

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

KEYSIGHT TECHNOLOGIES, INC.,
Petitioner,

v.

CENTRIPETAL NETWORKS, LLC,
Patent Owner.

Case IPR2023-00446
U.S. Patent No. 10,567,343

**DECLARATION OF PEDRO MARINHO
IN SUPPORT OF PATENT OWNER'S RESPONSE**

I, Pedro Marinho, declare:

1. I am over the age of 18 and make this declaration of my own personal knowledge.

2. Since March 2019, I have been Senior Security Analyst at Centripetal Networks (“Centripetal”). Before joining Centripetal, I obtained a Bachelor’s in Computer Science in 2010 from Pontifical Catholic University of Minas Gerais (PUC Minas).

3. Prior to starting at Centripetal, I also worked at Emerging Threats as a Malware Analysis & Vulnerability Researcher from November 2010 to January 2016. After Proofpoint acquired Emerging Threats, I joined Proofpoint as a Security Research Engineer until September 2018.

4. At Emerging Threats, I worked on vulnerability research and malware analysis. I also tested, built, and optimized Snort and Suricata signatures for Emerging Threats Pro.

5. I reviewed the Emerging Threats reference (found at <https://web.archive.org/web/20101202025325/http://rules.emergingthreats.net/open/snort-2.8.4/emerging-all.rules>). I am familiar with this list of Emerging Threats rules. In fact, I have authored over 20 rules found in the document, such as Rule SIDs 2008359, 2008682, 2009305, etc. See Ex. 1020 at 17, 129-130, 207.

6. I note that there are no “drop” rules in the Emerging Threats reference; all of the Snort rules use the “alert” keyword. Ex. 1020. The reason for this is that these rules, when run by Snort, would cause a lot of false positives and would be very “noisy.” That is, although some rules may mention a certain intent, e.g., using the msg (message) keyword, the Snort “alert” rules in the Emerging Threats list would frequently alert for reasons other than those specified in the msg field. I also note that many of the rules in the Emerging Threats reference are disabled by default by being commented out with a “#” annotation. Snort rules were commented out with a “#” annotation as a caution to potential users of such rules that these rules may be prone to false positives, which would cause performance problems.

7. I reviewed several of the Emerging Threats rules cited in Keysight’s petition, and I provide a summary of their functionality below. All of these summaries are based on my experience and knowledge.

8. For example, I reviewed this Rule SID 2003021, which is found on page 109 of Ex. 1020, and which I reproduced below. I note that this rule is commented out, likely for performance reasons.

```
#Application data stream
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET 1024:65535 (msg:"ET POLICY
TLS/SSL Encrypted Application Data on Unusual Port
SSLv3";flowbits:isset,BS.SSL.Established;flow:established,to_server;con
tent:"|17 03 00|"; depth:4; threshold:typelimit, count 1, seconds 120,
```

```
track by_src; classtype:unusual-client-port-connection;reference:url,doc.emergingthreats.net/2003021;reference:url,
www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_SSL_TLS_on_High_Port; sid:2003021;
rev:8;)
```

9. Rule SID 20033021 would alert (but not drop) upon matching a TCP packet encrypted using SSL version 3 that is directed to a port number in the range from 1024 to 65535, of which there are many legitimate uses. For example, Port 1080 is a well-known port for SOCKS proxy traffic, Port 1194 is used for OpenVPN, and there are many other legitimate uses for ports numbered from 1024 to 65535. The content match of three bytes is too short and will match frequently, due to different protocols and services running in a wide range of ports, even data stream such as online movies as well as encrypted and compressed data. The signature is not to be used to drop traffic because of false positives due to a short content match.

10. I also reviewed this Rule SID 2002526, which is found on page 87 of Ex. 1020, and which I reproduced below. I note that this rule is also commented out for performance reasons. It is my understanding that this Rule SID 2002526 was actually removed (*i.e.*, deleted) from the Emerging Threats ruleset on or around April 23, 2012.

```
#US Top Secret Not Releasable to Foreign Nationals
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY
HTTP - US Top Secret NOFORN"; flow:to_server,established;
```

```
pcr: "/(TOP\sSECRET|TS)//[\s\w,/-]*NOFORN[\s\w,/-]*(?=(25)?X[1-9])/ism"; classtype: policyviolation; reference: url, doc.emergingthreats.net/bin/view/Main/2002526; reference: url, www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/POLICY/POLICY_Classified_Information; sid: 2002526; rev: 4;)
```

11. Rule SID 2002526 (if the comment “#” was removed) would allegedly alert (but not drop) upon matching a packet based on using a regular expression pattern matching keyword “pcr”, but its regular expression pattern contains syntax errors. In my opinion, this rule would not be functional, even if its comment “#” were to be removed. The REGEX has a syntax error by not escaping the slashes and both the Snort and Suricata engines will fail to parse the signature and emit an error. This signature is not sufficient to match accurately in a file transiting the network. Even if the REGEX was correct it can match on different patterns due to the repetition of any spaces, characters from a to z, A to Z and 0 to 9 and all printable symbols or dash repeated zero or any times, the REGEX pattern match `[\s\w,\-]*`, sub pattern of the REGEX in the signature after the text TOP SECRET can nearly match on anything. To match accurately on a file it is necessary to extract the file from network traffic, save it on disk and perform a validation check such as a checksum or even parsing specific fields of the file. A PDF file for example has different fields, encrypted and compressed data also present in files such as Microsoft Word Doc, Excel, Power Point and Adobe PDF files due to these files are binary files and compressed. It is not possible to match

on a Text with a REGEX and expect it to match correctly on a field on a file transiting the network. Files such as mentioned above have innumerable fields and data structures, pointers to data structures within the file that sets Font type, start and end of other structures or different data types such as an image embedded in a the file. The resources to accurately perform match on a file after extract it from network traffic can't be accomplished with this rule alone. It is not so simple as to be able to prevent data exfiltration by matching on a pattern of text with a REGEX. The problem of preventing a file exfiltration demands more functionalities than only an IDS/IPS can provide in terms of matching network traffic against signatures. Also IDS/IPS have limited resources and the signatures need to be very simple and fast to run or quit to run as fast as it cannot match due to high number of packets it attempts to match. An IDS/IPS can have performance problems and loose packets, not being able to process every single packet if the signatures do expend too much time matching. This signature cannot be used to drop traffic.

12. I also reviewed this Rule SID 2002034, which is found on page 8 of Ex. 1020, and reproduced below.

```
#by Matt Jonkman
#
alert tcp $HOME_NET $HTTP_PORTS -> $EXTERNAL_NET any (msg:"ET
ATTACK_RESPONSE Possible /etc/passwd via HTTP (linux style)";
flow:established,from_server;
content:"root|3a|x|3a|0|3a|0|3a|root|3a|/root|3a|/";
nocase;classtype:miscactivity;reference:url,doc.emergingthreats.net/bin
/view/Main/2002034;reference:url,www.emergingthreats.net/cgibin/cvsweb.
```

```
cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_etc-passwd; sid:2002034;  
rev:8;)
```

13. Rule SID 2002034 would alert (but not drop) upon a TCP packet that contains the string “root:x:0:0:root:/root:/”. This signature falls into the same problem of not having necessary resources to be able to extract the file from network traffic and validating the file contents and should not be used to drop traffic due to risk of false positives and dropping legitimate traffic. The signature was designed to detect a **potential** download of a passwd file as a result of a successful attack against a linux system that would grant access to the /etc/passwd file. The rule text message states “**Possible**” which means it may also match on other contents in a response from webserver such as a web pages, setting this rule to drop may block legitimate traffic other than a passwd file download.

14. I also reviewed this Rule SID 2001328, which is found on page 109 of Ex. 1020, and reproduced below. I note that this rule is commented out for performance reasons. The comment preceding the rule says the rule should not be run internally.

```
#Submitted by Patrick Harper. pcre by Matt Jonkman  
#This rule is disabled by default. It should generally be run on the  
outside of your network, not internally. Enable it where useful.  
#  
#alert ip any any -> any any (msg:"ET POLICY SSN Detected in Clear Text  
(dashed)"; pcre:"/ ([0-6]\d\d|7[0-256] \d|73[0-3]|77[0-2])-\d{2}-\d{4}  
/"; classtype:policy-violation;  
reference:url,doc.emergingthreats.net/2001328;  
reference:url,www.emergingthreats.net/cgi-
```

```
bin/cvsweb.cgi/sigs/POLICY/POLICY_SSN_in_the_Clear; sid:2001328;  
rev:13;)
```

15. If Rule SID 2001328 had its comment “#” removed, it would alert (but not drop) upon matching an IP packet that contains a string matching a pattern that specifies a certain sequence of numbers, spaces, and dashes, such as “ xdd-dd-dddd” or “ 7y d-dd-dddd” or “ 73w-dd-dddd” or “ 77z-dd-dddd”, where d can be any digit, x is a digit from 0 to 6, y is a digit in the set {0,1,2,5,6}, w is a digit in the set {0,1,2,3}, and z is a digit in the set {0,1,2}, and the spaces are required. The REGEX pattern of this signature, and the fact it only has a REGEX pattern and not a content match makes it impossible to be used. The signature is going to generate lots of false positives and performance it will have performance issues due to running a REGEX everytime it matches a number. IDS/IPS is very sensitive to expensive signatures such as signatures that only has a REGEX and not a fixed content match that would match first and then attempting to match a REGEX. The signature matches a REGEX of numbers plus anything most to the left and to the right of the pattern. Anything preceding it and following the pattern will also match. This makes the signature match on almost every packet containing numbers followed by a dash. This pattern will match a lot even on encrypted traffic, SNMP traffic, and other network applications. The signature matches on a very broad pattern and cannot be used to drop traffic.

16. I also reviewed Rule SID 2005319, which found on page 45 of Ex. 1020, and reproduced below.

```
#from spyware LP data, by matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE
Bizconcept.info Spyware Checkin" ; flow:to_server,established;
content:"POST"; depth:5; nocase; uricontent: "/zuzu.php?&r="; nocase;
classtype:trojan-activity;
reference:url,doc.emergingthreats.net/bin/view/Main/2005319;
reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/MALWARE/
MALWARE_Bizconcept.info; sid:2005319; rev:3;)
```

17. Rule SID 2005319 would alert (but not drop) upon matching a TCP packet that contains a string “POST” in the beginning and contains a URI that includes the string “/zuzu.php?&r=”. This signature was not designed to be set to drop. Signatures that only have a short URL content match will false positive and should not be set to drop. There is a great chance of legitimate websites that have zuzu.php?&r= in the URLs, such as advertisements, making this rule prone to false positives. The signature was created to monitor for potential malware activity. But will not detect with 100% of accuracy based alone on a URL match that is very common. By setting this signature to drop it may also drop unintended urls.

18. I also reviewed Rule SID 2010234, which found on page 18 of Ex. 1020, and reproduced below.

```
#by anon 4
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET
CURRENT_EVENTS FakeAlert/FraudPack/FakeAV/Guzz/Dload/Vobfus/ZPack
HTTP Post 1"; flow:established,to_server; content:"POST"; depth:5;
uricontent: "/senm.php?data="; nocase; content: "data="; nocase;
```

```
classtype:trojan-activity; reference:url,  
threatinfo.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=TR0J_  
AGENT.GUZZ&VSect=T;  
reference:url,www.threatexpert.com/report.aspx?md5=7ca709f154e6abc678  
fbc4df8a3256b6; reference:url,www.threatexpert.com/threats/trojan-  
fraudpack-sd6.html; reference:url,doc.emergingthreats.net/2010234;  
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT  
_EVENTS/CURRENT_fakealerts; sid:2010234; rev:4;)
```

19. Rule SID 2010234 would alert (but not drop) upon matching a TCP packet that contains a string “POST” in the beginning and contains a URI that includes the string “/senm.php?data=” and then a string “data=”. This signature was not designed to be set to drop. Signatures that only have a short URL content match will false positive and should not be set to drop. There is a great chance of legitimate websites that have “/senm.php?data=” in the URLs, such as advertisements, making this rule prone to false positives. The signature was created to monitor for potential malware activity. But will not detect with 100% of accuracy based alone on a URL match that is very common. The “data=” content match will be unnecessary since the longest pattern match will match first and data= is a sub pattern of the longest content match. If it matches the URL pattern first it will match the subpattern “data=” making the rule inaccurate and prone to false positives. By setting this signature to drop it may also drop unintended urls.

20. I also reviewed Rule SID 2003326, which found on page 211 of Ex. 1020, and reproduced below.

```
#Blake Hartstein at Demarc  
#
```

```
alert tcp $EXTERNAL_NET $HTTP PORT5 -> $HOME_NET any (msg:"ET
WEB_CLIENT Apple Quicktime RTSP Overflow (1)";
flow:established,from_server; content:"|22|rtsp|3a|//"; nocase;
isdataat:400, relative; content:"|0a|"; distance:0; within:400;
content:"|22|"; distance: 0; within:400; classtype:attempted-admin;
reference:cve,2007-0015; reference:bugtraq,21829;
reference:url,doc.emergingthreats.net/2003326;
reference:url,www.emergingthreats.net/cgi-
bin/cvswb.cgi/sigs/WEB_CLIENT/WEB_Apple; sid:2003326; rev:6;)
```

21. Rule SID 2003326 would alert (but not drop) upon matching a TCP that is coming from an external-net address into a home-net address upon matching a packet that contains a string “rtsp://” and then is not followed by a linefeed and a double-quote. This signature has a short content match and is not accounting on the file type it intends to match. It cannot guarantee that the file is of the type of Apple Quicktime. Basically, will match on any packet that has the content “rtsp://” not followed by a line separator within 400 bytes. An Apple Quick Time file has different fields and data structures, and it is a binary file, it uses compression of its fields and the signature don’t have the resources of extracting the file from network traffic and parsing it, or even validating the file type. The signature roughly attempts to match a short pattern then checks if doesn’t have a one line separator byte ‘0x0a’ after matching the pattern. Files transitioning the network can be split in multiple packets and this signature might end up matching on different file types such as, movies, webpages, images and even compressed data due to the size of the content match being too short to match against network traffic flowing over HTTP ports. This signature was not designed to be set to drop since it may end up

dropping other traffic than an Apple Quick time download. This signature was not designed to be set to drop but to alert of potential file suspicious download.

22. I declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true, and that these statements were made with knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under section 1001 of Title 18 of the United States Code.

Executed this October 30, 2023, in Minas Gerais, Brazil.

A handwritten signature in black ink, appearing to read 'Pedro Marinho', is shown within a light gray rectangular box.

Pedro Marinho

CERTIFICATE OF SERVICE

The undersigned certifies, in accordance with 37 C.F.R. 42.6(e), and pursuant to agreement by the parties that filing with the Board through the Patent Trial and Appeal Case Tracking System (P-TACTS) constitutes electronic service, service was made on Petitioner as detailed below.

<i>Date of service</i>	October 30, 2023
<i>Manner of service</i>	Electronic Filing with the Board
<i>Documents served</i>	DECLARATION OF MR. PEDRO MARINHO IN SUPPORT OF PATENT OWNER'S RESPONSE
<i>Persons served</i>	REED SMITH LLP Gerard M. Donovan Peter J. Chassman Jonathan I. Detrixhe Sidharth Kapoor gdonovan@reedsmith.com pchassman@reedsmith.com jdetrixhe@reedsmith.com skapoor@reedsmith.com

/James Hannah/
James Hannah
Registration No. 56,369
Lead Counsel for Patent Owner