax number of the studio including country and area code,
- dialling number to reach the studio including country and area code,
- transmission speed in Kbit/s,
- name of contact person with telephone number and email address to be used by the EPO for communicating the detailed information about the videoconference connection.

IMPORTANT:

Please inform the EPO without delay in the event that the detailed information about the videoconference connection has not been received at least ten days before the scheduled date of the oral proceedings to be held via videoconference.

Please note that the oral proceedings will always take place as scheduled unless you are otherwise informed. The EPO will generally not send a reminder or a further communication prior to the date of oral proceedings.

1st Examiner:
Arbutina, Ljiljana

2nd Examiner:
Fiorenzo Catalano, M

Chairman:
van Praagh, Kay

For the Examining Division

Annexes:
Confirmation of receipt (Form 2936)
Communication (EPO Form 2906)

EP Application No.: 13 167 436.8
Applicant: WEBROOT INC.
Our Ref.: EP106738IEH
Date: September 4, 2018

5

New CLAIMS (marked-up copy against previously submitted claims)

1. A method of determining the protection that a first remote computer has from malware, the method comprising:

10

receiving at a database (7) of¹ a base computer (3) details-information² of all or selected security products ~~operating-loaded on or available³~~ at a point in time on said first remote computer (2);

15

receiving at the ~~base computer (3)~~ database (7)⁴ details-information⁵ of all or selected security products ~~operating-loaded on or available⁶~~ at a point in time on other remote computers (2) connected to the ~~base computer (3)~~ database (7)⁷ and details of processes run by said other remote computers (32) ~~that were not locally identified as being malware⁸~~, and storing the information in ~~a the database (7) at the base computer⁹ (3), wherein some processes in the database (7) are marked as being malware¹⁰;~~

20

searching the database (7) identifying any processes marked as being malware that ~~were not identified by said other remote occurred on¹¹~~ computers (2) having the same particular combination of security products as the first remote computer (2) and that were not locally detected¹²; and;

¹ Derivable from, e.g., page 36, line 15-19; or Fig 1; or page 17, lines 27-29;

² Derivable from, e.g., page 36, line 17-19; or page 37, lines 11-12; or page 38, lines 25-27;

³ Derivable from, e.g., page 36, line 18-19; or page 38, lines 25-27; or page 17, lines 27-33

⁴ Derivable from, e.g., page 36, line 15-19; or Fig 1; or page 17, lines 27-29;

⁵ Derivable from, e.g., page 36, line 17-19; or page 37, lines 11-12; or page 38, lines 25-27; – overcoming **objection 1.1**

⁶ Derivable from, e.g., page 37, lines 11-12 and page 36, line 18-19; or page 38, lines 25-27; or page 17, lines 27-33; – overcoming **objection 1.1**

⁷ Consistency of claim features; derivable from Fig 1

⁸ Overcoming **objection 1.2**; Feature “receiving ... details of processes run” is derivable from, e.g., page 37, lines 21-24.

⁹ Overcoming **objection 1.3**. Firstly, the term “information” is now clarified as it is introduced by the receiving steps. Secondly, the storing feature is derivable from the above-cited passages literally disclosing that this information is “provided to the database 7”, as well as from e.g., page 38, lines 25-30 disclosing that the database 7 is then searched when being provided with that information, which both implies and necessarily requires that the information is stored in the database.

¹⁰ Overcoming **objection 1.4**. However, these feature would also be unambiguously derivable from original parent claims 31-36 and respective description passages on pages 11-12, which clearly and unambiguously concern the same embodiment as on description page 36, line 15 – page 39, line 2.

¹¹ Overcoming **objection 1.5**. Derivable from, e.g., page 38, lines 5-7 and lines 27-30.

¹² Overcoming **objection 1.5**. Derivable from, e.g., page 38, lines 27-30.

providing the identified¹³ information to the user of said first remote computer (2) that said first remote computer (2) may be susceptible to attack by said malware processes on the basis of said identifying.

2. A method according to claim 1, wherein the details-information of all or selected security products includes the name of the security products, versions, and loaded signature files.

3. Apparatus for determining the protection that a first remote computer has from malware, the apparatus comprising:

a database (7) of a base computer (3) constructed and arranged to receive ~~computer details-information~~ of all or selected security products loaded on or available operating-at a point in time on said first remote computer (2);

the database (7) ~~base computer (3)~~ being constructed and arranged to receive details information of all or selected security products loaded on or available operating-at a point in time on other remote computers (2) connected to the database (7) ~~base computer (3)~~ and details of processes run by said other remote computer (2) ~~that were not locally identified as being malware~~ and to store the information in a-the database (7)-at the base computer (3), wherein ~~some processes in the database are marked as being malware~~; and,

the base computer (3) being constructed and arranged to search the database (7) to identify any processes marked as malware that ~~were not identified by said other remote occurred on~~ computers (2) having the same particular combination of security products as the first remote computer (2) and that were not locally detected, wherein the base computer (3) is constructed and arranged to provide the identified information to the user of said first remote computer (2) that said first remote computer (2) may be susceptible to attack by said malware processes on the basis of said identifying.

4. Apparatus according to claim 3, wherein the details-information of all or selected security products includes the name of the security products, versions, and loaded signature files.

5. A computer program comprising program instructions for causing a computer to perform the method of claim 1 or claim 2.

¹³ Mere clarification; derivable from, e.g., page 38, line 12 or line 30: "This information..." is presented/fed back to the user of the computer.

EP Application No.: 13 167 436.8
Applicant: WEBROOT INC.
Our Ref.: EP106738IEH
Date: September 4, 2018

5

CLAIMS

1. A method of determining the protection that a first remote computer has from malware, the method comprising:

10 receiving at a database (7) of a base computer (3) information of all or selected security products loaded on or available at a point in time on said first remote computer (2);

receiving at the database (7) information of all or selected security products loaded on or available at a point in time on other remote computers (2) connected to the database (7) and details of processes run by said other remote computers (2), and storing the information in the database (7);

15 searching the database (7) identifying any processes marked as being malware that occurred on computers (2) having the same particular combination of security products as the first remote computer (2) and that were not locally detected; and

providing the identified information to the user of said first remote computer (2) that said first remote computer (2) may be susceptible to attack by said malware processes on the basis of said identifying.

20
2. A method according to claim 1, wherein the information of all or selected security products includes the name of the security products, versions, and loaded signature files.
3. Apparatus for determining the protection that a first remote computer has from malware, the apparatus comprising:

25 a database (7) of a base computer (3) constructed and arranged to receive information of all or selected security products loaded on or available at a point in time on said first remote computer (2);

the database (7) being constructed and arranged to receive information of all or selected security products loaded on or available at a point in time on other remote computers (2) connected to the database (7) and details of processes run by said other remote computer (2) and to store the information in the database (7); and

30 the base computer (3) being constructed and arranged to search the database (7) to identify any processes marked as malware that occurred on computers (2) having the

same particular combination of security products as the first remote computer (2) and that were not locally detected, wherein the base computer (3) is constructed and arranged to provide the identified information to the user of said first remote computer (2) that said first remote computer (2) may be susceptible to attack by said malware processes on the basis of said identifying.

5

4. Apparatus according to claim 3, wherein the information of all or selected security products includes the name of the security products, versions, and loaded signature files.

5. A computer program comprising program instructions for causing a computer to perform the method of claim 1 or claim 2.

10

Moreover, in order to try to defeat anti-virus products, the malware writers use obfuscation techniques in order to attempt to hide the signature or signature base data of the virus code from detection. Typically, the obfuscation involves encrypting or packing the viral code.

US 2003/131256 A1 discloses a method for controlling a managing computer to manage malware protection within a computer network. A policy organizing server receives status information from the various computers of the network indicating the malware scanning products being used, the scanner engine versions and virus definition data versions being used and the security setting being applied within those different computers. The received status information is used to determine whether each computer within the networks runs out-of-date malware products and out-of-date malware definition data. When the policy organizing server has detected four logged data messages corresponding to a particular item of malware and also detects the pattern that none of these originate from a computer running out-of-date malware definition data, it forces the entire malware action of updating the malware definition data on those computers that are out-of-date.

WO-A-2004/097602 describes a system that analyses computer files received or generated by a local computer and compares these with a database of known files to determine whether a particular file is known and if so whether it has been known about long enough that it can be regarded as "safe". However, in practice, on its own this is not likely to provide for adequate protection because, for example, the active payload of a virus or Trojan may only be programmed to activate at a particular date, or upon receiving a message or instruction from a local or remote system or process, or on the occurrence of a particular event that may be many months or even years after the process has been first run or is released. Thus, just looking at the age of a file is an unsatisfactory way of determining whether it is properly safe and will remain so.

In the system of US-A-2004/0083408, a worm in a file is detected by examining connection attempts made by the specific file running on a computer.

US-A-6944772, US-A-6772346, EP-A-1549012 and EP-A-1280040 all disclose "community-based" anti-malware systems in which a plurality of "local" computers all connect via a network (which may be a LAN or the Internet, for example) to a central computer. On encountering a file that is not already known to them, the local computers send a request to the central computer for authorisation to run the file. If the file is recognised at the central computer, then the central computer can send permission for the local computer to run the file if the file is known to be safe or send a "deny" command if the file is known to be malicious. However, in each of these prior art proposals, if the file is not known at the central computer, then the whole file is sent to the central computer where it can be analysed to determine whether it should be regarded as safe or malware. Such analysis is typically carried out manually or "semi-manually" by

number of requests by that file on a single computer is received from the single local computer in a time period.

In the system of US-A-2004/0006704, a comparison is made between installed versions of software on a computer with a database of software versions and their known vulnerabilities. A user of the computer can therefore be informed of specific risks and how to minimise those risks by updating existing or installing new software.

In the system of WO-A-03/021402, a central database holds a virtual image of all files stored on each of plural local computers. If a threat in one local computer is identified, other local computers with a similar configuration can be notified of the risk.

Thus, the prior art systems either rely on deep analysis of a new object in order to determine whether or not the object is malicious, which introduces delay and therefore risk to users during the period that the file is analysed and new anti-malware signatures distributed, or limited analysis of the operation of the particular object or its method of transmission to a computer is carried out to decide a likelihood of the object being malicious.

It is therefore the object of the present invention to provide an improved method of determining the protection that a remote computer has from malware, as well as a corresponding apparatus and computer program.

This object is solved by the subject matter of the independent claims.

Preferred embodiments are defined by the dependent claims.

According to a first aspect of the present invention, there is provided a method of classifying a computer object as malware, the method comprising:

at a base computer, receiving data about a computer object from each of plural remote computers on which the object or similar objects are stored;
comparing in the base computer the data about the computer object received from the plural computers; and,
classifying the computer object as malware on the basis of said comparison.

Compared to the prior art that relies solely on signature matching, this aspect allows a comparison to be made between the objects and/or their effects

Grünecker PartG mbB Leopoldstr. 4 80802 München Germany

European Patent Office

Bob-van-Bentham-Platz 1
80469 München

Ihr Zeichen / Your Ref.

Unser Zeichen / Our Ref.

Datum / Date

EP1067381EHAmr

September 4, 2018

European Patent Application No. 13 167 436.8
Applicant: WEBROOT INC.

In response to the communication dated April 26, 2018:

Herewith submitted are:

- new claims 1 to 5 to replace all claims currently on file; and
- new description pages 2, 2a, 4, and 4a to replace corresponding description pages 2 and 4 as originally filed for this divisional application.

Also enclosed is a marked-up copy of the new claim set highlighting all claim amendments.

The claims have been amended in order to overcome all objections raised in the above-mentioned Official Communication.

I. Amendments and Clarity

In order to constructively deal with and overcome the various objections under Article 76(1) EPC against the previously submitted claims, the claims have been amended based on the explicit disclosure given in the description of the parent application as originally filed on page 36, line 15 to page 39 line 2.

MÜNCHEN
Patentanwälte
European Patent Attorneys
Hans Hilgers
Thomas Schuster
Dr. Klara Goldbach
Martin Aufenanger, LL.M., MM ¹
Gottfried Klitzsch
Dr. Heike Vogelsang-Wenke
Reinhard Knauer
Dietmar Kuhl
Dr. Franz-Josef Zimmer
Bettina K. Reichelt
Dr. Anton K. Pfau
Dr. Udo Weigelt, LL.M.
Rainer Bertram
Jens C. Koch, M.S. (U of PA)
Bernd Rothaemel
Thomas W. Laubenthal, LL.M.
Dr. Andreas Kayser
Dr. Jens Hammer
Dr. Thomas Eickelkamp
Dr. Peter Miltényi ²
Dr. Moritz Höffe, LL.M.
Gero Maatz-Jansen
Michael Heise
Christian Meisinger
Dr. Martin Ahr
Dr. Wolfgang Neubeck
Steven M. Zeman, Ph.D.
André Nickel
Felix Kahr
Dr. Alexander Stumvoll, LL.M.
Dr. Stefano Marchini ³
Dr. Thomas Kronberger
Yilin Jin
Dr. Georg Seisenberger
Dr. Olivia Nemethova, LL.M.
Dr. Rainer Plaggenborg
Victor Lopes Aguiar
Dr. Sabine Koch
Wolfram Thomas

Rechtsanwälte
Attorneys-at-Law
Dr. Helmut Eichmann
Gerhard Barth
Dr. Ulrich Blumenröder, LL.M.
Prof. Dr. Maximilian Kinkeldey, LL.M. ⁴
Dr. Karsten Brandt
Anja Franke, LL.M.
Ute Stephani
Dr. Bernd Allekotte, LL.M. ⁵
Dr. Elvira Bertram, LL.M.
Babett Ertle
Christine Neuhiel
Sabine Brandstätter
Cornelia Schmitt
Petra Lübke
Dr. Holger Gauss
Dr. Nicolás Schmitz
Marina Schlumberger
Kirsten Hammerstingl
Sebastian Clotten, LL.M.
Jennifer Rosenhäger, LL.M.
Mark Peters, LL.M.
Dr. Nicola Busch
Julia Bittner, LL.M.
Sebastian Ochs
Philipp Strommer
Jan Rether
Karin Lochner

BERLIN
Patentanwälte
European Patent Attorneys
Dr. Patrick P. Erk, M.S. (MIT)
Dr. Svenja Sethmann
Tino Rumpold

KÖLN
Patentanwälte
European Patent Attorneys
Dr. Martin Dropmann

PARIS ⁶
Conseil en Propriété Industrielle
European Patent Attorney
Dr. Wolfgang Neubeck

Grünecker Patent- und Rechtsanwälte PartG mbB

Leopoldstr. 4 Tel. +49 (0) 89 21 23 50
80802 München Fax +49 (0) 89 22 02 87
Germany Mail info@grunecker.de

Amtsgericht: München
Partnerschaftsregister:
PR 1397

Deutsche Bank München
SWIFT / BIC-code: DEUT DE MM
IBAN: DE47 7007 0010 0175 173400

¹ auch/also: Mediator ² auch/also: Agente de la Propiedad Industrial (España) ³ auch/also: Consulente in Brevetti (Italia)
⁴ Professor an der Fachhochschule für angewandtes Management ⁵ auch/also: Attorney-at-Law, New York ⁶ in Kooperation/in cooperation

The specific amendments are highlighted in the enclosed marked-up copy of the new claim set in which respective footnotes provide support in the original parent application for each claim amendment. Moreover, the respective objection under section 1 of the Official Communication is also indicated for the respective claim amendments.

At least in view of these claim amendments and the indicated support in the marked-up copy of the new claim set, the objections under Article 76(1) EPC and the related clarity objections raised under section 1 of the Official Communication are considered to be overcome.

The same passages cited as support in the original parent application are also included in the description as originally filed for the present divisional application, i.e. page 28 line 27 through page 30 line 28.

Accordingly, the new claims also comply with the requirements of Article 123(2) EPC.

The cited closest prior art document D1 has been identified and briefly acknowledged on new description page 2. Moreover, the description has been brought into conformity with the new claims by formulating the objective problem solved in view of the closest and cited prior art and by stating on new description page 4a that this object is solved by the subject matter of the independent claims.

II. Patentability

The comprehensive arguments under section 2 of the Official Communication with respect to the previous claims and closest prior art document D1 have been carefully considered and taken into account. With respect to the herewith submitted new independent claims, the Examining Division is kindly requested to consider the following arguments leading to the conclusion that the claimed subject matter involves an inventive step within the meaning of Article 56 EPC.

As discussed in the Official Communication, [0030] of D1 would be relevant to the claimed invention for the inventive step requirement. However, the teaching of D1 is conceptually different than the claimed invention according to new claims 1 and 3.

According to D1, a policy organizing server 32 receives status information from various computers indicating the malware scanning products used, the scanner engine versions

and the virus definition data versions (see [0025] of D1). This status information is used by server 32 only to be able to determine whether each computer within the network runs out-of-date malware products and out-of-date malware definition data and which computers run the most up-to-date versions. The reason and motivation for this determination in D1 is to eventually instruct those computers that are out-of-date to perform an updating of its malware definition data. Specifically, if the server of D1 receives messages from computers concerning a particular malware and if all messages originate from up-to-date computers only, the server instructs all other computers that are out-of-date to update their malware definition data.

While this solution of D1 certainly also provides a concept of improving malware protection of remote computers, the claimed invention according to new claims 1 and 3 does not use or implement such a suggested concept of a forced updating of out-of-date computers.

Instead, the claimed invention suggests a conceptually different concept that does not require that all computers must update to the same up-to-date malware definition data.

According to new claim 1, remote computers provide not only information of all or selected security products on the remote computer, but also details of processes that run on the remote computer. In addition – since this information is stored in the central database – computers having the same particular combination of security products as a specific (i.e. first) one of the remote computers can be identified. This is already different and non-obvious from D1, because the out-of-date computers (that are eventually forced to be updated) have a different particular combination of security products than the up-to-date computers that sent the malware messages concerning a malware process to the server 32 in D1.

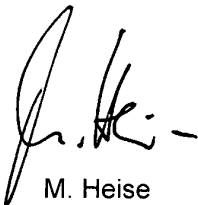
As a further distinction—instead of forcing a specific out-of-date computer to change/update its “security products” to the different up-to-date security products if a particular malware was detected by other computers with such different i.e. up-to-date security products, as in D1—the claimed invention then identifies those processes that are malware and occurred on computers having the same particular combination of security products but were not locally detected. Thus, instead of forcing an updating of the out-of-date security products of a first remote computer to those of other up-to-date computers as suggested by D1, the user of the first remote computer is provided with the information of identified processes

that are marked as malware but were not locally detected by other computers having the same combination of security products as the first computer.

These are two alternative, incompatible solutions for increasing the protection of local computers from malware. The solution of D1 (changing the settings of security products to that of other computers with different security products that have detected a malware process) neither implies nor suggests the alternative solution of the claimed invention (informing a computer of non-detected malware processes that were not detected by other computers with the same security products).

Consequently, the claimed subject matter does not arise from the available prior art in an obvious manner without applying hindsight knowledge from the present application, but involves an inventive step within the meaning of Article 56 EPC.

In view of the above, the outstanding objections are considered to be overcome. Should the Examining Division have further objections against the present application, it is kindly and respectfully requested to continue the proceedings in writing by issuing a further examination report. Only as a measure of precaution, oral proceedings are herewith requested and it is further requested to make use of video-conferencing.



M. Heise

Encl.

Claims 1 to 5 (clean and marked-up versions)
Description pages 2, 2a, 4 and 4a

Datum
Date 26.04.2018
Date

Blatt
Sheet 1
Feuille

Anmelde-Nr:
Application No: 13 167 436.8
Demande n°:

The examination is being carried out on the **following application documents**

Description, Pages

1-43 as originally filed

Claims, Numbers

1-5 filed in electronic form on 18-03-2014

Drawings, Sheets

1/3-3/3 as originally filed

Reference is made to the following document; the numbering will be adhered to in the rest of the procedure.

D1 US 2003/131256 A1 (ACKROYD ROBERT JOHN [GB]) 10 July 2003
(2003-07-10)

The applicant's letter of reply dated 18-03-2014 will be referred to as R1.

Added Subject-Matter

1. The present set of claims introduces subject-matter which extends beyond the content of the earlier application as filed, contrary to Article 76(1)EPC. The features concerned are the following:

1.1 Claims 1 and 3, feature

"receiving at the base computer details of all or selected security products operating at a point in time on other remote computers connected to the base computer...".

The applicant did not provide, and the examiner could not identify in the earlier application as filed the basis for this amendment.

1.2. Claim 1 and 3, feature

"... and details of processes run by said other remote computers that were not locally identified as being malware".

In R1, the applicant indicated page 37, lines 21 to 24 of the original PCT application as basis for this amendment. The indicated passage reads

"The community database 7 in this embodiment is also provided by the agent software with details of processes run by every computer 2 and thus knows whether or not a process has been detected by each computer 2."

As can be seen, the feature under consideration is neither disclosed in the passage, nor is it directly and unambiguously derivable therefrom.

1.3. Claims 1 and 3, feature

"storing the information in a database at the base computer".

First, it is noted that the scope defined by the term "information" is not clear in the context of the claim. One interpretation would be that the information refers to the data received at the base computer as recited in the features addressed here above in sections 1.1 and 1.2. Thus, since those features introduce subject-matter which extends beyond the content of the earlier application as filed, so does the feature under consideration.

Second, it is noted that the support indicated by the applicant, namely pages 36 to 38, is too vague, and does not appear to disclose any specific step of storing the information. Should the applicant consider that storing of some specific information is directly and unambiguously derivable, he should clarify which type of information, and specify wherefrom this would be directly and unambiguously derivable.

1.4. Claims 1 and 3, feature

"wherein some processes in the database are marked as being malware".

In R1, the applicant identified page 38, lines 25 to 30 as basis for this amendment.

The identified passage reads

"Thus, the community database 7, when provided with information relating to all the security products, etc. on a particular computer at a particular time, is searched for events for processes marked as "bad" that occurred on computers with that particular mix of security products and that were not locally detected. This information can then be fed back to the user of the particular computer, for example directly or by directing the user to a website. This information can be provided virtually in real-time, allowing a new user or a user of a new computer to be able to increase the computer's effective security very quickly."

First, it is noted that the identified passage does not appear to be linked directly and unambiguously to the method drafted in the previously filed claim 1 on which the present claim 1 is based. The identified passage is not disclosed in the context of a method of determining the protection that a specific remote server has from malware, which is the subject-matter of the previously filed claim 1. Therefore, the new feature

in combination with the features of the previously filed claim 1 (which corresponds to claim 31 of the earlier application as filed) extends the subject-matter beyond the content of the earlier application as filed.

Second, it is noted that the wording of the feature is not present in the identified passage, nor is it directly and unambiguously derivable therefrom. The closest to the wording of the feature under consideration appears to be "the community database ... is searched for events for processes marked as "bad"". This, however, is different from the scope of the feature as drafted: the wording itself is different, and moreover, what is searched for does not imply that the object of the search as such is present in the database.

1.5. Claims 1 and 3, feature

"searching the database identifying any processes marked as being malware that were not identified by said other remote computers having the same particular combination of security products as the first remote computer".

The applicant did not provide any support for this amendment, but stated in R1 that this amendment generally followed from the other amendments of the claim (referred to above).

Notwithstanding the fact that the other amendments are considered to be unallowable added subject-matter, even if they were allowable, the examiner does not see how the amendment under consideration would derive directly and unambiguously therefrom.

Inventive Step

2. Notwithstanding the above objections, the reasoning as why the subject-matter of claims 1 - 5 does not involve an inventive step within the meaning of Article 56 EPC will also be given.

2.1. Document D1 discloses in accordance with the features of claim 1 a method of determining the protection that a first remote computer has from malware, the method comprising:

a) receiving at a base computer details of all or selected security products operating at a point in time on said first remote computer (page 2, right-hand col., lines 10-15: "The policy organising server 32 also receives status information from the various computers indicating the malware scanning products being used, the scanner engine versions and virus definition data versions being used and the security settings being applied within those different computers on the network. ");

b) receiving at the base computer details of all or selected security products operating at a point in time on other remote computers connected to the base computer and details of processes run by said other remote computers that were not locally identified as being malware (same passage as for the feature a); it can be safely assumed that the security products operating on remote computers were not identified as malware; on the other hand, D1 discloses the negative logic with respect to this feature of the claim, namely, receiving details of processes run by said other remote computers that *were* locally identified as being malware, lines 6-10 of par. [0025]: "the policy organising server 32 also serves to receive logged data messages from the various different servers and client computers within the computer network 2 indicating detection of malware items by the malware scanners operating at those individual computers."), and

c) storing the information in a database at the base computer, wherein some processes in the database are marked as being malware (par.[0026]; it is noted that the messages relate to malware, as disclosed in lines 6-10 of par.[0025]);

d) searching the database identifying any processes marked as being malware that were not identified by said other remote computers having the same particular combination of security products as the first remote computer (page 3, left-hand col., lines 11-15: "When the policy organising server 32 has detected four logged data messages corresponding to the particular item of malware and also detects the pattern that none of these originate from a computer running out-of-date malware definition data"); and,

e) providing information to the user of said first remote computer that said first remote computer may be susceptible to attack by said malware processes on the basis of said identifying (lines 16-20 of par.[0030]: "the policy organising server 32 recognises the exceeding of a predetermined threshold in combination with a predetermined pattern of infection and serves to force the anti-malware action of updating the malware definition data on those computers that are out-of-date.").

Therefore, the subject-matter of claim 1 differs in receiving, at the base computer, "details of processes run by said other remote computers that were not locally identified as being malware".

Notwithstanding the fact that this feature is not allowable under Article 76(1) EPC, it is noted, as indicated above in relation to the citation for the feature b), that the feature is not clear in technical terms and as a result could be considered as being disclosed in D1, or, in another approach, as being implementation of a negative logic with respect to disclosure of D1, namely, logging details about processes identified as

malware versus logging details about processes not identified as malware. In either case, this feature cannot be considered as providing an inventive step over the prior art.

Therefore, the subject-matter of claim 1 does not comply with the requirements of Article 56 EPC.

It is believed that the applicant's arguments in favour of inventive step presented R1 have been fully replied to by the detailed inventive step reasoning given above. In particular, it is noted that D1 does disclose sending to the base computer details of the security products on remote computers, and also provides "targeted" information to remote computers (see the passage cited in the above reasoning).

2.2. The same reasoning given for claim 1 applies mutatis mutandis to corresponding apparatus claim 3 and computer program claim 5.

2.3. The additional subject-matter of claims 2 and 4 consists in minor implementation details which cannot be considered inventive in the sense of Article 56 EPC.

3. After carefully considering the arguments of the applicant, and the application as a whole, the examiner is of the opinion that there are no good prospects of bringing the procedure to a positive conclusion (Guidelines C-IV, 3). Therefore, the applicant may expect a summons to oral proceedings as the next procedural step and subsequent refusal of the application.



European Patent Office
Postbus 5818
2280 HV Rijswijk
NETHERLANDS
Tel: +31 70 340 2040
Fax: +31 70 340 3016



Grünecker Patent- und Rechtsanwälte
PartG mbB
Leopoldstraße 4
80802 München
ALLEMAGNE

Formalities Officer
Name: Berthon, Claude
Tel: +31 70 340 - 1001
or call
+31 (0)70 340 45 00

Substantive Examiner
Name: Arbutina, Ljiljana
Tel: +31 70 340 - 4522

Application No. 13 167 436.8 - 1217	Ref. EP1067381EHmf1	Date 26.04.2018
Applicant Webroot Inc.		

Communication pursuant to Article 94(3) EPC

The examination of the above-identified application has revealed that it does not meet the requirements of the European Patent Convention for the reasons enclosed herewith. If the deficiencies indicated are not rectified the application may be refused pursuant to Article 97(2) EPC.

You are invited to file your observations and insofar as the deficiencies are such as to be rectifiable, to correct the indicated deficiencies within a period

of 4 months

from the notification of this communication, this period being computed in accordance with Rules 126(2) and 131(2) and (4) EPC. One set of amendments to the description, claims and drawings is to be filed within the said period on separate sheets (R. 50(1) EPC).

If filing amendments, you must identify them and indicate the basis for them in the application as filed. Failure to meet either requirement may lead to a communication from the Examining Division requesting that you correct this deficiency (R. 137(4) EPC).

In case you withdraw the application within the above-mentioned period, the examination fee will be refunded at a rate of 50% (Art. 11 (b) RFees).

Failure to comply with this invitation in due time will result in the application being deemed to be withdrawn (Art. 94(4) EPC).



Arbutina, Ljiljana
Primary Examiner
For the Examining Division

Enclosure(s): 5 page/s reasons (Form 2906)



Application No.: 13167436.8

Substantive examination has started on 19.04.18 (see Notice from the European Patent Office dated 29.01.2013, OJ EPO 2013, 153).

For the Examining Division



European Patent Office
80298 MUNICH
GERMANY

Questions about this communication ?
Contact Customer Services at www.epo.org/contact



Grünecker Patent- und Rechtsanwälte
PartG mbB
Leopoldstraße 4
80802 München
ALLEMAGNE

Date
20.07.16

Reference EP1067381EHmf	Application No./Patent No. 13167436.8 - 1955 / 2629232
Applicant/Proprietor Webroot Inc.	

Communication of amended entries concerning the representative (R. 143(1)(h) EPC)

As requested, for the above-mentioned European patent application / European patent the entries concerning the representative have been amended as follows:

Grünecker Patent- und Rechtsanwälte
PartG mbB
Leopoldstraße 4
80802 München
DE

The amendment will be recorded in the Register of European Patents.

For the Examining Division



BeckGreener

John Raynor
Ian Bartlett
C. Rowland Brehnen
Ail Freeman
Ben Muir
John P. Hull
James A. Stones
Anna L. Hatt
Nick P. Bebbington
Deborah Selden
Jonathan P. J. Markham

Associates
Susan Davey
Duncan J. Morgan
Catherine Jewell
Charlotte Jemmett
Matthew Y.K. Ng
Kashif Syed
Consultant
Peter J. Smart

European Patent Office
Directorate General 2
D-80298 Munich
Germany

Our Ref: NPB/AC/P10717EP-W, P10717EP-1, P17017EP-2, P19050EP-W,
Date: P17048EP-W, P17048EP-1, P17048EP-2 & P18550EP
6 July 2016

VIA FAX

To: +49 89 2399 4465

From: +44 (0)20 7693 5601

Number of pages including this page: 1

Fax Transmission: This message and any attachments are confidential and may be legally privileged and protected by the laws of copyright. If you are not the intended recipient, please contact us immediately.

Dear Sirs

European Patent Application Nos. 06755686.0, 13167436.8, 13167434.3, 13745954.1,
12704768.6, 14161844.7, 14161847.0 & 14150462.1

Webroot Solutions Ltd

Responsibility for the prosecution of these applications have been transferred to the German Patent firm Grünecker. Accordingly, we withdraw as Representatives for these applications and request that all further correspondence concerning the applications should be addressed to the following address:-

Grünecker
Leopoldstr. 4
80802 Munich
Germany

Yours faithfully



Mr Nicholas P. Bebbington
Beck Greener (Association Registration No. 518)

Cc: Grünecker

European Patent Office

Bob-van-Benthem-Platz 1
80469 München

Ihr Zeichen / Your Ref.

Unser Zeichen / Our Ref.

Datum / Date

A28167EHmf

July 7, 2016

Transfer of European Patent Applications - WEBROOT INC.

We hereby take over representation of the below listed patent applications.

Please direct any further correspondence, by using our reference signs listed in the list, to

Grünecker Patent- und Rechtsanwälte
Leopoldstr. 4
80802 München
Germany

Tel.: +49 (0)89-21 23 50
Fax.: +49 (0)89-22 02 87
E-Mail: info@grunecker.de


Michael Heise

Encl.:
List of European Patent Applications

MÜNCHEN
Patentanwälte
European Patent Attorneys
Hans Hilgers
Thomas Schuster
Dr. Klara Goldbach
Martin Aufenanger, LL.M., MM.¹
Gottfried Klitzsch
Dr. Heike Vogelsang-Wenke
Reinhard Knauer
Dietmar Kuhl
Dr. Franz-Josef Zimmer
Bettina K. Reichelt
Anton K. Pfau
Dr. Udo Weigelt, LL.M.
Rainer Bertram
Jens C. Koch, M.S. (U of PA)
Bernd Rothaemel
Thomas W. Laubenthal, LL.M.
Dr. Andreas Kayser
Dr. Jens Hammer
Dr. Thomas Eickelkamp
Dr. Peter Miltényi²
Dr. Moritz Höffe, LL.M.
Gero Maatz-Jansen
Michael Heise
Christian Meisinger
Dr. Martin Ahr
Dr. Wolfgang Neubeck
Steven M. Zeman, Ph.D.
André Nickel
Felix Kahr
Dr. Alexander Stumvoll, LL.M.
Dr. Stefano Marchini³
Dr. Thomas Kronberger
Yilin Jin
Dr. Georg Seisenberger
Amir Nemetzade
Dr. Olivia Nemethova, LL.M.
Dr. Rainer Plaggenborg
Victor Lopes Aguiar
Rechtsanwälte
Attorneys-at-Law
Dr. Helmut Eichmann
Gerhard Barth
Dr. Ulrich Blumenröder, LL.M.
Prof. Dr. Maximilian Kinkeldey, LL.M.⁴
Dr. Karsten Brandt
Anja Franke, LL.M.
Uta Stephani
Dr. Bernd Allekotte, LL.M.⁵
Dr. Elvira Bertram, LL.M.
Babett Ertle
Christine Neuhiel
Sabine Brandstätter
Cornelia Schmitt
Petra Lübke
Dr. Holger Gauss
Dr. Nicolás Schmitz
Marina Schlumberger
Kirsten Hammerstingl
Sebastian Clotten, LL.M.
Jennifer Rosenhäger, LL.M.
Mark Peters, LL.M.
Dr. Nicola Busch
Julia Bittner, LL.M.
Sebastian Ochs
BERLIN
Patentanwälte
European Patent Attorneys
Dr. Patrick P. Erk, M.S. (MIT)
Dr. Svenja Sethmann
Tino Rumpold
KÖLN
Patentanwälte
European Patent Attorneys
Dr. Martin Dropmann
PARIS⁶
Conseil en Propriété Industrielle
European Patent Attorney
Dr. Wolfgang Neubeck

Grünecker Patent- und Rechtsanwälte PartG mbB

Leopoldstr. 4
80802 München
Germany
Tel. +49 (0) 89 21 23 50
Fax +49 (0) 89 22 02 87
Mail info@grunecker.de

Amtsgericht: München
Partnerschaftsregister:
PR 1397

Deutsche Bank München
SWIFT / BIC-code: DEUT DE MM
IBAN: DE 47 7007 0010 0175 173400

¹ auch/also: Mediator ² auch/also: Agente de la Propiedad Industrial (España) ³ auch/also: Consulente in Brevetti (Italia)
⁴ Professor an der Fachhochschule für angewandtes Management ⁵ auch/also: Attorney-at-Law, New York ⁶ in Kooperation/in cooperation

Application No.	Our Ref:
13745954.1	EP106737EHmfi
06755686.0	EP106738EHmfi
13167436.8	EP106738IEHmfi
13167434.3	EP106738IIEHmfi
12704768.6	EP106743EHmfi
14161844.7	EP106743IEHmfi
14161847.0	EP106743IIEHmfi
14150462.1	EP106745EHmfi



European Patent Office
80298 MUNICH
GERMANY

Questions about this communication ?
Contact Customer Services at www.epo.org/contact



Beck Greener
Fulwood House
12 Fulwood Place
London WC1V 6HR
ROYAUME UNI

Date
09.06.16

Reference NPB/P10717EP-1	Application No./Patent No. 13167436.8 - 1955 / 2629232
Applicant/Proprietor Webroot Inc.	

Communication

concerning the registration of amendments relating to

- ☒ a transfer (R. 22 and 85 EPC)
- ☐ entries pertaining to the applicant / the proprietor (R. 143(1)(f) EPC)

As requested, the entries pertaining to the applicant of the above-mentioned European patent application / to the proprietor of the above-mentioned European patent have been amended to the following:

AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IS IT LI LT LU LV MC
NL PL PT RO SE SI SK TR
Webroot Inc.
385 Interlocken Crescent
Broomfield, CO 80021/US

The registration of the changes has taken effect on 07.04.16.

In the case of a published application / a patent, the change will be recorded in the Register of European Patents and published in the European Patent Bulletin (Section I.12 / II.12).

Your attention is drawn to the fact that, in the case of the registration of a transfer, any automatic debit order only ceases to be effective from the date of its express revocation (cf. point 14(c) of the Arrangements for the automatic debiting procedure, supplementary publication 3 - OJ EPO 2015).

Receiving Section / For the Examining Division / For the Opposition Division / For the Legal Division *)



*) See note.

Note

This communication is issued by/for the department with whom responsibility lies. The Legal Division is responsible for the registration of transfers, changes of name (Articles 71, 72 and 74 EPC and Rules 22 and 85 EPC) as well as for the rectification of the designation of the inventor (Rule 21 EPC) (see Decision of the President of the EPO, OJ EPO 2013, 600). In all other cases, the Receiving Section, the Examining Division or the Opposition Division is responsible, depending on the stage in proceedings.



Acknowledgement of receipt

We hereby acknowledge receipt of the following subsequently filed document(s):

Submission number	4251211	
Application number	EP13167436.8	
Date of receipt	07 April 2016	
Filing Office	European Patent Office, The Hague	
Procedural phase	All procedures	
Your reference	NPB/P10717EP-1	
Documents submitted	package-data.xml ep-cms-sfd-request.pdf (2 p.) APPRASSI-1.pdf\P10717EP-1_EPO_ Record Assignment_07-04-16.pdf (1 p.)	ep-cms-sfd-request.xml APPRMISC-1.pdf\04584 Foreign Assignment - signed.pdf (5 p.)
Submitted by	CN=secure.epoline.org,OU=PDIS,O=European Patent Office,C=NL	
Method of submission	Online	
Date and time receipt generated	07 April 2016, 13:05 (CEST)	
Message Digest	84:68:01:04:0D:AC:6F:FF:AE:CA:36:61:2F:9E:23:AE:A6:8D:D2:0A	

/European Patent Office/

ASSIGNMENT

WHEREAS, WEBROOT SOLUTIONS LTD, a company formed under the laws of Great Britain, and having a principal place of business of 3 New Park Place, Pride Park, Derby, United Kingdom DE24 8DZ ("ASSIGNOR"), owns rights in, to and under the patent applications set forth in the attached Schedule A (the "Properties"); and

WHEREAS, WEBROOT INC., a company organized and existing under the laws of the State of Delaware, United States of America and having a principal place of business of 385 Interlocken Crescent, Broomfield, CO 80021 ("ASSIGNEE"), is desirous of acquiring ASSIGNOR'S entire right, title and interest in, to and under the Properties.

WHEREAS, ASSIGNOR, to the extent they own any right, title and interest in and to the Properties is desirous of assigning any and all such rights, title and/or interest to ASSIGNEE.

NOW THEREFORE, for good and valuable consideration, the receipt and adequacy of which are hereby acknowledged, the ASSIGNOR has sold, assigned, transferred and set over, and by these presents does hereby sell, assign, transfer and set over, unto the ASSIGNEE, its successors, legal representatives and assigns, the entire right, title and interest in, to and under the Properties and any and all letters patent or patents in the United States of America, the United Kingdom and all foreign countries which may be granted therefore and thereon (including any divisions, continuations, continuations-in-part, reissues, reexaminations or extensions of letters patents and other related applications arising from, corresponding to and/or claiming priority to any of the Properties) and the registration thereof, and all rights under the International Convention for the Protection of Industrial Property, the same to be held and enjoyed by the ASSIGNEE for its own use and enjoyment and for the use and enjoyment of its successors, legal representatives and assigns, to the full end of the term or terms for which letters patent may be granted, as fully and entirely as the same would have been held and enjoyed by the ASSIGNOR had this assignment not been made, and further including all income, royalties, damages and payments for past or future infringements and misappropriations thereof, all rights to sue for past, present and future infringements or misappropriations thereof, and all rights

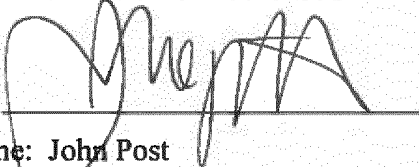
corresponding to any of the above throughout the world and for the full term or terms of assigned Properties;

AND for the same consideration, ASSIGNOR hereby covenants and agrees to and with ASSIGNEE, its successors, legal representatives and assigns, that ASSIGNOR will encourage its employees named as inventors on one or more of the assigned Properties, to make, execute and deliver any and all other instruments in writing as may be necessary to assign the Properties to ASSIGNEE, including, but not limited to, any and all further application papers, affidavits, assignments and other documents, and that ASSIGNOR will communicate to ASSIGNEE, its successors, legal representatives and assigns, all facts known to ASSIGNOR relating to the Properties, and that ASSIGNOR will testify in all legal proceedings and generally do all things which may be necessary or desirable to more effectually secure to and vest in ASSIGNEE, its successors, legal representatives and assigns, the entire right, title and interest in and to the Properties;

AND THE ASSIGNOR HEREBY authorizes and requests the Commissioner of the United States Patent and Trademark Office, and any official of any country or countries foreign to the United States, whose duty is to issue patents or other evidence or forms of industrial property protection on applications as aforesaid, to issue the same to the ASSIGNEE, its successors, legal representatives and assigns, in accordance with the terms of this instrument

IN WITNESS WHEREOF, the undersigned have executed this Patent Assignment this 4th day of April, 2016.

WEBROOT SOLUTIONS LTD

By: 
Name: John Post
Title: Director

WEBROOT INC.

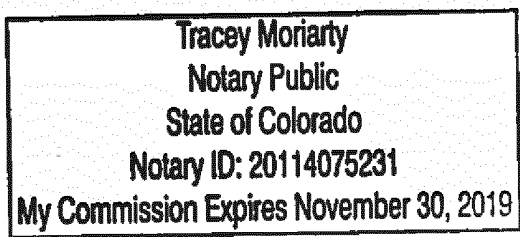
By: 
Name: Ryan Howe
Title: General Counsel

STATE OF Colorado)
City and) ss.
COUNTY OF Broomfield)

On this 9th day of April, 2016, before me personally appeared John Post and Ryan Howe to me known and known to me to be the persons described in and who executed the foregoing instrument, and John Post and Ryan Howe duly acknowledged to me that John Post and Ryan Howe executed the same for the uses and purposes therein set forth.

[SEAL]
Notary Public

Tracey Moriarty



Schedule A
ASSIGNED PATENT APPLICATIONS

Chinese Patent Application No. 201110036121.8, entitled "METHODS AND APPARATUS FOR DEALING WITH MALWARE," filed 30 June 2006.

Chinese Patent No. 201110036124.1, entitled "METHODS AND APPARATUS FOR DEALING WITH MALWARE," filed 30 June 2006.

Chinese Patent No. 200680023707.8, entitled "METHODS AND APPARATUS FOR DEALING WITH MALWARE," filed on 30 June 2006.

European Patent Application No. 13167436.8, entitled "METHODS AND APPARATUS FOR DEALING WITH MALWARE," filed on 30 June 2006.

European Patent Application No. 13167434.3, entitled "METHODS AND APPARATUS FOR DEALING WITH MALWARE," filed on 30 June 2006.

European Patent Application No. 06755686.0, entitled "METHODS AND APPARATUS FOR DEALING WITH MALWARE," filed on 30 June 2006.

Indian Patent Application No. 6058/CHENP/2007, entitled "METHODS AND APPARATUS FOR DEALING WITH MALWARE," filed on 30 June 2006.

Japanese Patent No. 4936294, entitled "METHODS AND APPARATUS FOR DEALING WITH MALWARE," filed on 30 June 2006.

Australian Patent Application No. 2012217181, entitled "METHODS AND APPARATUS FOR DEALING WITH MALWARE," filed on 14 February 2012.

Canadian Patent Application No. 2,827,385, entitled "METHODS AND APPARATUS FOR DEALING WITH MALWARE," filed on 14 February 2012.

Chinese Patent Application No. 201280018306.9, entitled "METHODS AND APPARATUS FOR DEALING WITH MALWARE," filed on 14 February 2012.

European Patent Application No. 14161844.7, entitled "METHODS AND APPARATUS FOR DEALING WITH MALWARE," filed on 14 February 2012.

European Patent Application No. 14161847.0, entitled "METHODS AND APPARATUS FOR DEALING WITH MALWARE," filed on 14 February 2012.

European Patent Application No. 12704768.6, entitled "METHODS AND APPARATUS FOR DEALING WITH MALWARE," filed on 14 February 2012.

Hong Kong Patent Application No. 14113078.2, entitled “METHODS AND APPARATUS FOR DEALING WITH MALWARE,” filed on 14 February 2012.

Hong Kong Patent Application No. 14113079.1, entitled “METHODS AND APPARATUS FOR DEALING WITH MALWARE,” filed on 14 February 2012.

Japanese Patent Application No. 2013-553909, entitled “METHODS AND APPARATUS FOR DEALING WITH MALWARE,” filed on 14 February 2012.



Letter accompanying subsequently filed items

Representative:

Beck Greener
12 Fulwood Place
London WC1V 6HR
United Kingdom

Phone: +-44-(0)-20-7693-5600

Fax: +-44-(0)-20-7693-5601

E-mail: mail@beckgreener.com

80298 Munich
Germany
Tel. +49(0)89 2399-0 | Fax -4465

P.O. Box 5818
NL-2280 HV Rijswijk
Netherlands
Tel. +31(0)70 340-2040 | Fax -3016

10958 Berlin
Germany
Tel. +49(0)30 25901-0 | Fax -840

The document(s) listed below is (are) subsequently filed documents pertaining to the following application:

Application number and/or EP publication number	EP13167436.8
Reference	NPB/P10717EP-1
Procedural phase	All procedures
Name of represented party	Webroot Solutions Ltd

	Description of document	Original file name	Assigned file name
1	Document concerning the applicant	04584 Foreign Assignment - signed.pdf	APPRMISC-1.pdf
2	Request for assignment	P10717EP-1_EPO_Record Assignment_07-04-16.pdf	APPRASSI-1.pdf

	Fees	Factor applied	Fee schedule	Amount to be paid
15-1	022 Registering of transfer	1	100.00	100.00
	Total:		EUR	100.00

	Payment	
1	Mode of payment	Debit from deposit account
	Currency:	EUR
	The European Patent Office is hereby authorised, to debit from the deposit account with the EPO any fees and costs indicated on the fees page.	
	Deposit account number:	28050163
	Account holder:	Beck Greener
2	Refund/Reimbursement	
	Reimbursement (if any) to be made to EPO deposit account:	28050163
	Account holder:	Beck Greener

Signature 1

Place: London
Date: 07 April 2016

Signed by: /N bebbington/
Association: Beck Greener
Capacity: Representative 1

Smart card certificate 1

Common name: Nick Bebbington 13019
EPO ID: 13019
Issued by: European Patent Office CA G2

European Patent Office
Directorate General 2
D-80298 Munich
Germany

Our Ref: NB/HC/P10717EP-1
Date: 7 April 2016

Dear Sirs

**European Patent Application No. 13167436.8-1957
Webroot Solutions Ltd**

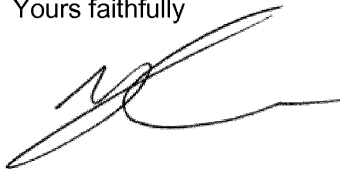
We request that the assignment of this application from Webroot Solutions Ltd to Webroot Inc be recorded in the register.

The address of the assignee, Webroot Inc, is:

385 Interlocken Crescent
Broomfield
CO 80021
United States of America

We are filing herewith a copy of the assignment document signed by both parties and dated 4 April 2016.

Yours faithfully



Nick Bebbington
Beck Greener (Association Registration No. 518)



European Patent Office
80298 MUNICH
GERMANY

Questions about this communication ?
Contact Customer Services at www.epo.org/contact



Beck Greener
Fulwood House
12 Fulwood Place
London WC1V 6HR
ROYAUME UNI

Date	03.11.14
------	----------

Reference NPB/P10717EP-1	Application No./Patent No. 13167436.8 - 1957 / 2629232
Applicant/Proprietor Webroot Solutions Ltd	

Communication

concerning the registration of amendments relating to

- ☐ a transfer (R. 22 and 85 EPC)
- ☒ entries pertaining to the applicant / the proprietor (R. 143(1)(f) EPC)

As requested, the entries pertaining to the applicant of the above-mentioned European patent application / to the proprietor of the above-mentioned European patent have been amended to the following:

AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IS IT LI LT LU LV MC
NL PL PT RO SE SI SK TR
Webroot Solutions Ltd
3 New Park Place
Pride Park
Derby DE24 8DZ/GB

The registration of the changes has taken effect on 24.10.14.

In the case of a published application / a patent, the change will be recorded in the Register of European Patents and published in the European Patent Bulletin (Section I.12 / II.12).

Your attention is drawn to the fact that, in the case of the registration of a transfer, any automatic debit order only ceases to be effective from the date of its express revocation (cf. point 14(c) of the Arrangements for the automatic debiting procedure, Supplementary publication 4 - OJ EPO 2014).

Receiving Section / For the Examining Division / For the Opposition Division / For the Legal Division *)



*) See note.

Note

This communication is issued by/for the department with whom responsibility lies. The Legal Division is responsible for the registration of transfers, changes of name (Articles 71, 72 and 74 EPC and Rules 22 and 85 EPC) as well as for the rectification of the designation of the inventor (Rule 21 EPC) (see Decision of the President of the EPO, OJ EPO 2013, 600). In all other cases, the Receiving Section, the Examining Division or the Opposition Division is responsible, depending on the stage in proceedings.



CERTIFICATE OF INCORPORATION ON CHANGE OF NAME

Company Number **4181251**

The Registrar of Companies for England and Wales hereby certifies that
under the Companies Act 2006:

PREVX LTD

a company incorporated as private limited by shares; having its registered
office situated in England and Wales; has changed its name to:

WEBROOT SOLUTIONS LTD

Given at Companies House on **1st May 2014**



Companies House



**THE OFFICIAL SEAL OF THE
REGISTRAR OF COMPANIES**



CERTIFICATE OF INCORPORATION ON CHANGE OF NAME

Company Number **5400865**

The Registrar of Companies for England and Wales hereby certifies that
under the Companies Act 2006:

PREVX GROUP LIMITED

a company incorporated as private limited by shares; having its registered
office situated in England and Wales; has changed its name to:

WEBROOT SOLUTIONS GROUP LTD

Given at Companies House on **1st May 2014**

European Patent Office
Directorate General 2
D-80298 Munich
Germany

Our Refs: NPB/A20147
P17017EP-W/-1/-2
P17048EP-W/-1/-2
Date: 24 October 2014

Dear Sirs

**European Patent Applications Nos. 06755686.0, 12704768.6, 13167434.3, 13167436.8
14161844.7 & 14161847.0
Currently in the name of Prevx Ltd**

The applicant of the above applications has changed its name from Prevx Limited to Webroot Solutions Ltd as set out in the attached Certificate of Incorporation on Change of Name issued by Companies House in the United Kingdom. The applicant's address remains the same.

Please record this change of name in the Register. We look forward to receiving your confirmation that the applications are proceeding in the name of Webroot Solutions Ltd.

Yours faithfully



Nicholas P. Bebbington
Beck Greener (Association Registration No. 518)

Enc



Acknowledgement of receipt

We hereby acknowledge receipt of the following subsequently filed document(s):

Submission number	2649772	
Application number	EP13167436.8	
Date of receipt	18 March 2014	
Receiving Office	European Patent Office, The Hague	
Your reference	NPB/P10717EP-1	
Applicant	All applicants as on file	
Documents submitted	package-data.xml epf1038.pdf (2 p.) CLMS-1.pdf\Claims cc SO response 18-3-14.pdf (2 p.)	ep-sfd-request.xml WOREPLY-1.pdf\P10717EP-1_EPO SO response 18-3-14.pdf (4 p.) CLMS-HWA-1.pdf\Claims redline SO response 18-3-14.pdf (2 p.)
Submitted by	CN=Nick Bebbington 13019	
Method of submission	Online	
Date and time receipt generated	18 March 2014, 17:07 (CET)	
Message Digest	A3:35:E8:F4:CD:CE:ED:32:C0:F6:E1:EA:DD:2D:35:24:05:8A:A4:34	

Correction by the EPO of errors in debit instructions filed by eOLF

Errors in debit instructions filed by eOLF that are caused by the editing of Form 1038E entries or the continued use of outdated software (all forms) may be corrected automatically by the EPO, leaving the payment date unchanged (see decision T 152/82, OJ EPO 1984, 301 and point 6.3 ff ADA, Supplement to OJ EPO 10/2007).

/European Patent Office/

CLAIMS

1. A method of determining the protection that a first remote computer has from malware, the method comprising:
 - 5 receiving at a base computer (3) details of all or selected security products operating at a point in time on said first remote computer (2);
receiving at the base computer (3) details of all or selected security products operating at a point in time on other remote computers (2) connected to the base computer (3) and details of processes run by said other remote
10 computers (3) that were not locally identified as being malware, and storing the information in a database (7) at the base computer (3), wherein some processes in the database (7) are marked as being malware;,
searching the database (7) identifying any processes marked as being malware that were not identified by said other remote computers (2) having the
15 same particular combination of security products as the first remote computer (2); and,
providing information to the user of said first remote computer (2) that said first remote computer (2) may be susceptible to attack by said malware processes on the basis of said identifying.
20
2. A method according to claim 1, wherein the details of all or selected security products includes the name of the security products, versions, and loaded signature files.
- 25 3. Apparatus for determining the protection that a first remote computer has from malware, the apparatus comprising:
 - a base computer (3) constructed and arranged to receive computer details of all or selected security products operating at a point in time on said first remote computer (2);
30 the base computer (3) being constructed and arranged to receive details of all or selected security products operating at a point in time on other remote computers (2) connected to the base computer (3) and details of processes run

by said other remote computer (2) that were not locally identified as being malware and to store the information in a database (7) at the base computer (3), wherein some processes in the database are marked as being malware; and, the base computer (3) being constructed and arranged to search the
5 database (7) to identify any processes marked as malware that were not identified by said other remote computers (2) having the same particular combination of security products as the first remote computer (2), wherein the base computer (3) is constructed and arranged to provide information to the user of said first remote computer (2) that said first remote computer (2) may be
10 susceptible to attack by said malware processes on the basis of said identifying.

4. Apparatus according to claim 3, wherein the details of all or selected security products includes the name of the security products, versions, and loaded signature files.

15

5. A computer program comprising program instructions for causing a computer to perform the method of claim 1 or claim 2.

CLAIMS

1. A method of determining the protection that a first remote computer has from malware, the method comprising:
- 5 receiving at a base computer (3) details of all or selected security products operating at a point in time on said first remote computer (2);
- receiving at the base computer (3) details of all or selected security products operating at a point in time on other remote computers (2) connected to the base computer (3) and details of processes run by said other remote
- 10 computers (3) that were not locally identified as being malware, and storing the information in a database (7) at the base computer (3), wherein some processes in the database (7) are marked as being malware;
- searching the database (7) identifying any processes marked as being malware that were not identified by said other remote computers (2) having the
- 15 same particular combination of security products as the first remote computer (2); and,
- providing information to the user of said first remote computer (2) that said first remote computer (2) may be susceptible to attack by said malware processes on the basis of said identifying.
- 20
2. A method according to claim 1, wherein the details of all or selected security products includes the name of the security products, versions, and loaded signature files.
- 25
3. Apparatus for determining the protection that a first remote computer has from malware, the apparatus comprising:
- a base computer (3) constructed and arranged to receive computer details of all or selected security products operating at a point in time on said first remote computer (2);
- 30 the base computer (3) being constructed and arranged to receive details of all or selected security products operating at a point in time on other remote computers (2) connected to the base computer (3) and details of processes run

Deleted: similar information from

Deleted: and

Deleted: malware

Deleted: that

Deleted: .¶
¶
2. A method according to claim 1, further comprising

Deleted:

Deleted: 3

Deleted: or claim 2

Deleted: 4

by said other remote computer (2) that were not locally identified as being malware and to store the information in a database (7) at the base computer (3), wherein some processes in the database are marked as being malware; and,

5 the base computer (3) being constructed and arranged to search the database (7) to identify any processes marked as malware that were not identified by said other remote computers (2) having the same particular combination of security products as the first remote computer (2), wherein the base computer (3) is constructed and arranged to provide information to the user of said first remote computer (2) that said first remote computer (2) may be
10 susceptible to attack by said malware processes on the basis of said identifying.

4. Apparatus according to claim 3, wherein the details of all or selected security products includes the name of the security products, versions, and loaded signature files.

15

5. A computer program comprising program instructions for causing a computer to perform the method of claim 1 or claim 2.

Deleted: similar information from other remote computers connected to the base computer

Deleted: malware

Deleted: that

Deleted: ¶
5. . Apparatus according to claim 4

Deleted: 6. . Apparatus according to claim 4 or claim 5, wherein the details of all or selected security products includes the name of the security products, versions, and loaded signature files.¶
7

Deleted: any of claims 1 to 3

European Patent Office
P. B. 5818
Patentlaan 2
2280 HV Rijswijk (ZH)
The Netherlands

Your Ref: 1957
Our Ref: NPB/JV/P10717EP-1
Date: 18 March 2014

By electronic submission

Dear Sirs

European Patent Application No. 13167436.8
Divided from European Patent Application No. 06755686.0
Prevx Limited

We refer to the search report published on 2 October 2013.

We herewith enclose instructions to your Cash & Accounts Department to take the necessary examination and designation fees for this application from our deposit account No. 28050163.

In response to the search opinion, we file amended claims on pages 44 and 45. We request that examination be carried out on these replacement claims taking into account the comments below. For the examiner's convenience, a tracked version of the claims is also enclosed showing the amendments now made.

Amendments and A123(2) EPC

Basis for the amendments now made is generally given in relation to the original PCT application. The present application is a divisional of the PCT application and has an identical (although repaginated) description and drawings.

Claim 1 has generally been amended to attempt to address the examiner's various clarity and other objections. In particular, claim 1 has been amended to refer to a first remote computer to more clearly distinguish this remote computer from the recited "other remote computers".

The expression "similar information" has been deleted and instead the claim specifically requires that the base computer receives information comprising "details of all or selected security products operating at a point in time on other remote computers".

Claim 1 also now requires that the information the base computer receives comprises "details of processes run by the other remote computers that were not locally identified as being malware" from the remote computers. Basis for this can be found in the original PCT application at page 37, lines 21 to 24.

Claim 1 now requires that “the information” (i.e. the details of security products and processes) is stored in a database at the base computer. Basis for this can be found throughout the original PCT description on pages 36 to 38.

Claim 1 also now requires that some processes in the database “are marked as being malware”. Basis for this amendment can be found in the original PCT description at page 38, lines 25 to 30, which describes how the database is searched for processes marked as bad, i.e. malware processes.

The final clause of claim 1 as originally filed has been clarified to say that the database is searched in order to identify processes marked as being malware that were not identified by the other remote computers having the same particular combination of security products as the first remote computer. These amendments generally follow on from the other amendments referred to above. This addresses the examiner’s objection that it was not clear in the original claim 1 what was meant by “that particular combination of security products”.

Finally, claim 1 has been amended to incorporate the subject matter of previous claim 2, namely that the user is provided with information that their computer may be susceptible to attack by said malware processes.

Similar amendments have been made to independent apparatus claim 3. A new dependent apparatus claim 4 has been added, corresponding to dependent method claim 2.

Reference numerals have been added throughout the claims.

Objections

In item 2.1, the examiner objects that the terms “security products” and “selected security products” are not clear. We do not see any difficulty with the term “security products”. Any program running on a computer providing security services to the computer, for example a firewall or antivirus program, would for example fall into this category. The skilled person would have no difficulty identifying from his common general knowledge whether or not a program on a computer is a security product and performs security functions. “Selected security products” simply indicates that it is not essential that details of all security products present on a remote computer be reported to the base computer. We submit that both these terms are clear. Finally, the term “similar information” has now been deleted from the claim.

Regarding item 2.2, as mentioned above, the phrase “that particular combination” has been clarified.

Regarding item 2.3, it is submitted that the above mentioned amendments have addressed the examiner’s points. As is clear from the description, the present invention, broadly speaking, provides a way of alerting users to possible security vulnerabilities in the particular combination of security products on their computer. The present invention involves collecting in a database at a base computer details of the security products running on remote computers and the processes that are being run on those remote computers and considered safe. At some point, it is determined that a particular process is actually a malware process and this process is marked as being “bad” in the community database. Various novel and advantageous techniques for identifying an object/process as being malware are disclosed in the present application (as claimed in the parent application or co-pending divisional

application). Any of these techniques, can be used to identify a process as being malware at the base computer. However, other techniques can be used. In principle, any known technique can be used, including for example analysis of objects by a human analyst. As will be evident, the particular method used for this is not important to what is currently claimed.

In which ever way the malware process is identified, the collection of information at the community database can be used to warn users of potential “holes” in their security products that leave them vulnerable to particular malware objects. This proceeds as follows. For a particular remote computer (the first remote computer in the language of claim 1), details of the security products on that computer are sent to the base computer. A search is then conducted of the database for malware processes that were allowed to run on other remote computers (i.e. not identified as malware) having that combination of security products. This indicates that the first computer is vulnerable to these malware processes. Thus, the user of the first remote computer can be warned and can take appropriate action in response.

We submit that all of the essential features of the invention are defined in the present independent claims, and the skilled person could implement the invention without any inventive effort based on what is taught in the application.

Prior Art

Regarding D1, this document teaches a process for centrally logging messages from security products on individual computers within a local network, wherein the messages indicates instances of malware being detected on those computers by those security products. This information is used to detect various patterns of malware detection across the network as a whole and used to prompt the user to take appropriate action. Paragraph [0030] of D1 teaches recognising at the central server from the messages received that up-to-date security programs have identified a threshold number of malware infections on remote computers, whereas no messages have been received from not up-to-date security programs relating to that malware. This prompts the server to force the remote computers to update to the latest version of the security program.

This scheme of D1 is different and much cruder compared to the present invention. There appears to be no teaching or suggestion in D1 of sending to the base computer details of processes which are allowed to run on the remote computers that are not identified as malware, nor of sending details of the security products on those computers. On the contrary, D1 only sends messages when malware is detected by the security products on remote computers. Thus, in D1 the central server has no knowledge of programs which are allowed to run on remote computers and which combination of security programs has allowed them to run. D1 merely “assumes” that “old” versions of security products have let malware processes run, but has no actual knowledge that those processes have been run on the remote computers.

Thus the present invention has the advantage of building a database of processes allowed to run under various combinations of security products. If a process is later identified as being malware, the database can be searched to find precisely which combinations of security products are vulnerable to the process. D1 does not teach or suggest searching a database to identify processes marked as being malware that were not identified by the remote computers having the same particular combination of security products, as required by claim 1.

The present invention therefore provides more “targeted” information to a remote user with a particular combination of security products that they are vulnerable to malware processes. In contrast, D1 merely instructs all remote computers to update their security products. Furthermore, the present invention is suitable for use on an internet wide scale, involving potentially millions of remote computers. D1 in contrast appears to be restricted to use in a local, private network in an organisation, which allows the network administrator for that organisation to make sure that the computers in the network are kept up to date.

Thus, there is a fundamental difference in approach between the present invention and the prior art which would not be derivable from the prior art without considerable inventive activity. We therefore submit that the present invention is novel and inventive over the cited prior art.

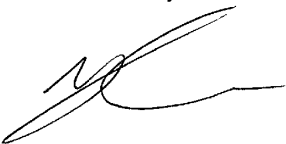
General

It is respectfully submitted that the present application is now in order for grant. Nevertheless, if the examiner does have any outstanding objections, he is requested to telephone the writer to discuss the matter or possibly to arrange an interview, or to issue a further written communication. As a precaution against premature rejection, Oral Proceedings are hereby requested before any final rejection of the application. Nevertheless, whilst Oral Proceedings have been requested, we emphasise that this is only as a precaution as it is believed that if there are any outstanding objections, they can be best resolved without the additional delay and expense of Oral Proceedings.

In the unlikely event oral proceedings should prove to be necessary, we request that, if possible, such proceedings should take place by video conference using IP technology, in accordance with OJ EPO 2012, 354.

It should be noted for the avoidance of doubt that the applicant is specifically not abandoning any subject matter which may be regarded as deleted by the filing of these replacement claims. The applicant reserves the right to file one or more divisional applications directed to any subject matter deleted by this amendment, whether alone or in combination with any remaining subject matter. Any deletion of subject matter is made without prejudice to the right of the applicant to reintroduce the subject matter, either in this application or in any divisional application. Furthermore, the applicant specifically reserves the right to revert to the wording of the claims as originally filed.

Yours faithfully



Nicholas P. Bebbington
Beck Greener (Association Registration No. 518)

Enc



Letter accompanying subsequently filed items

Representative:

Beck Greener
518
12 Fulwood Place
London WC1V 6HR
United Kingdom

Phone: + 44 (0) 20 7693 5600
Fax: + 44 (0) 20 7693 5601
E-mail: mail@beckgreener.com

80298 Munich
Germany
Tel. +49(0)89 2399-0 | Fax -4465

P.O. Box 5818
NL-2280 HV Rijswijk
Netherlands
Tel. +31(0)70 340-2040 | Fax -3016

10958 Berlin
Germany
Tel. +49(0)30 25901-0 | Fax -840

The document(s) listed below is (are) subsequently filed documents pertaining to the following application:

Application number

13167436.8

Applicant's or representative's reference

NPB/P10717EP-1

	Description of document	Original file name	Assigned file name
1	Reply to search opinion/written opinion/IPER	P10717EP-1_EPO SO response 18-3-14.pdf	WOREPLY-1.pdf
2	Amended claims (clean copy)	Claims cc SO response 18-3-14.pdf	CLMS-1.pdf
3	Amended claims with annotations	Claims redline SO response 18-3-14.pdf	CLMS-HWA-1.pdf

	Fees	Factor applied	Fee schedule	Amount to be paid
15-1	005e Designation fee - For all contracting States designated for applications filed on/after 01.04.2009	1	555.00	555.00
15-2	006 Examination fee - For applications filed on/after 01.07.2005	1	1 555.00	1 555.00
	Total:		EUR	2 110.00

	Payment	
1	Mode of payment	Debit from deposit account
	Currency:	EUR
	The European Patent Office is hereby authorised, to debit from the deposit account with the EPO any fees and costs indicated on the fees page.	
	Deposit account number:	28050163
	Account holder:	Beck Greener
2	Refund/Reimbursement	
	Reimbursement (if any) to be made to EPO deposit account:	28050163

NPB/P10717EP-1

	Account holder:	Beck Greener
--	-----------------	--------------

Signatures

Place: London
Date: 18 March 2014
Signed by: Nick Bebbington 13019
Association: Beck Greener
Capacity: (Representative)



European Patent Office
80298 MUNICH
GERMANY

Questions about this communication ?

Contact Customer Services at www.epo.org/contact



Beck Greener
Fulwood House
12 Fulwood Place
London WC1V 6HR
ROYAUME UNI

Date
17.03.14

Reference NPB/P10717EP-1	Application No./Patent No. 13167436.8 - 1957 / 2629232
Applicant/Proprietor Prevx Limited	

Communication of amended entries concerning the representative (R. 143(1)(h) EPC)

As requested, for the above-mentioned European patent application / European patent the entries concerning the representative have been amended as follows:

Beck Greener
Fulwood House
12 Fulwood Place
London WC1V 6HR
GB

The amendment will be recorded in the Register of European Patents.

Receiving Section



BeckGreener

John Raynor
Peter J. Smart
Ian Bartlett
C. Rowland Buehrlen
Avi Freeman
Ben Muir
John P. Hull
James A. Stones
Anna L. Hatt
Nick P. Bebbington

Associates
Deborah Selden
Jonathan P. J. Markham
Susan Davey
Duncan J. Morgan
Robert C. McDougall

Consultant
Jacqueline Needle

European Patent Office
Directorate General 2
D-80298 Munich
Germany

Our Ref: ALH/M34617
Date: 4 March 2014

Dear Sirs

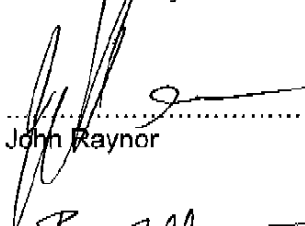
Change of Representative from Attorneys to Association Beck Greener (Association Registration No. 518)

We write in connection with European patent matters for which the undersigned representatives are recorded.

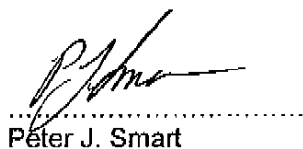
We request that these representatives be replaced in all Beck Greener EPO matters with the association of representatives Beck Greener (Association Registration No. 518). This association includes each of the undersigned representatives.

We should be grateful for confirmation that this change has been recorded.

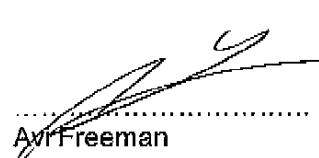
Yours faithfully



John Raynor



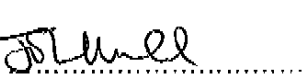
Peter J. Smart



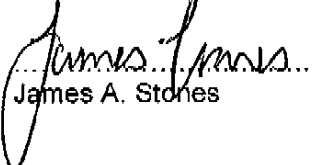
Avi Freeman



Benjamin M. J. Muir



John P. Hull



James A. Stones



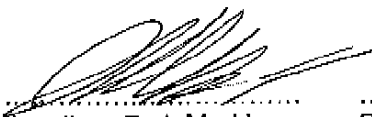
Anna L. Hatt



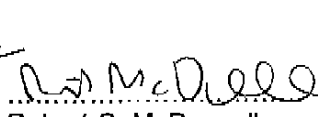
Nicholas P. Bebbington



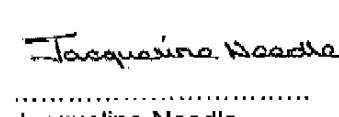
Deborah A. Selden



Jonathan P. J. Markham



Robert C. McDougall



Jacqueline Needle

Chartered & European Patent Attorneys | Trade Mark Attorneys | IP Litigators
Fulwood House, 12 Fulwood Place, London WC1V 6HR Tel: +44 20 7693 5600 Fax: +44 20 7693 5601
mail@beckgreener.com www.beckgreener.com Regulated by IPREG

Duration: 07.03.2014 16:07:41 - 07.03.2014 16:07:57. This page 1 of 1 was completed at 07.03.2014 16:07:57

Received at the EPO on Mar 07, 2014 16:07:57. Page 1 of 1



European Patent Office
Postbus 5818
2280 HV RIJSWIJK
NETHERLANDS
Tel. +31 (0)70 340-2040
Fax +31 (0)70 340-3016



Bebbington, Nicholas Paul
Beck Greener
Fulwood House
12 Fulwood Place
London WC1V 6HR
ROYAUME UNI

**For any questions about
this communication:**

Tel.: +31 (0)70 340 45 00

Date
08.10.13

Reference NPB/P10717EP-1	Application No./Patent No. 13167436.8 - 1957 / 2629232
Applicant/Proprietor Prevx Limited	

Communication pursuant to Rule 69 EPC - reminder concerning payment of the designation fee (Art. 79(2) EPC) and of the examination fee (Art. 94(1) EPC) - and invitation pursuant to Rule 70a(1) EPC

The date on which the European Patent Bulletin mentions the publication of the European search report for the above-mentioned European patent application is: 02.10.13.

Your attention is drawn to Article 79(2) and Rule 39(1) EPC as well as Article 94(1), Rule 70(1) and Rule 70a(1) EPC, according to which within **six months** of the above-mentioned publication date of the search report

- the designation fee must be paid,
- the request for examination must be filed and the examination fee must be paid,
- comments on the objections raised in the opinion accompanying the European search report and/or any amendments to the description, claims and drawings correcting any deficiencies noted in the opinion must be filed (R. 70a(1), 137(2) EPC; Guidelines for Examination in the EPO, B-XI, 8).

1. Payment of the designation fee and of the examination fee

The current designation fee for one or more Contracting States designated is: EUR 555,00

The current examination fee is: EUR 1555,00

If the written request for examination is filed in an admissible non-EPO language in accordance with Article 14(4) EPC, a reduction of the examination fee according to Rule 6(3) EPC applies.

If the designation fee and the examination fee are not paid within the period laid down in Rule 39(1) and Rule 70(1) EPC, the application **will be deemed to be withdrawn** (R. 39(2) and Art. 94(2) EPC).

Any extension fees are also payable within the above-mentioned period.

Registered letter

EPO Form 1081 11.12 (NFS/RTB/ESOP01=N)

2. Comments on the opinion accompanying the European search report and filing of amendments

Should the reply to the invitation pursuant to Rule 70a(1) EPC be filed in an admissible non-EPO language, a translation is to be submitted within one month of its filing (R. 6(2) EPC).

If filing amendments, you must identify them and indicate the basis for them in the application as filed. Failure to meet either requirement may lead to a communication from the Examining Division requesting that you correct this deficiency (R. 137(4) EPC).

Should you not comply with this invitation within the time limit, the application **will be deemed to be withdrawn** in accordance with Rule 70a(3) EPC.

Note to users of the automatic debiting procedure

Unless the EPO receives prior instructions to the contrary, the examination fee and the designation fee will be debited on the last day of the period for payment. For further details see the Arrangements for the automatic debiting procedure, Supplement to OJ EPO 3/2009.

Important information concerning fee amounts

Following any amendment to the Rules relating to Fees, the amount(s) mentioned in this communication may be different from the amount(s) **actually due on the date of payment**. The latest version of the Schedule of fees and expenses, published as a Supplement to the Official Journal of the EPO, is also available on the EPO website (www.epo.org) and can be found under www.epo.org/schedule-of-fees, which allows the viewing, downloading and searching for individual fee amounts, both current and previous.

Payments by cheque delivered or sent direct to the EPO are no longer accepted as from 1 April 2008 (see OJ EPO 2007, 626).

Note concerning renewal fees

Under Article 86 EPC renewal fees shall be paid to the EPO for the European patent application. These fees shall be due in respect of the third and each subsequent year, calculated from the date of filing. Due account should be taken that the EPO will not send invoices or reminders to pay any fees in due time.

Receiving Section





Acknowledgement of receipt

We hereby acknowledge receipt of the following subsequently filed document(s):

Submission number	2327358	
Application number	EP13167436.8	
Date of receipt	01 October 2013	
Receiving Office	European Patent Office, The Hague	
Your reference	NB/P10717EP-1	
Applicant	All applicants as on file	
Documents submitted	package-data.xml epf1038.pdf (1 p.)	ep-sfd-request.xml INVT-1.pdf\P10717EP-1_EPO 1-10-13.pdf (1 p.)
Submitted by	CN=Nick Bebbington 13019	
Method of submission	Online	
Date and time receipt generated	01 October 2013, 16:23 (CEST)	
Message Digest	F2:94:CF:84:68:76:F4:4A:E5:8B:81:C4:24:48:41:A2:1E:E7:0C:5D	

Correction by the EPO of errors in debit instructions filed by eOLF

Errors in debit instructions filed by eOLF that are caused by the editing of Form 1038E entries or the continued use of outdated software (all forms) may be corrected automatically by the EPO, leaving the payment date unchanged (see decision T 152/82, OJ EPO 1984, 301 and point 6.3 ff ADA, Supplement to OJ EPO 10/2007).

/European Patent Office/



Letter accompanying subsequently filed items

Representative:

Mr Nicholas BEBBINGTON
Beck Greener
Fulwood House
12 Fulwood Place
London London WC1V 6HR
United Kingdom

Phone: + 44 (0) 20 7693 5600
Fax: + 44 (0) 20 7693 5601
E-mail: nbebbington@beckgreener.com

80298 Munich
Germany
Tel. +49(0)89 2399-0 | Fax -4465

P.O. Box 5818
NL-2280 HV Rijswijk
Netherlands
Tel. +31(0)70 340-2040 | Fax -3016

10958 Berlin
Germany
Tel. +49(0)30 25901-0 | Fax -840

The document(s) listed below is (are) subsequently filed documents pertaining to the following application:

Application number

13167436.8

Applicant's or representative's reference

NB/P10717EP-1

	Description of document	Original file name	Assigned file name
1	Documents concerning the inventorship	P10717EP-1_EPO 1-10-13.pdf	INVT-1.pdf

Signatures

Place: London
Date: 01 October 2013
Signed by: , Nick Bebbington 13019
Capacity: (Representative)

NB/P10717EP-1

European Patent Office
P. B. 5818
Patentlaan 2
2280 HV Rijswijk (ZH)
The Netherlands

Your Ref: 1245
Our Ref: NB/JV/P10717EP-1
Date: 1 October 2013

By electronic submission

Dear Sirs

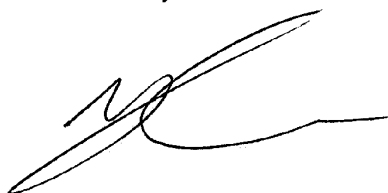
European Patent Application No. 13167436.8
Divided from European Patent Application No. 06755686.0
Prevx Limited

We refer to the official communication dated 9 August 2013 regarding the address of inventor Markus Hartwig.

Please be advised that the inventor's new address is:

101 Avon Way
Derby
DE65 5AE
United Kingdom

Yours faithfully



Nicholas P. Bebbington
Authorised European Patent Attorney



European Patent Office
Postbus 5818
2280 HV RIJSWIJK
NETHERLANDS
Tel. +31 (0)70 340-2040
Fax +31 (0)70 340-3016



Bebbington, Nicholas Paul
Beck Greener
Fulwood House
12 Fulwood Place
London WC1V 6HR
ROYAUME UNI

**For any questions about
this communication:**

Tel.: +31 (0)70 340 45 00

Date
30.08.13

Reference NPB/P10717EP-1	Application No./Patent No. 13167436.8 - 1957 / 2629232
Applicant/Proprietor Prevx Limited	

Communication

The extended European search report is enclosed.

The extended European search report includes, pursuant to Rule 62 EPC, the European search report (R. 61 EPC) or the partial European search report/ declaration of no search (R. 63 EPC) and the European search opinion.

Copies of documents cited in the European search report are attached.

☒ 0 additional set(s) of copies of such documents is (are) enclosed as well.

The following have been approved:

☒ Abstract ☒ Title

☐ The Abstract was modified and the definitive text is attached to this communication.

The following figure(s) will be published together with the abstract: 1

Refund of search fee

If applicable under Article 9 Rules relating to fees, a separate communication from the Receiving Section on the refund of the search fee will be sent later.

Should you wish to further prosecute this application in the examination phase, your attention is drawn to the provisions of Rule 70a EPC. An invitation to respond to the extended European search report will be issued once the date of publication of the European search report has been mentioned in the European Patent Bulletin (R. 69(1), R. 70(2) EPC).



The examination is being carried out on the **following application documents**

Description, Pages

1-43 as originally filed

Claims, Numbers

1-7 as originally filed

Drawings, Sheets

1/3-3/3 as originally filed

Reference is made to the following document; the numbering will be adhered to in the rest of the procedure.

D1 US 2003/131256 A1 (ACKROYD ROBERT JOHN [GB]) 10 July 2003
(2003-07-10)

1.0. The application does not meet the requirements of Article 83 EPC, because the invention is not disclosed in a manner sufficiently clear and complete for it to be carried out by a person skilled in the art, for the following reason:

The last feature of claims 1 and 4, namely, the step of "identifying any malware processes that were not identified by said other remote computers having that particular combination of security products" is defined in terms of results to be achieved. It is not evident for a skilled person how to implement this step, and the documents of the application as filed do not indicate any way of doing it.

The claimed invention is described at page 28, line 28 to page 30, line 28. The description recites, page 30, lines 4-8, "if for example the database knows that a computer in the past has version A of anti-virus product B ..., but that a particular malware process P was not detected by this combination", and, further on, lines 23-24, "the database ... is searched for events for processes marked as "bad" that occurred on computers with that particular mix of security products and that were not locally detected", which amounts to the statement of the same result to be achieved.

Since the application does not indicate any way which would enable a skilled person to implement this step without inventive effort, it is considered that it does not fulfill the requirements of Art.83 EPC.

2.0. The application does not meet the requirements of Article 84 EPC, because claims 1 and 4 are not clear, as follows:

2.1. The terms "security products", "selected security products" and "similar information" used in claims 1 and 4 are not clear. A skilled person does not have means to distinguish if a certain product, or a certain information, falls under the claimed scope.

2.2. It is not clear to what refers "that particular combination" in the last feature of claims 1 and 4.

2.3. Claims 1 and 4 appear to be missing essential technical features. The claim does not define how, and if at all, the remote computers are identifying malware processes. Therefore, it is not clear how the information about malware processes not identified by such computers (even if this information could be provided, see par.1.0. here above), could contribute to solution of the problem of determining the protection from malware on one remote computer.

3.0. Due to issues regarding Art. 83 and 84 EPC, the claims cannot be assessed for novelty/inventive step. However, it is noted that document D1 appears to be very relevant for the present invention, since it discloses a system for monitoring and enforcing security settings on the computers within a computer network, using information about malware scanning products and malware detection on the client computers, the information being received and analyzed on the central server, see in particular par.[24] to par.[30] of D1.

3.1. In addition, it is noted that claims are not compliant with requirements of Rules 43 (1) and (7) EPC.



Europäisches
Patentamt
European
Patent Office
Office européen
des brevets

EUROPEAN SEARCH REPORT

Application Number
EP 13 16 7436

DOCUMENTS CONSIDERED TO BE RELEVANT			
Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
A	US 2003/131256 A1 (ACKROYD ROBERT JOHN [GB]) 10 July 2003 (2003-07-10) * page 2, paragraph 24 - paragraph 30 * -----	1-7	INV. G06F21/56 G06F21/57
			TECHNICAL FIELDS SEARCHED (IPC)
			G06F H04L
The present search report has been drawn up for all claims			
Place of search The Hague		Date of completion of the search 25 July 2013	Examiner Arbutina, Ljiljana
CATEGORY OF CITED DOCUMENTS X : particularly relevant if taken alone Y : particularly relevant if combined with another document of the same category A : technological background O : non-written disclosure P : intermediate document T : theory or principle underlying the invention E : earlier patent document, but published on, or after the filing date D : document cited in the application L : document cited for other reasons & : member of the same patent family, corresponding document			

1
EPO FORM 1503 03 82 (P04C01)

**ANNEX TO THE EUROPEAN SEARCH REPORT
ON EUROPEAN PATENT APPLICATION NO.**

EP 13 16 7436

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EPO file on

The members are as contained in the European Patent Office EDP file on

The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

25-07-2013

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2003131256 A1	10-07-2003	NONE	

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82



European Patent Office
Postbus 5818
2280 HV RIJSWIJK
NETHERLANDS
Tel. +31 (0)70 340-2040
Fax +31 (0)70 340-3016



Bebbington, Nicholas Paul
Beck Greener
Fulwood House
12 Fulwood Place
London WC1V 6HR
ROYAUME UNI

**For any questions about
this communication:**

Tel.: +31 (0)70 340 45 00

Date
09.08.13

Reference NPB/P10717EP-1	Application No./Patent No. 13167436.8 - 1957 / 2629232
Applicant/Proprietor Prevx Limited	

Communication pursuant to Rule 19(1) EPC

The communication issued pursuant to Rule 19(3) EPC, sent to the inventor designated below, has been returned by the postal services.

You are requested to indicate the correct address of the inventor (R. 19(1) EPC).

Inventor : Hartwig, Markus
Exchange House 494 Midsummer Boulevard
GB / Milton Keynes, Buckinghamshire MK9 2EA

Receiving Section





European Patent Office
Postbus 5818
2280 HV RIJSWIJK
NETHERLANDS
Tel. +31 (0)70 340-2040
Fax +31 (0)70 340-3016



Hartwig, Markus
Exchange House
494 Midsummer Boulevard
Milton Keynes, Buckinghamshire MK9 2EA
ROYAUME UNI

**For any questions about
this communication:**

Tel.: +31 (0)70 340 45 00

Date
05.07.13

Reference	Application No./Patent No. 13167436.8 - 1957
Applicant/Proprietor Prevx Limited	

Designation as inventor - communication under Rule 19(3) EPC

You have been designated as inventor in the above-mentioned European patent application. Below you will find the data contained in the designation of inventor and further data mentioned in Rule 143(1) EPC:

DATE OF FILING : 30.06.06
PRIORITY : GB/30.06.05/ GBA 0513375
TITLE : Methods and apparatus for dealing with malware
DESIGNATED STATES : AT BE BG CH CY CZ DE DK EE ES FI FR GB GR
HU IE IS IT LI LT LU LV MC NL PL PT RO SE SI SK
TR

INVENTOR (PUBLISHED = 1, NOT PUBLISHED = 0):

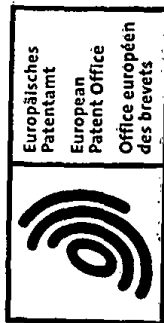
1/Morris, Melvyn/Redmire Gap Intake Lane/Turnditch, Derbyshire DE56 2LU/GB
1/Stubbs, Paul/7 Rookery Road/Wybston, Bedfordshire MK44 3AX/GB
1/Hartwig, Markus/Exchange House 494 Midsummer Boulevard/Milton Keynes,
Buckinghamshire MK9 2EA/GB
1/Harter, Darren/178 Barnwood Road, Hucclecote/Gloucester, Gloucestershire GL4 3JZ/GB

DECLARATION UNDER ARTICLE 81 EPC:

The applicant(s) has (have) acquired the right to the European patent as employer(s).

Receiving Section





Europäisches
Patentamt
European
Patent Office
Office européen
des brevets

40 EUROPEAN
PATENT
CONVENTION
YEARS 1973-2013
Innovation matters



Port Betaald
Port Payé

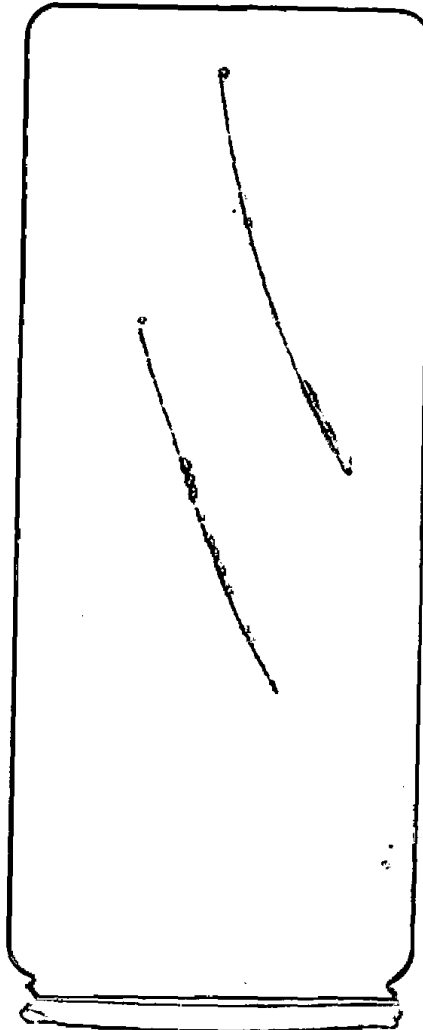


Pays-Bas

EPA EPO OEB
tel: (070)3403002

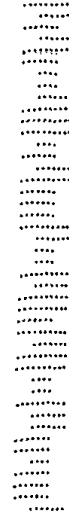
01-08-2013

Mailroom 7



RTS

4.111



17



Application No.: 13167436.8

The search has started on 25.07.13 (see Notice from the European Patent Office dated 03/2013, OJ EPO 2013, 153).

Receiving Section



European Patent Office
Postbus 5818
2280 HV RIJSWIJK
NETHERLANDS
Tel. +31 (0)70 340-2040
Fax +31 (0)70 340-3016



Bebbington, Nicholas Paul
Beck Greener
Fulwood House
12 Fulwood Place
London WC1V 6HR
ROYAUME UNI

**For any questions about
this communication:**

Tel.: +31 (0)70 340 45 00

Date
24.07.13

Reference NPB/P10717EP-1	Application No./Patent No. 13167436.8 - 1957 / 2629232
Applicant/Proprietor Prevx Limited	

**Notification of European publication number and information on the application of
Article 67(3) EPC**

You are hereby informed that the technical preparations for the publication of the above-mentioned European patent application have been completed.

The application will be published on 21.08.13 without the European search report.

The publication number is: 2629232.

The publication will be mentioned in European Patent Bulletin number 2013/34.

(<http://bulletin.european-patent-office.org>).

The provisional protection under Article 67(1) and (2) EPC in the individual contracting states becomes effective only when the conditions referred to in Article 67(3) EPC have been fulfilled. For further information, also with respect to extension states, please refer to the EPO brochure "National Law relating to the EPC" (<http://www.epo.org/patents/law/legal-texts/national-law-epc.html>).

The title of the invention in the three official languages of the European Patent Office is worded as follows:

Verfahren und Vorrichtung zum Behandeln von Malware
Methods and apparatus for dealing with malware
Procédés et appareil de gestion de logiciels malveillants

In all future communications to the EPO, please quote the application number as indicated above, i.e. including the final four figures (which identify the Directorate responsible for the subsequent procedure).

Remark

The publication can be downloaded, free of charge, from the EPO publication server <https://data.epo.org/publication-server/> or can be ordered from the Vienna sub-office upon payment of a fee (see Decision of the President of the EPO dated 12 July 2007 concerning the form of publication of European patent applications, European search reports and European patent specifications, Special edition No. 3, OJ EPO 2007, 97).

Note concerning renewal fees

Under Article 86 EPC renewal fees shall be paid to the EPO for the European patent application. These fees shall be due in respect of the third and each subsequent year, calculated from the date of filing. Due account should be taken that the EPO will not send invoices or reminders to pay any fees in due time.

Receiving Section



European Patent Office
Postbus 5818
2280 HV RIJSWIJK
NETHERLANDS
Tel. +31 (0)70 340-2040
Fax +31 (0)70 340-3016



Bebbington, Nicholas Paul
Beck Greener
Fulwood House
12 Fulwood Place
London WC1V 6HR
ROYAUME UNI

Formalities Officer

Name: van Pomeran, Patrick
Tel.: 4795
or call:
+31 (0)70 340 45 00

Date

01-07-2013

Reference NPB/P10717EP-1	Application No./Patent No. 13167436.8 - 1957
Applicant/Proprietor Prevx Limited	

BRIEF COMMUNICATION

Subject: ☐ Your letter of
☐ Our telephone conversation of
☐ Communication of
☐

Enclosure(s): ☐ Letter from the proprietor of the patent of
☐ Copy (copies)
☐ Communication:

Formal examination pursuant to Art. 90 EPC has revealed that the title mentioned on EPO Form 1001 is different to the title mentioned in the Description.

Please note that the title in the Description will be used for the further procedures.

Please take note.

Receiving Section



☐ **Registered letter**

EPO Form 2911 12.07 (26/06/13)

PV04077

ABSTRACT

METHODS AND APPARATUS FOR DEALING WITH MALWARE

5 In one aspect, a method of classifying a computer object as malware
includes receiving at a base computer data about a computer object from each
of plural remote computers on which the object or similar objects are stored. The
data about the computer object received from the plural computers is compared
in the base computer. The computer object is classified as malware on the basis
10 of said comparison. In one embodiment, the data about the computer object
includes one or more of : executable instructions contained within or constituted
by the object; the size of the object; the name of the object; the logical storage
location or path of the object on the respective remote computers; the vendor of
the object; the software product and version associated with the object; and,
15 events initiated by or involving the object when the object is created, configured
or runs on the respective remote computers.



Acknowledgement of receipt

We hereby acknowledge receipt of your request for grant of a European patent as follows:

Submission number	2124073	
Application number	EP13167436.8	
File No. to be used for priority declarations	EP13167436	
Date of receipt	13 May 2013	
Your reference	NPB/P10717EP-1	
Applicant	Prevx Limited	
Country	GB	
Title	Methods and Apparatus for Dealing with Malware - Divisional	
Documents submitted	package-data.xml application-body.xml SPECEPO-3.pdfabstract.pdf (1 p.) SPECEPO-1.pdfdescription.pdf (43 p.) OTHER-1.pdfP10717EP-1_EPO 10-5-13.pdf (1 p.) f1002-2.pdf (1 p.) f1002-4.pdf (1 p.)	ep-request.xml ep-request.pdf (5 p.) SPECEPO-4.pdfdrawings.pdf (3 p.) SPECEPO-2.pdfclaims.pdf (2 p.) f1002-1.pdf (1 p.) f1002-3.pdf (1 p.)
Submitted by	CN=N. Bebbington 13019,O=Beck Greener,C=GB	
Method of submission	Online	

Date and time
receipt generated

13 May 2013, 12:48 (CEST)

Message Digest

51:C1:10:20:89:13:8F:06:FC:7E:E2:50:B1:DF:34:CD:1A:58:07:82

Correction by the EPO of errors in debit instructions filed by eOLF

Errors in debit instructions filed by eOLF that are caused by the editing of Form 1038E entries or the continued use of outdated software (all forms) may be corrected automatically by the EPO, leaving the payment date unchanged (see decision T 152/82, OJ EPO 1984, 301 and point 6.3 ff ADA, Supplement to OJ EPO 10/2007).

/European Patent Office/

CLAIMS

1. A method of determining the protection that a remote computer has from malware, the method comprising:
 - 5 receiving at a base computer details of all or selected security products operating at a point in time on said remote computer;
receiving similar information from other remote computers connected to the base computer; and,
identifying any malware processes that were not identified by said other
10 remote computers having that particular combination of security products.
2. A method according to claim 1, further comprising providing information to the user of said remote computer that said remote computer may be susceptible to attack by said malware processes on the basis of said identifying.
15
3. A method according to claim 1 or claim 2, wherein the details of all or selected security products includes the name of the security products, versions, and loaded signature files.
- 20 4. Apparatus for determining the protection that a remote computer has from malware, the apparatus comprising:
 - a base computer constructed and arranged to receive computer details of all or selected security products operating at a point in time on said remote computer;
 - 25 the base computer being constructed and arranged to receive similar information from other remote computers connected to the base computer; and,
the base computer being constructed and arranged to identify any malware processes that were not identified by said other remote computers having that particular combination of security products.
- 30 5. Apparatus according to claim 4, wherein the base computer is constructed and arranged to provide information to the user of said remote computer that

said remote computer may be susceptible to attack by said malware processes on the basis of said identifying.

6. Apparatus according to claim 4 or claim 5, wherein the details of all or
5 selected security products includes the name of the security products, versions, and loaded signature files.

7. A computer program comprising program instructions for causing a computer to perform the method of any of claims 1 to 3.

METHODS AND APPARATUS
FOR DEALING WITH MALWARE

The present invention relates generally to methods and apparatus for
5 dealing with malware. In one aspect, the present invention relates to a method
and apparatus for classifying a computer object as malware. In another aspect,
the present invention relates to a method and apparatus for determining the
protection that a remote computer has from malware. In another aspect, the
present invention relates to a method and apparatus for classifying a computer
10 object as malware or as safe. In another aspect, the present invention relates to
a method of installing software on a computer.

The term "malware" is used herein to refer generally to any executable
computer file or, more generally "object", that is or contains malicious code, and
15 thus includes viruses, Trojans, worms, spyware, adware, etc. and the like.

A typical anti- malware product, such as anti-virus scanning software,
scans objects or the results of an algorithm applied to the object or part thereof
to look for signatures in the object that are known to be indicative of the
20 presence of a virus. Generally, the method of dealing with malware is that when
new types of malware are released, for example via the Internet, these are
eventually detected. Once new items of malware have been detected, then the
service providers in the field generate signatures that attempt to deal with these
and these signatures are then released as updates to their anti-malware
25 programs. Heuristic methods have also been employed.

These systems work well for protecting against known malicious objects.
However, since they rely on signature files being generated and/or updated,
there is inevitably a delay between a new piece of malware coming into
30 existence or being released and the signatures for combating that malware being
generated or updated and supplied to users. Thus, users are at risk from new
malware for a certain period of time which might be up to a week or even more.

Moreover, in order to try to defeat anti-virus products, the malware writers use obfuscation techniques in order to attempt to hide the signature or signature base data of the virus code from detection. Typically, the obfuscation involves encrypting or packing the viral code.

5

WO-A-2004/097602 describes a system that analyses computer files received or generated by a local computer and compares these with a database of known files to determine whether a particular file is known and if so whether it has been known about long enough that it can be regarded as "safe". However, in practice, on its own this is not likely to provide for adequate protection because, for example, the active payload of a virus or Trojan may only be programmed to activate at a particular date, or upon receiving a message or instruction from a local or remote system or process, or on the occurrence of a particular event that may be many months or even years after the process has been first run or is released. Thus, just looking at the age of a file is an unsatisfactory way of determining whether it is properly safe and will remain so.

20

In the system of US-A-2004/0083408, a worm in a file is detected by examining connection attempts made by the specific file running on a computer.

25

US-A-6944772, US-A-6772346, EP-A-1549012 and EP-A-1280040 all disclose "community-based" anti-malware systems in which a plurality of "local" computers all connect via a network (which may be a LAN or the Internet, for example) to a central computer. On encountering a file that is not already known to them, the local computers send a request to the central computer for authorisation to run the file. If the file is recognised at the central computer, then the central computer can send permission for the local computer to run the file if the file is known to be safe or send a "deny" command if the file is known to be malicious. However, in each of these prior art proposals, if the file is not known at the central computer, then the whole file is sent to the central computer where it can be analysed to determine whether it should be regarded as safe or malware. Such analysis is typically carried out manually or "semi-manually" by

30

subjecting the file to detailed analysis, for example by emulation or interpretation, which can still take days given the human involvement that is typically required. There is therefore still a considerable period of time before a new file is classified as safe or as malware. In the case of these prior art systems, the request for
5 authorisation to run the file that is sent by a local computer to the central computer may comprise sending a checksum or "signature" or "key" that uniquely represents the file.

A similar community-based anti-malware system is disclosed in
10 WO-A-02/33525. In this system, in the case that a local computer is seeking clearance to run a file that is not known by the central computer to be safe or malware, some limited audit information about the prevalence of the file on other local computers can be sent to a human system administrator associated with the local computer that is seeking permission to run the file. The human system
15 administrator can therefore make a better informed though still "manual" decision as to whether or not the file is safe to run.

In the system of US-A-2004/0073810, a metafile containing data about an attachment or other transmitted file is sent to a central computer. The data
20 about that file is analysed to determine a likelihood of the transmitted file being malware. A specific example given is that if the transmitted file has been transmitted via at least a certain number of servers, then it should be treated as malware.

25 In the systems disclosed in US-A-2005/0021994 and US-A-2004/0153644, pre-approved files, which may be certified as safe by for example the software vendor associated with the files, may be permitted always to run without further checking. In one embodiment of the system of US-A-2004/0153644, monitoring is carried out to decide that a file is malicious if
30 an abnormally high number of requests by that file is received at a central authority from plural local computers in a time period or if an abnormally high

number of requests by that file on a single computer is received from the single local computer in a time period.

5 In the system of US-A-2004/0006704, a comparison is made between installed versions of software on a computer with a database of software versions and their known vulnerabilities. A user of the computer can therefore be informed of specific risks and how to minimise those risks by updating existing or installing new software.

10 In the system of WO-A-03/021402, a central database holds a virtual image of all files stored on each of plural local computers. If a threat in one local computer is identified, other local computers with a similar configuration can be notified of the risk.

15 Thus, the prior art systems either rely on deep analysis of a new object in order to determine whether or not the object is malicious, which introduces delay and therefore risk to users during the period that the file is analysed and new anti-malware signatures distributed, or limited analysis of the operation of the particular object or its method of transmission to a computer is carried out to
20 decide a likelihood of the object being malicious.

According to a first aspect of the present invention, there is provided a method of classifying a computer object as malware, the method comprising:
at a base computer, receiving data about a computer object from each of
25 plural remote computers on which the object or similar objects are stored;
comparing in the base computer the data about the computer object received from the plural computers; and,
classifying the computer object as malware on the basis of said
comparison.

30

Compared to the prior art that relies solely on signature matching, this aspect allows a comparison to be made between the objects and/or their effects

on the different remote computers to determine whether or not a particular object should be classed as good or as malware. Sophisticated pattern analysis can be carried out. This allows a rapid determination of the nature of the object to be made, without requiring detailed analysis of the object itself as such to determine
5 whether it malware and also avoids the need to generate new signatures to be used for signature matching as in the conventional prior art anti-virus software.

In a preferred embodiment, the data about the computer object that is sent from the plural remote computers to the base computer and that is used in
10 the comparison includes one or more of: executable instructions contained within or constituted by the object; the size of the object; the current name of the object; the physical and folder location of the object on disk; the original name of the object; the creation and modification dates of the object; vendor, product and version and any other information stored within the object; the object header or
15 header held by the remote computer; and, events initiated by or involving the object when the object is created, configured or runs on the respective remote computers.

Preferably, the comparing identifies relationships between the object and
20 other objects. In an example, this can be used immediately and automatically to mark a child object as bad (or good) if the or a parent or other related object is bad (or good). Thus, if at least one other object to which said object is related is classed as malware, then the method may comprise classifying said object as malware. Said other objects include the object or similar objects stored on at
25 least some of the remote computers. Said other objects may include other objects that are parent objects or child objects or otherwise process-related objects to said object.

In a most preferred embodiment, the data is sent in the form of key that is
30 obtained by a hashing process carried out in respect of the objects on the respective remote computers. A major advantage of using such a key is that it keeps down the volume of data that needs to be transmitted to the base

computer. Given that there may be thousands or even millions of connected remote computers and further given that each may send details about very many objects, this can be an important advantage.

5 The key preferably has at least one component that represents executable instructions contained within or constituted by the object. This important preferred feature allows a comparison to be made at the base computer of only the executable instructions of the object. This means for example that differently named objects that basically have the same executable
10 instructions, which is often an indicator that the objects are malware, can nevertheless be regarded as the "same" object for this purpose. As another example, a new version of a program may be released which has minor changes compared to a previous version already known to the base computer and which in substance, at least in respect of the executable instructions, can be regarded
15 as being the same as the previous version. In that case, the minor differences can be ignored and the objects regarded as being the same. Not only is this useful in distinguishing between malware and for example revised versions of previous software, it also keeps down the data transmission and storage requirements because the base computer can inform the remote computers that
20 an apparently new object is for this purpose the same as a previously known object, thus avoiding having the remote computers send full details about the object or the object itself to the base computer.

 The key preferably has at least one component that represents data about
25 said object. Said data about said object may include at least one of: the current name of the object; the physical and folder location of the object on disk; the original name of the object; the creation and modification dates of the object; vendor, product and version and any other information stored within the object; the object header or header held by the remote computer; and, events initiated
30 by or involving the object when the object is created, configured or runs on the respective remote computers.

The key preferably has at least one component that represents the physical size of the object.

Where more than one of these components are present in the key, the
5 plural components are preferably severable.

The method may comprise initially classifying an object as not malware, generating a mask for said object that defines acceptable behaviour for the object, and comprising monitoring operation of the object on at least one of the
10 remote computers and reclassifying the object as malware if the actual monitored behaviour extends beyond that permitted by the mask. This provides an efficient and effective way of monitoring the behaviour of an object that has been classified or regarded as good and allows the object to be reclassified quickly as malware if the behaviour of the object warrants it.

15 According to a second aspect of the present invention, there is provided apparatus for classifying a computer object as malware, the apparatus comprising:

a base computer constructed and arranged to receive data about a
20 computer object from each of plural remote computers on which the object or similar objects are stored;

the base computer being constructed and arranged to compare the data about the computer object received from said plural computers; and,

the base computer being constructed and arranged to classify the
25 computer object as malware on the basis of said comparison.

According to a third aspect of the present invention, there is provided a method of providing data about a computer object from a remote computer to a base computer so that a comparison can be made at the base computer with
30 similar data received from other remote computers, the method comprising:

providing from a remote computer to a base computer data about a computer object that is stored on the remote computer;

the data including one or more of: executable instructions contained within or constituted by the object; the size of the object; the current name of the object; the physical and folder location of the object on disk; the original name of the object; the creation and modification dates of the object; vendor, product and
5 version and any other information stored within the object; the object header or header held by the remote computer; and, events initiated by or involving the object when the object is created, configured or runs on the respective remote computers;

the data being sent in the form of key that is obtained by a hashing
10 process carried out in respect of the object on the remote computer.

This method, which may be carried out by so-called agent software running on the remote computer, allows for efficient sending of data to the base computer, which minimises data transmission and storage requirements and
15 also permits rapid analysis to be made at the base computer.

The key preferably has at least one component that represents executable instructions contained within or constituted by the object.

20 The key preferably has at least one component that represents data about said object. Said data about said object may include at least one of: the current name of the object; the physical and folder location of the object on disk; the original name of the object; the creation and modification dates of the object; vendor, product and version and any other information stored within the object;
25 the object header or header held by the remote computer; and, events initiated by or involving the object when the object is created, configured or runs on the respective remote computers.

The key preferably has at least one component that represents the
30 physical size of the object.

According to a fourth aspect of the present invention, there is provided a method of determining the protection that a remote computer has from malware, the method comprising:

- receiving at a base computer details of all or selected security products
- 5 operating at a point in time on said remote computer;
- receiving similar information from other remote computers connected to the base computer; and,
- identifying any malware processes that were not identified by said other remote computers having that particular combination of security products.

10

- In this way, the base computer can be used to obtain information as to whether for example a particular, specific combination of operating system and various security products, including settings and signature files existing at a point in time, renders a particular computer having those products and settings
- 15 susceptible or vulnerable to any particular malware object. The user can be advised accordingly and for example provided with recommendations for remedying the situation.

- The method may therefore comprise providing information to the user of
- 20 said remote computer that said remote computer may be susceptible to attack by said malware processes on the basis of said identifying.

- The details of all or selected security products preferably includes the name of the security products, versions, and loaded signature files.

25

- According to a fifth aspect of the present invention, there is provided apparatus for determining the protection that a remote computer has from malware, the apparatus comprising:
- a base computer constructed and arranged to receive computer details of
- 30 all or selected security products operating at a point in time on said remote computer;

the base computer being constructed and arranged to receive similar information from other remote computers connected to the base computer; and,
the base computer being constructed and arranged to identify any malware processes that were not identified by said other remote computers
5 having that particular combination of security products.

According to a sixth aspect of the present invention, there is provided a method of classifying a computer object as malware or as safe, wherein said computer object is a descendant or otherwise related object of a first computer
10 object, the method comprising:
classifying a first computer object as malware or as safe;
identifying in a key relating to said first computer object a component that uniquely identifies the first computer object and that is inherited or otherwise present in the key of a descendant or other related computer object of the first
15 computer object; and,
classifying said computer object as malware or as safe as the case may be on the basis of the unique identifier component being present in the key of said computer object.

20 This aspect uses the concept of ancestry to enable objects to be marked as malware. For example, any particular process may spawn child processes which are therefore related. The key relating to the first object may be inspected to identify a component that uniquely identifies the first object and that is inherited or otherwise present in the key of a descendant or other related object
25 of the first object.

The method may comprise monitoring activities of said first computer object and reclassifying the first computer object as malware in the case that it was initially classified as safe and subsequently determined to be malware, the
30 method further comprising automatically classifying as malware any computer object that has a key in which said unique identifier component is present.

According to a seventh aspect of the present invention, there is provided apparatus for classifying a computer object as malware or as safe, wherein said computer object is a descendant or otherwise related object of a first computer object, the apparatus comprising:

5 a computer constructed and arranged to classify a first computer object as malware or as safe;

 the computer being constructed and arranged to identify in a key relating to said first computer object a component that uniquely identifies the first computer object and that is inherited or otherwise present in the key of a
10 descendant or other related computer object of the first computer object; and,

 the computer being constructed and arranged to classify said computer object as malware or as safe as the case may be on the basis of the unique identifier component being present in the key of said computer object.

15 According to an eighth aspect of the present invention, there is provided a method of installing software on a computer, the method comprising:

 on initiation of installation of software on a computer, providing a computer-generated prompt on the computer to a user to ascertain whether the user authorises the installation; and,

20 ceasing the installation if a user authorisation is not received, else:

 receiving at the computer the user's authorisation to proceed with the installation;

 proceeding with the installation;

 obtaining data about computer objects that are created or used during the
25 installation;

 storing said data at the local computer.

 This provides for security when a user is installing new software and is not for example connected to a base computer having a community database of the
30 type mentioned above. In that case, the method, which may be implemented in agent software running on the local computer, allows the user to permit the

installation to proceed whilst at the same time gathering data about the objects (such as processes, new files, etc.) that are created during the installation.

Preferably, the locally stored data is referred to during the installation to
5 ensure that all objects created or used during the installation are part of the installation process, and, if it is found that objects created or used during the installation are not part of the installation process, either or both of: (i) ceasing the installation and (ii) providing a computer-generated prompt on the computer to the user accordingly. This allows the method to ensure that only those objects
10 that are required for the installation are permitted to be created or used and thus avoids unwittingly allowing malware to install (given that malware often creates objects that are not expected as part of a normal installation of new software).

In a preferred embodiment, the method comprises connecting the
15 computer to a community database that is connectable to a plurality of computers, and uploading the stored data to the community database for comparison with similar data provided by other computers.

The method may comprise downloading data about trusted installers to
20 the computer, said data about trusted installers being referred to during the installation such that any objects relating to or created by the trusted installer are automatically authorised to proceed. This facilitates installation of software that is known a priori to be trustworthy.

25 Said data about trusted installers may be referred to only for a predetermined time period following receipt at the computer of the user's authorisation to proceed with the installation.

The present invention also includes computer programs comprising
30 program instructions for causing a computer to perform any of the methods described above.

Although the embodiments of the invention described with reference to the drawings comprise computer processes performed in computer apparatus and computer apparatus itself, the invention also extends to computer programs, particularly computer programs on or in a carrier, adapted for putting the
5 invention into practice. The program may be in the form of source code, object code, a code intermediate source and object code such as in partially compiled form, or in any other form suitable for use in the implementation of the processes according to the invention. The carrier be any entity or device capable of carrying the program. For example, the carrier may comprise a storage medium,
10 such as a ROM, for example a CD ROM or a semiconductor ROM, or a magnetic recording medium, for example a floppy disk or hard disk. Further, the carrier may be a transmissible carrier such as an electrical or optical signal which may be conveyed via electrical or optical cable or by radio or other means.

15 Embodiments of the present invention will now be described by way of example with reference to the accompanying drawings, in which:

Figure 1 shows schematically apparatus in which an embodiment of the present invention may be implemented;

20

Figure 2 is a flowchart showing schematically the operation of an example of a method according to an embodiment of the present invention;

Figure 3 is a flowchart showing schematically the operation of another
25 example of a method according to an embodiment of the present invention; and,

Figure 4 is a flowchart showing schematically an information obtaining stage.

30 Referring to Figure 1, a computer network is generally shown as being based around a distributed network such as the Internet 1. The present invention may however be implemented across or use other types of network,

such as a LAN. Plural local or "remote" computers 2 are connected via the Internet 1 to a "central" or "base" computer 3. The computers 2 may each be variously a personal computer, a server of any type, a PDA, mobile phone, an interactive television, or any other device capable of loading and operating
5 computer objects. An object in this sense may be a computer file, part of a file or a sub-program, macro, web page or any other piece of code to be operated by or on the computer, or any other event whether executed, emulated, simulated or interpreted. An object 4 is shown schematically in the figure and may for example be downloaded to a remote computer 2 via the Internet 1 as shown by
10 lines 5 or applied directly as shown by line 6.

In one preferred embodiment, the base computer 3 holds a database 7 with which the remote computers 2 can interact when the remote computers 2 run an object 4 to determine whether the object 4 is safe or unsafe. The
15 community database 7 is populated, over time, with information relating to each object run on all of the connected remote computers 2. As will be discussed further below, data representative of each object 4 preferably takes the form of a so-called signature or key relating to the object and its effects. As will also be discussed further below, the database 7 may further include a mask for the
20 object 4 that sets out the parameters of the object's performance and operation.

Referring now to Figure 2, at the start point 21, a computer object 4 such as a process is run at a remote computer 2. At step 22, by operation of local "agent" software running on the remote computer 2, the operation of the process
25 is hooked so that the agent software can search a local database stored at the remote computer 2 to search for a signature or key representing that particular process, its related objects and/or the event. If the local signature is present, it will indicate either that the process is considered to be safe or will indicate that that process is considered unsafe. An unsafe process might be one that has
30 been found to be malware or to have unforeseen or known unsafe or malevolent results arising from its running. If the signature indicates that the process is safe, then that process or event is allowed by the local agent software on the

remote computer 2 to run at step 23. If the signature indicates that the process is not safe, then the process or event is stopped at step 24.

It will be understood that there may be more than two states than "safe" or "not-safe" and choices may be given to the user. For example, if an object is considered locally to be not safe, the user may be presented with an option to allow the related process to run nevertheless. It is also possible for different states to be presented to each remote computer 2. The state can be varied by the central system to take account of the location, status or ownership of the remote computer or timeframe.

If the object is unknown locally, then details of the object are passed over the Internet 1 or other network to the base computer 3 for storing in the community database 7 and preferably for further analysis at the base computer 3. In that case, the community database 7 is then searched at step 25 for a signature for that object that has already been stored in the community database 7. The community database 7 is supplied with signatures representative of objects, such as programs or processes, run by each monitored remote computer 2. In a typical implementation in the field, there may be several thousands or even millions of remote computers 2 connected or connectable to the base computer 3 and so any objects that are newly released upon the Internet 1 or that otherwise are found on any of these remote computers 2 will soon be found and signatures created and sent to the base computer 3 by the respective remote computers 2.

When the community database 7 is searched for the signature of the object that was not previously known at the remote computer 2 concerned, then if the signature is found and indicates that that object is safe, then a copy of the signature or at least a message that the object is safe is sent to the local database of the remote computer 2 concerned at step 26 to populate the local database. In this way, the remote computer 2 has this information immediately to hand the next time the object 4 is encountered. A separate message is also

passed back to the remote computer 2 to allow the object to run in the current instance.

5 If the signature is found in the community database 7 and this indicates for some reason that the object is unsafe, then again the signature is copied back to the local database and marked "unsafe" at step 27, and/or a message is sent to the remote computer 2 so that running of the object is stopped (or it is not allowed to run) and/or the user given an informed choice whether to run it or not.

10 If after the entire community database 7 has been searched the object is still unknown, then it is assumed that this is an entirely new object which has never been seen before in the field. A signature is therefore created representative of the object at step 28, or a signature sent by the remote computer 2 is used for this purpose, and this signature is initially marked as bad
15 or unsafe community database 7 at step 29. The signature is copied to the local database of the remote computer 2 that first ran the object at step 30. A message may then be passed to the remote computer 2 to instruct the remote computer 2 not to run the object or alternatively the user may be given informed consent as to whether to allow the object to run or not. In addition, a copy of the
20 object itself may be requested at step 31 by the community database 7 from the remote computer 2.

If the user at the remote computer 2 chooses to run a process that is considered unsafe because it is too new, then that process may be monitored by
25 the remote computer 2 and/or community database 7 and, if no ill effect occurs or is exhibited after a period of time of n days for example, it may then be considered to be safe. Alternatively, the community database 7 may keep a log of each instance of the process which is found by the many remote computers 2 forming part of the network and after a particular number of instances have been
30 recorded, possibly with another particular number of instances or the process being allowed to run and running safely, the signature in the community

database 7 may then be marked as safe rather than unsafe. Many other variations of monitoring safety may be done within this concept.

5 The details of an object 4 that are passed to the base computer 3 are preferably in the form of a signature or "key" that uniquely identifies the object 4. This is mainly to keep down the data storage and transmission requirements. This key may be formed by a hashing function operating on the object at the remote computer 2.

10 The key in the preferred embodiment is specially arranged to have at least three severable components, a first of said components representing executable instructions contained within or constituted by the object, a second of said components representing data about said object, and a third of said components representing the physical size of the object. The data about the
15 object in the second component may be any or all of the other forms of identity such as the file's name, its physical and folder location on disk, its original file name, its creation and modification dates, vendor, product and version and any other information stored within the object, its file header or header held by the remote computer 2 about it; and, events initiated by or involving the object when
20 the object is created, configured or runs on the respective remote computers. In general, the information provided in the key may include at least one of these elements or any two or more of these elements in any combination.

In one preferred embodiment, a check sum is created for all executable
25 files, such as (but not limited to) .exe and .dll files, which are of the type PE (Portable Executable file as defined by Microsoft). Three types of checksums are generated depending on the nature of the file:

30 Type 1: five different sections of the file are check summed. These include the import table, a section at the beginning and a section at the end of the code section, and a section at the beginning and a section at the end of the entire file. This type applies to the vast majority of files that are analysed;

Type 2: for old DOS or 16 bit executable files, the entire file is check summed;

- 5 Type 3: for files over a certain predefined size, the file is sampled into chunks which are then check summed. For files less than a certain predefined size, the whole file is check summed.

- For the check summing process, in principle any technique is possible.
10 The MD5 (Message-Digest algorithm 5) is a widely-used cryptographic hash function that may be used for this purpose.

- This allows a core checksum to be generated by viewing only the executable elements of the checksum and making a comparison between two
15 executables that share common executable code.

- For the type 1 checksum mentioned above, three signature processes may be used. The first defines the entire file and will change with almost any change to the file's content. The second attempts to define only the processing
20 instructions of the process which changes much less. The third utilises the file's size, which massively reduces the potential of collisions for objects of differing sizes. By tracking the occurrences of all signatures individually appearing with different counterparts, it is possible to identify processes that have been changed or have been created from a common point but that have been edited
25 to perform new, possibly malevolent functionality.

This "meta data" enables current and newly devised heuristics to be run on the data in the community database 7.

- 30 The data stored in the community database 7 provides an extensive corollary of an object's creation, configuration, execution, behaviour, identities and relationships to other objects that either act upon it or are acted upon by it.

The preferred central heuristics use five distinct processes to establish if an object is safe, unsafe or suspicious.

- 5 The first of the said processes utilises the singularity or plurality of names, locations, vendor, product and version information captured and correlated from all of the remote computers 2 that have seen the object. By considering the plurality of this information for a single object, a score can be determined which can be used as a measure of the authenticity and/or credibility of the object.
- 10 Most safe objects tend not to use a large plurality of identifying information or locations. Rules can be established to consider this information in respect of the type of object and its location. For example, temporary files often utilise a plurality of system generated file names which may differ on each remote computer for the same object. Where an object has little plurality, then it
- 15 provides a reference point to consider its behaviour in comparison to the known behaviours of other objects that have previously used that identifying information. For example, a new object that purports to be a version of notepad.exe can have its behaviour compared with the behaviour of one or more other objects that are also known as notepad.exe. This comparison may be
- 20 against a single other object or multiple other objects that use the same or even similar identifying information. In this way, new patterns of behaviour can be identified for the new object. Also it allows the preferred embodiment to police an object's behaviour over time to identify new behavioural patterns that may cause an object that was previously considered safe to have its status
- 25 reconsidered. Alternatively, the score based on identities may be considered along with scores for other objects or scores created by other processes on this object to be considered in combinations.

- The second of the said processes utilises an object's relationship to other
- 30 objects that act upon it or upon which it acts. For example, analysis can be made of which object created this object, which objects this object created, which objects created a registry key to run or configure this object, which objects

were configured by or had registry keys created by this object, etc. In this regard an object is considered to have a relationship based on the event performed by it upon another object, or upon it by another object. This simple 1-to-1 relationship chain provides a complex series of correlation points, allowing ancestral

5 relationships to be considered for any object and its predecessors by event or its issue (i.e. child and sub-child processes) by event. This allows a score to be developed that describes its relationships and associations with known, unknown, known safe or known bad objects or a combination thereof. Objects that have specific relationships, volumes of relationships or mixes of

10 relationships to one type or another may be judged safe or unsafe accordingly. Alternatively, the relationship-based score may be considered along with other scores to arrive at a determination of safe or unsafe. This data can also be used to deduce a number of factors about objects related directly or via other objects and their behaviours. For example it is possible to deduce how one object's

15 behaviour can be influenced or changed by its association or linkage to another. Consider for example notepad.exe as supplied by Microsoft with the Windows series of operating systems. It has a limited range of functionality and would not be expected therefore to perform a wide variety of events, such as transmitting data to another computer or running other programs etc. However, the

20 behaviour of notepad.exe could be modified by injecting new code into it, such as via dynamic link library injection (DLL injection). In this case notepad.exe would now have new capabilities derived by the code injection or linkage to another object. Using the data that defines the relationships between objects it is possible to deduce that the new behaviours of a program can be attributed to

25 the association with another object. If that new behaviour is malevolent, then it is possible to mark either or all processes as unsafe as appropriate.

The combination of behaviours captured provide a basis to determine if the object is safe or unsafe. Malware typically exhibit certain behaviour and

30 characteristics. For example, malware frequently has a need to self-persist. This manifests itself in the need to automatically restart on system restarts or upon certain events. Creating objects in specific locations to auto restart or

trigger execution is a typical characteristic of malware. Replacing core objects of the Windows system environment are another example of typical characteristics of malware. By providing a pattern of behaviour, the determination of objects to be unsafe or safe can be automated. The centralisation of the community data
5 in the community database 7 provides the ability to rapidly assimilate object behaviours, allowing for the rapid identification and determination of malware. Objects may also perform events upon themselves which can be considered in deriving a score.

10 The third said process involves time and volumes. Relevant data includes when the object was first seen, when it was last seen, how many times it has been seen, how many times it has been seen in a given interval of time, and the increase or decrease of acceleration in it being seen. This information is highly relevant in determining the prevalence of an object in the community of remote
15 computers. A score is developed based on these metrics which can be used to determine if an object is safe, unsafe or too prevalent to allow it to execute or propagate without very thorough examination. In this case, the object can be temporarily held or blocked from executing pending further information about its behaviour or relationships. This score may also be used in combination with
20 scores from other processes. Time is also highly relevant in combination with other information, including but not limited to behaviours and identities. For example in the case of polymorphic or randomly named objects, time is a powerful qualifier. (A polymorphic virus changes its encryption algorithm and the corresponding encryption keys each time it replicates from one computer to
25 another and so can be difficult to detect by conventional measures.) A program that creates other programs can often be considered normal or abnormal based on its activity over time.

30 The fourth said process considers the behaviour of an object. This allows a score to be developed based on the types of events performed by an object or events performed on it by itself or other objects. The centralised system of the community database 7 allows for an unlimited number of event types and can

consider the object performing the event or the object having the event performed upon it, or both. Some event types also relate to external information other than objects, for example a program performing an event to connect with an Internet Chat Relay site, or a program modifying a non-executable file such as the Windows hosts file. The behavioural events of an object, be they as "actor" (i.e. the object doing something to another object) or as "victim" (i.e. the object has something done to it by another object) of any event can be considered in many ways, such as in combination, in sequence, in volume, in presence or absence, or in any combination thereof. The behavioural events in the preferred embodiment may have been provided by a remote computer 2 or from other external sources. The process can consider these in isolation or in combination. Furthermore it is a feature of the preferred embodiment that the behavioural events can be considered in combination with the status of other objects upon which the object acts or that act upon the object. For example, creating a program may have a different score if the program being created is safe, unsafe, new, unknown or suspicious. Similarly, a program that is created by a known bad program will likely have a different score attributed to its creation event depending on the status of the object creating it.

20 The fifth process considers the behaviour of a web page or script. In this respect, the web page and url combination is assigned a unique identity which allows its behaviour to be tracked as if it were an object like any other executable file. In this example, the web page may perform events that would normally be seen as events performed by the web browser (e.g. IExplore.exe or Firefox.exe). 25 The preferred embodiment substitutes the identifying details and signatures of the web browser for the "pseudo" object identity associated with the web page being displayed or executing within the browser. In this respect, the status of the web page and/or web site to which it relates may be determined as safe, unsafe, unknown or suspicious in the same way as any other object. The web page's 30 "pseudo" object identity also allows the preferred embodiment to block, interject or limit the functionality of that web page or web site to prevent some or all of its potentially unsafe behaviour or to provide the remote user with qualifying

information to guide them about the safety of the web site, web page or their content.

Amongst other types, the types of meta data captured might be:

5

"Events": these define the actions or behaviours of an object acting upon another object or some other entity. The event has three principal components: the key of the object performing the act (the "Actor"), the act being performed (the "Event Type"), and the key of the object or identity of an other entity upon which the act is being performed (the "Victim"). While simple, this structure allows a limitless series of behaviours and relationships to be defined. Examples of the three components of an event might be:

	<u>Actor</u>	<u>Event Type</u>	<u>Victim</u>
15	Object 1	Creates Program	Object 2
	Object 1	Sends data	IP Address 3
	Object 1	Deletes Program	Object 4
	Object 1	Executes	Object 2
	Object 2	Creates registry key	Object4

20

"Identities": these define the attributes of an object. They include items such as the file's name, its physical location on the disk or in memory, its logical location on the disk within the file system (its path), the file's header details which include when the file was created, when it was last accessed, when it was last modified, the information stored as the vendor, the product it is part of and the version number of the file and its contents, its original file name, and its file size.

25

"Genesisactor" – the key of an object that is not the direct Actor of an event but which is the ultimate parent of the event being performed. For example in the case of a software installation, this would be the key of the object

30

that the user or system first executed and that initiated the software installation process, e.g. Setup.exe.

"Ancillary data": many events may require ancillary data, for example an event such as that used to record the creation of a registry run key. In this situation the "event" would identify the Actor object creating the registry run key, the event type itself (e.g. "regrunkey"), and the Victim or subject of the registry run key. The ancillary data in this case would define the run key entry itself; the Hive, Key name and Value.

10

"Event Checksums": because the event data can be quite large extending to several hundred bytes of information for a single event, its identities for the Actor and Victim and any ancillary data, the system allows for this data itself to be summarised by the Event Checksums. Two event checksums are used utilising a variety of algorithms, such as CRC and Adler. The checksums are of the core data for an event. This allows the remote computer 2 to send the checksums of the data to the central computer 3 which may already have the data relating to those checksums stored. In this case, it does not require further information from the remote computer 2. Only if the central computer 3 has never received the checksums will it request the associated data from the remote computer 2. This affords a considerable improvement in performance for both the remote and central computers 2,3 allowing much more effective scaling.

Thus, the meta data derived from the remote computers 2 can be used at the community database 7 to define the behaviour of a process across the community. As mentioned, the data may include at least one of the elements mentioned above (file size, location, etc.) or two or three or four or five or six or all seven (or more elements not specifically mentioned here). This may be used accordingly to model, test and create new automated rules for use in the community database 7 and as rules that may be added to those held and used in the local database of the remote computers 2 to identify and determine the

30

response of the remote computers 2 to new or unknown processes and process activity.

Moreover, it is possible to monitor a process along with any optional sub-
5 processes as an homogenous entity and then compare the activities of the top level process throughout the community and deduce that certain, potentially malevolent practices only occur when one or more specific sub-processes are also loaded. This allows effective monitoring (without unnecessary blocking) of programs, such as Internet Explorer or other browsers, whose functionality may
10 be easily altered by downloadable optional code that users acquire from the Internet, which is of course the principal source of malevolent code today.

The potentially high volume of active users gives a high probability of at least one of them being infected by new malware. The speed of propagation can
15 be detected and recorded so that the propagation of malware can be detected and malware designated as bad on the basis of the speed of propagation, optionally in combination with the other factors discussed above, such as file size, location and name. The simple volume of infection can also be used as a trigger. In a further embodiment, difference of naming of an otherwise identical
20 piece of code combined with acceleration of first attempts to execute the code within the community allows pattern matching that will show up an otherwise identically signed piece of code as bad.

This feature allows the statement in some embodiments that "nothing will
25 propagate in our community faster than X without being locked down", so that if any process or event propagates more quickly over a given duration, it is marked as bad. This is for reasons of safety given that if for example an object is propagating quickly enough, then it might infect computers before it can be analysed to determine whether or not it is malware.

30

This process can be automated by the identification of the vector of propagation in the community (i.e. the source of type of propagation), from

timestamp data held in the community database and the marking of a piece of code that has these attributes as bad. By comparison, it is believed that all other anti-malware providers rely on a simplistic known bad model and therefore are reliant primarily on malware infection actually occurring on terminals and being reported.

Thus, the community database 7 can be used to make early diagnosis, or simply to take precautionary measures, and thus stop potentially fast propagating worms and other malware very, very early in their life cycle. Given that it is possible to create a worm that can infect every computer connected to the Internet within a matter of a few minutes, this feature is highly desirable.

Even faster determination may be made by combining data defining the speed of propagation of a new piece of software with metadata collected by the agent software from the remote computers 2 and fed to the community database 7. This includes monitoring processes that attempt to conceal themselves from the user by randomly changing name and/or location on the remote computers 2. It also includes a process's attempt to create an identical copy (i.e. with identical code contents) on the computer but with a different name. This is a classic attribute of a worm.

The signature of an object may comprise or be associated with a mask which can be built up with use of that object and which indicates the particular types of behaviour to be expected from the object. If an object is allowed to run on a remote computer 2, even if the initial signature search 22 indicates that the object is safe, then operation of that object may be monitored within the parameters of the mask. The mask might indicate for example, the expected behaviour of the object; any external requests or Internet connections that that object might legitimately have to make or call upon the remote computer 2 to make, including details of any ports or interfaces that might be required to be opened to allow such communication; any databases, either local or over a local area network or wide area network or Internet, that may be expected to be

interrogated by that object; and so on. Thus, the mask can give an overall picture of the expected "normal" behaviour of that object.

In practice, therefore, in one embodiment the behaviour of the object is
5 continually monitored at the remote computer(s) 2 and information relating to
that object continually sent to and from the community database 7 to determine
whether the object is running within its expected mask. Any behaviour that
extends beyond the mask is identified and can be used to continually assess
whether the object continues to be safe or not. Thus, if for example the object,
10 on a regular basis (say monthly or yearly) opens a new port to update itself or to
obtain regular data, then this information is flagged. If it is found that the object
has done this on other remote computers and has had no ill effects, or this
behaviour is known from other objects and known to be safe, then this behaviour
might be considered as safe behaviour and the mask is then modified to allow
15 for this. If it has been found previously that this new behaviour in fact causes
unsafe or malevolent results, then the object can then be marked as unsafe even
if previously it was considered safe. Similarly, if the object attempts to connect
to a known unsafe website, database or to take action that is known as generally
being action only taken by unsafe programs, then again the object may be
20 considered to be unsafe.

This is shown schematically in Figure 3. Figure 3 also shows the concept
that any object can be pre-authorised by, for example a trusted partner, such as
a major software company, a verification authority, a Government department,
25 and so on. Pre-authorisation enables a supplier of a new object, which has not
been released before, to get pre-authorisation for that object, and optionally
includes the provision by that supplier of a mask detailing the expected and
allowable behaviour of that object.

30 Referring to Figure 3 for example, when a process is run, the local and/or
community databases are searched as before at step 31. If the process is not a
pre-authorised one, then the steps of Figure 2 may be taken and the process

might be allowed to run or not at step 32. If the process is pre-authorised, as determined at step 33, then it is immediately allowed to run, step 34. This may terminate the operation of the method. However, in a preferred variation, the process is then monitored whilst running, and is monitored each time it is run in
5 the future in a monitoring state step 35 to determine whether its behaviour falls within its pre-authorised mask 36. If the behaviour falls within the pre-authorised behaviour, then the process is allowed to continue to run. If the behaviour extends beyond the allowed mask, such as by trying to instigate further processes or connections that have not been pre-authorised, then this behaviour
10 is flagged at an alert step 37. Various actions could be taken at this stage. The process might simply not be allowed to run. Alternatively, the trusted authority that initially enabled pre-authorisation might be contacted, who may be able to confirm that this behaviour is acceptable or not. If it is acceptable, then the mask could be modified accordingly. If not acceptable, then the process might be
15 marked as unsafe. Many other actions may be taken upon the noting of such an alert state.

If the process has been found not to be pre-authorised at step 33 but is nevertheless allowed to run, then the process is monitored at step 38 in order to
20 generate a mask 39 representative of the normal behaviour of that process. Data representative of this mask might be sent to the community database 7 for scanning when other computers run that process. By continually monitoring a process each time it is run or during running of the process, any behaviour that differs from previous behaviour of the process can be noted and the mask can
25 be modified, or this behaviour might be used to determine that a process that was once considered safe should now be considered to be unsafe.

In another embodiment, a computer 2 may have agent software installed that periodically or on-demand provides information to the community database
30 7 that is representative of all or selected ones of the software products loaded on or available the computer 2. In particular, this may be information on one or more of: all the locally-loaded security products (such as anti-malware systems

including anti-virus software, anti-spyware, anti-adware and so on), firewall products, specific settings and details of which signature files are currently loaded, version details for the operating system and other software, and also information such as which files are operating and the particular version and
5 software settings at any time. (It will be understood from the following that auditing and testing for a match for more of these criteria increases the likelihood of computers being very similarly arranged and thus reduces the rate of false negatives and positives during the match search.)

10 The information relating to these software products, etc. may be provided individually to the community database. Preferably however, again for reasons of data quantity for storage and transmission, the information is provided as a signature or key representative of the information (e.g. by a hashing or
15 compression function at the computer 2). Figure 4 shows schematically how the details of all local security products, versions, signature files, firewall settings, etc. 40 are used to create a key 41. The key is transmitted to the community database 7. Since the community database 7 is provided with such information from many, possibly millions, of users' computers 2, it is likely to hold
20 corresponding information for other computers 2 that have the same or a similar configuration of security products, etc. Thus, the community database 7 can be searched at step 42 for other computers 2 having the same or a similar combination of security products including the same setting, signature files loaded and so on.

25 The community database 7 in this embodiment is also provided by the agent software with details of processes run by every computer 2 and thus knows whether or not a process has been detected by each computer 2.

30 In this way, the community database 7 can be used to obtain information as to whether for example a particular, specific combination of operating system and various security products, including settings and signature files existing at a

point in time, renders a particular computer 2 having those products and settings susceptible or vulnerable to any particular malware object.

In a simple example, if for example the database knows that a computer
5 in the past has version A of anti-virus product B with downloaded signature
update C, and also has a firewall D with particular settings E, and perhaps anti-
spyware software F with signature updates G, but that a particular malware
process P was not detected by this combination of programs at that point in time,
then this information can be provided to a computer 2 that is known as having
10 that combination of security programs/settings, and can be used to indicate that
that computer 2 is vulnerable in the short term to attack by that particular
malware process. This information can be presented to the user either by
displaying a window 43 on the screen display of the computer 2 or by directing
the user to a particular website which explains the position in more detail. The
15 user might be informed for example that their particular combination of security
products, etc., exposes their computer to a risk of being infected by the Sobig
virus as that virus is not detectable by their computer. The user might be offered
specific advice (e.g. to update a particular anti-virus program with a particular
signature file) or software to download and install to remove the risk.

20
Thus, the community database 7, when provided with information relating
to all the security products, etc. on a particular computer at a particular time, is
searched for events for processes marked as "bad" that occurred on computers
with that particular mix of security products and that were not locally detected.
25 This information can then be fed back to the user of the particular computer, for
example directly or by directing the user to a website. This information can be
provided virtually in real-time, allowing a new user or a user of a new computer
to be able to increase the computer's effective security very quickly.

30 The preferred method also tracks which objects are related to each other
and uses the concept of ancestry to enable objects to be marked as malware.
For example, any particular process may spawn child processes which are

therefore related. The key relating to the first object may be inspected to identify a component that uniquely identifies the first object and that is inherited or otherwise present in the key of a descendant or other related object of the first object. This component is referred to herein as a "gene". This general
5 technique may be used in a number of ways:

a) A known and trusted parent process is afforded the ability to create child processes which may be automatically marked as safe to run on the local computer. It is also possible that this "inherited" property may be passed down
10 to grand children processes and so on. This safe status is passed to the parent's child processes and possibly, through them, further child processes (referred to here as "issue"), such signatures for the issue can all automatically be recorded in the local database as good. This allows the issue processes to be quickly marked as good, even if a connection to the community database 7 is
15 not available.

b) By monitoring activity of the parent process, if it is later found that the parent process is malware, then all of the issue processes can all automatically be recorded in the local database as bad.
20

c) Similarly, by monitoring activity of the issue processes, if it is later found that one of the issue processes is malware, then one or more of the parent process and all of the other issue processes (i.e. all of the related processes in this context) can all automatically be recorded in the local database as bad.
25

d) Parental creation of a signature for a child or children including the ability for these to be automatically marked as either good or bad depending on the parent's behaviour and determination. Note that in some embodiments the product can "watch" or monitor the birth of a child process and automatically
30 create the signature upon arrival. This provides the ability to monitor the creation of a bad program by another bad program. It is possible therefore to monitor the ancestry of a program so if for example the grandfather creates a

program (the father) and this in turn creates a bad program (the son), it is possible automatically to determine the father as a bad program.

e) A feature may be included that allows for automatic forfeiture of a child's inherited ability to trigger the automatic creation of signatures on any further births because the child, as parent, has already produced bad offspring. Preferably, a rule is that if a file has one bad offspring then the inherited ability can be automatically removed.

f) An ability to watch clones or identical twins of objects (e.g. the same process running on other systems in the community) to compare the pattern of their issue and to make decisions as to whether or not to treat any particular process as malware.

One or more of these features a) to f) can be used to provide a solution to the problem of producing a security product that can be used effectively without 100% reliance on being permanently connected to the Internet, which is often impractical. Examples of this are Windows Update and other processes used more and more by vendors who wish to be able to roll out product updates automatically across the worldwide web.

Possible benefits of these types of features above conventional software are as follows. Antivirus software tends to have a cache of known bad signatures. The problem is keeping this up to date. Take the simple example of someone buying a new computer. The computer comes with an antivirus product preloaded with a signature cache. Between the time when the PC was built, shipped to the store and bought by the user several days or weeks will have passed. The user starts the PC and is exposed to any new virus or malware which was created after the PC was built. Full protection requires the user to connect to the internet and download updates. This cannot be guaranteed to occur ahead of other activities by the user on the internet (almost physically impossible to guarantee). With a local cache of known good

processes, as in the embodiments of the present invention, it is possible to ship the computer/terminal preloaded with a pre-generated cache of signatures for all of the good (clean) software preloaded by the computer manufacturer. In this case the user can connect to the internet knowing that any new or updated
5 programs will be immediately detected and verified. Also any auto-updating software can function forcing signatures to be automatically built for its children and more remote off-spring (i.e. grandchildren, great-grandchildren, etc).

Reference is now made to "Defeating Polymorphism: Beyond Emulation"
10 by Adrian Stepan of Microsoft Corporation published in "Virus Bulletin Conference October 2005" and also to US 60/789156 filed on 5th April 2006, the entire content of which are hereby incorporated by reference. In that paper and patent application, there are disclosed methods of decrypting files to allow the files to be analysed to determine whether or not the file actually is malware. In
15 US 60/789156 in particular, there is disclosed a method of unpacking/decrypting an executable computer file using a host computer, the method comprising: partitioning the executable computer file into plural basic blocks of code; translating at least some of the basic blocks of code into translated basic blocks of code that can be executed by the host computer; linking at least some of the
20 translated basic blocks of code in memory of the host computer; and, executing at least some of the translated basic blocks of code on the host computer so as to enable the executable computer file to be unpacked or decrypted, whereupon the unpacked or decrypted executable computer file can be analyzed to determine whether the executable computer file is or should be classed as
25 malware. There is also disclosed in US 60/789156 a method of unpacking/decrypting an executable computer file, the method comprising: partitioning the executable computer file into plural basic blocks of code; creating at least a read page of cache memory for at least some of the basic blocks, the read page of cache memory storing a read cached real address corresponding
30 to a read cached virtual memory address for the respective basic block, and creating at least a write page of cache memory for at least some of the basic blocks, the write page of cache memory storing a write cached real address

corresponding to a write cached virtual memory address for the respective basic block; and, emulating the executable file by executing at least some of the basic blocks of code so as to enable the executable computer file to be unpacked or decrypted, whereupon the unpacked or decrypted executable computer file can
5 be analyzed to determine whether the executable computer file is or should be classed as malware; wherein during the execution of a basic block, at least one of the read page and the write page of cache memory is checked for a cached real address corresponding to the virtual address that is being accessed for said basic block.

10

The techniques disclosed in these documents can be used in the present context when it is desired to analyse a file in detail. More generally however, the techniques disclosed in these papers, and particularly the enhanced techniques disclosed in US 60/789156, can be used to provide information about the activity
15 of a file when it is run on a computer because the techniques disclosed in these papers emulate the running of the file and therefore allow the file's activity to be interpreted.

A further situation arises when users wish to install software while offline.
20 In a preferred embodiment, when a user attempts to install new software while offline, agent software running on the user's computer 2 prompts the user for authorisation to allow the installation process to proceed such that the execution of the installation can itself be "authorised" by the user. This authorisation by the user is treated as a "Genesis" event and will be so termed hereinafter. However
25 there are some processes commonly used in installation of software that communicate with other existing programs on the installation machine, e.g. Microsoft's MSIEXEC.

The Genesis approach involves a process that generates signatures as a
30 result of the user's authorisation on the user's computer 2. Those signatures are stored in the local database on the user's computer 2. In one embodiment, those locally stored signatures are referred to as necessary by the agent

software during the installation process so that the installation can proceed. Alternatively, the security checks made by the agent software can be switched off during the installation process. The switching off may only be for a limited duration, such as a few minutes which should be sufficient to allow most
5 software to be installed, the off time optionally being user-configurable.

In any event, once the installation has been completed and the user's computer 2 connected to the community database 7, the agent software on the user's computer 2 can upload the signatures relating to the installation from the
10 user's local database to the community database 7. With corresponding data from other users' computers 2, the community database 7 can then be used to make a rapid determination that the installation of this particular software is benign.

15 As a variant to this embodiment, when a user's computer 2 is at some point in time on-line, the agent software on the user's computer 2 may download signatures of a so-called "trusted installer" or "licensed installer". This allows the operation of a method such that a "licensed installer" and any child processes of the licensed installer are permitted to execute while a Genesis event is "current",
20 e.g. within a period of minutes after an authorisation from the user. Preferably signatures of licensed installers are always downloaded, as and when added to the community database 7, to a remote computer 2 while online.

There may be further refinements to this method, such as to prevent
25 licensed installers executing if a media change has occurred during the currency of a Genesis event. However, any unknown processes, which may be malware, may still be detected and blocked. Having a small number of licensed installers facilitates download, as minimal data is required, especially compared to downloading virus signature files. As another example, super-trusted installers,
30 such as for example "Windows Update", may be employed whereby all new processes created by the super-trusted installer are marked immediately as safe.

In the case of an installation occurring when the remote computer 2 is connected to the community database 7, another option is that if the software that is about to be installed is not known to the community database 7, then the system will block the installation or alert the user. For example, a message may
5 be displayed at the user's computer 2 to the effect that "You are about to install some software. This software is not known to [the community]. Are you sure you wish to proceed?".

Embodiments of the present invention have been described with particular
10 reference to the examples illustrated. However, it will be appreciated that variations and modifications may be made to the examples described within the scope of the present invention.

The following numbered clauses on pages 37 to 43 of the present
15 description correspond to the claims of European patent application no. 06755686.0 as filed. The claims of the present application as filed, which is divided from European patent application no. 06755686.0, can be found on the subsequent pages 44 to 45 of the specification which begin with the heading "CLAIMS".

1. A method of classifying a computer object as malware, the method comprising:
 - at a base computer, receiving data about a computer object from each of plural remote computers on which the object or similar objects are stored;
 - 5 comparing in the base computer the data about the computer object received from the plural computers; and,
 - classifying the computer object as malware on the basis of said comparison.
- 10 2. A method according to claim 1, wherein the data about the computer object that is sent from the plural remote computers to the base computer and that is used in the comparison includes one or more of: executable instructions contained within or constituted by the object; the size of the object; the current name of the object; the physical and folder location of the object on disk; the
15 original name of the object; the creation and modification dates of the object; vendor, product and version and any other information stored within the object; the object header or header held by the remote computer; and, events initiated by or involving the object when the object is created, configured or runs on the respective remote computers.
- 20 3. A method according to claim 1 or claim 2, wherein the comparing identifies relationships between the object and other objects.
4. A method according to claim 3, wherein if at least one other object to
25 which said object is related is classed as malware, then classifying said object as malware.
5. A method according to claim 3 or claim 4, wherein said other objects include the object or similar objects stored on at least some of the remote
30 computers.

6. A method according to any of claims 3 to 5, wherein said other objects include other objects that are parent objects or child objects or otherwise process-related objects to said object.
- 5 7. A method according to any of claims 1 to 6, wherein the data is sent in the form of key that is obtained by a hashing process carried out in respect of the objects on the respective remote computers.
8. A method according to claim 7, wherein the key has at least one
10 component that represents executable instructions contained within or constituted by the object.
9. A method according to claim 7 or claim 8, wherein the key has at least one component that represents data about said object.
- 15 10. A method according to claim 9, wherein said data about said object includes at least one of: the current name of the object; the physical and folder location of the object on disk; the original name of the object; the creation and modification dates of the object; vendor, product and version and any other
20 information stored within the object; the object header or header held by the remote computer; and, events initiated by or involving the object when the object is created, configured or runs on the respective remote computers.
11. A method according to any of claims 7 to 10, wherein the key has at least
25 one component that represents the physical size of the object.
12. A method according to any of claims 1 to 11, comprising initially classifying an object as not malware, generating a mask for said object that defines acceptable behaviour for the object, and comprising monitoring operation
30 of the object on at least one of the remote computers and reclassifying the object as malware if the actual monitored behaviour extends beyond that permitted by the mask.

13. Apparatus for classifying a computer object as malware, the apparatus comprising:

5 a base computer constructed and arranged to receive data about a computer object from each of plural remote computers on which the object or similar objects are stored;

the base computer being constructed and arranged to compare the data about the computer object received from said plural computers; and,

10 the base computer being constructed and arranged to classify the computer object as malware on the basis of said comparison.

14. Apparatus according to claim 13, wherein the base computer is constructed and arranged so as to compare the data where the data includes one or more of: executable instructions contained within or constituted by the object; the size of the object; the current name of the object; the physical and
15 folder location of the object on disk; the original name of the object; the creation and modification dates of the object; vendor, product and version and any other information stored within the object; the object header or header held by the remote computer; and, events initiated by or involving the object when the object
20 is created, configured or runs on the respective remote computers.

15. Apparatus according to claim 13 or claim 14, wherein the base computer is constructed and arranged so that the comparing identifies relationships between the object and other objects.

25

16. Apparatus according to claim 15, the base computer is constructed and arranged so that if at least one other object to which said object is related is classed as malware, then said object is classified as malware.

30 17. Apparatus according to claim 15 or claim 16, wherein the base computer is constructed and arranged so that said other objects include the object or similar objects stored on at least some of said remote computers.

18. Apparatus according to any of claims 15 to 17, wherein the base computer is constructed and arranged so that said other objects include other objects that are parent objects or child objects or otherwise process-related
5 objects to said object.

19. Apparatus according to any of claims 13 to 18, wherein the base computer is constructed and arranged so as to be able to process data that is sent in the form of key that is obtained by a hashing process carried out in
10 respect of the objects on said respective remote computers.

20. Apparatus according to claim 19, wherein the key has at least one component that represents executable instructions contained within or constituted by the object.
15

21. Apparatus according to claim 19 or claim 20, wherein the key has at least one component that represents data about said object.

22. Apparatus according to claim 21, wherein said data about said object
20 includes at least one of: the current name of the object; the physical and folder location of the object on disk; the original name of the object; the creation and modification dates of the object; vendor, product and version and any other information stored within the object; the object header or header held by the remote computer; and, events initiated by or involving the object when the object
25 is created, configured or runs on the respective remote computers.

23. Apparatus according to any of claims 19 to 22, wherein the key has at least one component that represents the physical size of the object.

30 24. Apparatus according to any of claims 19 to 23, wherein the base computer is constructed and arranged to generate a mask for an object that is initially classed not as malware, said mask defining acceptable behaviour for the

object, and the base computer is constructed and arranged to monitor operation of the object on at least one of the remote computers and to reclassify the object as malware if the actual monitored behaviour extends beyond that permitted by the mask.

5

25. A method of providing data about a computer object from a remote computer to a base computer so that a comparison can be made at the base computer with similar data received from other remote computers, the method comprising:

- 10 providing from a remote computer to a base computer data about a computer object that is stored on the remote computer;
- the data including one or more of: executable instructions contained within or constituted by the object; the size of the object; the current name of the object; the physical and folder location of the object on disk; the original name of
- 15 the object; the creation and modification dates of the object; vendor, product and version and any other information stored within the object; the object header or header held by the remote computer; and, events initiated by or involving the object when the object is created, configured or runs on the respective remote computers;
- 20 the data being sent in the form of key that is obtained by a hashing process carried out in respect of the object on the remote computer.

26. A method according to claim 25, wherein the key has at least one component that represents executable instructions contained within or

25 constituted by the object.

27. A method according to claim 25 or claim 26, wherein the key has at least one component that represents data about said object.

30 28. A method according to claim 27, wherein said data about said object includes at least one of: the current name of the object; the physical and folder location of the object on disk; the original name of the object; the creation and

modification dates of the object; vendor, product and version and any other information stored within the object; the object header or header held by the remote computer; and, events initiated by or involving the object when the object is created, configured or runs on the respective remote computers.

5

29. A method according to any of claims 25 to 28, wherein the key has at least one component that represents the physical size of the object.

30. A computer program comprising program instructions for causing a
10 computer to perform the method of any of claims 25 to 29.

31. A method of classifying a computer object as malware or as safe, wherein said computer object is a descendant or otherwise related object of a first computer object, the method comprising:

15 classifying a first computer object as malware or as safe;
identifying in a key relating to said first computer object a component that uniquely identifies the first computer object and that is inherited or otherwise present in the key of a descendant or other related computer object of the first computer object; and,
20 classifying said computer object as malware or as safe as the case may be on the basis of the unique identifier component being present in the key of said computer object.

32. A method according to claim 31, comprising monitoring activities of said
25 first computer object and reclassifying the first computer object as malware in the case that it was initially classified as safe and subsequently determined to be malware, the method further comprising automatically classifying as malware any computer object that has a key in which said unique identifier component is present.

30

33. A computer program comprising program instructions for causing a computer to perform the method of claim 31 or claim 32.

34. Apparatus for classifying a computer object as malware or as safe, wherein said computer object is a descendant or otherwise related object of a first computer object, the apparatus comprising:

5 a computer constructed and arranged to classify a first computer object as malware or as safe;

the computer being constructed and arranged to identify in a key relating to said first computer object a component that uniquely identifies the first computer object and that is inherited or otherwise present in the key of a

10 descendant or other related computer object of the first computer object; and,

the computer being constructed and arranged to classify said computer object as malware or as safe as the case may be on the basis of the unique identifier component being present in the key of said computer object.

15 35. Apparatus according to claim 34, wherein the computer is constructed and arranged to monitor activities of said first computer object and reclassify the first computer object as malware in the case that it was initially classified as safe and subsequently determined to be malware, the computer further being
20 constructed and arranged to automatically classify as malware any computer object that has a key in which said unique identifier component is present.

Designation of inventor

User reference: NPB/P10717EP-1
Application No:

Inventor	Name:	HARTER, Mr. Darren
	Address:	178 Barnwood Road, Hucclecote Gloucestershire Gloucester Gloucestershire GL4 3JZ United Kingdom
The applicant has acquired the right to the European patent:		As employer

Designation of inventor

User reference: NPB/P10717EP-1
Application No:

Inventor	Name:	STUBBS, Mr. Paul
	Address:	7 Rookery Road
		Wyboston Bedfordshire MK44 3AX
		United Kingdom
The applicant has acquired the right to the European patent:		As employer

Designation of inventor

User reference: NPB/P10717EP-1
Application No:

Inventor	Name:	HARTWIG, Mr. Markus
	Address:	Exchange House 494 Midsummer Boulevard Buckinghamshire Milton Keynes Buckinghamshire MK9 2EA United Kingdom
The applicant has acquired the right to the European patent:		As employer

Designation of inventor

User reference: NPB/P10717EP-1
Application No:

Inventor	Name: MORRIS, Mr. Melvyn Address: Redmire Gap Intake Lane Derbyshire Turnditch Derbyshire DE56 2LU United Kingdom The applicant has acquired the right to the European patent: As employer
----------	---

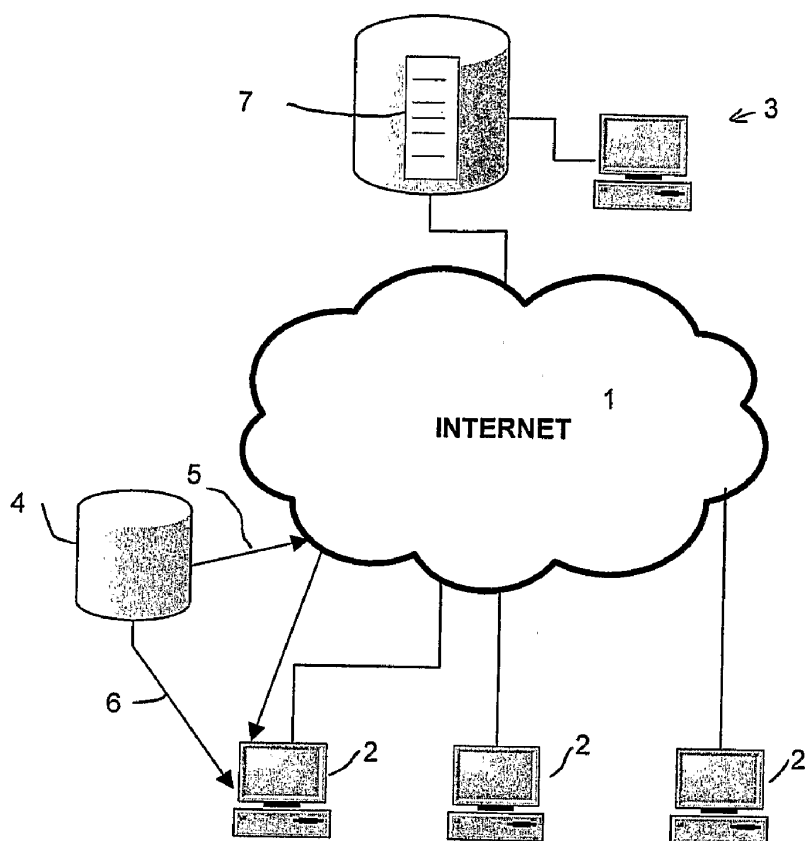
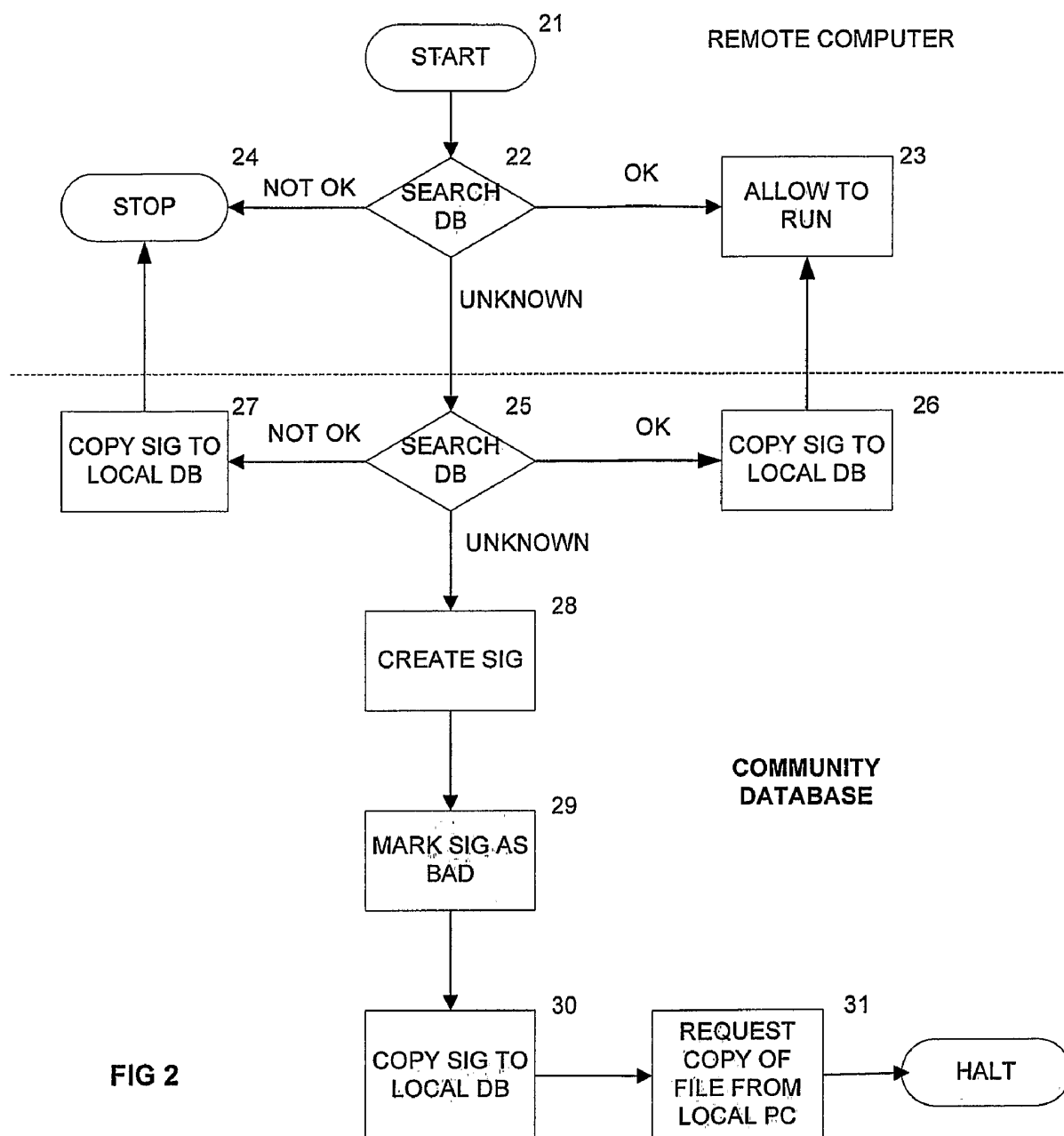


FIG. 1



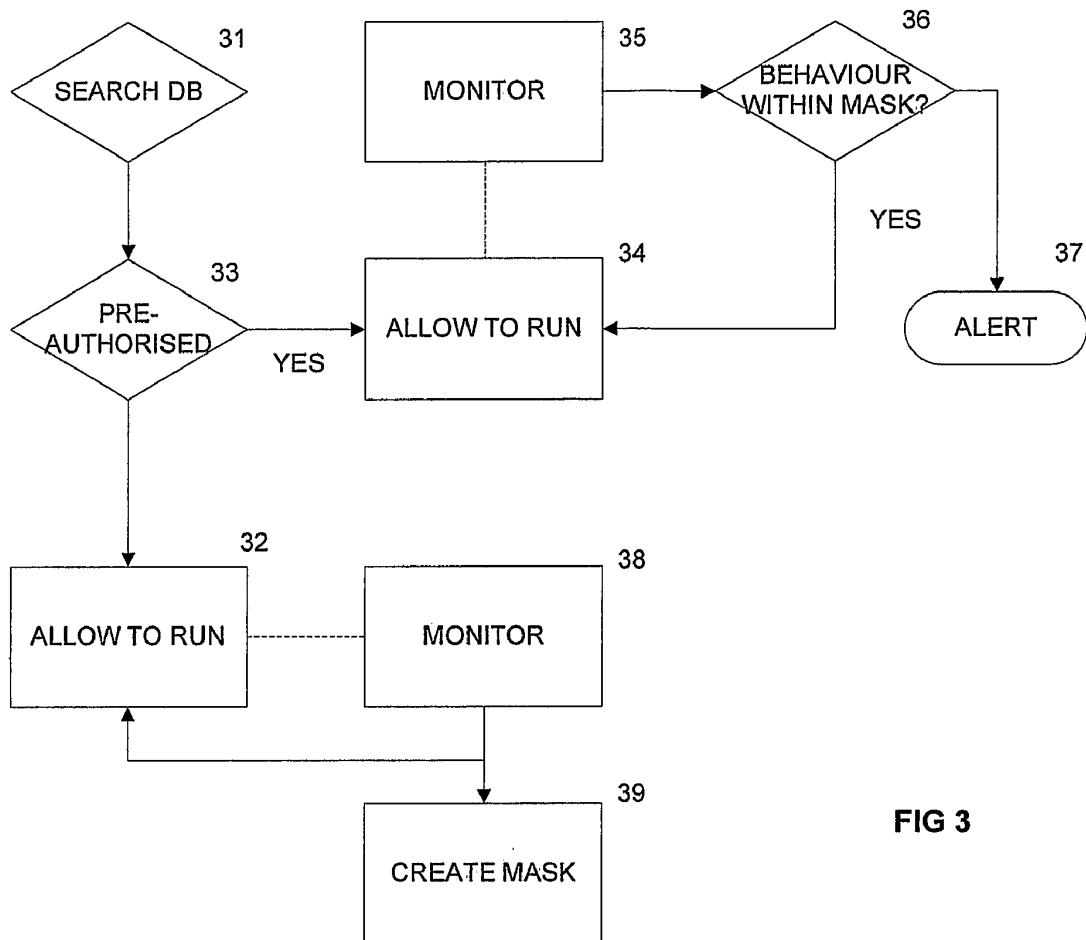


FIG 3

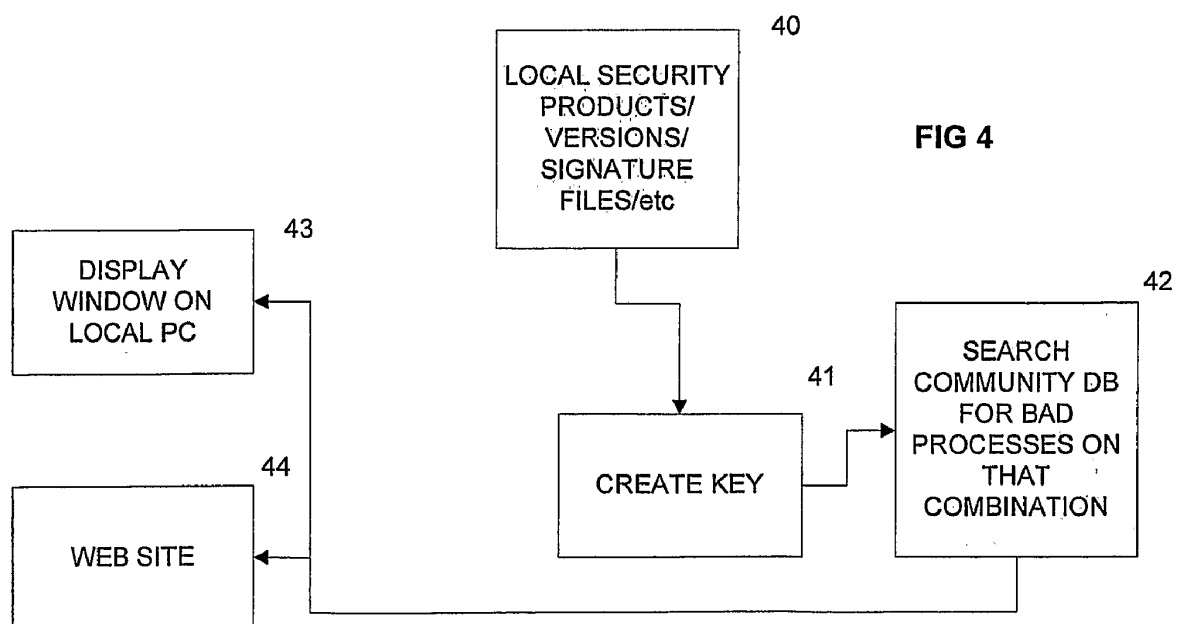


FIG 4

European Patent Office
Directorate General 2
D-80298 Munich
Germany

Your Ref: 1245
Our Ref: NPB/JV/P10717EP-1
Date: 10 May 2013

By electronic submission

Dear Sirs

**New Divisional Patent Application
Divided from European Patent Application No. 06755686.0
Prevx Limited**

I file herewith a new divisional patent application, divided from application number 06755686.0.

The present divisional application includes as an annex a copy of the whole of the claims as originally filed in respect of the parent application. The examiner will understand that this is so as to ensure that this divisional application includes the entire content of the parent application. It is expected that this annex will be deleted in response to the first examination report.

Support in Application as Filed

Claims 1 to 6 correspond to claims 31 to 36 as originally filed in the parent EP application and claim 7 is directed to a computer program for carrying out the method of claims 1 to 3. This invention is described in the original parent EP specification at page 36, line 15 to page 39, line 2.

Yours faithfully



Nicholas P. Bebbington
Authorised European Patent Attorney

Enc



Request for grant of a European patent

<i>For official use only</i>		
1 Application number:	MKEY	MKEY - EP13167436.8
2 Date of receipt (Rule 35(2) EPC):	DREC	DREC - 13 May 2013
3 Date of receipt at EPO (Rule 35(4) EPC):	RENA	
4 Date of filing:		

5 Grant of European patent, and examination of the application under Article 94, are hereby requested. ☒

5.1 The applicant waives his right to be asked whether he wishes to proceed further with the application (Rule 70(2)) ☐

Procedural language:

Description and/or claims filed in:

6 Applicant's or representative's reference

Applicant 1

7-1 Name:

8-1 Address:

10-1 State of residence or of principal place of business:

Representative 1

15-1 Name:

Company:

16-1 Address of place of business:

17-1 Telephone:

17-1 Fax:

17-1

e-mail:

nbebbington@beckgreener.com

Inventor(s)

23 Inventor details filed separately



24 Title of invention

Title of invention:

Methods and Apparatus for Dealing with Malware
- Divisional

25 Declaration of priority (Rule 52)

A declaration of priority is hereby made for the following applications

	State	Filing date	Kind	Application number:	Search results required under Rule 141(1) EPC
Priority 01	GB	30.06.2005	ap	0513375.6	☐

25.2 This application is a complete translation of the previous application



25.3 It is not intended to file a (further) declaration of priority



26 Reference to a previously filed application

27 Divisional application



Application number of earlier application:

EP06755686.0

Date of Filing (Art. 80/Rule 40 EPC):

30 June 2006

27.1 Date of Examining Division's first communication in respect of the earliest application for which a communication has been issued (Rule 36(1)(a) EPC):

16 May 2011

28 Article 61(1)(b) application



29 Claims

Number of claims:

7

29.1



as attached

29.2



as in the previously filed application (see Section 26.2)

29.3



The claims will be filed later

30 Figures

It is proposed that the abstract be published together with figure No.

1

31 Designation of contracting states

All the contracting states party to the EPC and valid for the parent application at the time of filing of this divisional application are deemed to be designated (see Article 76(2)).

32 Different applicants for different contracting states

33 Extension of the European patent

This application is deemed to be a request to extend the European patent application and the European patent granted in respect of it to all non-contracting states to the EPC with which extension agreements are in force on the date on which the application is filed. However, the request is deemed withdrawn if the extension fee is not paid within the prescribed time limit.

33.1 It is currently intended to pay the extension fee(s) for the following states:

34 Biological material

38 Nucleotide and amino acid sequences

The European patent application contains a sequence listing as part of the description

☐

The sequence listing is attached in computer-readable format in accordance with WIPO Standard ST.25

☐

The sequence listing is attached in PDF format

☐

Further indications

39 Additional copies of the documents cited in the European search report are requested

Number of additional sets of copies:

40 Refund of the search fee under to Article 9 of the Rules relating to Fees is requested

☐

Application or publication number of earlier search report:

42 Payment

Mode of payment

Debit from deposit account

The European Patent Office is hereby authorised, to debit from the deposit account with the EPO any fees and costs indicated on the fees section below.

Currency:

EUR

Deposit account number:

28050163

Account holder:

Beck Greener

43 Refunds

Any refunds should be made to EPO deposit account:

28050163

Account holder:

Beck Greener

Fees	Factor applied	Fee schedule	Amount to be paid
001 Filing fee - EP direct - online	1	115.00	115.00
002 Fee for a European search - Applications filed on/after 01.07.2005	1	1 165.00	1 165.00
033 Renewal fee for the 3rd year	1	445.00	445.00
034 Renewal fee for the 4th year	1	555.00	555.00
035 Renewal fee for the 5th year	1	775.00	775.00
036 Renewal fee for the 6th year	1	995.00	995.00
037 Renewal fee for the 7th year	1	1 105.00	1 105.00
501 Additional filing fee for the 36th and each subsequent page	14	14.00	196.00
Total:		EUR	5 351.00

44-A Forms

Details:

System file name:

A-1	Request		as ep-request.pdf
A-2	1. Designation of inventor	1. Inventor	as F1002-1.pdf
A-3	2. Designation of inventor	2. Inventor	as F1002-2.pdf
A-4	3. Designation of inventor	3. Inventor	as F1002-3.pdf
A-5	4. Designation of inventor	4. Inventor	as F1002-4.pdf

44-B Technical documents

Original file name:

System file name:

B-1	Specification	abstract.pdf abstract	SPECEPO-3.pdf
B-2	Specification	drawings.pdf 4 figure(s)	SPECEPO-4.pdf
B-3	Specification	description.pdf Description	SPECEPO-1.pdf
B-4	Specification	claims.pdf 7 claims	SPECEPO-2.pdf

44-C Other documents

Original file name:

System file name:

C-1	Covering letter	P10717EP-1_EPO 10-5-13.pdf	OTHER-1.pdf
------------	-----------------	----------------------------	-------------

45

General authorisation:

46 Signature(s)

Place: London

Date: 13 May 2013

Signed by: GB, Beck Greener, N. Bebbington 13019

Capacity: (Representative)

Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/GB2006/002439

International filing date: 30 June 2006 (30.06.2006)

Document type: Certified copy of priority document

Document details: Country/Office: GB
Number: 0513375.6
Filing date: 30 June 2005 (30.06.2005)

Date of receipt at the International Bureau: 17 July 2006 (17.07.2006)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)



World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse



For Innovation

PCT/GB 2006 / 0 0 2 4 3 9

The Patent Office
Concept House
Cardiff Road
Newport
South Wales
NP10 8QQ

I, the undersigned, being an officer duly authorised in accordance with Section 74(1) and (4) of the Deregulation & Contracting Out Act 1994, to sign and issue certificates on behalf of the Comptroller-General, hereby certify that annexed hereto is a true copy of the documents as originally filed in connection with the patent application identified therein.

In accordance with the Patents (Companies Re-registration) Rules 1982, if a company named in this certificate and any accompanying documents has re-registered under the Companies Act 1980 with the same name as that with which it was registered immediately before re-registration save for the substitution as, or inclusion as, the last part of the name of the words "public limited company" or their equivalents in Welsh, references to the name of the company in this certificate and any accompanying documents shall be treated as references to the name with which it is so re-registered.

In accordance with the rules, the words "public limited company" may be replaced by p.l.c., plc, P.L.C. or PLC.

Re-registration under the Companies Act does not constitute a new legal entity but merely subjects the company to certain additional company law rules.

Signed

Dated 11 July 2006

Page 242 of 242

IPR2023-01050
CrowdStrike EX1003 Page 242

The
Patent
OfficeJ114381/ 002 D02396 P01/77FEE.....
02JUL05 30.00 CHEQUE 0513375.6

Request for grant of a patent

(An explanatory leaflet on how to fill in this form is available from the Patent Office)

0513375.6

THE PATENT OFFICE

30 JUN 2005

NEWPORT

The Patent Office

Cardiff Road
Newport
South Wales

NP10 8QQ 30 JUN 2005

1. Your reference:

(optional)

13532:JK

2. Full name, address and postcode of the applicant
or of each applicant *(underline all surnames)*:Retento Limited
3 New Park Place
Pride Park
Derby DE24 8DZ
United KingdomPatents ADP number *(if you know it)*:

9127234001

If the applicant is a corporate body, give the
country/state of its incorporation

United Kingdom

3. Title of the invention

Computer Security

4. Name of your agent *(if you have one)*:

Saunders & Dolleymore

"Address for service" in the United Kingdom
to which all correspondence should be sent
*(including the postcode)*9 Rickmansworth Road
Watford
Hertfordshire WD18 0JUPatents ADP number *(if you know it)*:

1453001

5.

Priority declaration: Are you claiming
priority from one or more earlier-filed
patent applications? If so, please give
details of the application(s):

Country

Application number
*(if you know it)*Date
*(day/month/year)*6. Divisionals, etc: Is this application a divisional
application, or being made following resolution
of an entitlement dispute about an earlier
application? If so, please give the application
number and filing date of the earlier application:

Number of earlier UK application

Date of filing
(day/month/year)

7. Inventorship: (Inventors must be individuals not companies)

(Please tick the appropriate boxes)

Are all the applicants named above also inventors?

YES ☐NO ☒

If yes, are there any other inventors?

YES ☐NO ☐

8. Are you paying the application fee with this form?

YES ☒NO ☐

Patents Form 1/77

Patents Form 1/77

9. Accompanying documents: not counting duplicates, please enter the number of pages of each item accompanying this form:

Continuation sheets of this form:

Description:

Claim(s):

Abstract:

Drawing(s):

If you are not filing a description, please give details of the previous application you are going to rely upon:

Country Application number Date of filing

10. If you are also filing any of the following, state how many against each item.

Priority documents:

Statement of inventorship and right to grant of a patent (Patents Form 7/77):

1

Request for search (Patents Form 9A/77):

1

Request for substantive examination (Patents Form 10/77):

Any other documents:
(please specify)

11. I/We request the grant of a patent on the basis of this application.

Signature(s):

Date: 29 June 2005

12. Name, e-mail address, telephone, Fax and/or mobile number, if any of a contact point for the applicant:

John Kensett
01923 238311
info@dolleymores.com

Warning

After an application for a patent has been filed, the Comptroller of the Patent Office will consider whether publication or communication of the invention should be prohibited or restricted under section 22 of the Patents Act 1977. You will be informed if it is necessary to prohibit or restrict your invention in this way. Furthermore, if you are resident in the United Kingdom and your application contains information which relates to military technology, or would be prejudicial to national security or the safety of the public, section 23 of the Patents Act 1977 prohibits you from applying for a patent abroad without first getting written permission from the Patent Office unless an application has been filed at least 6 weeks beforehand in the United Kingdom for a patent for the same invention and either no direction prohibiting publication or communication has been given, or any such direction has been revoked.

Notes

A leaflet on how to fill in this form is available from the Patent Office. If you would like a copy of the leaflet it is available on our website at <http://www.patent.gov.uk/patent/info/fact05.pdf> or alternatively you could telephone 08459 500505 or send an email to enquiries@patent.gov.uk to request a copy.

Patents Form 1/77

13532:JK

- 1 -

Computer Security

This invention relates to computer security. In particular, it relates to methods and systems for detecting whether a process operated on a computer is likely to be one which is safe to operate or is likely to be malware.

Background to the Invention

The term "malware" is intended to mean any process which might possibly be harmful to the computer, its software, firmware or data stored on the computer or its performance, reliability, control and utilisation. Non-limiting examples of malware are viruses, Trojans, worms, spyware, adware or similar.

Anti-malware systems have been in existence for nearly as long as malware processes have existed and several service providers produce anti-virus and other anti-malware software and services. Generally, the method of dealing with malware is that when new types of malware are released upon the Internet for example these are eventually detected and possibly infect user's computers or special monitoring computers specially connected to the Internet for this purposes. Once new items of malware have been detected, then the service providers in the field generate signatures which attempt to deal with these and these signatures are then released as updates to their anti-malware programs. Heuristic methods have also been employed.

These systems work well for protecting against known risks. However, since they rely on signature files being generated and/or updated, there is inevitably a delay between a

new piece of malware coming into existence or being released and the signatures for combating that malware being generated/updated and supplied to users. Thus, users are at risk from brand new malware for a certain period of time which might be up to a week or even more. During this time, many users can inadvertently become infected before proper
5 signatures have been disseminated.

WO 2004/0976 A2 describes a system which analyses computer files received or generated by a local computer and compares these with a database to determine whether the file is known and if so whether it has been known about long enough that it can be regarded
-----10 as safe. If it can be regarded as safe, then the file is subject to a less thorough processing for detecting malware than a program about which it is not known whether it is safe or not.

The system disclosed therein appears to only look at whole files rather than processes. A process may be included as part of a file or may be a separate item altogether.
15 Furthermore, this previously proposed system assumes that once a file has been known about for "long enough" it is inherently safe. This is not necessarily the case in real life when, for example, the active payload of a virus or Trojan may only be programmed to happen at a particular date or event which may be many months or even years after the process has been first run or is released. Thus, just looking at the age of a file is an
20 unsatisfactory way of determining whether it is properly safe and will remain so.

Furthermore malware may be programmed to become effective based on other criteria which may not be date or duration based, for example threshold values or other parameters.

An object of the invention is to be able to detect whether a process or component operated on a computer is likely to be one which is safe to operate or is likely to be malware.

A further object is to seek to eliminate or reduce risk in malware in the inter-regnum
5 between its emergence and the generation of signatures. This might be known as zero-date risk.

Brief Summary of the Invention

According to the present invention in a first aspect, there is provided a computer
10 network comprising at least one local terminal, at least one anti-malware service provider database terminal remote from the terminal, a local database on the local terminal which is populated as processes are run or downloaded onto the terminal, a server database on the or each server database terminal and means for determining, when a process is found at the local terminal, whether that process is known or unknown at the local terminal and is
15 considered safe or unsafe and, if unknown, whether the process is known at the server database and is considered safe or unsafe, and means for dynamically altering the database contents and safe/unsafe status using predetermined conditions.

The invention further provides a method of protecting a local computer terminal
20 against malware, comprising providing a local process signature database on the local computer and a remote database on a computer which is remote from the local terminal, searching the local database at the terminal when a process is run to determine whether the process is known or not at that terminal and, if known, is considered safe or unsafe; if the process is not known then searching the remote database to determine if the process is

known and, if so, is determined safe or unsafe; and if the process is known at the remote database submitting the safe/ unsafe result back to the local terminal.

According to a further aspect, there is provided a computer system including means
5 for minimising the risk of malware infection, the system comprising at least one local terminal and a community database comprising a plurality of databases each on a different computer remotely distributed from each other and from the local terminal, whereby signature and/or mask files representative of known processes are stored and built up on the community database to obtain, over time, a community database storing signature and/or
-----10 mask files relevant to or known processes and indicating whether each process is considered safe or unsafe.

According to a yet further aspect there is provided a method of determining the protection which a computer terminal has from malware, the method comprising providing
15 a database remote from the terminal; transmitting from the terminal to a database details of all or selected security products operating at a point in time on that terminal; obtaining similar information from other terminals connected to the database; searching for the same combination of security products used by machine; and identifying any malware processes which were not identified by said other machine having that particular combination of
20 security products and process.

In a further aspect, the invention comprises a database populated with information from a plurality of client terminals representative of the combination of security products and processes used by each client terminal at a point in time, and details of any known

malware processes that were not detected by said unique combination for each particular terminal combination.

Embodiments of the invention may respond to events, not to recognition of files themselves, and to time, both points in time when events occur and to elapsed time, and may also be responsive to volume and acceleration of apparently associated events captured by the database.

Description of the Drawings

10 Embodiments of the invention will now be described, by way of example only, with reference to the accompanying drawings, in which:

Figure 1 shows a network;

Figure 2 is a flowchart showing the running of a process;

Figure 3 is a flowchart showing further processing steps; and

15 Figure 4 is a flowchart showing an information obtaining stage.

Detailed Description of Preferred Embodiments of the Invention

Referring to Figure 1, a computer network is generally shown as being based around a distributed network such as the Internet 1. A local computer terminal 2 is connected to
20 the Internet by any suitable means as will be known in the art. The terminal 2 may be a computer, a PDA, mobile phone, an interactive television or any other device capable of loading and operating processes. A process may be a computer file, may be part of a file or may be a sub-program, macro, web page or any other piece of code to be operated by the terminal or any other event whether executed, emulated, simulated or interpreted. A

process 3 is shown in the figure and this may be applied directly to the terminal locally, as shown by line 4 or may be downloaded to the terminal via the Internet as shown by line 5.

Systems according to the invention utilise a database connected to the Internet and
5 which can interact with the local terminal when that terminal runs a process to determine whether the process is safe or unsafe. The database may be provided on a single server connected to the Internet but is preferably provided over a distributed "community" database 5 as shown in Figure 1, which comprises a number of data servers 5a, 5b, ... 5n. The provision of a distributed community database of this type firstly enables each
10 individual device to require less storage and more importantly makes the database much less vulnerable to denial of service or other attacks since if one server is attacked, then, particularly if entries in the database are duplicated, performance of the database will not be significantly affected.

15 The community database is populated, over time, with information relating to each process run on all of the local terminals within the system. A user of a terminal might subscribe to the services of the database provider or may alternatively be able to download software for free, which enables him to use such services. Data representative of each process may take the form of a so-called signature or key relating to the process and its
20 affects and to a mask which sets out the parameters of the processes performance and operation. The mask will be described in more detail further below.

Figure 2 shows how the system may run in one embodiment.

At the start point 21, a computer process is run at the local terminal, either directly or being downloaded or run direct from a site over the Internet 1. The local terminal then searches its local database 6 at step 22 to search for a signature or key representing that particular process. If the local signature is present, it will indicate either that the process is considered to be safe or OK (in the manner described further below), or will indicate that that process is considered unsafe. An unsafe process might be one which has been found to be malware or to have unforeseen or known unsafe or malevolent results arising from its running. If the signature indicates that the process is OK, then that process is allowed to run at step 23. If the signature indicates that the process is not OK, then the process is stopped 24:

Alternatively, the user may be presented with a choice of whether to allow the process to run or not, but is informed that the process is not considered safe. Ultimately, it will be the user's choice whether to risk running the process or not.

15

In preferred embodiments there may be more than two 'states': GOOD-BAD-UNKNOWN AT LOCAL TERMINAL-UNKNOWN IN 'COMMUNITY DATABASE'. If the process is GOOD then it is, for example, always allowed to run. If BAD then it is NOT allowed to run - the user is given no choice in this. If UNKNOWN locally or in the Community then the user may be given informed choices of viewing or not. Other states and levels may of course be used.

If the process is unknown, then this means that the process has not been run before at that local terminal. In this case, details of the process are passed over the Internet or

other network to the community database and the community database is searched for a signature for that process at step 25. The community database is supplied with signatures representative of programs or processes run by each monitored local terminal (and in a typical version in the field there may be several millions of these terminals and so any processes which are newly released upon the Internet, etc will soon be found and signatures created). When the community database is searched, if the signature is found and indicates that that process is safe, then firstly a copy of the signature is sent to the local terminal database (step 26), to begin populating the local database so that the local terminal has this information immediately to hand then next time the process is run and a message is passed back to the local terminal allowing the process to run.

If the signature is found and this indicates for some reason that the process is unsafe, then again the signature is copied back to the local database and marked UNSAFE (step 27), and then the process is either stopped (or not allowed to run) or the user given an informed choice whether to run it or not.

If after the entire community database has been searched the process is still unknown, then it is assumed that this is a brand new process which has never been seen before in the field. A signature is therefore created representative of the process at step 28 and this signature is initially marked as bad or unsafe at step 29. The signature is copied to the local database of the terminal which first ran the process at step 30 and, in addition, a copy of the file or process itself may be requested at step 31 by the community database from the local terminal. A message may then be passed to the local terminal which

instructs the terminal not to run the process or alternatively the user may be given informed consent as to whether to allow the process to run or not.

If the user chooses to run a process which is considered unsafe because it is too new, then that process may be monitored by the local terminal and/or community database and, if no ill effect occurs or is exhibited, it may then be considered to be safe after a period of time of n days for example. Alternatively, the community database may keep a log of each instance of the process which is found by the many local terminals forming part of the network and after a particular number of instances have been recorded, possibly with another particular number of instances or the process being allowed to run and running safely, the signature may then be marked as safe rather than unsafe. Many other variations of monitoring safety may be done within this concept.

The signature of a process may comprise or include a mask which can be built up with use of that process and which indicates the particular types of behaviour to be expected from the process. If a process is allowed to run on a local terminal, even if the initial signature search 22 indicates that the process is safe, then operation of that process may be monitored within the parameters of the mask. The mask might indicate for example, the expected behaviour of the process; any external requests or Internet connections that that process might legitimately have to make or call upon the local terminal to make, including details of any ports or interfaces which might be required to be opened to allow such communication; any databases, either local or over a local area network or wide area network or Internet, which may be expected to be interrogated by that

process and so on. Thus, the mask can give an overall picture of the expected “normal” behaviour of that signature of that process.

The behaviour of the process is continually monitored both at the local terminal and
 5 also by continually sending information to and from the community database relating to
 that process to determine whether the process is running within its expected mask. Any
 behaviour which extends beyond the mask is identified and can be used to continually
 assess whether the process continues to be safe or not. Thus, if the process, on a regular
 basis (say monthly or yearly) opens a new port to update itself for example or to obtain
 -----10----- regular data, then this information is flagged. If it is found that the process has done this on
 other terminals and has had no ill effects, or this behaviour is known from other processes
 and known as being safe, then this behaviour might be considered as safe behaviour but the
 mask is then modified to allow for this. If it has been found previously that this new
 behaviour in fact causes unsafe or malevolent results, then the process can then be marked
 15 as unsafe even if previously it was considered safe. Similarly, if the process attempts to
 connect to a known unsafe website, database or to take action which is known as generally
 being action only taken by unsafe programs then again the process may be considered to be
 unsafe.

20 Thus, embodiments of the invention can continually modify a processes safe or
 unsafe rating with time.

This is shown in Figure 3. However, Figure 3 also introduces the concept that any
 process can be pre-authorised. Typically, it will be pre-authorised by a trusted partner, such

as a major software company, a verification authority, a Government department and so on. Pre-authorisation enables a supplier of a new process, which has not been released before, to get pre-authorisation for that process, and includes the provision by that supplier of a mask detailing the expected and allowable behaviour of that process. Thus, the mask

5 defines the limits of that processes behaviour. Pre-authorisation may be done by the software provider themselves (if they are considered to be a Trusted Provider), or by the software provider providing details of that process to a trusted authority such as a Government or verification authority who in turn verifies the process and then enables the relevant electronic "documentation" to be provided to the database provider for its required
----- 10 pre-authorisation technique. So a new process or software item by a trusted software provider can be pre-authorised and have no risk of being prevented from running. Similarly, if a bespoke item of software is created for an organisation then that organisation may be able to give or obtain immediate pre-authorisation

15 Referring to Figure 3, when a process is run, the local and/or community database are searched as before at step 31. If the process is not a pre-authorised one, then the steps of Figure 2 are taken, for example and the process might be allowed to run or not at step 32. If the process is pre-authorised, as determined by step 33, then it is immediately allowed to run, step 34. This may be the end of the matter. However, in a preferred
20 variation, the process is then monitored whilst running, and is monitored each time it is run in the future in a monitoring state step 35 to determine whether its behaviour falls within its pre-authorised mask 36. If the behaviour falls within the pre-authorised behaviour then the process is allowed to continue to run. If the behaviour extends beyond the allowed mask,

such as by trying to instigate further processes or connections which have not been pre-
authorised, then this behaviour is flagged at an alert step 37.

Various actions could be taken at this stage. The process might simply not be
5 allowed to run. Alternatively, the trusted authority which initially enabled pre-authorisation
might be contacted, who may be able to confirm that this behaviour is acceptable or not. If
it is acceptable, then the mask could be modified. If not acceptable, then the process might
be marked as unsafe. Many other actions may be taken upon the noting of such an alert
state.

10

If the process has been found not to be pre-authorised at step 33 and is allowed to
run, then the process is monitored at step 38 in order to generate a mask 39 representative
of the normal behaviour of that process. Data representative of this mask might be sent to
the community database for scanning when other terminals run that process. By
15 continually monitoring a process each time it is run or during running of the process, any
behaviour which differs from previous behaviour of the process can be noted and the mask
can modified, or this behaviour might be used to determine that a process which was once
considered safe is now considered to be unsafe.

20 When a user of a local terminal subscribes to a service according to an aspect of the
invention, or downloads software enabling this, his system may periodically provide
information to the community database representative of all or selected ones of the software
products loaded on or available to his system. In particular, this may be all the locally-
loaded security products (such as anti-malware systems including anti-virus software, anti-

spyware, anti-adware and so on), firewall products, etc and includes version details, specific settings and details of which signature files are currently loaded, and also information such as which files are operating and the particular version and software settings at any time and similar types of software. Whilst these may be provided

- 5 individually to the community database, it may prefer to generate a signature or key at the local terminal representative of the sum information (eg by a hashing or compression function) which can then be transmitted to the database for storage. Figure 4 shows how the details of all local security products, versions, signature files, firewall settings, etc 40 are used to create a key 41. The key is transmitted to the community database. Since the community database is provided with such information from many, possibly millions, of user's terminals, it can search for other terminals having the same combination of security products including the same setting, signature files loaded and so on.

- 15 The community database can also be provided with details of processes run by every machine and knows whether a process has been detected by each local machine or not, hence the database can be used to obtain information as to whether a particular, specific, combination of security products, including settings and signature files existing at a point in time, render a particular terminal susceptible or vulnerable to any particular malware process. That is, if the database knows that a terminal in the past has version A of anti-virus product B, with downloaded signature update C and also has a firewall D with 20 particular settings E and perhaps anti-spyware software F with signature updates G, but that a particular malware process P was not detected by this combination of programs at that point in time, then this information can be provided to a local terminal which is known as

having that combination of security programs/settings and can be used to indicate that that terminal is vulnerable in the short term to attack by that particular malware process.

This information can be presented to the user either by displaying a window 43 on the screen display of the local terminal or by directing the user to a particular website which explains the position in more detail. In other words, the community database, when provided with information relating to all the security products on a particular terminal at a particular time, searches for events for processes marked as "bad" that occurred on systems with that particular mix of security products and were not locally detected. It might indicate that process P1 was "bad" and process P2 was "bad" and so on. This information is then fed back to the terminal user either directly or by directing him to a website. A message might be provided on a window on his terminal which reads, for example;

"Your system currently comprises the following security products, versions and signature files:

Anti-virus system A, version A₁, signatures files A₁₁ dated 01/06/05,

Anti-spyware system B, version B₁, signature files B₁₁ dated 04/06/05

Firewall C, updated 30/05/05, etc ...

Be aware that your system may not protect against malware process P1, P2, etc"

The message will generally give these bad processes the names commonly associated with them (eg Sobig virus, and so on). The user may be directed to further guidance on a website for example where he may be given suggestions of how to deal with this situation.

While there may be a suggestion to download different software, it could alternatively be suggestions for downloading particular patches, closing particular ports, or so on. This information could be provided virtually in real-time and will generally only be applicable to a particular point in time.

5

It will be seen from the above that the community database can store a great deal of information about the security and other software products installed on a user's terminal and also about potential risks and malware processes and their effects. Up to now, anti-virus software providers generally provide databases on their website which a user can look up for details of particular viruses and possible suggestions as to preventing infection by them or eradicating any infection. A database generated in accordance with embodiments of the present invention, can provide a lot more detail including:

the name of malware and all the other names it is known by;

the way it propagates its prevalence; and

15 which folders and authorised processes it infects or affects, and so a more extensive database than before can be built up which users can interrogate. The database can also include details, as described above, of the interaction between these or various security products on their terminal and various malware products in order for the user to determine himself the best combination. Also, by continually obtaining details of the software set up
20 on user's terminals and storing these as archive files, if a user's terminal does crash or is affected by malware, the contents of the archive of the community database may be used to provide a more effective backup to restore the user's terminal to a previous safe configuration.

Note that whereas much prior art Anti-Virus software attempts to identify by a scan of files newly introduced to the local computer or network that are known to be bad by virtue of a match against an index file of malware signatures and stops any part of said files from executing, embodiments of the present invention trap the execution activity of all code components on the subject computer and check the signature of each code component against a local database and/or remote database of previously benign activity. If any component is about to execute a not previously known type of activity, that execution is, by default, blocked. Accordingly, in embodiments of the invention all executing code is monitored and any code executing in a manner not previously known to be benign is blocked. Sometimes it is not possible to trap which particular component (of a known suite of executing code components) is producing suspect activity. In such a case composite signatures can be used to tie back or relate to a particular suspect event and thereby to a specific component that is suspect malware. For example, the well known browser "Internet Explorer" has different installations (for different operating systems, configurations etc.) which use many different types of subsidiary code components. At execution time it is not always possible to distinguish which particular code component is triggering a previously unknown event. The community database can collect data that allows a signature to be made of any user's configuration of composite sets of components, to achieve this.

20

In some embodiments of the invention meta data can be captured in the community database, this enables current and refined newly devised heuristics to be run on the community meta database. This in turn allows the ability to model heuristic techniques which themselves can be propagated to the agent level when the new heuristic has been

proved. "what if" modelling can also be done on the community metadata – e.g. what if we mark this code component as bad for the time being, or, what other applications among what number of users might be affected?

5 Amongst other types, the types of meta data captured might be:

 "alias" – related to the frequency with which a code component appears in code that has a name different from other named code it has already been seen to be present in, and;

10 "event key" – being a signature that ties an event to a particular configuration of component code element present on the machine on which the event has occurred. This permits lowest common denominator/ higher-common factor type analysis on the community metadata to determine code components that are malware.

15 It should be noted that in contrast to previously proposed "signature" based methods, with methods according to the present invention there is intrinsic protection even for offline users since the system can be arranged, while out of contact with the community database (i.e. off-line or because of a problem connection therewith), to "lock down" (e.g. prevent execution of, or give the user informed consent) an unknown process. In effect, if a
20 process is unknown at the local terminal then in such circumstances it can be considered, at least initially, automatically to be bad or suspect.

 A further situation arises when users wish to install authorised software while offline.

By prompting the user when they attempt to install new software while offline, the execution of the installation can itself be “authorised” – the authorisation by the user is treated as a “Genesis” event and will be so termed hereinafter. However there are some
5 processes commonly used in installation of software that communicate with other existing programs on the installation machine, e.g. Microsoft’s MSIEXEC.

The Genesis approach involves a process that generates signatures as a result of the user’s authorisation on the user’s terminal.

10

Further, systems according to the invention may download signatures of so-called “licensed installer”, being known code components, to users machines while they are online. This allows the operation of a method such that a “licensed installer” is permitted to execute while a Genesis event is “current”, i.e. within a period of minutes after an
15 authorisation from the user. There may be refinements to this method, such as to prevent licensed installers executing if a media change has occurred during the currency of a Genesis event.

The method may be such that a “licensed installer” together with any child
20 processes of the licensed installer is permitted to execute while a GENESIS event is “current”, i.e. within a period of minutes after an authorisation from the user. However, any unknown processor, which may be malware, may still be detected and processed.

There may be refinements to this method, such as to prevent licensed installers executing if a media change has occurred during the currency of a Genesis event and super-trusted installers such as for example 'Windows Update', where all new processes created by the super-trusted installer are marked immediately as safe.

5

Preferably signatures of licensed installers are ALWAYS downloaded, as and when added to the community database, to an agent machine while online. There probably are not that many of these.

10

When the terminal is connected to a network, the other aspect to this feature is that the system will, if the about to be installed program is not known to the community database, block the installation, or alert the user, i.e. "you are about to install some software, this software is not known to [community]. Are you sure you wish to proceed?". Having a limited number of licensed installers facilitates download, as minimal data is required, compared to downloading virus signature files:

15

Note that embodiments of the invention can be applied within servers (e.g. in a server-enterprise environment) and therefore can be executed on any computer or terminal within a network, including ones which may be connected to a network or not, from time to time. Even a server itself may be a local 'terminal' as the term is used in this specification.

20

The potentially high volume of active users (i.e. terminals) (which will in practice be many millions) gives a high probability of at least one of them being infected by new malware. The speed of propagation is detected and recorded in embodiments of the

invention so that the propagation of malware can be detected and malware designated as bad, and can be used to identify an incident emerging across the community as malware, or simple volume of infection can be used as a trigger.

- 5 In a further feature, difference of naming, of an otherwise identical piece of code combined with acceleration of first attempts to execute the code within the community allows pattern matching that will show up an identical signed piece of code as bad.

 This feature allows the statement in some embodiments, “nothing will propagate in
10 our community faster than X without being locked down”, so that if any process or event propagates quicker over a given duration, it is marked as bad.

- This process can be automated by the identification of the vector of propagation in the community, from timestamp data held in the community database and the marking of a
15 piece of code that has these attributes as bad. By comparison, it is believed that all other anti-malware providers rely on a simplistic known bad model and therefore are reliant primarily on malware infection actually occurring on terminals and being reported.

- One method for plotting the acceleration of a suspect piece of code involves
20 timestamping of each report of the same piece of code, showing how many terminals had reported the code within successive timeslots, within seconds or minutes initially but then perhaps against a more logarithmic set of lengthening time periods i.e. the method by which timestamping is done usually cannot be maintained at the same rate as during the earliest period of first detection. This logarithmic method avoids the database becoming swamped

with stamp data by avoiding a linear method of data capture, e.g. every few seconds of all incidents of the same code. Where appropriate, in some embodiments, suspect files can be uploaded automatically from individual terminals to the community database for more detailed examination.

5

Amongst other features and inventions, the following aspects form part of the present invention, any one or more of which, or any combination of which, or any one or more feature or combination hereinbefore described, are considered as possible claimable inventions in their own right.

10

- a) The concept of a known and trusted parent process having an identifying component in its signature that uniquely defines the process (referred to here as a "gene"). By virtue of such gene being inherited in the signature of all of the parent's child processes and through them further child processes (referred to here as "issue") such signatures are all automatically recorded in the local database as good. The concept also allows the inherited gene to be removed should any issue abuse it, such as by creating a suspect child or one that becomes suspect. This concept, combined with Genesis, allows the extension of the trusted status of parent processes notwithstanding the involvement of surrogate programs (like Microsoft's MSIExed for example) in generating further issue. The marking of child process signatures as good might otherwise fail because of the involvement of surrogates like MSIExec, and other licensed installer programs. Alternatively, a parent process which is not necessarily known and trusted may have a unique identifier, which may possibly be considered inherently safe, unsafe or given other attributes. More than one identifier (gene) may be used. The attribute may be security related or may be related to other aspects such

15

20

as being subscription related so that a process can only be executed whilst a subscription is current, and so on.

- b) Parental creation of a signature for a child or children including the ability for these to be automatically marked as either good or bad depending on the parent's behaviour and determination. Note that in some embodiments the product can 'watch' or monitor the birth of a child process and automatically create the signature upon arrival.
- c) Genesis creation through a licensed or trusted installer or surrogate who may pass on the true parents (99% good) genes. The 'genesis' process allows the product to capture the birth and apply the appropriate genetic determination.
- d) A feature may be included that allows for automatic forfeiture of a child's inherited ability to trigger the automatic creation of signatures on any further births because the child, as parent has already produced bad offspring. Preferably, a rule is that if a file has one bad offspring then the inherited ability can be automatically removed.
- e) An ability to watch the clones or identical twins (i.e. the same process running on other systems in the community) to compare the pattern of their off-spring to ensure that Genesis events are definitely part of the same genetic line and remove any determination for an off spring which is not prevalent as a child of the clones or identical twins, or to make the determination unknown causing it to be watched intensely throughout the community before a determination can be made.

Some of the features a) to e) represent a solution to the issues of producing a product which can be used effectively without 100% reliance on being permanently connected to the internet, which is often impractical. Examples of this are Windows Update, and other processes used more and more by vendors who wish to be able to roll out
5 other product updates automatically across the worldwide web.

Possible benefits of these types of features above conventional software are as follows. Antivirus software tends to have a cache of known bad signatures. The problem is keeping this up to date. Take the simple example of someone buying a new computer. The
10 computer comes with an antivirus product preloaded with a signature cache. Between the time when the PC was built, shipped to the store and bought by the user several days or weeks will have passed. The user starts the PC and is exposed to any new virus or malware which was created after the PC was built. Full protection requires the user to connect to the internet and download updates. This cannot be guaranteed to occur ahead of other activities
15 by the user on the internet (almost physically impossible to guarantee). With a local cache of known good processes, as in the embodiments of the present invention, it is possible to ship the computer/terminal preloaded with a pre-generated cache of signatures for all of the good (clean) software preloaded by the computer manufacturer. In this case the user can connect to the internet knowing that any new or updated programs will be immediately
20 detected and verified. Also any auto-updating software can function forcing signatures to be automatically built for its children and more remote off-spring (i.e. grandchildren, great-grandchildren, etc).

f) The ability to monitor a process along with any optional sub-processes as an homogenous entity and then compare the activities of the top level process throughout the

community and deduce that certain, potentially malevolent practices only occur when one or more specific sub-processes are also loaded. This allows effective monitoring (without unnecessary blocking) of programs like Internet Explore (browsers) whose functionality may be easily altered by downloadable optional code that users acquire from the internet, 5 the principal source of malevolent code today.

g) The ability, using the community database to make early diagnosis, or simply to take precautionary measures to stop potentially fast propagating worms and malware very, very early in their life cycle. Given that it is theoretically possible to create a 10 worm which could infect every computer connected to the internet within a matter of a few minutes this feature is highly desirable.

h) The ability to make even faster determination by combining data defining the speed of propagation of a new piece of software with meta data collected by the Agent 15 and fed to the database. This includes monitoring processes that attempt to conceal themselves from the user by randomly changing name and/or location on the local terminal, or every computer or network on which it installs. It also includes a process's attempt to create an identical copy (i.e. with identical code contents) on the computer but with a different name. This is a classic attribute of a worm.

20

i) The use of meta data derived from terminal agents defining the behaviour of a process across the community and held in a central database to model, test and create new automated rules for use in the central database and as rules that may be added to those held

and used in the local (terminal) database to identify and determine the agent's (system) response to new or unknown processes and process activity.

j) The use of two signature processes. One which defines the entire files and
5 will change with almost any change to the files content. The other which attempts to define
only the processing instructions of the process which changes much less. By tracking the
occurrences of both signatures individually appearing with different counterparts it is
possible to identify processes which have been changed or have been created from a
common point but which have been edited to perform new, possibly malevolent
10 functionality.

k) The use of an event mask which enables an agent to monitor a known
process and detect if it performs abnormal events which could indicate the emergence of a
new purpose from a Trojan. This enables the agent to take immediate protect action to
15 block the abnormal activity and to report it to the central database.

l) A technique to enable an efficient and practical form of communication
between the agent (i.e. local terminal) and the remote database which allows the local
terminal and community to operate without unnecessary delay or impact on the users'
20 enjoyment of the computer and processes he/she choose to use.

m) The technique of recording which security products, operating system,
updates, settings and security patches are installed and active when an event occurs and to
use this to help assess the likelihood of a malevolent process bypassing specific security

13532:JK

- 26 -

products or combinations thereof. To use this information to warn users about the need to bolster their defences to prevent attack.

Claims

1. A computer network comprising at least one local terminal, at least one anti-malware service provider database terminal remote from the terminal, a local database on
5 the local terminal which is populated as processes are run or downloaded onto the terminal, a server database on the or each server database terminal and means for determining, when a process is found at the local terminal, whether that process is known or unknown at the local terminal and is considered safe or unsafe and, if unknown, whether the process is known at the server database and is considered safe or unsafe, and means for dynamically
10 altering the database contents and safe/unsafe status using predetermined conditions.
2. A system as claimed in Claim 1, wherein the server database is distributed over a plurality of server computers.
- 15 3. A method of protecting a local terminal against malware, comprising providing a local process signature database on the local and a remote database on a computer which is remote from the local terminal, searching the local database at the terminal when a process is about to be run to determine whether the process is known or not at that terminal and, if known, is considered safe or unsafe; if the process is not known then searching the remote
20 database to determine if the process is known and, if so, is determined safe or unsafe; and if the process is known at the remote database submitting the safe/ unsafe result back to the local terminal.

4. A method as claimed in Claim 3, wherein when a process is first seen, a signature file is created at the local terminal and/or remote database representative of that process.
5. A method as claimed in Claim 3 or Claim 4, wherein if the process is not known at the remote database, a signature of the process is created at the remote database and initially marked as unsafe and a copy of the signature is sent to the local database.
6. A method as claimed in Claim 3, wherein if a process is marked as safe by the local or remote database it is allowed to run.
7. A process as claimed in Claim 3, wherein if a process is marked as unsafe by the local or remote database it is not allowed to run.
8. A process as claimed in Claim 3, wherein if a process is marked as unsafe by the local or remote database the user of the local terminal is provided with an informed choice as to whether to allow the process to run or not.
9. A method as claimed in Claim 3, wherein a mask is generated for each or a collection of processes, which mask defines the acceptable behaviour for that process or collection.
10. A method as claimed in Claim 3, wherein the mask includes one or more parameter selected from the group comprising;

the expected behaviour of the process or collection of processes; any external requests or Internet connections that that process or collection might legitimately have to make or call upon the local terminal to make, including details of any ports or interfaces which might be required to be opened to allow such communication; any databases, either
5 local or over a local area network or wide area network or Internet, which may be expected to be interrogated by that process or collection.

11. A method as claimed in Claim 9, wherein after the process is allowed to run, its behaviour is monitored and if its behaviour extends beyond that allowed by the mask an
10 alert is raised.

12. A method as claimed in Claim 10, wherein after the alert is raised, a determination is made as to whether the modified behaviour renders the process safe or unsafe, even if the process was originally considered safe.

15

13. A method as claimed in Claim 1 or Claim 3, wherein a process may be pre-authorized.

14. A method as claimed in Claim 13, wherein the process is pre-authorized by a
20 software provider or by a trusted authority.

15. A method as claimed in Claim 13, wherein if a process is not pre-authorized and is allowed to run, its behaviour is monitored and is used to create a mask representative of its behaviour, the behaviour continuing to be monitored to determine whether it expands

beyond the mask, in which case the modified behaviour can be analysed to determine whether the mask itself should be modified to take the modified behaviour into account or whether the modified behaviour indicates that acceptable behaviour has been exceeded and the process should now be considered unsafe.

5

16. A computer system including means for minimising the risk of malware infection, the system comprising at least one local terminal and a community database comprising a plurality of databases each on a different computer remotely distributed from each other and from the local terminal, whereby signature and/or mask files representative of known

10 processes are stored and built up on the community database to obtain, over time, a community database storing signature and/or mask files relevant to or known processes and indicating whether each process is considered safe or unsafe.

17. A system as claimed in Claim 16, wherein even after signatures and masks have
15 been established, behaviour of a process is monitored to determine whether its status is still safe or unsafe.

18. A method of determining the protection which a computer terminal has from
malware, the method comprising providing a database remote from the terminal;
20 transmitting from the terminal to a database details of all or selected security products operating at a point in time on that terminal; obtaining similar information from other terminals connected to the database; searching for the same combination of security products used by machine; and identifying any malware processes which were not identified by said other machine having that particular combination of security products and

25

process.

19. A method as claimed in Claim 18, further comprising providing information to the user of said first local terminal that his system may be susceptible to attack by said malware processes.

20. A method as claimed in Claim 19, wherein the combination of processes includes security products, versions, signature files loaded and other security products.

21. A method as claimed in Claim 19, wherein information is provided to a user on a display associated with the local terminal.

22. A method as claimed in Claim 19, wherein the information is displayed on a website.

15

23. A database populated with information from a plurality of client terminals representative of the combination of security products and processes used by each client terminal at a point in time, and details of any known malware processes that were not detected by said unique combination for each particular terminal combination.

20

24. A method as claimed in claim 3 wherein files, or data representative of files can be uploaded from the local database to the remote database.

25. A method as claimed in claim 3 wherein composite sets of data are analysed to

determine their status.

26. A method as claimed in claim 3 wherein metadata is collected and stored in the local and/or remote database.

5

27. A method as claimed in claim 26 when the metadata includes at least one member of the set comprising "alias" and "Event Key".

28. A method as claimed in claim 3 whereas if a local terminal is not connected to the

10 remote database and a process unknown to that terminal is attempted to be executed an alert is raised that the process might be unsafe.

29. A method as claimed in claim 28 when the possibly unsafe process is not allowed to execute.

15

30. A method as claimed in claim 3 wherein a process unknown to a terminal can be preauthorised for loading onto or executing on said terminal while the terminal is not connected to the remote database.

20 31. A method as claimed in claim 30 wherein one or more "licensed installer" signatures are pre-supplied to said terminal.

32. A method as claimed in claim 3 wherein volume of infection and/or speed of propagation is used to determine whether a process is safe or unsafe.

33. A method as claimed in claim 32 wherein a vector of propagation is used to determine whether a process is safe or unsafe.

5 34. A method as claimed in claim 32 or 33 wherein propagation is determined by timestamping each report of the same process, and providing an indication of the number of terminals reporting attempted invocation of the process within successive time slots.

10 35. A method as claimed in class 34 wherein an at least partially logarithmic timescale is used.

36. An anti-malware system, arranged to detect the spread of new processes across a network and to consider a process as bad if the volume or speed of propagation exceeds a predetermined threshold.

15 37. An anti-malware system as claim in claim 36 wherein each report of the same process is timestamped and comprising counting the number of terminals in the network reporting that process in successive time periods.

20 38. An anti-malware system as claimed in claim 37 wherein a logarithmic set of time periods is used.

39. A method as claimed in claim 3 wherein there are more than two possible states representing different levels of safe or unsafe, and the process is allowed to be run or not, or the user given informed choice, depending on the level.

5 40. A method as claimed in claim 39 wherein the states are GOOD-BAD-UNKNOWN LOCALLY and UNKNOWN IN REMOTE DATABASE.

41. A method as claimed in claim 3 wherein an application may be labelled as super trusted and any child processor generated, or instigated as a result thereof, be considered
10 safe at least for a period.

42. A computer program product or method, wherein a signature relating to a parent process includes a component that uniquely identifies it and which is inherited in the signature of any child or other descendant of the parent, such unique identifier being used
15 to ascribe one or more attributes to the descendants.

43. A product or method as claimed in Claim 42, wherein the parent process is known and trusted and whereby an attribute is that the descendant process is safe.

20 44. A product or method as claimed in Claim 42 or 43, wherein if the parent or a descendant exhibits behaviour which might be unsafe or suspicious the attribute is, or is changed to, the process being unsafe.

13532:JK

- 35 -

45. A product or method as claimed in any of Claims 42 to 44, wherein the attribute is security related.

46. A product or method as claimed in any of Claims 42 to 45, wherein the attribute is
5 not security related.

Abstract**Computer Security**

- 5 A computer network is disclosed with minimised risk of malware infection, comprising at least one local terminal, at least one malware service provider database remote from the terminal, a local database on the local terminal which is allowed to populate and processes are run or downloaded onto the terminal, a server database on the or each server database terminal and means for determining, when a process is found at the
- 10 local terminal, whether that process is known or unknown at the local terminal and is considered safe or unsafe and, if unknown, whether the process is known at the server database and is considered safe or unsafe, and means for dynamically altering the database contents and safe/unsafe status using predetermined conditions.

1/3

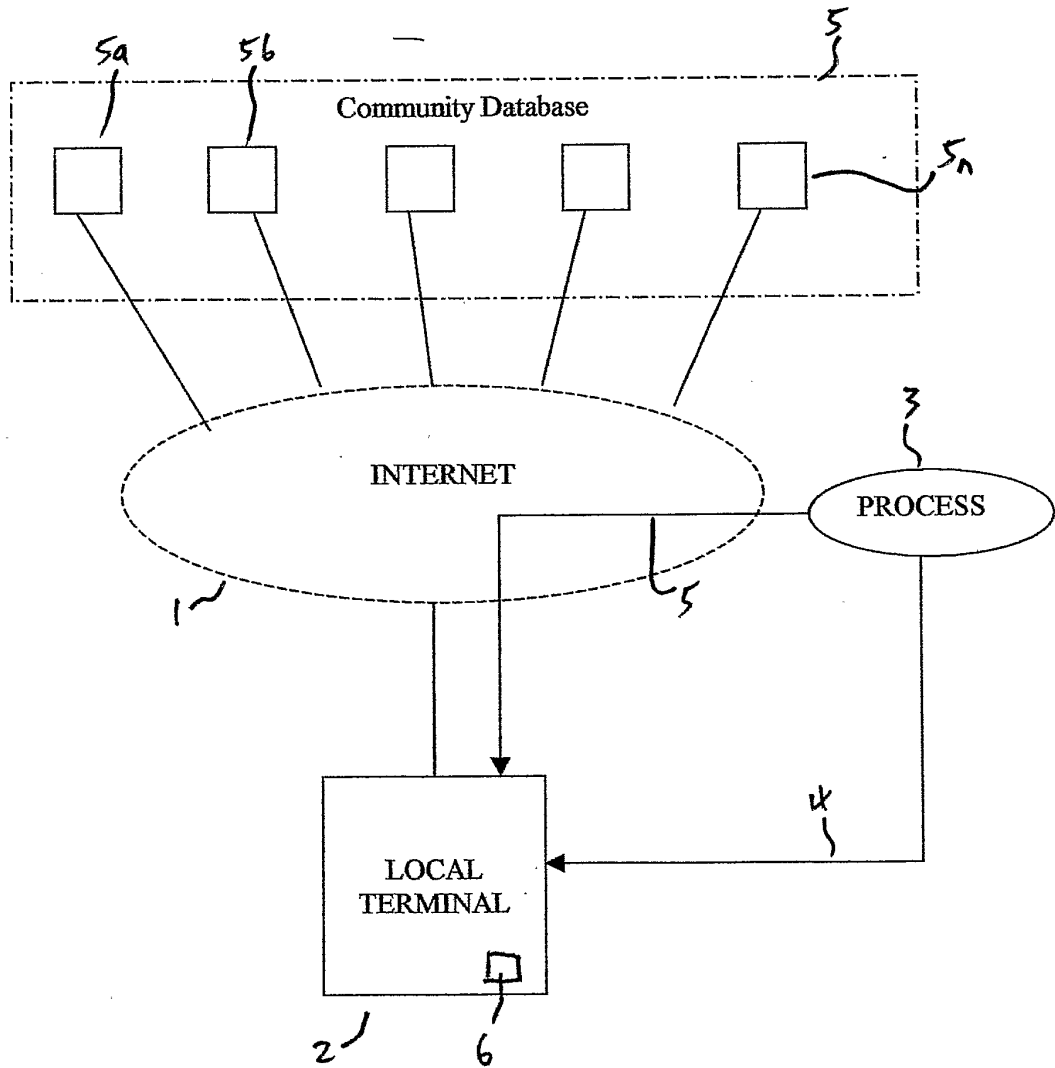


FIG 1

4. The fourth part of the document addresses the challenges associated with data collection and analysis. It identifies common pitfalls and provides strategies to overcome them, ensuring that the data is reliable and actionable.

6. The sixth part of the document provides a summary of the key findings and conclusions. It reiterates the importance of a systematic approach to data collection and analysis and the need for continuous improvement in the process.

7. The seventh part of the document includes a list of references and sources used in the research. It provides a comprehensive overview of the literature and resources that informed the study.

8. The eighth part of the document contains a list of appendices and supplementary materials. These include detailed data tables, charts, and other supporting documents that provide further context and detail to the main text.

9. The ninth part of the document includes a list of figures and tables. These visual aids are used to present complex data in a clear and concise manner, making it easier for the reader to understand the results.

10. The tenth part of the document includes a list of footnotes and endnotes. These provide additional information and references that are not included in the main text but are relevant to the study.

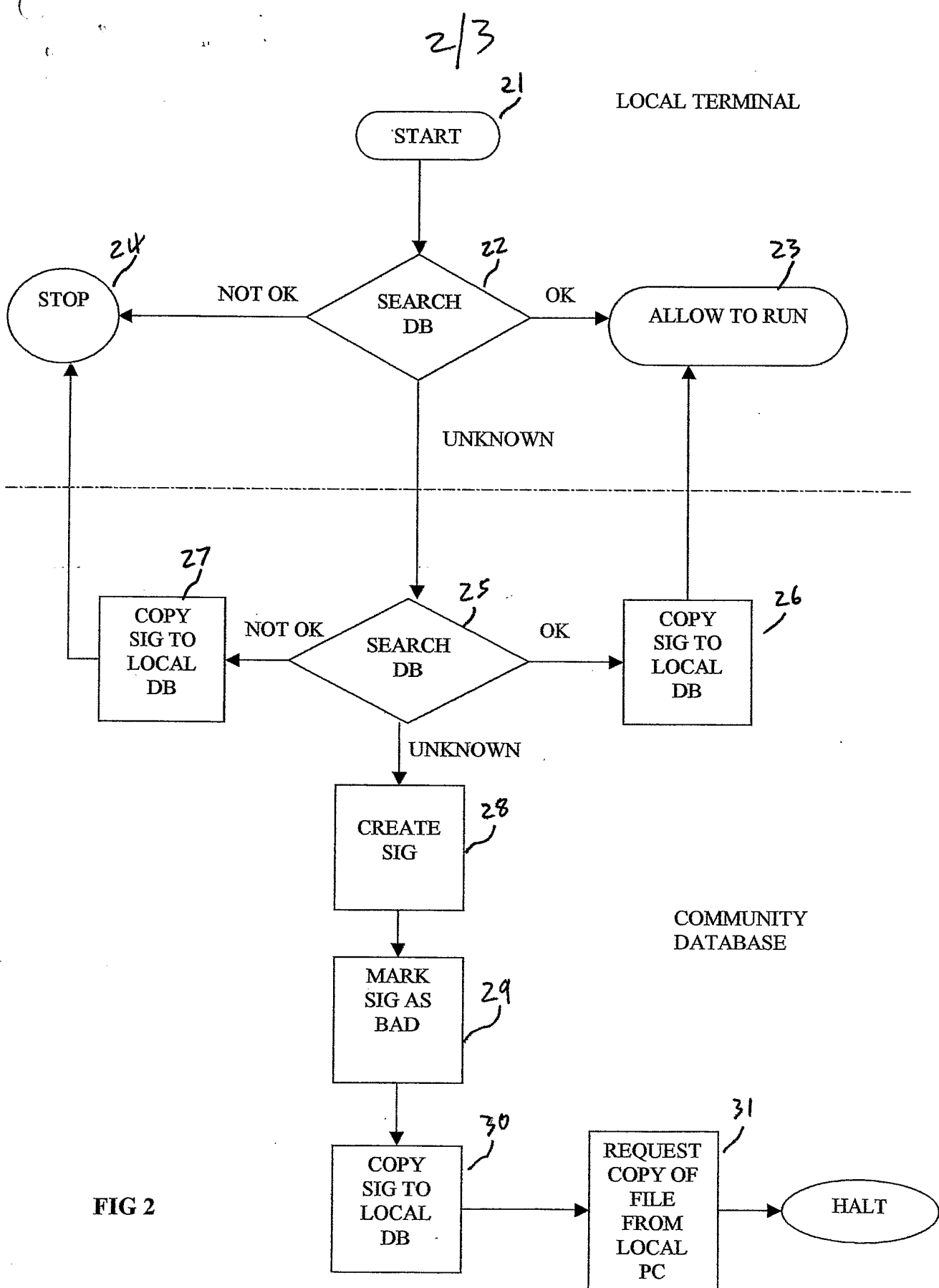


FIG 2

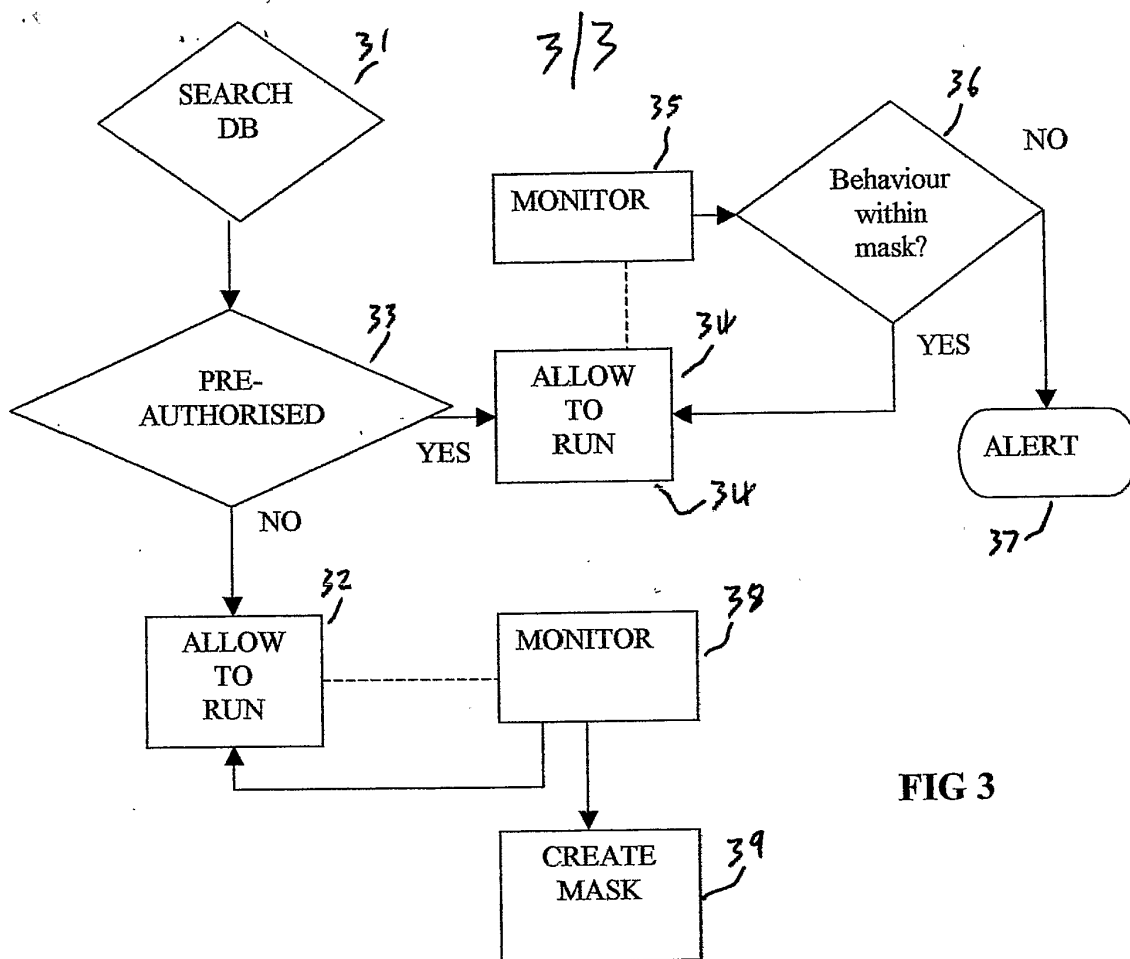


FIG 3

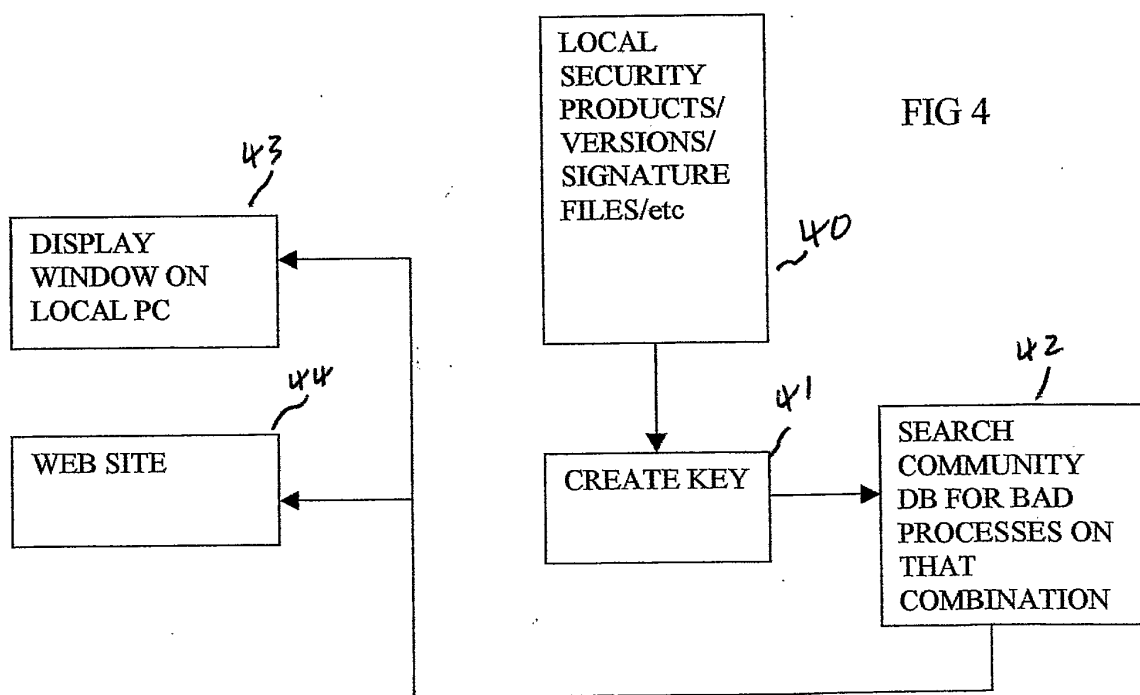


FIG 4

[Faint, illegible text covering the majority of the page, likely bleed-through from the reverse side.]