

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

KEYSIGHT TECHNOLOGIES, INC.,)
)IPR2023-00446
Petitioner,)U.S. Patent 10,567,343
)
v.)
)
CENTRIPETAL NETWORKS, INC.,)
)
Patent Owner.)
-----)

REMOTE PROCEEDINGS OF THE
DEPOSITION OF PEDRO MARINHO
TUESDAY, JANUARY 23, 2024

REPORTED BY NANCY J. MARTIN
CSR. NO. 9504, RMR, RPR
PAGES 1 - 129

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

KEYSIGHT TECHNOLOGIES, INC.,)
)IPR2023-00446
Petitioner,)U.S. Patent 10,567,343
)
v.)
)
CENTRIPETAL NETWORKS, INC.,)
)
Patent Owner.)
-----)

- - -
Tuesday, January 23, 2024
- - -

Remote Deposition of PEDRO MARINHO
beginning at 9:57 a.m., before Nancy J. Martin, a
Registered Merit Reporter, Certified Shorthand
Reporter. All parties appeared remotely.

1 A P P E A R A N C E S :
2

JEFFEREY H. PRICE, ESQ.

3 KRAMER LEVIN NAFTALIS & FRANKEL LLP

1177 Avenue of The Americas

4 New York, New York 10036

(212) 715-7502

5 jprice@kramerlevin.com

Counsel for Patent Owner

6

7

GERARD DONOVAN, ESQ.

8 JOHN WOROBIJ, ESQ.

REED SMITH LLP

9 1301 K Street, N.W.

Suite 1000 - East Tower

10 Washington, D.C. 20005

(202) 414-9200

11 gdonovan@reedsmith.com

Counsel for Petitioner

12

13

14

15

16

17

18

19

20

21

22

23

24

25

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

I N D E X

TESTIMONY OF PEDRO MARINHO	PAGE
BY MR. DONOVAN	5
BY MR. PRICE	123
BY MR. DONOVAN	124

EXHIBITS PREVIOUSLY MARKED

NUMBER	PAGE
Exhibit 1020	48
Exhibit 2031	9

1 BELO HOIZONTE, BRAZIL, TUESDAY, JANUARY 23, 2024;
2 9:57 A.M.

3 - - -

4 PEDRO MARINHO,
5 having been sworn/affirmed,
6 was examined and testified as follows:

7

8 EXAMINATION

9 BY MR. DONOVAN:

10 Q. Good morning, Mr. Marinho. My name is Gerard
11 Donovan, and I'll be taking your deposition today.
12 Since we're taking this remotely, I just wanted to
13 confirm you can hear me fine?

14 A. Yes, sir. I can hear you loud and clear.

15 Q. And you can see the Zoom screen?

16 A. I can see, yes.

17 Q. We're going to be marking a few exhibits
18 today, and we'll put them in the exhibit portal so you
19 can review the documents. We'll also be putting them
20 up on screen to hopefully make things easier for you.

21 If you want us to navigate to any portion of
22 the document that's on the screen, just let us know.

23 Okay?

24 A. Yes, sir.

25 Q. And since we're doing this remotely, I can't

Page 5

1 see what you're doing on your computer. Can you
2 confirm that you'll only use your computer to
3 participate in this deposition, you won't use it to
4 communicate with others while we're taking the
5 deposition?

6 A. I do confirm that I'm not communicating with
7 anyone using this computer during the deposition, yes.

8 Q. Great.

9 And if anyone does communicate with you
10 during the deposition over the phone or anything else,
11 can you tell us so we'll have a complete record?

12 A. Yes, sir. And my phone is turned off. So
13 it's impossible to contact me over the phone right
14 now.

15 Q. Perfect. That makes it easier.

16 Have you ever been deposed before?

17 A. Can you repeat the question, please?

18 Q. Sure. I'll rephrase it.

19 Have you ever had your deposition taken
20 before?

21 A. No. This is my first time.

22 Q. Okay. Then just to -- I'm sure your counsel
23 explained some of this to you, but today, I'm going to
24 ask you questions, and you have to answer those
25 questions truthfully.

1 Do you understand?

2 A. Yes, sir. Uh-huh.

3 Q. And if you have a problem understanding a
4 question I ask, can you let me know so I can attempt
5 to rephrase it?

6 A. Right. I can do that. Thank you. Yes.

7 Q. And today, Nancy will be taking down a
8 transcript of what we say. So please make sure your
9 answers are verbal, in words, as opposed to nods or
10 gestures.

11 Does that make sense?

12 A. Yes, of course. I will do that.

13 Q. Is there any reason you can't give complete
14 and truthful testimony today?

15 A. Can you repeat this question, please?

16 Q. Sure.

17 Is there any reason you cannot give complete
18 and truthful testimony today?

19 A. There isn't any reason why I could not give
20 complete testimony and tell everything I know about
21 it.

22 Q. Okay. Thank you.

23 A. Yes.

24 Q. And we'll probably take some breaks during
25 the deposition, but if you need a break at any time,

Page 7

1 just let me know and we can go off the record. I'll
2 just ask that you answer the question that's
3 outstanding before we take a break.

4 Does that make sense?

5 A. That makes sense, yes, sir.

6 Q. And you understand that you're under oath
7 today?

8 A. I do understand, yes, sir.

9 Q. Great.

10 Do you have any documents with you?

11 A. "Documents"?

12 Q. Yes.

13 A. Do you mean my driver's license? What kind
14 of documents?

15 Q. Do you have any documents relating to this
16 case with you within your deposition -- sorry, your
17 declaration or any other papers you reviewed in
18 relation to this case?

19 A. I do have what is on the -- what you guys
20 shared on the Veritext share that's the Exhibit 1020,
21 and the other one, it's the Exhibit 2031. That's what
22 I have.

23 Q. Those are the only documents you have?

24 A. Let me -- I also have what was -- legal team
25 sent to me about this deposition that is SNORT rules

1 and about the proceeding.

2 Q. I don't need to know about any communications
3 from your counsel to you. If you refer to any
4 documents today during the deposition, will you please
5 let us know what you're referring to?

6 A. Yes, sir. I will do.

7 MR. DONOVAN: Thank you. Let's first bring
8 up Exhibit 2031.

9 (Previously marked Exhibit 2031 was made
10 available to the witness.)

11 THE WITNESS: Are you sharing your -- okay.

12 BY MR. DONOVAN:

13 Q. It's shared on screen. That's hopefully
14 easiest for you, but you also have the document if you
15 need to refer to anything.

16 A. Okay.

17 Q. And do you see Exhibit 2031?

18 A. I do see it, yes, sir.

19 Q. And do you recognize this as the declaration
20 that you signed on October 20 of 2023?

21 A. I do.

22 Q. Okay. Again, if you need us to navigate to
23 any portion of the document, just let us know.

24 A. Yes, sir.

25 Q. Let's first turn to Paragraph 2. It says,

1 that "Since March 2019" you've "been a Senior Security
2 Analyst at Centripetal Networks ('Centripetal')."

3 Is that still the case?

4 A. Yes, sir.

5 Q. And has your role at Centripetal remained the
6 same the entire time?

7 A. Yes, it did.

8 Q. And what is your role at Centripetal?

9 A. I work with threat intelligence. I'm an
10 intelligence analyst. My role is to like watch out.
11 I'm like a -- what can I say? I'm like a sentinel.
12 I'm watching my clients' network, looking at the
13 events, and reporting to them anyone that is a threat
14 that is on their environment and it was detected by a
15 threat intelligence gateway.

16 And that's what I do. I do report to the
17 clients, manage the CleanINTERNET, the policies of
18 threat intelligence that we are using to shoot
19 malicious threats. And that's basically what I do.

20 Q. What do you mean you manage the policies that
21 are used to shoot malicious threats?

22 A. Policies are viewed on the system that
23 protect the clients' network, and these policies have
24 the so-called indicators of compromise, and these
25 indicators of compromise are units, such as ID

1 addresses, domain names, and other indicators, such as
2 URLs. So we use that to correlate the network traffic
3 with a potential threat.

4 Q. You said, "URLs"?

5 A. URL is one of the types of indicators of
6 compromise, yes, sir.

7 Q. How is a URL an indicator of compromise?

8 A. A URL -- we work with a complete URL from
9 Anjuan (phonetic), and these URLs, they are provided
10 to be sent by the threat intelligence providers. So
11 we work with more than one threat intelligence
12 provider, and these URLs are observed by these threat
13 intelligence providers as a sign that someone
14 navigated, for example, to one of these URLs when
15 clicking on a phishing link, for example.

16 The link to a phishing website is actually a
17 URL. So these URLs -- when the Centripetal system
18 matches one of these URLs against the network traffic,
19 it is emitted an event, and it's on this event that we
20 as analysts are looking for these pieces of evidence,
21 these events to report to the client that something
22 malicious could have happened on their network.

23 Q. And in -- I'm sorry. Did you have more to
24 say?

25 A. This is what I have about the URLs.

1 Q. And where in the traffic would you find the
2 URL?

3 MR. PRICE: Objection. Foundation.

4 THE WITNESS: Can you repeat the question?

5 BY MR. DONOVAN:

6 Q. Sure.

7 If I understood correctly, you're explaining
8 that you would check traffic for the URL. And so my
9 question is where in the traffic would you find the
10 URL?

11 A. Where in traffic? Usually, we see URLs on
12 the -- on the tracker of the HTTP protocol. That's
13 where we see URLs.

14 Q. And in an HTTP protocol packet, where would
15 the URL be found?

16 A. On the HTTP header.

17 Q. And that would be an application packet
18 header; is that correct?

19 A. The HTTP is an application protocol. So
20 that's correct, yes, sir.

21 Q. Let's turn -- back in Paragraph 2 it says,
22 "Before joining Centripetal" you "obtained a
23 Bachelor's in computer science in 2010 from Pontifical
24 Catholic University of Minas Gerais."

25 I may have not pronounced that great, but is

Page 12

1 that correct?

2 A. That's correct, sir. Yes.

3 Q. And what years did you attend the university?

4 A. In which state?

5 Q. No. In what years did you attend the
6 university?

7 A. I joined in 2001. 2001, and I left in 2010.

8 Q. Sorry. 2001 to 2010?

9 A. Yes, sir. Yes.

10 Q. So you were at the university for nine years?

11 A. That's correct. Yes.

12 Q. While you were at the university, did you
13 have any courses that related to Emerging Threats?

14 MR. PRICE: Objection. Form.

15 THE WITNESS: To Emerging Threats, no, I did
16 not.

17 BY MR. DONOVAN:

18 Q. When did you first come to learn of Emerging
19 Threats?

20 A. When I was in the university, I got an
21 internship where I used to manage IDSes, intrusion
22 detection systems, and that's how you found out about
23 the Emerging Threats ruleset because I found it to be
24 very useful to have on my IDSes so that we could flag
25 potential threats. This is how I heard about Emerging

1 Threats.

2 Q. And who was that internship with?

3 A. I was making an internship with the -- a
4 company in Brazil called -- I can't remember right
5 now. It's a company that doesn't exist anymore, but
6 their name is IT system, if I'm not mistaken, or
7 something like -- I cannot remember, sorry, the name
8 of the company.

9 Q. That's no problem. Do you recall what years
10 you interned there?

11 A. It was before 2010.

12 Q. Do you recall --

13 A. 2010, between like 2008 and 2010 or something
14 like that. Yes.

15 Q. Did someone there inform you about Emerging
16 Threats?

17 A. No. I saw on the SNORT mailing list that I
18 participated. There was a SNORT mailing list where
19 people discuss the rules, the SNORT rules, ask
20 questions, and I participated on this mailing list.
21 And then I saw some people from Emerging Threats also
22 answering questions.

23 So I thought that I should also join the
24 other mailing list for Emerging Threats. This is how
25 I found out about it.

1 Q. And SNORT, that's S-N-O-R-T; is that correct?
2 A. Yes, sir.
3 Q. What is SNORT?
4 A. SNORT is an intrusion prevention system.
5 Q. And you refer to a "SNORT mailing list."
6 What is that?
7 A. It is a mailing list that people that uses
8 SNORT, the users, they participate -- so you subscribe
9 to this mailing list, and you will receive E-mails
10 about it with people asking questions to the SNORT
11 team, and the SNORT team would answer these questions
12 regarding the rules, the signatures, and other topics,
13 such as SNORT configuration, all of that.
14 Q. And how did you learn about the SNORT mailing
15 list?
16 A. Just because on this internship, I had to
17 manage SNORT and I start researching on the Internet
18 about more information about it, and this is how I
19 found that you could subscribe to this mailing list
20 and participate and ask questions, and the SNORT
21 developers -- not the developers, but people that work
22 with SNORT at the time, they would answer your
23 questions.
24 And I even made a couple of questions there
25 about something that I needed to know and I didn't.

Page 15

1 So it was a useful way of finding answers to these
2 questions.

3 Q. And you also referred to an Emerging Threats
4 mailing list; is that right?

5 A. Yes.

6 Q. What was that?

7 A. Just like the SNORT mailing list. So you
8 subscribe to it. You give your E-mail, and you start
9 receiving E-mails with questions, and you can ask
10 questions. They answer questions about their
11 rulesets, and this is a mailing list. Yes.

12 Q. And is it correct that you learned about the
13 Emerging Threats mailing list by your participation on
14 the SNORT mailing list?

15 A. That is correct. I've seen people from the
16 Emerging Threats mailing list answering questions,
17 asking questions to the SNORT team, and they were
18 answering. And then I realized that there was an
19 Emerging Threats, and they were very good on writing
20 these signatures too.

21 Q. And do you recall when you learned of
22 Emerging Threats?

23 A. Pardon me? Can you ask me again?

24 Q. Yes.

25 Do you recall when you learned of Emerging

1 Threats?

2 A. I can't recall exactly the year, but it was
3 before 2010, while I was in college.

4 Q. So sometime between 2001 and 2010?

5 A. That's right.

6 Q. And when the people from Emerging Threats
7 were responding to the SNORT mailing list, was that
8 responding to everyone in the SNORT community?

9 A. That is right, yes.

10 MR. PRICE: Objection. Form.

11 BY MR. DONOVAN:

12 Q. Would it be correct that anyone receiving the
13 SNORT mailing list would have seen E-mails from the
14 Emerging Threats team?

15 A. Yes, that's right. If you reply to the
16 mailing list, everybody that is receiving the E-mail
17 would see the reply.

18 Q. And were you a member of the mailing so you
19 received all the replies on the SNORT mailing list?

20 A. Yes, I was a member of both mailing lists.
21 Both the Emerging Threats and also the SNORT mailing
22 list.

23 Q. Got it.

24 A. Yes.

25 Q. Were you aware of Emerging Threats having a

1 website as well?

2 A. Yes.

3 Q. And what was the Emerging Threats website?

4 A. I believe it was EMERGINGTHREATS.NET, if I'm
5 not mistaken.

6 Q. Did it have a different name before it had
7 the name Emerging Threats?

8 A. It used to be called bleeding edge or
9 bleeding something. I cannot remember exactly because
10 it's so long time ago. More than 13 years ago.
11 Bleeding. Bleeding edge. I believe it was bleeding
12 edge, but I cannot confirm that.

13 Q. Was it the same team that was with the
14 bleeding edge or bleeding SNORT project that then
15 became Emerging Threats?

16 A. That is right.

17 Q. Was it the same ruleset that was with either
18 bleeding edge or bleeding SNORT that then became
19 Emerging Threats?

20 A. It was the same ruleset that later got
21 expanded and improved, yes.

22 Q. And when you say, "ruleset," what is the
23 Emerging Threats ruleset?

24 A. Emerging Threats ruleset is a set of rules to
25 Suricata, which is an intrusion protection system, and

1 also SNORT are the signatures that these IDS systems
2 do use.

3 Q. And how -- well, did you ever download the
4 Emerging Threats ruleset from the Emerging Threats
5 website?

6 A. Yes, I did.

7 Q. And when did you first do that?

8 A. I believe it was when I was in the internship
9 before the year of 2010.

10 (Indiscernible crosstalk.)

11 THE WITNESS: Yes.

12 BY MR. DONOVAN:

13 Q. How did you download the ruleset from
14 Emerging Threats?

15 A. Navigating through the website and
16 downloading a file that was compressed with all the
17 rule files in it.

18 Q. Do you recall how you were able to find that
19 from the website?

20 A. I was able to find it on the website, yes,
21 sir. That's right.

22 Q. I'm sorry. But do you recall how you were
23 able to find it? Do you recall where on the website
24 you had to go to find it?

25 A. /rules or something like that. A URL like

1 that, rules -- /rules, I believe.

2 Q. Was there a link to download it from the home
3 page, do you recall?

4 A. Yes, I believe so.

5 Q. Did you have any trouble downloading the
6 rules from the Emerging Threats ruleset?

7 A. No, never had a trouble downloading it. Just
8 as easy as clicking on a link and download, and yes.

9 Q. And when you download that, though, that
10 would download a file with all of the rules from the
11 Emerging Threats; is that right?

12 A. That's right, yes. That's correct.

13 Q. You said you learned of the Emerging Threats
14 ruleset from your work with SNORT rules. Did you
15 learn of any other third-party providers of SNORT
16 rules?

17 A. Not that I can remember. I don't think we
18 had one outside of Emerging Threats. Yeah. No.

19 Q. Was Emerging Threats the most well known
20 third-party provider of SNORT rules at the time?

21 A. I mean yes. I believe so because they were
22 the only one. So I believe so. Had another one? I
23 simply don't know.

24 Q. Did you have any other -- other than the
25 internship, did you have any other positions where you

1 managed intrusion detection systems?

2 A. No, sir.

3 Q. Did you know other people that managed
4 intrusion detection systems?

5 A. Did I know? Only the people that were
6 replying on the mailing list. I mean I didn't even
7 know them. I was the only one, I guess, that used to
8 work with that.

9 Q. You were the only person in your internship
10 that worked with managing IDSes?

11 A. Yes, sir.

12 Q. Did other people on the mailing list manage
13 IDSes?

14 A. On the mailing list, yes. Lots of people
15 managed IDS.

16 Q. And that's -- what do you mean when you say,
17 "lots of people managed IDSes"?

18 A. I mean because there were so many questions
19 about the rules, about false positives, about SNORT on
20 the mailing list that these people, they can only work
21 with IDS. Otherwise, why would they ask these
22 questions; right?

23 Q. Do you know how large the community was that
24 used the SNORT mailing list?

25 A. I have no idea.

1 Q. Would you expect it's at least thousands of
2 people?

3 MR. PRICE: Objection. Calls for
4 speculation.

5 THE WITNESS: I can't say because I don't
6 know the exact number.

7 BY MR. DONOVAN:

8 Q. Do you know why the name changed from either
9 bleeding SNORT or bleeding threats to Emerging
10 Threats?

11 A. I don't know. I didn't work -- when that
12 happened, I didn't work through Emerging Threats
13 officially, and I didn't work with marketing in my
14 life. So I have no idea why they changed the name.

15 Q. The company was -- or the project was
16 Emerging Threats when you became an employee; is that
17 right?

18 A. That's right.

19 Q. Okay. And that was in 2010?

20 A. When I became an employee it was -- I mean I
21 was not an employee. I was like third party working
22 from -- remotely to Emerging Threats, not an employee.
23 So it was in 2010 that the Emerging Threats asked me
24 if I wanted to work full time for them as a
25 contractor, and I accepted because that job was fun.

Page 22

1 I love to write IDS rules. It's challenging,
2 and, so yes.

3 Q. So in Paragraph 3 of your declaration you
4 say, "I worked at Emerging Threats as a Malware
5 Analyst and Vulnerability Researcher from November
6 2010 to January 2016." That was -- that's as a
7 contractor for Emerging Threats?

8 A. Yes, sir.

9 Q. So starting in November 2010 you were a full
10 time contractor, and at that time the company was --
11 or the project was called "Emerging Threats."

12 Is that fair?

13 A. That is fair, yes.

14 Q. And you first started using Emerging Threats
15 rules, though, before you started as a contractor with
16 Emerging Threats; right?

17 A. That is right.

18 Q. And we talked about downloading the rules
19 from the website.

20 How do you use the rules after you download
21 them?

22 A. You just get these rules and you copy them to
23 a directory where the IDS system will read these rules
24 when it's loading up its process, and it will load all
25 of the rules, and it will start inspecting network

Page 23

1 traffic and matching the network traffic against the
2 rules. This is how.

3 You copy to a directory, and you would start
4 the process with the command.

5 Q. And you yourself did download the rules and
6 used them with an IDS system at that time?

7 A. That is right, sir.

8 Q. And when you loaded the rules into the
9 system, did you use all of the rules in the Emerging
10 Threats ruleset?

11 A. No, not all of the rules because there are
12 rules that do generate lots of false positives. So we
13 cannot enable all of the rules. There are rules that
14 are so expansive, in terms of CPU sites that these
15 rules would require to run in trying to match against
16 network traffic, that it makes them unusable. And a
17 lot of the rules -- all of these rules that are on
18 these -- I don't even know how to say this.

19 All of these rules, they have a very bad
20 performance. I can say that. They have a really bad
21 performance, and they do generate false positives.
22 So, for example, the rules that -- for top secret, you
23 can't use that rule because it generates too many
24 false positives.

25 Q. So whether -- I'm sorry. Did you have more

1 to say?

2 A. Yeah. A lot of these rules are commented out
3 on the files because they are just generating a lot of
4 false alarms, and this is why I am answering that I
5 don't use all of the rules. Nobody does, yes.

6 Q. When you load the Emerging Threats ruleset
7 into an IDS, did you use all of the rules that were
8 not commented out?

9 A. Not all of the rules because there are some
10 rules that are only checking for IP addresses, and
11 these rules that only check on the IP header just the
12 values of the IP address, they're so expansive that
13 SNORT have some performance problems if we enable all
14 these rules.

15 So even though these rules are not set -- are
16 not commented out, I did not use these rules files for
17 rules that are just an IP match.

18 Q. So you would disable those rules when you
19 were loading them into the IDS? Is that how you would
20 manage that so you would not get the false positives?

21 A. That is correct, sir.

22 Q. And would you ever enable rules for a system?

23 A. Enable rules. I don't remember having to
24 enable a specific rule to detect something. Yeah,
25 that didn't happen.

1 Q. Did you ever modify any rules?

2 A. "Modify any rules." I -- what do you mean by
3 modify a rule?

4 Q. Did you ever take a rule that you saw on
5 Emerging Threats, or anywhere else, and then make
6 changes to the rule to implement it in your IDS?

7 A. No, I did not.

8 Q. When you said the name of the IDS you were
9 working with, what was that?

10 A. Suricata.

11 Q. Is that S-u-r-i-c-a-t-a?

12 A. Yes, sir.

13 Q. And were there any other IDSes that you were
14 aware of at that time?

15 A. These are the only two that I had contact
16 with. So they could have others, but I did not work
17 with them.

18 Q. The two being SNORT and Suricata?

19 A. Yes, sir.

20 Q. And are you aware of what Sourcefire is?

21 A. Sourcefire, yes, it was a company back then.

22 Q. Were you aware of Sourcefire back in the 2008
23 to 2010 time frame?

24 A. If I knew about it?

25 Q. Do you recall if you knew about it at the

1 time?

2 A. I'd heard about it, yes. Sourcefire. They
3 were the ones that developed SNORT.

4 Q. And back then, what did you understand
5 Sourcefire to be?

6 A. A company that developed SNORT and had the
7 ruleset for SNORT. It was a company founded by Martin
8 Roesch. I think he was the guy that founded that
9 company. And this is everything that I knew about it.
10 They had, of course, an IPS system, appliance, but
11 I've never seen that appliance. I only worked with
12 SNORT.

13 Q. And then "IPS," that stands for intrusion
14 protection system?

15 A. Intrusion prevention system.

16 Q. Intrusion prevention system. Thank you for
17 the clarification.

18 So SNORT was an intrusion prevention system;
19 is that -- sorry. Sourcefire was an intrusion
20 prevention system; is that right?

21 A. Sourcefire, yes.

22 Q. And it would use -- is it correct that it
23 would use SNORT rules?

24 A. That is correct, sir.

25 Q. So you could load rules from Emerging Threats

Page 27

1 into Sourcefire to use those rules; is that right?

2 A. Could you repeat the question? Sorry.

3 Q. Sure. Someone could load rules from Emerging
4 Threats into Sourcefire to use the rules; is that
5 right?

6 A. From Emerging Threats on Sourcefire. Yes.
7 Sourcefire, I didn't work with this IPS. I only
8 worked with SNORT. SNORT. Because the Sourcefire, it
9 was an appliance, and you have -- I've seen, you have
10 a graphic interface to manage the rules and all of
11 that. I've never worked with that, unfortunately.

12 The only one I worked with was with SNORT.
13 SNORT, you download it, you install it, and you run it
14 as a demonstrative on a Linux or Unix system, and you
15 can load -- the answer to your question, yes, you can
16 load the Emerging Threats rules on SNORT, but I'm not
17 sure if you can load them on Sourcefire because I've
18 never done that.

19 Q. Okay. Did you use SNORT IPSes or intrusion
20 prevention systems in addition to SNORT IDSes or
21 intrusion detection systems?

22 A. No, sir.

23 Q. And what's the difference between an
24 intrusion detection system and an intrusion prevention
25 system?

1 A. The difference, I think both do the same
2 thing, but only the intrusion prevention system, you
3 can also have the option to drop traffic, which IPS --
4 IDS is like only monitoring, and IPS is actually
5 dropping traffic.

6 Q. And what's the difference between monitoring
7 and dropping traffic?

8 A. Monitoring, you have a signature that will
9 meet an alert when it matches against the network
10 traffic, and it only emits an alert. It doesn't
11 modify the network threat or act to queue up a
12 connection, stop a connection, reset a connection.

13 And IPS, it can actually drop packets
14 accordingly to the rules that you have that will match
15 the network threat and drop if it matches.

16 Q. And do you know how a rule would be written
17 to either alert traffic or drop traffic?

18 A. Yes, sir. There is an action. Each one of
19 these rules have a keyword that is an action. The
20 action keyword, you have three options or two. You
21 can alert. So the rule would have the keyword alert
22 if it is an IDS rule that is monitoring threat.

23 If the action is drop, you have drop as the
24 action on a rule, it will actually drop traffic.
25 That's the difference between a rule that monitors and

1 one that drops traffic.

2 Q. And if you implanted a rule -- well, could
3 you take a rule that was written to alert and
4 implement it on an IPS to drop traffic?

5 A. You can do that, but you are modifying a rule
6 that like was not designed to actually drop traffic
7 because usually, the rules that are written to alert,
8 they may generate a false positive.

9 So if you drop the traffic, you may end up
10 dropping legitimate traffic, and that will have a
11 negative impact on the customer network. So you can
12 do that, but you need to be very careful to not cross
13 the line between what I can drop and what I cannot
14 drop because these rules they are not exact.

15 When you are matching a network traffic, it's
16 very complicated, and it simply generates lots of
17 false positives sometimes. It's inevitable, and this
18 is why the great majority of the people that work with
19 IDS, they choose not to drop traffic using these rules
20 because of false positives. And this is what I know
21 about, best of my knowledge.

22 Q. And if you were going to change a rule from
23 an alert rule to a drop rule, how would do you so?

24 A. To change a rule from an alert rule to a drop
25 rule, you would have to replace the keyword of the

1 action that is alert with the keyword of the action
2 that is drop.

3 Q. And have you ever had a job where you managed
4 intrusion prevention systems?

5 A. No, I haven't, sir.

6 Q. So your experience is limited to managing
7 IDSes?

8 A. That is correct.

9 Q. On Paragraph 3 of your declaration, you say
10 you "worked at Emerging Threats as a Malware Analysis
11 and Vulnerability Research from" 2010 -- "November
12 2010 to January 2016," and we discussed that you were
13 a contractor at that time.

14 What was your role in that position?

15 A. My role was -- can I say about this.
16 Emerging Threats had a way -- I cannot get into too
17 many details, but a secure way of executing malware
18 and extracting from the malware execution information
19 about which URL the malware is accessing, what IP
20 address is communicating, what is sending out over
21 network traffic. What kind of processes it is
22 creating on the operational system and other
23 information that would enable us to view a signature
24 that would match some aspect of the malware
25 communication over the network.

1 This was the malware analysis. The
2 vulnerability was we have plenty of vulnerabilities,
3 and these vulnerabilities are grouped as they are
4 indexed by a common vulnerability enumeration that
5 rates the criticality of the vulnerabilities. The
6 great majority of the vulnerabilities is not detected
7 by an IDS. It was not detected in 2010. It is not
8 detected today.

9 The great majority of the vulnerabilities --
10 there is a small portion of vulnerabilities that
11 are -- it's possible to create a rule that will match
12 an attempt to exploit that vulnerability. There's a
13 small portion we can create IDS rules that would match
14 on an attempt to exploit these vulnerabilities. So
15 that was the other side of my drop.

16 The vulnerability side where I used to go
17 through all of these proof of concepts exploits and
18 execute them and see what people was sending over the
19 network and trying to create a signature that would
20 match these attacks.

21 Q. And what do you mean by creating a signature
22 that would attempt to match an attempt to -- I'm
23 paraphrasing, but exploit a vulnerability?

24 A. Yes. A computer's vulnerability, it is a
25 condition that enables that a threat actor can take

1 advantage of a problem that it has on the source code
2 of that application that allows the threat actor to
3 execute code and to gain unauthorized access to a
4 system so that we have a piece of code that would
5 launch a malicious payload against a system that is
6 vulnerable, and this malicious code would have in its
7 byte the conditions that would enable this malicious
8 code to be run on the target system.

9 So when this happens over the network, which
10 is not all of the cases, we have the great majority of
11 the vulnerabilities we cannot detect over the network
12 with an IDS and IPS.

13 So the small portion of vulnerabilities that
14 we can actually create some sort of IDS rule to be
15 able to at least flag on a potential attempt to
16 exploit a vulnerability, yes, then I would go and
17 write an IDS rule that would flag or alert that there
18 is a potential for an attempt to exploit a
19 vulnerability. I'm not sure if that's clear.

20 Q. I think it's helpful.

21 When did you start writing, I guess, SNORT
22 rules, if that's the right terminology?

23 A. When I started was back in like 2010 or
24 something like that because I started as, more or
25 less, a vulnerability researcher, and one of my jobs

1 was exactly write these rules. So I would say like
2 2010 or so.

3 Q. And did you contribute any rules to the
4 Emerging Threats ruleset before 2010?

5 A. Yes. Yes, I did. This is how -- and I was
6 invited to participate, to join Emerging Threats
7 because I was volunteering, submitting rules to the
8 Emerging Threats mailing list. One of the things of
9 the mailing list was the ability you had to provide
10 the rules to the mailing list, and the guys from
11 Emerging Threats they would evaluate your rule, and if
12 it was a good rule, they would include it on the
13 rulesets.

14 So yes. The answer is yes.

15 Q. So before you started at Emerging Threats in
16 November of 2010, you had submitted rules to the
17 Emerging Threats ruleset that you wrote; is that
18 right?

19 A. That is right, sir.

20 Q. And how did you learn to write those rules?

21 A. Reading documents about the rule syntax,
22 about how these rules actually work, and trying to
23 understand and looking at examples, like because I
24 work with IDS, I could see the rule and I could see
25 the network traffic, it matches at.

1 So I start understanding the mechanics of how
2 these rules work. It was easy for me. I was a
3 computer science student. So to write one rule, it's
4 just one line. It's one line of code. It doesn't do
5 magic, though. It cannot prevent like data
6 exfiltration. One rule cannot prevent data
7 exfiltration.

8 To prevent data exfiltration you need much
9 more than just an IDS. But back in the time, this was
10 how I learned how to write these rules, yes, sir.

11 Q. And you say a rule is just one line of
12 syntax. Can you just briefly explain what's contained
13 in the SNORT rule?

14 A. I can, yes, sir. So it starts with the
15 action. We have alerts or we have drop, and then we
16 have the protocol. It could be TCP. It could be UDP.
17 It could be an application layer protocol. No. SNORT
18 doesn't have that. Sorry. So it could be TCP, UDP,
19 or IP.

20 Then we have the header of the addresses --
21 the header of the rule that says that the direction of
22 the traffic. You have -- like home net, for example,
23 is the -- my network, and then you have the external
24 network. That means that from the home network to the
25 external network, that's the direction outbound of the

1 traffic. If you have like external network, and then
2 home net, that means it will match only on inbound
3 traffic coming through your network.

4 So then we have the rule options. You have a
5 parenthesis, and then you have the rule options. It
6 doesn't have an order, but usually, we start with the
7 message of the rule, what we are going to see on these
8 events -- like it could be like exploit against
9 Microsoft Windows IIS server, CVE, and the common
10 vulnerability enumeration attempt, for example.

11 A message that we can immediately know that
12 these alert means what's happening. Then we have the
13 other options that are the content matches, and the
14 content matches modifiers. So we have different
15 modifiers for these content matches so that we can
16 match on the network traffic, on protocol fields, on
17 any values that we need to match in order to emit an
18 event that will help the network administrators to
19 start an investigation or to correlate that event with
20 other systems -- other systems to start an
21 investigation.

22 So this is exactly what I did.

23 Q. And this is what you started doing before you
24 joined Emerging Threats. You were writing these rules
25 and then submitting them to the Emerging Threats

1 mailing list; is that right?

2 A. Because I was asking questions one day,
3 someone from Emerging Threats asked me if I wanted to
4 volunteer to work for them for free just to learn
5 about how to write these rules, and then they gave me
6 access to these secure environment where we can
7 execute malware and -- in a secure way and analyze
8 what the malware is saying over the network, what is
9 happening.

10 And based on that, I started submitting rules
11 to the Emerging Threats based on this research. I
12 performed that for free because I was just learning
13 about it, and I thought it was a great opportunity.
14 Yes, sir.

15 Q. That work you did for free for Emerging
16 Threats, was that prior to you becoming a contractor
17 in November of 2010?

18 A. That's correct, sir. While I had the
19 internship that I worked with IDS, at the same time I
20 was volunteering to -- to research malware and to
21 develop a signature for Emerging Threats for free,
22 just to learn.

23 Q. And so this is also while you were a student.
24 So prior to 2010 you were both a student at the
25 university and you were an intern managing IDSes, and

1 you were volunteering with Emerging Threats; is that
2 right?

3 A. That is right.

4 Q. And during that time, you wrote SNORT rules
5 that you submitted to Emerging Threats through the
6 mailing list?

7 A. That's correct.

8 Q. And then do you know how Emerging Threats
9 determined which of the rules submitted through the
10 mailing list made it onto their all rules ruleset?

11 A. Back on this time I did not. I only found
12 out how they did that, how they curated the rules
13 after I joined. I didn't have any participation on
14 the vetting of the rules.

15 Q. When you joined Emerging Threats in November
16 of 2010, did you then learn how they curate the rules
17 for the all rules ruleset?

18 A. Yes.

19 Q. And how was that done?

20 A. I cannot talk about that because this is a
21 proprietary information about processes of this
22 company, and I cannot reveal about like -- their
23 internal process, I cannot talk about that.

24 Q. Without going into their internal processes,
25 were all rules that were submitting to the mailing

1 list, did they all make it onto the all rules ruleset?

2 A. Not all of the rules because there was a
3 bunch of rules that just like the -- these rules that
4 are on these documents, they have a very bad
5 performance, and sometimes they used to discard these
6 rules or even ship the rules with a comment sign
7 before the rule so that the IDS engine would not load
8 these rules.

9 So not all of the rules would make it into
10 the all rules ruleset.

11 Q. When you were an intern -- or is "intern" the
12 right terminology for your work at Emerging Threats
13 before you started in November 2010?

14 A. No. To Emerging Threats, I was not an
15 intern. I was a volunteer. But yes.

16 Q. When you were a volunteer in Emerging
17 Threats, how many people did you work with at Emerging
18 Threats?

19 A. I can't say for sure how many people worked
20 in the Emerging Threats back at the time because I
21 mean I only had contact with like two or three people.
22 So I cannot say like how many people did work to
23 Emerging Threats when I joined because I didn't know
24 everybody.

25 Q. And were there other volunteers assisting

1 Emerging Threats at the time?

2 A. I'm sure they did, but I cannot remember
3 their names, but yes, we used to have more people that
4 would volunteer, submit rules for Emerging Threats,
5 but I just can't remember.

6 Q. Do you recall how many volunteers there were
7 that you worked with?

8 A. I don't remember.

9 Q. Did you work on a SAN net project?

10 MR. PRICE: Objection. Foundation.

11 THE WITNESS: "Sand net project." That is
12 the name of a system where we can execute more
13 security. So yes, but I didn't develop it. My job
14 was just to use it. I was a user of this system.

15 BY MR. DONOVAN:

16 Q. And how did you use the SAN net system?

17 A. Executing malware. You have a malware table.
18 You execute it, and then you get all the logs about
19 the malware execution, what it did, and what it
20 communicated over the network so that you can analyze
21 and potentially write in ideas to match on some
22 aspects of the malware communication.

23 Q. Do you know how large the Emerging Threats
24 community was before you joined Emerging Threats?

25 A. I don't know if it was big or not. I can't

1 say that.

2 Q. And do you know, once you joined, how many
3 people were involved in the Emerging Threats
4 community?

5 A. I can't say for sure.

6 Q. Can you estimate?

7 A. I cannot estimate because I can't say it's
8 100 people or 1,000 people. I just don't know.

9 Q. Do you know how many people submitted rules
10 to Emerging Threats?

11 A. It was not a lot of people that did that. It
12 was not a lot of people, and -- but we used to have
13 some submission of rules, but it was not a lot.

14 (Indiscernible crosstalk.)

15 BY MR. DONOVAN:

16 Q. I'm sorry. I didn't mean to speak over you.
17 Did you have more to say?

18 A. No, sir.

19 Q. Do you know how many people were downloading
20 rules from Emerging Threats?

21 A. I don't know how many people. Really, I
22 didn't have access to the logs of the system to say,
23 "Hey, today we got like that many thousand downloads."
24 I have no idea. My job was not this one. I was not a
25 system administrator. My job was just to create these

1 rules and -- and testing.

2 Q. Were you aware of any conferences where
3 Emerging Threats rules were discussed?

4 A. I don't -- I never heard of a conference
5 where Emerging Threats rules were -- I never heard of
6 a conference where Emerging Threats rules were
7 discussed back in that time. No. Not aware of that.

8 Q. So you've never attended a conference where
9 Emerging Threats rules were discussed?

10 A. I've never. I've never had time to go and
11 travel and -- I mean I've never heard of any
12 conference exclusively to discuss Emerging Threats
13 rules. I don't think that ever happened. So the
14 answer is no.

15 Q. Are you aware of conferences at which
16 Emerging Threats rules were discussed?

17 A. No, sir.

18 Q. Even if they were discussed in addition to
19 other material?

20 A. They probably were not discussed on a
21 conference. I know about the conference of the open
22 security -- open, O-I-S-F. Open security foundation,
23 information foundation, which was the foundation that
24 created Suricata, and probably they would discuss
25 rules on this OISF Suricata conferences, but it's not

1 about the rules. It's about the engine, Suricata.

2 There were lots of other topics that were
3 discussed besides rules on these Suricata conferences.
4 But I never attended to one of these.

5 Q. Do you know when those conferences were?
6 Were they prior to 2010?

7 A. They were not prior to 2010 because Suricata
8 was under development. So they happened, like years
9 later.

10 Q. In Paragraph --

11 A. Yes, sir.

12 Q. I'm sorry. Did you have more?

13 A. No, sir.

14 Q. Paragraph 4 of your declaration it says you
15 "worked on vulnerability research and malware
16 analysis." We discussed a little bit of that before.

17 In that role, are you familiar with a
18 category of cyber attacks known as "exfiltration"?

19 A. Yes, sir.

20 Q. And what is exfiltration?

21 A. Exfiltration is unauthorized leak of
22 confidential data, confidential files. So it's like
23 stealing.

24 Q. So you consider stealing sensitive data or
25 credentials via the Internet to be a form of

1 exfiltration?

2 A. Yes, sir.

3 Q. It also says you "tested, built, and
4 optimized SNORT and Suricata signatures for Emerging
5 Threats Pro."

6 What is a SNORT signature? Is that what we
7 were talking about before with SNORT rules?

8 A. That's correct, sir.

9 Q. And so --

10 A. I said is not a rule, yeah.

11 Q. Are those terms the same thing as -- is a
12 SNORT signature another name for a SNORT rule?

13 A. That's right, yes.

14 Q. And what's "Emerging Threats Pro"?

15 A. Emerging Threats Pro is a subset of the
16 Emerging Threats rule that you got to pay a
17 subscription in order to download this -- this subset.

18 Q. Is there a difference -- is there also an
19 Emerging Threats Open?

20 A. That's right, yes, sir.

21 Q. And what's the difference between Open and
22 Pro?

23 A. Open are rules under GPL license, and people
24 can download it and people can submit their own rules.
25 People can ask questions about it openly. It used to

1 be like that. Today, I don't know how Emerging
2 Threats handles that, but back in the time, people
3 participated on the mailing list would discuss these
4 open rules, submit rules.

5 Eventually the submitted rules would get into
6 the Open ruleset, and there was no -- you could
7 download it for free.

8 The Pro you would have to pay a license to be
9 able to download these rules. And that's the main
10 difference.

11 Q. And when you said prior to your work at
12 Emerging Threats you were able to go to the website
13 and download the all rules, those would have been the
14 open rules; is that correct?

15 A. That's correct, yes.

16 Q. This next paragraph, Paragraph 5, refers to
17 the Emerging Threats reference, and then you have the
18 archived URL. It shows "emerging-all.rules." Is that
19 the all rules ruleset that you were referring to
20 before that you would download from the Emerging
21 Threats website?

22 A. That is right, sir.

23 Q. And when you say you were familiar with the
24 list of Emerging Threats rules, what do you mean by
25 that?

1 A. Because I've worked with the rules. One of
2 my jobs was to not only develop the rules, but also,
3 after I joined as a full time contractor, I used to
4 test the rules for performance and false positives,
5 QA, vetting the rules. So this is why I'm familiar
6 with the Emerging Threats rules.

7 I know lots of these rules, and I wrote lots
8 of these rules. So this is why I'm familiar.

9 Q. And this Emerging Threats reference was from
10 the rules in December of 2010; is that right?

11 A. Yes. Yes.

12 Q. You recognize these as the rules that were
13 available on the Emerging Threats website shortly
14 after you started working for Emerging Threats as a
15 contractor?

16 A. Yes, I do.

17 Q. It says here that you "authored over 20 rules
18 found in the document" and provide some examples.

19 A. Yes.

20 Q. Do you know how many rules in the document
21 you offered -- authored?

22 A. I don't remember all the rules that I wrote,
23 but it was about like 20 or so. But I can't remember
24 exactly which ones. Too many rules. 10 years, I mean
25 working with that like from 2010 to 2016, that's six

1 years of rules is a lot of rules. I can't remember
2 all the rules, but I wrote a lot of rules that I can
3 say. I created a lot of rules.

4 Q. Could it be over 50 rules?

5 A. Over 50. That's for sure.

6 Q. Could it be over 100?

7 A. Over 100.

8 Q. And do you know if every rule that you
9 submitted made it onto the all rules ruleset?

10 A. Can you clarify if it was made -- are you
11 asking if the rules that I submitted were before I
12 joined Emerging Threats while I was working as a
13 volunteer or --

14 Q. Thanks for the follow-up.

15 When you submitted rules to the Emerging
16 Threats list before you were an employee at Emerging
17 Threats, did all of those make it onto the All Rules
18 ruleset?

19 A. I don't think all of them made it into,
20 especially when I was very inexperienced writing
21 rules, I don't believe that all of the rules that I
22 submitted before I have any experience with writing
23 rules were accepted as a rule on the Open ruleset. So
24 I cannot say it was.

25 MR. DONOVAN: We've been going for about an

1 hour. Do you want to take a quick break, or do you
2 want to keep going?

3 THE WITNESS: I can keep going if you want.
4 If you want to take a break, we can pause.

5 MR. PRICE: Yeah, I wouldn't mind a quick
6 break.

7 THE WITNESS: Okay. I'll be here.

8 MR. DONOVAN: Let's go off the record.

9 (A recess was taken from 11:00 a.m.
10 to 11:08 a.m.)

11 MR. DONOVAN: All right. Mr. Marinho, before
12 the break we were discussing that you had submitted
13 various rules to Emerging Threats.

14 I'd like to bring up Exhibit 1020 which is
15 the Emerging Threats reference, and bring up Page 162.

16 (Previously marked Exhibit 1020 was made
17 available to the witness.)

18 BY MR. DONOVAN:

19 Q. Mr. Marinho, we'll bring these up on the
20 screen. Hopefully that makes it easier and keeps us
21 all on the same page, but if you need to reference the
22 document, you have a copy as well.

23 Go to the rule that ends with "sid:2008805,"
24 and it's eight up from the bottom.

25 A. Uh-huh. (Unintelligible.)

1 Q. There it is. Able to read that, Mr. Marinho?
2 I know it's a little small.

3 A. It's written by Pedro Marinho and Matt
4 Jonkman. Downloader agent bnm -- DNS change -- bnm,
5 that's the name of the malicious -- of the malware
6 there. Yes, I can. Yes, sir.

7 Q. So is this -- it says, "By pedromarinho."
8 That would be you; right?

9 A. That's correct, sir.

10 Q. And is this a rule that you wrote?

11 A. Probably, but I can't remember. There's so
12 many rules. It's probably one of the rules that I
13 wrote, but I can't confirm that. I can't remember.

14 Q. Okay. Generally, do the rules indicate who
15 wrote them in the comments?

16 A. Yes. Yes.

17 Q. So you would assume this is a rule that you
18 and Matt Jonkman wrote?

19 A. I would assume, yes. I mean I don't recall
20 this rule, but I would assume that's the case.

21 Q. And who is Matt Jonkman?

22 A. Matt Jonkman is the -- was the Emerging
23 Threats CTO at the time. He used to write rules too.

24 Q. And you worked with him to write this rule
25 would be your --

1 A. Probably. Yes.

2 Q. And looking at this rule, can you tell what
3 this rule does?

4 A. Yes. So this rule, I mean it will not be
5 loaded by the IDS because we have a hashtag -- or how
6 do you guys call this, pound sign in English?

7 Q. We can call it a hash sign or a pound sign,
8 whichever is the most comfortable to you.

9 A. Let's call it a hashtag, then.

10 So when rules are preceded by a hashtag, that
11 means that the rule is disabled from the ruleset, and
12 the reason is because this rule, as you can look at
13 the rule, it has only a tiny content match, 2 bytes,
14 and the reason why it's commented out, it's because it
15 just generates a lot of false alarms. Lots of false
16 alerts.

17 So this is a rule that ships disabled by
18 default because the false positives are so high. I
19 mean we would never be able to set this rule to drop
20 traffic because it would end up dropping things that
21 it was not supposed to, but these rules -- do you want
22 me to describe exactly what it's doing?

23 Q. Are you able to explain what this was
24 intended to detect?

25 A. It was intended to detect communication, like

1 keep alive or starting -- the -- message says --
2 states that it's a common control channel start
3 response. So this is a response, or at least matches
4 a response. Unfortunately, it's so complicated that
5 it may end up matching on other traffic that is not
6 malware because as I told you, the size of the content
7 match is just too short. 2 bytes is too short for
8 network traffic, and this will match a lot.

9 But these rules, it's checking if -- when a
10 malware communicates with the command control server,
11 the common control server sends out a reply, a
12 response. And that's what we are trying to match on
13 this rule because this rule, it is matching on the
14 response from the external network for ports below
15 1024 to the home network as a response from a malware
16 common control.

17 That doesn't make sense.

18 Q. Let me just see if I can understand this
19 correctly, and let me know if I get it wrong.

20 But this would be alerting, if this was
21 activated, when there would be a response from a
22 malware server command and control server on an
23 external network to a device on the internal network;
24 is that right?

25 A. That is right, sir.

1 Q. Okay. While this is commented out, this
2 was -- was this designed to be used in some
3 circumstances?

4 A. It's up to the -- it's up to the users. This
5 is a rule you can enable on a SAN net, because if you
6 have a control in the environment and if you want it
7 to be flagged -- just to know what kind of malware is
8 this, but I would never turn this rule on a real, live
9 threat.

10 Like if you're protecting a network of a
11 hospital, I would never turn on this rule because it
12 would match on so much different things. Data stream,
13 voice over IP. We have a rule that is
14 unfortunately -- it's matching on a content match that
15 is so short, 2 bytes. It happens like all of the time
16 you see |0b 01|. This would match a lot.

17 It's just like having lottery with two
18 numbers only to guess, you know, and you can imagine
19 the number of winners you have if we have lottery with
20 only two numbers. So yeah, this rule is basically
21 matching on anything.

22 So we cannot use this on a real, live
23 network, but it's there for a reference for people
24 that wants to perhaps enable this on a controlled
25 environment, on a SAN net.

1 Q. Just so I understand, is this checking the
2 content on 2 bytes, is it 1, 2, 3, 4, 5, 6 -- 16
3 bytes?

4 A. You have pointed before to the rule just
5 below this one. Now you changed to the rule above it.

6 Q. I'm sorry. I thought I identified sid 28805.

7 A. Okay. So you made a mistake. That's
8 okay. So this rule -- again, let me tell you this
9 because you guys, you don't know. You guys are not a
10 network administrator. You guys never worked with
11 this, but this pattern of |0b 01|, and then we have a
12 bunch of zeros, this can happen just like every time
13 on network threat. This can happen on different
14 protocols. This can happen on voice over IP. This
15 can happen on compressed data being transferred from
16 my server because protocols use lubes. Lubes is 000.
17 A lot of protocols use lube to make the data on a size
18 that it can be interpreted by the application layer.

19 So content matches that have lots of lubes --
20 lubes is the zeros -- are prone to generate a very
21 high number of false positives. So this rule is a
22 very good example of a rule that is commented out. It
23 is disabled by default because the number of false
24 positives is just out of the normal.

25 This rule would generate so many false alerts

1 that we just should disable because people get this
2 enabled on the network, and all of a sudden they
3 download and this rule is going to generate tons of
4 false alerts. This is why the rule is commented out.

5 Ultimately, these kind of rules were never
6 designed to drop traffic. I got to say this because
7 if you guys are trying to say that these rules do
8 things that they were not designed to do, these rules
9 were not designed to drop traffic, and ultimately,
10 these rules cannot prevent any sort of data
11 exfiltration. These rules exist to give evidence that
12 some network administrator can correlate an event on
13 the network with other events with other systems in
14 order to start an investigation.

15 So I need to make this really clear because I
16 believe that what you guys are trying to do, you guys
17 got these rules, and you were trying to -- and I'm
18 going to get these rules back to what they really do
19 because you guys are saying that these rules do drop
20 traffic. They do not drop traffic. They were not
21 designed to prevent data exfiltration, and if you try
22 to convince people that this rule can do what it
23 cannot, you are creating a false sense of security,
24 and a false sense of security, it charges a price that
25 money cannot pay.

1 And you guys know that because the
2 United States have encountered, and I'm glad I'm here
3 to clarify what these rules can do and to make sure
4 that you guys understand and the United States
5 authorities understand that to prevent direct
6 exfiltration, you cannot do it with just one line of
7 code like this. It's much more complicated than
8 that.

9 So I wish you put this out because I just --
10 this makes me very worried, you know, that you guys
11 got these rules and are using these as a defense
12 system to prove that you can prevent data
13 exfiltration.

14 If that what's the case, we would not have as
15 many data exfiltration as we have. It's not that
16 simple to resolve this problem. Just an IPS system.
17 And it's naive to think that. This makes me very
18 uncomfortable, but I'm here to help clarify that. So
19 please go on and ask your questions.

20 Q. Sure. And so the transcript is clear, I
21 think you're referring to where there's the 00's.
22 Were you saying those are nos, like n-o?

23 A. N-u-l-l-s in English.

24 Q. Nulls. Thank you.

25 A. Like nullify. Thank you. Yes, sir.

1 Q. And also earlier, I was asking questions
2 about the 5-tuple check, and we were talking about it
3 being from the external net to the internal net. I
4 would understand that that testimony was about the
5 rule sid 008806; is that right?

6 A. The one that has the content match with only
7 2 bytes is the 2008806, yes.

8 Q. So when we were earlier talking about the
9 detecting traffic from the external net to the
10 internal net, that was with regard to Rule -806, not
11 -805; right?

12 A. Can you repeat please.

13 Q. Sure. Earlier, you testified about a rule
14 was from the external net to the internal net that it
15 was detecting traffic, and I just wanted to clarify,
16 that was in the context of Rule -806, not -805; right?

17 A. That's right. Yes. -805 has the opposite
18 direction from the internal Internet to the external
19 Internet.

20 Q. Let's go down to -- or up, I guess, to
21 Page 43 of Exhibit 1020, and go to the rule with
22 sid 2010630, and it's the second one from the top.

23 Just to make sure we're on the same page, do
24 you see 2010630?

25 A. I do see, yes, sir.

1 Q. And do you recognize this as a rule that you
2 submitted?

3 A. I do. I mean I cannot remember, but because
4 it's written by me, I did submit this rule. Of course
5 I cannot remember, but yes. Probably one of the rules
6 that I wrote. Probably.

7 Q. And looking at this rule, do you recall why
8 you wrote it?

9 A. This is probably matching on some adware
10 install reports. Adware code that has to be -- have a
11 URI -- URL that matches these subpattern of a URL,
12 like "nsi_installed.php?" You know, this is a rule to
13 match a communication from a piece of hardware, a
14 malicious program with probably the server that
15 controls this adware, and on the URI of that
16 communication we observed NSI_installed.php and all of
17 this.

18 So we are assuming that this traffic is
19 unencrypted because I mean these rules -- you got to
20 keep in mind, these rules are matching on unencrypted
21 traffic, but not every single malware does send data
22 unencrypted. In fact, the great majority of these
23 malwares they would send over TLS, and we do not have
24 a way or didn't have that in 2010, to decrypt TLS
25 traffic. That's not something that an IPS does.

Page 57

1 So that's another reason why these rules,
2 they cannot prevent fully a data exfiltration. If
3 it's over TLS, we never -- the IS would never match on
4 this because it is encrypted. How can you match on
5 something that is encrypted.

6 So you need to keep in mind because when you
7 push something like I can't prevent data exfiltration
8 with an IPS system, that is not true and that is
9 something that is dangerous because it plays into the
10 hands of let's call the enemies of these, and the
11 price to pay for a false sense of security, it's more
12 than what money can buy.

13 It was a lot of exfiltrated data that plays
14 into the hands of the enemies of peace, and by doing
15 that, what you guys are doing, you get these rules and
16 you are trying to show that these -- with these rules
17 I can prevent data exfiltration while we cannot. It
18 puts a false sense of security, and that's something
19 that I will not allow you guys to do.

20 So I'm here to clarify what these rules
21 really can do, and I hope that we can go through all
22 of these rules and go back to our daily tasks because
23 I have a lot of things to do.

24 I have networks that I'm defending today and
25 require my attention, require my time, and here we are

1 trying to show -- I mean I feel like I'm going into a
2 booby trap tunnel with all of these questions you guys
3 are making about these rules, and just to prove that
4 something that's not right. And I want to give this
5 testimony because I'm feeling very uncomfortable with
6 the situation because it looks like we live on an
7 upside down world.

8 Look what's happening on the Middle East.
9 Look what's happening on the Red Sea. Look what's
10 happening in the world right now. And we need to make
11 sure that the United States authorities, they know
12 exactly that we cannot prevent data exfiltration from
13 an IPS system. An IPS can't do all of the functions
14 necessary to prevent data exfiltration. You need
15 other systems. You need other signals in the network
16 in order to prevent data exfiltration.

17 So I wish to let this register here on this
18 call, and please continue with your questions.

19 Q. Thank you. And just to make sure we can move
20 efficiently, I'll try to keep my questions pretty
21 specific so that we can address the issues here.

22 A. Yes, sir.

23 Q. And so in this rule that we're looking at
24 with sid 2010630, in the syntax of the rule, does part
25 of this rule check packet header field values?

1 A. Packet header field values. It does check if
2 the source IP, it's on the range of my WAN IPs, the
3 home network IP addresses with the variable -- you
4 have action alert, you have the protocol CPT. Then
5 you have a variable dollar sign home net, and this is
6 the -- where you validate if the IP address, the
7 source IP matches the WAN IPs of the network to
8 determine -- to know what's the direction of the
9 traffic.

10 In this case, it's outbound traffic from the
11 home network to the external network. So yes, when
12 you have here the header that would match the IP
13 headers -- or actually, the TCP because we are also
14 matching the destination ports on this case.

15 So yes. The answer is yes.

16 Q. Okay. And just for the transcript you were
17 saying the WAN network, W-A-N; correct?

18 A. That's right.

19 Q. And alert here means that if this rule was
20 triggered by a packet, it would send an alert. It
21 would not drop the packet; right?

22 A. It would only emit an alert. It will never
23 drop the packet.

24 Q. And then where we have a "content:'GET';
25 depth:4" in the rule -- do you see that?

1 A. I do, yes, sir.

2 Q. What does that do?

3 A. This is matching on a -- or attempting to
4 match on the HTTP method, which is a function of the
5 HTTP protocol. It could be put, get, post, had, and
6 other methods. So in this case, it's mentioned on the
7 get method.

8 Q. And is the method an HTTP application packet
9 header value?

10 A. The H- -- yes, it is. Yes, it is.

11 Q. And what is the "uricontent" part of the
12 rule?

13 A. The uricontent is the content match that will
14 match on the URL, URI. On a part of the URI. It's
15 important to make this distinction because URIs, they
16 can be huge and they have parameters. As you can see
17 here, you have an ampersand FID equals, and then you
18 have a value, and then value could be anything. It
19 could be a number. It could be whatever.

20 So when writing IDS rules, I cannot match on
21 the entire URL because if I can match on the entire
22 URL, then I have 100 percent accuracy. But this
23 doesn't happen in reality because the URL, it's
24 holding different values that are being passed as
25 parameters to these applications so that we are

1 limited to match the parts of the URL that will not
2 change.

3 And because of that, it make these rules
4 match sometimes on a tiny portion of a URL, and that
5 could be common to other URLs that is not related to
6 this application. To this malware, for example. And
7 this is where we have false positives, and this is why
8 promoting all of these -- I'm sorry, these rules to
9 drop traffic causes problems.

10 And thus, we cannot use these rules because
11 they do generate false positives. We cannot set these
12 rules to drop traffic. We can only set these rules to
13 monitor.

14 Q. All right. Mr. Marinho, we were talking
15 about the URI content check. Where in the network
16 traffic would it be checking for the portion of URI
17 content in the rule?

18 A. In the -- in the HTTP header, the URI.

19 Q. And that would be an application header field
20 value?

21 A. That is, yes.

22 Q. Let's go back to Exhibit 1020, and we'll go
23 to Page 115 of the PDF. I'm actually going to the
24 rule that spans Pages 115 and 116. It has sid
25 2011232.

1 Mr. Marinho, do you see that?

2 A. I'm sorry. It's so tiny. Where is it?

3 Q. It's -- the comment starts on the bottom of
4 Page 115, and then the body of the rule is on
5 Page 116.

6 A. Yes I do.

7 Q. It says, "by pedro marinhi," but that looks
8 like a typo in your name. Would you understand this
9 as being a rule that you authored?

10 A. I think so. Probably. Someone committed a
11 mistake with my name. Probably, yes.

12 Q. And do you recall writing this rule?

13 A. I don't remember, sir. This was a long time
14 ago, like 2011.

15 Q. And from looking at this rule, are you able
16 to tell what this rule was intended to detect?

17 A. It's detecting this user agent, eChanblard,
18 eChanblard. He's one of the HTTP header values user
19 agent. So it would have to match on an HTTP header
20 user agent. So traffic outbound over HTTP.

21 Q. And what is the "'GET'; depth:4" part of this
22 rule indicate?

23 A. Again, this is matching on an HTTP method.
24 In this case, it's mentioning the get method of the
25 HTTP protocol.

Page 63

1 Q. And do you recall why -- or can you tell from
2 looking at this why this rule would be triggered by
3 the user agent in the HTTP request?

4 A. Can you repeat, please. Sorry.

5 Q. Sure. Well, let me back up.

6 If I understand right, the content check here
7 is checking for user agent in the HTTP request; is
8 that correct?

9 A. That's correct, yes.

10 Q. And do you know why this rule was checking
11 for that?

12 A. Because these peer-to-peer called, what,
13 eChanblard? I have no idea what is that. I cannot
14 remember if this is a peer-to-peer application or
15 something like that, but it is matching on that to
16 create an alert in case we see an outbound connection
17 over parts HTTP where the user agent equals
18 eChanblard. Does that make sense?

19 Q. And what is the user agent in an HTTP
20 request?

21 A. User agent is a field of the HTTP protocol
22 that emits information about the application to the
23 server. Like, for example, if I'm accessing a web
24 server with a browser, the browser will emit a user
25 agent stream to say, "Hey, I'm a Safari browser,

1 Version XYZ running on a Mac OS." So you have a
2 stream with the information about the application that
3 is accessing the server.

4 In this case we have eChanblard on the user
5 agent. So this is something to say, "Hey, I'm a
6 client of these" whatever, peer-to-peer applications.

7 Q. And the part of this rule checking the packet
8 header field values is checking for outbound packets
9 from the home net to an external net; right?

10 A. That is correct.

11 Q. Let's go to Page 126 of Exhibit 1020, and
12 seventh up from the bottom is the rule with
13 sid 2010220.

14 A. Yes.

15 Q. Let me make sure we're on the same page.

16 A. (Unintelligible.)

17 Again, it's the same situation. We have a
18 rule that is inspecting traffic from the home net to
19 the external net with outbound traffic over ports
20 HTTP, assuming this traffic is unencrypted, which
21 cannot be; right? We know the great majority of
22 applications work over HTTPS.

23 So once this gets encrypted, the IDS is false
24 negative and it will never be able to match because
25 the threat is encrypted. We are matching over HTTP on

1 a user agent field that has the extreme
2 "ClickAdsbyIE." That's what this rule is doing.

3 Q. And so is it correct that like the last rule,
4 this is checking content in the HTTP application
5 packet header to see if it matches the rule?

6 A. That is correct, sir.

7 Q. And this is another rule that you authored;
8 right?

9 A. Probably. I cannot remember because as I
10 told you, I wrote hundreds of rules, and I can't
11 remember each one of the rules that I wrote anymore.
12 This was from 2010. So this is probably too old. I
13 cannot remember.

14 Q. Sure. Yep. 14 years ago, or 13 years ago.

15 A. Yes, sir.

16 Q. Let's go to Page 177 of Exhibit 1020, and the
17 fourth rule up from the bottom has sid 2008389.

18 A. Yes, sir.

19 Q. And does this appear to be another rule that
20 you wrote?

21 A. It appears to be by the name there, my name
22 there. Probably.

23 Q. And from looking at this rule, can you intend
24 (sic) what it's intended to do?

25 A. Yes, I can. So it is checking if we have

1 post followed by space slash and a plus sign on the
2 depth 7 bytes the beginning of the packet with the
3 depth 7 keyword. And we -- because this is so noisy,
4 this will generate so many false positives. It has
5 the flowbits:noalerts that not even alerting because
6 this would generate like 1 million events in one hour,
7 depending on the network, over ports 3128, which is
8 one of the ports that probably this malware
9 communicated with its common control server over this
10 3128 port.

11 It also has a flowbit setting, a flowbit, and
12 this is what it's doing. Does that make sense?

13 Q. I think so. Does that mean that if this rule
14 was used, it wouldn't send an alert. Instead, it
15 would set the flowbits to prevent other rules from
16 sending an alert? If I have that wrong, if you could
17 just explain to make sure I understand.

18 A. Yes, I can explain.

19 So at the flowbits it's being set on this
20 rule, but the rule is too noisy. It generates too
21 many false alerts. So we have the option of raising
22 this flag, this flowbits, but not emitting an alert
23 every time it raises the flag or sets the flowbits.

24 Does that make sense?

25 Q. So this rule would set a flag, but it

1 wouldn't send an alert every time it's triggered?

2 A. That is correct.

3 Q. And so if additional traffic hit this rule
4 multiple times, the flag would be set once -- or the
5 flag would, I guess, remain set, but you wouldn't set
6 an alert for each packet that would hit the rule; is
7 that correct?

8 A. Yes. That's correct.

9 Q. And the 5-tuple portion of this rule is
10 checking for outbound TCP traffic from a home net to
11 an external net and port 3128?

12 A. Yes. That's right.

13 Q. And what does the content post depth 7
14 portion of this mean?

15 A. This is matching on a -- post controller.

16 This is matching on a post followed by space
17 followed by a slash followed by a plus sign on the
18 very first 7 bytes of a packet payload.

19 Q. Would this be checking the HTTP application
20 packet header for it being a post method?

21 A. I can't say for sure that this post is a HTTP
22 because we have malware that can send something that
23 looks like HTTP, but it's not. It's trying to blend
24 in. It can send like something that's very close to
25 HTTP but it's not.

1 So I cannot say this malware is doing that
2 but it could be that this is matching on a post method
3 followed by slash and a plus sign, which would be part
4 of the URL, but I can't say for sure this is a post of
5 the HTTP protocol because these -- they can -- they
6 can -- how to say this.

7 They can send something that is very close,
8 looks like HTTP, but it's not. Do you know what I'm
9 saying? It's difficult to explain. That's what I
10 think is happening here.

11 Q. And if this was just checking for a post in a
12 standard HTTP protocol, would that just be checking a
13 post in the first 4 bits of the application header?

14 A. Yes, sir.

15 Q. And that would be a broader rule than this
16 rule that's checking 7 bits; right?

17 A. Can you clarify? What do you mean by
18 broader?

19 Q. More traffic would trigger the rule if you
20 were only checking for a post in the first 4 bits
21 rather than a post/plus in the first 7 bits; is that
22 correct?

23 A. Yes. But even though -- and I tell you this.
24 If you turn this rule on, you'll see hits on it.
25 There is a lot of URLs that starts with a slash and a

1 post. But yes, you are right. It's matching on a
2 post followed by the first bytes, but I believe it is
3 a comment. I don't know if this is an HTTP post or
4 this is just a custom protocol that these malware -- I
5 mean like it's a post of their own protocol.

6 I mean there are malwares that they have
7 their own custom protocol. So I cannot say this is an
8 HTTP. I can't remember. I would have to look. And
9 you can see -- so, yes. So that's probably a post
10 from HTTP, probably.

11 Q. Does this rule, 2008389 is probably an HTTP
12 post method it's checking for with the additional
13 slash plus?

14 A. Probably, yes.

15 Q. Let's go back to Exhibit 2031, which is your
16 declaration.

17 A. Yes, sir.

18 Q. And we'll go down to Paragraph 6.

19 A. Okay.

20 Q. Earlier, we were talking about the syntax
21 rules, and here, you say -- you note "there are no
22 'drop' rules in the Emerging Threats reference; all of
23 the Snort rules use the 'alert' keyword."

24 In order to change those from alert rules to
25 drop rules, someone would need to change that from

1 "alert" to "drop"; right?

2 A. That's right, yes.

3 Q. And then going on, you say, "I also note that
4 many of the rules in Emerging Threats reference are
5 disabled by default by being commented out with a" --
6 we'll call that a hash annotation; right?

7 A. That's right.

8 Q. And then to activate those rules, you would
9 remove the hash annotation before loading them into a
10 SNORT system; right?

11 A. That is correct.

12 Q. In Paragraph 7 you state you "reviewed
13 several of the Emerging Threats rules cited in
14 Keysight's petition, and I provide a summary of their
15 functionality below."

16 How did you select which rules to analyze
17 below?

18 A. How did I select these rules? I don't
19 understand this question.

20 Q. Did you choose which rules to analyze below,
21 or did your counsel?

22 MR. PRICE: Objection.

23 Sorry. Hold on, Pedro.

24 Objection to the extent that it calls for
25 privileged communications.

1 So Pedro, any communications between you and
2 us are privileged. So you can answer the question as
3 long as it doesn't divulge privileged communications
4 between you and counsel.

5 BY MR. DONOVAN:

6 Q. And also just to clarify, I'm not asking for
7 any discussions with your counsel. I'm just asking if
8 you selected these or if they were selected by your
9 counsel.

10 MR. PRICE: Again, you can answer the
11 question to the extent that you don't divulge
12 privileged communications.

13 Go ahead.

14 THE WITNESS: I can answer. Okay.

15 Yes. So these rules, they were picked by my
16 counsel.

17 BY MR. DONOVAN:

18 Q. Let's go to Paragraph 8, which is addressing
19 Rule 2003021. Do you see that?

20 A. Yes, I see.

21 Q. Do you recall when you first reviewed this
22 rule?

23 A. When I first reviewed it, I cannot remember.

24 Q. Was it within the last few months?

25 A. It was in the last few months, yes.

Page 72

1 Q. And you say, "this rule is commented out,
2 likely for performance reasons."

3 What do you mean by that?

4 A. Because this rule -- if you check this
5 rule -- let's have a look together.

6 From the home net to the external net to out
7 ports are both 1024. Out ports; right? And then we
8 have a 3 bytes control match. So you can see here
9 this rule is going to match almost every time over
10 things that are not even TLS. They are other things
11 over ports -- I mean we have what, 64- -- no. 64,000
12 ports. That can happen anything from voice over IP,
13 from video conferences, data transfers, all of the --
14 everything can happen over these ports, and we have a
15 3 bytes match. So this rule is going to match a lot.

16 So when the rules match on every single
17 packet, it will have the cost of processing and
18 checking if the flowbits is set, and this causes great
19 performance issues. So this is why rules that have a
20 very short, very tiny content match are rules -- not
21 only have poor performance, because it will match so
22 much, and then the ideas will have to evaluate every
23 other option because it matches. It's very short.

24 Also, this rule also has the problem -- and
25 it's not here, but these rules will generate a ton of

1 false positives. So it's not something we can use to
2 drop traffic, never, because if we end up dropping
3 traffic that is not what this rule is mean -- was
4 designed to detect, because you guys don't know, but
5 it's difficult to have 100 percent accuracy when
6 you're trying to match things over a network, over
7 network traffic.

8 It's very difficult to be 100 percent
9 accurate. I mean as I told you, we have like of
10 thousands of common vulnerability enumeration,
11 thousands of vulnerabilities. Only a small portion of
12 vulnerabilities can be detected by an IDS. What about
13 the other vulnerabilities? I mean how can we prevent
14 data exfiltration with only matching network traffic.

15 This doesn't make sense. I mean this claim
16 doesn't make any sense. This is not true, and I hope
17 that by the end of this call we can prove that because
18 these systems, they are critical and they are
19 protecting a lot of critical things. They are
20 protecting power grid. They are protecting things
21 that your enemies can attack.

22 So we need to be 100 percent sure of what
23 this can and what it cannot do because to prevent data
24 exfiltration, you need more than just an IPS. You
25 need other systems. You need systems that would check

1 the integrity of the files on the system, that we will
2 need logs each time these files are accessed, and in
3 combination all of these alerts, all of these other
4 events in combination, they can lead to a -- starting
5 an investigation.

6 But these rules alone, they can not prevent
7 data exfiltration. But yes, please go on.

8 Q. And to be efficient today, I ask that you do
9 try to focus on answering the question that's asked.

10 So still looking at this rule on Page 2 of
11 your declaration, if somebody wanted to use this rule,
12 what would they do?

13 A. They would have to remove the hash sign that
14 precedes the rule, so that the rule would be enabled.

15 Q. That would be the hash line or the pound
16 sign?

17 A. The pound sign or hash.

18 Q. And then they would load it into a
19 SNORT-based system to use the rule; right?

20 A. Or to recap, which is not SNORT based.

21 Q. They could load it into a SNORT or a Suricata
22 system?

23 A. That's correct, sir.

24 Q. And the first portion of this rule, where it
25 says, "alert tcp HOME_NET any" to "EXTERNAL_NET" any,"

1 and then the port range 1024 to 65535, that's checking
2 application header field values to determine which
3 packets this rule applies to; is that correct?

4 I'm sorry. Strike that. I misworded my
5 question.

6 That's not checking application header field
7 values. That's checking packet header field values;
8 is that correct?

9 A. Packet header. So the -- you're talking
10 about the HOME_NET any to the external net and the
11 port interval; right?

12 Q. Yes.

13 A. That is checking package header data on the
14 IP header. On the TCP -- sorry, because we have the
15 ports. On the TCP header.

16 Q. That's checking packet header values in the
17 IP and TCP packet header; right?

18 A. That's correct, yes.

19 Q. And then this rule is also inspecting traffic
20 to determine if it includes content, and then it has a
21 |17 03 00| a depth:4; right?

22 A. That's correct.

23 Q. Would that be triggered for SSL D3 traffic?

24 A. That is right.

25 Q. Earlier, you referred to a "false positive."

1 What is a false positive?

2 A. False positives is when these rules match on
3 traffic that it was not the intent of which the rule
4 was designed to match. Like you match -- this rule
5 could match on a video call over port 65,000 because
6 it matched on a |17 03 00| that happens to be inside a
7 packet that was with compressed voice over IP, for
8 example, and then this is not TLS. This is just a
9 voice over IP.

10 So this is a false positive. It's when these
11 rules match on not what they were designed for. This
12 is why we cannot promote -- we cannot change this rule
13 to drop, because they were not designed to drop
14 traffic. They were designed to monitor traffic
15 because of the possibility of having false positives.

16 Q. Is it correct that this rule was created to
17 detect traffic that's being sent on SSL V3, but it
18 could also have false positives that would detect
19 other traffic that also has the content match of
20 |17 03 00| in the first 4 bits of the application
21 packet header?

22 A. That's correct, sir, yes.

23 Q. And does that mean if -- well, if malware was
24 exfiltrating data encrypted can SSL V3 from a network
25 to a port between 1024 and 65535, would that trigger

1 this rule?

2 A. It could trigger the rule.

3 Q. But there's also other traffic that would not
4 be exfiltrating data that could trigger this rule; is
5 that right?

6 A. Exactly. And these are the false positives
7 that I'm trying to explain.

8 Q. So is it correct that this rule would both be
9 triggered by malware exfiltrating data and other
10 traffic that was not exfiltrating data?

11 A. That is correct, sir.

12 Q. Let's go down to Paragraph 9. And the first
13 sentence says, the "Rule would alert (but not drop)
14 upon matching a TCP packet encrypted using SSL
15 version 3 that is directed to a port number range from
16 1024 to 65535, of which there are many legitimate
17 uses."

18 A. That is right.

19 Q. And what are the "many legitimate uses"
20 you're referring to here?

21 A. Every other application that runs over ports
22 between 1024 and 65535, we have different applications
23 that runs over these ports, like, for example, you can
24 have file transfer over these ports on an FTP
25 protocol. Transfers data over ports above 1024

1 usually.

2 So if you're transferring a file over FTP and
3 the file happens to have a |17 03 00| bytes in the
4 file and the file is big and the file gets fragmented
5 by many packets, because it's too big to transmit, and
6 it happens to have a |17 03 00| on the initial bytes
7 of any one of these fragmented packets, then this rule
8 would trigger on a file transfer of a protocol FTP
9 that has nothing to do with the SSL Version 3.

10 So there are many other legitimate
11 applications that runs over -- between the 1024 and
12 65535 that would trigger an alert on this rule because
13 the rule is too inaccurate to match exactly on an SSL
14 version without having any other negative impact
15 mentioned on things that are not SSL. I hope that
16 clarifies this.

17 Q. Let's go down to Paragraph 10. This is
18 addressing Rule 2002526.

19 A. Yes, sir.

20 Q. And you referred to if the comment was
21 removed. This would be referring to the hash sign
22 that is before the alert or to activate the rule; is
23 that right?

24 A. That is right, sir. Let me tell you a little
25 bit of story on -- about these rules because on the

1 23rd of April, it's right here, of 2012, these rules
2 were removed from the ruleset because it not only have
3 a terrible performance, because we do not have a
4 content match here. You can see that we only have a
5 regular expression, and without a content match here,
6 it will run this regular expression for every single
7 packet that is going from the home network to the
8 external network, and a regular expression has a huge
9 weight in the consumption of the CPU, computer
10 processing power to run a regular expression for every
11 single packet that's leaving the network over ports
12 associated with the HTTP protocol.

13 It's just a rule that we cannot have enabled
14 because the performance is just too bad, and it makes
15 the overall performance of the system really go bad,
16 as well as a regular expression that matches on things
17 like stop secretly going to -- because you can see
18 here, we have a repetition of a /S /W, repeated zeros,
19 or many times /W is basically matching on any
20 principal character like A to Z, 0 to 9. So it can
21 match on anything.

22 So on the 23rd of April of 2012, these rules
23 were removed from the ruleset because it's just a rule
24 that doesn't help. It not only cannot detect
25 exfiltration of a document, it will emit false alerts.

1 It will be terrible for the performance, and this is
2 why the rules were removed. So I hope with that, we
3 can move forward. If you don't have any questions.

4 Q. I do.

5 Focusing on the actual syntax of the rule,
6 what is pcre? Do you see where it says, "pcre:" and
7 then there's a match?

8 A. Yes. That's the regular expression that I
9 was talking to you about just right now, and this pcre
10 match is so expansive that this rule is unviable.
11 It's not viewable to an IDS to have a rule that's only
12 matching on a regular expression because the cost of
13 the processing power to run a regular expression, each
14 time it -- for every packet that's leaving our network
15 is just something that's unacceptable, and it will
16 make the overall performance of the system go really,
17 really bad.

18 So these rules were removed from the ruleset
19 because it not only will have a terrible performance,
20 it will generate false positives and it will not help
21 detect a file exfiltration like the people that
22 designed this rule intended to because it's not that
23 easy.

24 Let me explain why. I can go over.

25 These files are binary. The PDF file is

1 binary. It's a file that has different fields. It's
2 compressed. Fields on a PDF file are compressed
3 because otherwise, this file would be huge. It would
4 have like 100 megabytes of a PDF file. So these
5 files, they have fields that are compressed within the
6 file, and in order to match on something like the
7 title of the document, like top secret or something
8 like that, you would have to decompress the file.

9 You'd have to extract the file from the
10 network traffic in order to validate if this file is
11 actually a PDF file -- if it is indeed a PDF file or
12 if it's a Microsoft Word file, and then after they
13 decompress and parsing the file, you would have to
14 look and see if you can find a title like top secret,
15 and these other things here.

16 So this rule doesn't do what you guys imagine
17 that it does because you don't get it, do you? You
18 never worked with these IDSes. You never tested these
19 rules to see how many false positives you would have
20 with a rule like this.

21 So I don't know what else can I say about
22 this rule. It's just something that will never help
23 detect. Unfortunately, it's not that easy. It's not
24 that simple to detect a file over transiting a network
25 like with a regular expression, like it's not that

1 easy.

2 Q. Is it fair to say that this rule was intended
3 to alert for exfiltrations, but it has too many false
4 positives and uses too much processor that's -- never
5 be practically used in application?

6 A. That's correct, sir.

7 Q. So if this rule was run, it would detect
8 exfiltrations. It would just be extremely intensive
9 on the system and would also have a lot of false
10 positives; is that right?

11 A. I can't say if it will defect an exfiltration
12 because as I told you, a file -- a PDF file, a
13 Microsoft Word file, pick one file format. These are
14 binary. It's not -- you cannot open the file and see
15 the text immediately because the text is compressed in
16 fields within the file, and these files, they have a
17 file format for which the application reads the file,
18 and it decompresses the fields and it samples the
19 file, and this information is exhibited to you on a
20 Microsoft Word reader or in Adobe Acrobat reader.

21 But the file itself, it is -- half these
22 fields are compressed. It's a huge file. In order to
23 be able to accurately match on a file like this, we
24 would have to be able to extract the file from the
25 network traffic and do lots of checks, like is this a

1 PDF file. Is this a Microsoft Word file. Is this --
2 the title of the file has this.

3 But what if the title is compressed on a
4 field within the files? Then we'd have to decompress
5 this field in order to match. So this rule, it has a
6 very good -- I mean intention -- let's say the
7 intention is good, but it doesn't work. The reality
8 is that this rule doesn't work.

9 Q. Mr. Marinho, what's a false negative?

10 A. False negative is when you -- it's when you
11 have a rule to detect something, but you couldn't
12 detect -- for example, let's suppose you have a rule
13 that is matching on top secret. Okay? It's matching
14 on top secret, and then a file, top secret file was
15 transferred over the network but it was encrypted.
16 The connection was encrypted.

17 So this rule is not able to decrypt the
18 traffic in order to match on a top secret because it
19 was over TLS, and the file was transiting encrypted.
20 So these rules, they don't do miracles. They have
21 very strong limitations, and it's used to alert of a
22 potential -- something a network administrator have to
23 correlate with other logs of other systems in order to
24 start an investigation.

25 So I hope that clarifies because we need to

1 clarify to the United States authorities exactly what
2 these systems can and cannot do because we need to
3 develop better systems. We need to develop better
4 systems. This is not an easy win. This is not easy
5 as writing a rule by preventing data exfiltration.

6 The reality is not that, and data
7 exfiltration is happening while we're talking, and
8 it's a very complex problem, and it's naive to think
9 that these rules alone can prevent data exfiltration.
10 It's very complicated.

11 Please, go ahead.

12 Q. Focusing back on the rule in Paragraph 10 of
13 your declaration, would it be right to say that this
14 rule would be triggered if there was activity by
15 documents leaving the network that included the text
16 top secret, that it would have both false positive and
17 false negatives as well?

18 A. As I said, depending on the document --
19 because, as I said, a PDF file it has fields that are
20 within the file that are compressed.

21 When you compress something, you have a text.
22 When you compress, that text is transformed into
23 something smaller. Bytes. Binary. So in order to
24 match on a file like this, it's not possible to do.
25 Sometimes with an idea, because you would have to

1 extract the file, make sure that the type of the file
2 is the PDF or Microsoft Word.

3 Then you would have to decompress the
4 different fields in order to start matching all the
5 file. Okay. That's my -- my answer.

6 Q. Going down to -- on Page 5, seven lines down
7 from the top, you say, "The problem of preventing a
8 file exfiltration demands more functionalities than
9 only an IDS/IPS can employ in terms of matching
10 network traffic against signatures."

11 What do you mean by that?

12 A. We have -- in order to detect a data
13 exfiltration, there is lots of things that we need to
14 check, like we need to check the -- I mean we have an
15 operational system where these files are stored. So
16 the file is stored on an operational system.

17 And to access the file, I need to have a user
18 on the system. So at this point, I already have
19 another piece of evidence that have nothing to do with
20 an IDS because it happens on the operational system
21 level, an access, unauthorized access to a file. So
22 we have to have another kind of logs on the
23 operational system level that would be monitoring
24 access to these files.

25 So this is one piece of evidence that would

1 help a network administrator, a defender to understand
2 if an unauthorized access happened on the file. And
3 this is all on the operational system level. We're
4 not talking about the file that already transferred
5 the network. We're talking about evidence, events on
6 the operational system.

7 In conjunction with these protections you can
8 create all sort of protection to these files, to the
9 system itself so that you harden the access to these
10 files. You can create a user that is -- has a very
11 complex password, and only this user can access these
12 files. So there is a series of other things that we
13 need in order to detect that a network -- a file
14 exfiltration happened.

15 You can't just do that when a file is
16 transiting the network because there is other systems
17 that, in conjunction with when you concentrate all of
18 these logs in one place, you can find okay, so a user
19 was created. This user transferred this file. This
20 file was transferred via file transfer protocol over
21 the network, for example. And it was encrypted,
22 transferred over, FTP encrypted.

23 So once it's encrypted, we lose the
24 visibility of the traffic. We can only match on
25 what's not encrypted. So you know I what I'm saying?

1 Let's suppose a threat actor infiltrated a hospital
2 and he got one file, and he uploaded the file to
3 Dropbox. I mean how can you possibly detect that
4 someone copied a file to Dropbox because the Dropbox
5 used TLS encryption. Sorry. Dropbox used TLS
6 encryption.

7 The IDS cannot match on encrypted traffic.
8 So the only way would have to have other types of
9 monitoring systems that will monitor on the
10 operational system level the access to these files.
11 So this is why I said that the problem of preventing a
12 file exfiltration demand more functionalities that
13 only an ID SIP can provide because of the example I
14 just gave to you. A guy breaks into a hospital
15 network and transfers a file into Dropbox using TLS,
16 HTTPS. The IDS cannot match on that.

17 So this is why I told that. I hope it's
18 clear because this is serious, and I'm worried. I'm
19 worried about this.

20 Q. Could a system -- I'm sorry.

21 Did you have more?

22 A. I asked if that makes sense.

23 Q. I think so, and I think this is consistent
24 with -- well, helps to clarify a point maybe.

25 Could a system prevent exfiltration by

1 matching an HTTP method in an application header field
2 value?

3 MR. PRICE: Objection.

4 THE WITNESS: Can I answer that?

5 MR. PRICE: Yes.

6 THE WITNESS: I think it's true. It's not
7 that simple. As I told you, we transfer a file to
8 keep HTTPS. Then the headers are gone because they're
9 encrypted on the TLS tracker. How can I match the
10 header if the threat is encrypted. How can an IPS
11 stop that if it cannot unencrypt the network traffic,
12 extract the file, validates the -- each file has a
13 different format.

14 PDF files have different format. Excel
15 formats have a different -- binary. The file is
16 binary. It's not something you walk in and you
17 immediately see the title. It's only bytes. So it's
18 not -- it's not possible. It's not accurate to say
19 that with one IDS rule that checks the HTTP post I
20 can't prevent the exfiltration because it will happen
21 over encrypted communication protocols, such as TLS,
22 HTTPS.

23 And also IPS don't have time, I would say,
24 persistent power. You cannot waste too much time
25 attempting to decompress data even if it was not

1 encrypted, but to decompress and parse a file.
2 There's a huge cost, computational cost to open a
3 file -- first to extract the file from lots of packets
4 that the file is fragmented in multiple packets.

5 We have to reassemble the file, extract it
6 from the network traffic, open the file to read and to
7 restart validating, what kind of file is this. Is
8 this the type of the file that I'm looking for. Is
9 this a PDF file, or is this a Microsoft Word document
10 file because there is a difference between these two
11 file formats that's completely different.

12 After you parse this file, you identify the
13 part of the file, you need to go parsing the file.
14 These files, they have a format that is not human
15 readable. It's all binary, and only the application
16 is able to parse the file and put together all of the
17 pieces of the file before it can exhibit the file.

18 So it's naive to think that, and to try to
19 push these to the United States authorities, I think
20 it creates a false sense of security. As I told you
21 before, it can create a false sense of security. It's
22 like I'm secure. I have an IPS, and my files will not
23 be exfiltrated. You guys know that's not true.

24 The engineers, if you were asking if this
25 rule can prevent data exfiltration, they will say it

1 cannot because it's not that simple. It's not that
2 simple to resolve this problem just with an IDS or IPS
3 rule. It's very complex, and this is why I'm glad to
4 be here to clarify because the last thing we want,
5 especially right now that we are seeing that the world
6 is going through a very difficult time with all of
7 these wars going on, especially now we need to make
8 sure that the U.S. authorities know exactly what these
9 technologies can and cannot do because if they cannot
10 do what we need it to do, we need to develop new
11 technology.

12 We need to work more to make it happen.

13 So --

14 BY MR. DONOVAN:

15 Q. Mr. Marinho, I think I understood, but your
16 answer went off topic. I just want to make sure I
17 understand.

18 Is it correct that you're saying a system
19 could not prevent exfiltration by checking the HTTP
20 method in an application header field value?

21 A. I said that it cannot by checking only that.
22 It needs to check much more things, and things that an
23 IPS cannot check, just as I told you. To parse a
24 Microsoft Word file -- do you know how many lines of
25 code the Microsoft Word application has? How many

1 lines of code Adobe Reader has? It has thousands of
2 lines of code to parse these files.

3 So these IPS systems, they are already
4 overwhelmed with network threats they are trying to
5 match. They cannot stop to extract a file and try to
6 parse this file. It's not something that these
7 systems were designed to do.

8 Q. These systems were designed to also check
9 packet header field values; right?

10 A. That is correct, sir.

11 Q. Would a system that was designed to check
12 packet header field values against a rule and check
13 whether an application header rule value matched an
14 HTTP method prevent exfiltration?

15 A. I think it cannot.

16 Q. And could a system that checks application
17 header field values for an SSL or TLS version prevent
18 exfiltration?

19 A. It cannot prevent exfiltration. It can help
20 flagging on a potential event, a security event that
21 needs to be investigated and correlated with
22 different, other events emitted by different, other
23 systems by the operational system where these files
24 are residing in.

25 So the answer is no, it cannot.

1 Q. Earlier, we were talking about you had a role
2 at Emerging Threats as a vulnerability researcher;
3 right?

4 A. That is correct, sir.

5 Q. Are you aware of SSL V3 having any
6 vulnerabilities?

7 A. SSL V3 vulnerabilities.

8 I can't remember. I used to have -- I don't
9 remember if bleeding -- what was the name? I believe
10 it was a few vulnerabilities with SSL. There were
11 vulnerabilities. Hard to believe, but I can't
12 remember if this was on an SSL Version 3. I cannot
13 remember right now if these vulnerability heart
14 bleeding, or something like that, was on -- I cannot
15 remember, sir.

16 Q. Okay. And to clarify, I wasn't asking about
17 any specific vulnerability, but whether it's your
18 recollection that SSL Version 3 had vulnerabilities.

19 A. I believe I seen vulnerabilities on it, but I
20 cannot remember what was the version of the SSL
21 protocol of these vulnerabilities that I've seen
22 before. I cannot recall right now if it's on the
23 Version 3 or TLS 1.2 or something like that. I cannot
24 remember exactly on which version of the protocol
25 these vulnerabilities that I've seen were.

1 Q. And SSL Version 3 predated TLS; right?

2 A. SSL Version 3, yes. I believe so, yes. Yes.

3 Q. Do you recall that early versions of TLS also
4 had vulnerabilities?

5 A. I remember I seen a few vulnerabilities of
6 the SSL protocol, but I cannot remember which version
7 these vulnerabilities were affected. Which versions
8 were affected by these vulnerabilities. Sorry for my
9 poor English.

10 Q. Sorry. I think I understood this from your
11 testimony before, but checking the SSL or TLS version
12 in an application header field value can be used to
13 prevent exfiltration?

14 A. It cannot because it's too -- it's too short.
15 It's too unprecise. It's too inaccurate to matching
16 on a header of a packet, on an HTTP method and then
17 say, "Hey, I can prevent data exfiltration with that
18 because as I told you, all of the nuances of parsing a
19 file, such as a PDF file, a Word document file, it's
20 not something that an IPS was designed to do.

21 So in combination of what an IDS, IPS can do,
22 is to emit an alert of a potential condition that a
23 network administration needs to validate and correlate
24 with other events of other systems in order to
25 determine or -- that a data exfiltration is happening

1 and do the precautions to prevent it. But that alone,
2 that match on a header, on a direction, that alone is
3 not going to prevent data exfiltration. Lots of other
4 things need to happen to do that.

5 Q. Is that because detecting on the packet
6 header field values and the application header field
7 value indicating that SSL or TLS version would have
8 too many false positives?

9 A. Not because of that. It's just because when
10 you exfiltrate a file over SSL, the IPS system cannot
11 match on the file. It cannot match on the file
12 because it's encrypted over an SSL. Once these
13 connections are encrypted, the IPS, it loses. Even if
14 it has a rule to match on that file, it will not -- it
15 will never be able to match on encrypted traffic over
16 SSL. So it was -- yeah.

17 Q. When you say -- and this is again in
18 Paragraph 10, that the problem demands more
19 functionality than only an IDS, IPS can provide, is
20 that because no exfiltration can be detected by
21 matching signatures?

22 A. I say that because not every -- not
23 100 percent -- it's not 100 percent. It's not
24 something that can be prevented just with an IPS, IDS.
25 If we transfer a file over FTPS, secure FTP, the

1 traffic is encrypted over TLS, SSL, whatever
2 encryption protocol you're using.

3 So once this is encrypted, the IDS loses its
4 functionality of being able to match because it can
5 only match on things that are not encrypted. So this
6 is why I'm saying that that alone cannot prevent a
7 data exfiltration.

8 MR. DONOVAN: I think we've been going for
9 over an hour. Do you want to take a short break?

10 MR. PRICE: Yeah. How much longer do you
11 think we're going to go? Is this a good time for
12 lunch or...

13 MR. DONOVAN: I certainly -- well, I expect
14 less than another hour. Some parts of the questions
15 have taken longer than I expected. So I don't know.

16 THE WITNESS: Sorry about that.

17 (A recess was taken from 12:28 p.m.
18 to 12:36 p.m.)

19 MR. DONOVAN: All right, Mr. Marinho. We're
20 turning back to your declaration, Exhibit 2031 on
21 Paragraph 13.

22 John, could you go ahead and pull that up.

23 And in the middle of this paragraph, I don't
24 know if you see the bold word "potential," but the
25 sentence reads, "The signature was designed to detect

1 a potential download of a password file as a result of
2 a successful attack."

3 Q. Do you see that?

4 A. Yes, I do. Yes, sir.

5 Q. And what does that mean? And feel free to
6 review the portion before this if you need to for
7 context.

8 A. Uh-huh. Yes. I know exactly what this rule
9 is, and "potential" means we have the potential of
10 having false positives. Unfortunately, even if we
11 string like, we have hooch (phonetic) column, 00
12 hooch, hooch, hooch, and other variables in between.

13 Even with that, because we think as a human;
14 right? You see this -- you as a human, you look at
15 these and you, okay, so this is very unique; right?
16 This is what you think when you see this. This is
17 very unique. How can these false positive -- how can
18 they generate a false positive.

19 Believe it or not, those generate false
20 positives. So it's something that even a pattern that
21 you think is unique can generate false positives. So
22 this is why I say it's detecting a potential download
23 of a past DD file because it could have a false
24 positive, and it is not a past DD file.

25 Even when we look at these we might think,

1 okay, so this is a unique pattern. It will not have
2 any false positives. But when you test these rules,
3 when you run these rules over network traffic,
4 depending where you are running -- a university -- for
5 example, there's a lot of traffic on a university
6 coming back and forth and lab students accessing
7 different files, peer-to-peer and all of that.

8 When you get an environment like this and you
9 turn on a rule like that, you might end up finding
10 false positive things that are not an exfiltration of
11 a past DD file. So this is why we have the English
12 word "potential" because it has a chance of being a
13 path double DD file, but it can also have false
14 positives.

15 So that clarifies the phrase there. Please,
16 go on.

17 Q. Sure. And this is referring to the rule
18 sid 2002034; right?

19 A. That is correct, sir.

20 Q. And is it correct that that rule would alert
21 if a password file was leaving a network as a result
22 of a successful attack against a Linux system?

23 A. That is correct.

24 Q. And this rule would also alert false
25 positives if another file matched the rule; is that

1 right?

2 A. The file could be any other -- we can't say
3 exactly what would trigger that, but what I can say is
4 that it can trigger an alert for things that are not a
5 path DD file leaving the origin. So this is why this
6 rule, it could not be set to drop because these kind
7 of rules can drop things that are not a file
8 exfiltration. Path DD file exfiltration. It can
9 match other things.

10 I know someone copying a Windows
11 installation -- I can't think of a good example right
12 now, but it can match on other things that -- and
13 trigger alerts that is not -- I mean this is not
14 100 percent accurate. This rule will not match exact
15 100 percent of the time on a path DD file leaving or
16 not. It can match on other things, and it does
17 generate false positives.

18 And this is the reason why all of these
19 rules, they have the keyword alert. We are not
20 designing -- we were -- we were not designing rules to
21 drop traffic because of the potential of false
22 positives. The risk of blocking a traffic that is not
23 supposed to block can cause problems on our customer
24 networks.

25 So these rules, they are just for alerting

1 and not to drop traffic. And please, go on.

2 Q. Is it your understanding that the intention
3 of the rule sid 002034, was to be triggered if there
4 was a successful attack and a password file analytic
5 system was leaving a network?

6 A. That is the goal of this rule, yes.

7 Q. All right. Let's go to Paragraph 14. And
8 this is addressing rule sid 00101238.

9 Do you see that?

10 A. I do see, yes, sir.

11 Q. And it says this was submitted by Patrick
12 Harper and then pcre by Matt Jonkman.

13 Did you know Patrick Harper?

14 A. I've never met this person.

15 Q. This would be someone else submitting rules
16 to the Emerging Treats rule set?

17 A. That is right, sir, yes.

18 Q. And does "pcre" by Matt Jonkman mean that he
19 added the regular expression of the rule?

20 A. That is correct, sir.

21 Q. And the comment before the rule says, "This
22 rule is disabled by default. It should generally be
23 run on the outside of your network, not internally.
24 Enable it where useful."

25 Do you see that?

1 A. I do see that, yes.

2 Q. And what do you understand that to mean?

3 A. It doesn't make too much sense to me because
4 this is another example of a rule that it's commented
5 out, and it's matching on anything. It's matching on
6 anything. This is going to be a nightmare to someone
7 that is attempting to -- to protect a network because
8 this is going to generate so many events that I mean
9 it cannot be used as a -- as a rule on an IPS system.

10 You cannot block this because this regular
11 expression it's matching on the pattern we find on a
12 Social Security number, but also, it matches on
13 everything else. It matches on any sequence of
14 numbers that happen to have these dashes in between.

15 So this rule, it will not prevent data
16 exfiltration. To think that that rule is going to
17 detect Social Security number is to assume that we
18 have a rule capable with 100 percent of accuracy, and
19 this is the worst rule. I believe this is the worst
20 rule of the entire rule set because it only has a
21 regular expression matching numbers and dashes. It
22 can match on anything because it's matching on any
23 port on any direction, and it should be run outside of
24 your network, not internally.

25 I don't understand what these guys mean about

1 that back in the time. So I cannot answer that. I
2 don't know what this means. It should generally be
3 run on the outside of the network, not internally.
4 Yeah, that part doesn't make too much sense to me,
5 this comment. I did not write this comment. So I
6 cannot understand it, why run it outside of a network.
7 I don't know what they mean by that.

8 Q. Where it says, "enable it where useful,"
9 would you understand that as Mr. Harper and
10 Mr. Jonkman thinking this rule might be useful to some
11 people?

12 A. Maybe where useful, yes. Or at least that's
13 what we understand about reading this. Enable it
14 where useful. That's part of the English phrase.
15 Enable it where you think it's useful. That's what it
16 is.

17 Q. And would you understand "enable it where
18 useful" to mean if this rule would be useful, remove
19 the hash before alert and then load it into a system
20 to use the rule?

21 A. Yes. That means exactly -- because enable
22 means doing exactly what you just said. Removing the
23 dash (sic) sign, symbol here, and this will be loaded.
24 But as I told you, these regular expressions, it
25 matches any number followed by dashes, and then you

1 have a number and you have a dash over every single
2 port. So you cannot use this -- excuse me. I'm
3 sorry.

4 You cannot use this rule to drop traffic, and
5 it will generate a million events in minutes, and it
6 will also have the worst performance possible because
7 as I told you, it will attempt to run this regular
8 expression for every packet. It doesn't matter if
9 it's outbound, on every packet it's going to run this
10 regular expression.

11 So this is -- I mean this rule is something
12 that -- it cannot be loaded. Even if you enabled
13 where it's useful, you are going to make your life a
14 nightmare because you see so many alerts, it will say
15 what is this? This is not a Social Security number.
16 This is something else, and you waste your time. And
17 if you set this rule to drop, you're going to drop
18 traffic that was not supposed to be dropped because if
19 you think about this, Mr. Donovan, when we have
20 encrypted -- when we have a rule like this, any, any,
21 any, any on the header of the rule, it doesn't have a
22 port number. It doesn't have a direction.

23 It's matching on any traffic that's over the
24 network. Any traffic. It's matching on TCP. It's
25 matching on UDP. It's matching on every single

1 packet. And these regular expressions will match a
2 lot. Trust me, this regular expression will match a
3 lot. This rule is not -- it's impossible to prevent
4 data exfiltration with this rule.

5 Q. So a question, I think, just to make sure
6 there's not a translation issue here. I think you
7 referred to "dash alert." Is it correct -- are you
8 referring to the number sign or the hash sign before
9 the word "alert"?

10 A. That's correct, sir. Hash sign. I'm sorry I
11 said dash. It's hash.

12 Q. Thank you.

13 So the hash sign before alert, h-a-s-h, is
14 showing here that the rule is disabled; right?

15 A. That is correct, sir.

16 Q. And where it says, "enable where useful," in
17 order to enable this rule you would remove the hash
18 sign before alert and then load it into either a SNORT
19 or another compatible system; right?

20 A. That is right, yes.

21 Q. Thank you.

22 Let's go down to Paragraph 17 of your
23 declaration.

24 A. Yes, sir.

25 Q. And this is discussing rule sid 2005319.

1 A. Yes.

2 Q. Do you see that rule?

3 A. Yes, I do.

4 Q. And what is this rule intended to do?

5 A. This rule is checking on a URL -- a part of a
6 URL. It's not a complete URL. We need to make sure
7 we know this because when you work with these rules
8 and you validate these rules, you test it, you see
9 lots of URLs that match this substream zuzu.php. So
10 this rule is attempting to match access to this URL,
11 but it's not the complete URL. It's just a part. And
12 we have URLs that are bigger and they can have this
13 pattern on the URLs, and this rule, again, it can
14 false positive.

15 And that's why we do ship these rules with an
16 alert option instead of drop because it can generate
17 false positives. It can end up blocking things that
18 is not malware. So this is what this rule can and
19 cannot do. Like it cannot drop traffic because it
20 could drop legitimate traffic. And what it's doing,
21 it's attempting to match on a pattern that a malware
22 was using to communicate this common control server.

23 Q. And this is checking TCP packets going from
24 the home net on any port to an external net on HTTP
25 ports; right?

1 A. That is correct, sir.

2 Q. And this rule, where it says, "content:
3 'POST'; depth:5," what does that mean?

4 A. It is attempting to match on the HTTP a
5 method post that on the five first -- five initial
6 bytes of the packet's payload.

7 Q. And that's an application header field value
8 and an HTTP packet; right?

9 A. That is right.

10 Q. And do you see the part of the rule that says
11 "uricontent zuzu.php"?

12 A. I do.

13 Q. That's what you were referring before, where
14 it's checking whether that's a portion of the URL in
15 the HTTP packet; right?

16 A. That is correct. Yes.

17 Q. And what would happen in this rule if you
18 removed the URI content portion?

19 A. If I remove the URI content portion? Can you
20 scroll up a little bit so that I can see the rule
21 because I --

22 Q. Yes.

23 A. It would match on everything leaving your
24 network over port 80 -- I mean http port, sorry, that
25 has a post on the very first 5 bytes of the packet

1 payload. It would basically match on every single
2 post.

3 Q. So it would be matching, then, on every HTTP
4 packet that had a post in its application header field
5 value; is that right?

6 A. That is right, yes.

7 Q. And would that have more false positives?

8 A. That would have more false positives, yes.
9 That's correct.

10 Q. Could that rule detect exfiltration from the
11 network that's using an HTTP post method?

12 A. Can you clarify if you're asking after
13 removing the URI content or with the URI content?

14 Q. Sure. Without the URI content, would this
15 rule detect exfiltration from a network that was using
16 an HTTP post method?

17 A. No.

18 Q. Why is that?

19 A. Because it would detect every single HTTP
20 request that is leaving the network. So -- and these
21 are not data exfiltration. It's just a normal web
22 traffic. So if you do that, you basically are not
23 detecting anything and generating a bunch of events
24 that you -- basically, you don't have anything to do
25 with these events.

1 I mean you would have one event, one alert
2 every time someone accesses a website that is not
3 encrypted, I mean doesn't use HTTPS. So these will
4 align with just a post content match. It will not
5 prevent or detect any sort of a data exfiltration. It
6 will only generate noise and false alerts, alarms.

7 Q. So detecting a post content match in an HTTP
8 packet application header field value can't be used to
9 detect exfiltration?

10 A. Again -- again, it would be not that alone.
11 Just mentioned on a post method will not enable you to
12 detect the exfiltration because that alone is not --
13 it's much more complex than that. Data exfiltration,
14 if a guy copies a file to Gmail, when he copies the
15 file and sending out to another E-mail, this threat is
16 encrypted. So the post content match will never match
17 because it's encrypted.

18 So you cannot assume that with only a content
19 post, a content match to a post through the HTTP match
20 it's able to detect and prevent data exfiltration
21 because the great majority of the connections there
22 happen over encrypted channels which you don't have
23 the great majority of the connections happening over
24 any encrypted channels.

25 The great majority happens over Port 443, not

1 over HTTP ports, and when it's encrypted, the IPS,
2 IDS, it loses visibility on the traffic because it's
3 encrypted and you cannot match on encrypted data. And
4 that's why.

5 Q. Do you see the message field here? It says,
6 "'ET MALWARE Bizconcept.info Spyware Checkin"?

7 A. I do see, yes, sir.

8 Q. I can't is -- what do you understand that to
9 mean?

10 A. That is -- first, we have a category, a
11 malware. That's what this rule was designed to
12 detect, and then we have the name of these spyware
13 that is business content.info. Excuse me. This is
14 basically a message to say, "Hey, network
15 administrator, I've seen an outbound connection to a
16 suspicious URL, and it could be this malware. Have a
17 look."

18 It's like this is what these rules were
19 intended for. It's emitting an alert that would start
20 an investigation. It was not designed to prevent and
21 to block connections, preventing data exfiltration.
22 This is not what these rules were designed for.

23 Q. And what is spyware?

24 A. Spyware is a type of malware that it gets
25 installed on our computer and it can do a variety of

1 things. Basically, it's a type of malware. It's a
2 malware --

3 (Indiscernible crosstalk.)

4 BY MR. DONOVAN:

5 Q. What are the -- what are the variety of
6 things that spyware is used for?

7 A. Spyware, it can -- it can like take a
8 screenshot of our screen and send it out over a common
9 control to a server. It can capture what you're
10 typing on a text file and send it out to a common
11 control server. So spywares were designed to actually
12 spy, collect information on the system and exfiltrate
13 it.

14 Q. Okay. Let's go down to Paragraph 18. Do you
15 see rule sid 2010234?

16 A. Yeah, I do see. Yes.

17 Q. And this rule says, "message 'ET
18 CURRENT_EVENTS FakeAlert/FraudPack/FakeAV/Guxx.Dload
19 /Vobfus/ZPack HTTP Post 1.'"

20 Do you see that?

21 A. I do see, yes, sir.

22 Q. Do you have an understanding of what this
23 rule does?

24 A. It's just like the rule we just reviewed.
25 It's checking for a piece of malware that communicates

Page 110

1 over its common control but accessing this URL that's
2 on the URI content match, and it also sends data using
3 an HTTP post method. So this is what this rule is
4 trying to -- it was designed to emit an alert if we
5 see an HTTP outbound connection over an encrypted, of
6 course, because IDS cannot match encrypted data.

7 If it's unencrypted, then the IDS can match.
8 So if it's unencrypted and it's accessing that URL, it
9 will generate an alert. So the network administrators
10 have something to start an investigation, to look and
11 say could be that this host is an effective malware.
12 What can I do? Let me check other logs. Let me check
13 the antivirus that's running on the host.

14 If we have more evidence, which process, and
15 then they can start an investigation with other
16 evidences that are not created by an IPS system.

17 Q. And this rule would be triggered by traffic
18 that's going from the home net to the external net on
19 HTTP ports; right?

20 A. That is correct, sir.

21 Q. And this would be outbound traffic in --
22 well, in an HTTP post method; right?

23 A. That is correct.

24 Q. So it would be checking the IP packet header
25 values for the -- to make sure it's traffic going from

1 the internal net to the external net, and then it
2 would be checking the HTTP packet header values to
3 make sure it's a post; is that right?

4 A. That is right.

5 Q. And the URI content, and then it has a
6 portion of the URL match. Below this you say -- and
7 this is Paragraph 19, "Signatures that only have a
8 short URL content match will false positive and should
9 not be set to drop."

10 That's the same explanation you gave in the
11 context of the prior rule. I assume that's the same
12 as why you were saying you wouldn't expect the other
13 rule to drop?

14 A. Exactly the same reason, sir. And I know
15 that because I was working with the rules, and I used
16 to test this rules. We -- as humans, we might think
17 that, okay, so this URL it's very unique, but the
18 number of URLs that has php, a question mark, data
19 equals, it's beyond what you can imagine that would
20 happen.

21 There are so many where else (sic) that has
22 PHP question mark data, and there is a lot of URLs
23 that can start with this that makes these rules not
24 eligible to be said to drop. I mean these rules, they
25 have the potential of blocking traffic that is not

1 tended to drop, and this is why these rules were
2 shipped with the action as alert, because of that.

3 When we mention URLs, we might think, you,
4 me -- even me, that I work with this, I might look at
5 this and say, "This is unique enough that it will
6 never false positive. I can't block -- I can't set
7 this rule to drop." And then we find we block things
8 that it was not supposed to.

9 So when matching on URLs, it's very, very
10 dangerous because there are so many URLs out there
11 from advertisements, from things that -- websites and
12 other things that are on the web that these rules,
13 they have the potential of false positives because
14 less -- how do you say this. The shorter the content
15 match, the greater are the chances of having false
16 positives. And this URL you can think of it -- you
17 can ignore .php question mark data equals because this
18 happens a lot.

19 On a lot of different URLs you have php
20 question mark data equals. So this URL is going to
21 match a ton. If we have a URL starting with /SENN.
22 and then you have a php question mark data equals,
23 then you have a false positive, and I mean this rule
24 is not bulletproof. It's not perfect. It's not
25 100 percent accurate. It can generate false

1 positives, and this is why these rules were shipped
2 with an alert instead of dropping.

3 So I hope this clarifies because it's the
4 same situation as the rule we just reviewed. We have
5 a very short URL, and it's very dangerous to set these
6 rules to drop because URLs, they are a whole universe.
7 We have -- we have like billions of URLs, and we are
8 only mentioning a portion of URL.

9 If we have the complete URL, it was a pattern
10 that's very precise, then we would think about that we
11 can drop with the rules. But this doesn't happen
12 because when a URL -- the reality is that on a URL you
13 are passing parameters, and these parameters, they
14 change because they are passing numbers that will
15 change. Data equals will change every time. It will
16 not be the same.

17 What comes next, the equal here will change.
18 So we cannot view the rule that will match on the data
19 on the parameters that are being passed. We can only
20 match on a small portion of the URL, and URLs are very
21 big and URLs short like this have a great chance of
22 generating false positives. So I hope it's clear.

23 Q. So turning back to the -- and thank you for
24 that answer.

25 Turning back to the syntax of the rule

1 itself, this rule would be checking on packets that
2 match the packet header values with the TCP home net
3 any external net to HTTP ports; right?

4 A. That is right, yes. That's the header of the
5 rule. It will match the header of the TCP protocol.

6 Q. And in order for this rule to alert, it would
7 have to both match in the application packet header --
8 well, the application packet header values would have
9 to include the post method, and they would also have
10 to include the URI content/SEMM.php?data equals;
11 right?

12 A. That is correct, sir.

13 Q. And so if a packet was leaving the network
14 that matched the packet header field values set forth
15 in this rule, and also included the application header
16 field values post and the URI content specified here,
17 that would then trigger the rule; right?

18 A. That's correct, sir, yes.

19 Q. And is it fair that this rule could be used
20 to detect exfiltration but it would also have a lot of
21 other false positives, in your view?

22 A. Yes. And this is why -- and because of the
23 false positives, these rules were not made to drop
24 traffic. They were made to alert, and when you alert
25 you don't block, and then you cannot prevent a file

1 from exfiltrating your network because this rule was
2 not designed to detect a file exfiltration or even
3 prevent a file exfiltration.

4 It was designed to detect a potential malware
5 communication with its common controls server. So
6 this rule is just to emit an alert so that you can
7 initiate an investigation with other types of logs in
8 advance from other systems so that you can determine
9 if something out of the usual has happened.

10 It doesn't -- it cannot contain 100 percent
11 data exfiltration because it's not 100 percent
12 accurate. As I told you, the size of the URL, the
13 content match is too short. The shorter the size, the
14 length -- sorry. The shorter the length, greater are
15 the chances of having false positives. And that's
16 true.

17 Q. Is one reason why malware communicates with
18 its commanding control server to exfiltrate data?

19 MR. PRICE: Objection.

20 THE WITNESS: I cannot understand this
21 question. Can you please repeat?

22 BY MR. DONOVAN:

23 Q. Sure.

24 And just for context, if I understand right,
25 this rule is designed to be triggered when malware on

1 the system is communicating outbound to a command and
2 control server; is that correct?

3 A. That is correct, yes.

4 Q. And is one reason why malware on a system
5 would be communicating outbound from a network to a
6 command and control server to exfiltrate data?

7 A. It could be one of the functions of a
8 malware, but malwares do communicate with common
9 control server also over HTTPS, not only over HTTP.
10 So how can the IDS matches on something that's
11 encrypted? I mean it would have to unencrypt and then
12 match.

13 So I mean this is why I'm saying -- these
14 rules, they are a weak signal. They are a signal that
15 a network administrator has to start an investigation.
16 This should go after all the types of logs, other
17 events that happened on the level of the operation of
18 system in order to understand if something is
19 happening.

20 This is like it's an alert. This is not a
21 drop in traffic. So that we need to make sure that we
22 do not assume that these rules have the -- the power
23 of doing something that it was not designed for.
24 So...

25 Q. But this rule -- if I understand right, this

1 rule was designed for sending an alert when it detects
2 that there is outbound traffic from malware to a
3 command and control center; right?

4 A. Yes. That's correct.

5 Q. And is it correct that one of the reasons
6 that malware would communicate with the command and
7 control server is to exfiltrate data?

8 A. That's correct, sir, yes. One of the
9 reasons. Yes, sir.

10 Q. In Paragraph 19, seven lines down there's a
11 sentence that says, "The signature was created to
12 monitor for potential malware activity. But will not
13 detect with 100 percent of accuracy based alone on a
14 URL match that is very common."

15 Is this going to what you were discussing
16 before, that this will match on traffic going from the
17 malware to the command and control server, but it
18 won't be perfect?

19 A. It won't be perfect, yes. You want to have
20 100 percent of accuracy, because we are matching only
21 a portion of the URL. We are not matching on the
22 entire URL. As I told you, URLs, they carry
23 parameters. We are passing numbers that will change
24 all the time. So we cannot build an IDS rule that
25 would mention what malware is sending over a URL that

1 match with 100 percent accuracy, because we cannot
2 match on the entire URL. We can only match on a small
3 portion of the URL, and that makes these rules not 100
4 percent accurate.

5 So this is why.

6 Q. Mr. Marinho, if we can go down to
7 Paragraph 22 of your declaration. And here you say
8 that you "declare that all statements made herein are
9 of my knowledge are true and that all statements made
10 on information and belief are believed to be true."

11 A. Yes, sir. I do, and I swear solemnity,
12 everything that I say, from the best of my knowledge
13 and with honor to the United States, to your country,
14 everything that I said, to the best of my knowledge,
15 is true. I'm not lying, and everything I said is
16 true.

17 Q. Did you write this declaration yourself?

18 A. I did not write this. This was -- this was
19 the counsel.

20 Q. So you reviewed the declaration after counsel
21 wrote it, and then you signed it?

22 MR. PRICE: Objection.

23 BY MR. DONOVAN:

24 Q. You can answer the question.

25 THE WITNESS: Can I answer?

1 MR. PRICE: Yes.

2 THE WITNESS: Can you ask again, please?

3 BY MR. DONOVAN:

4 Q. Yes.

5 You reviewed this application after your
6 counsel wrote it, and then you signed it?

7 MR. PRICE: Objection.

8 THE WITNESS: No. This was not the way it
9 happened. I written every single explanation about
10 why these rules cannot detect and prevent with
11 100 percent accuracy. After writing that, this
12 declarations, this was added to this document. And
13 after reading the entire document, I did sign.

14 So there was no -- I mean they didn't wrote
15 all of this and I just sign it. That's not true.

16 BY MR. DONOVAN:

17 Q. Thank you for the clarification.

18 A. Yes, sir.

19 Q. And did you meet with anyone to prepare for
20 your deposition today?

21 THE WITNESS: Can I answer that?

22 BY MR. DONOVAN:

23 Q. And also, just to clarify, I'm not asking
24 about your communications with counsel. I'm asking if
25 you did meet with anyone.

Page 120

1 MR. PRICE: Again, I'll just caution the
2 witness, you may answer the question. Just do not
3 divulge the contents of our communications.

4 THE WITNESS: Yes, sir. The answer is yes.

5 BY MR. DONOVAN:

6 Q. All right. I'm going ask a few more
7 questions. For all of them, I'm not asking about the
8 contents of your communication with counsel.

9 A. Yes, sir.

10 Q. Who did you meet with to prepare for this
11 deposition?

12 THE WITNESS: Can I answer?

13 MR. PRICE: You may.

14 THE WITNESS: Jeffrey.

15 BY MR. DONOVAN:

16 Q. Anyone else?

17 A. No, sir.

18 Q. And when did you meet?

19 THE WITNESS: Can I answer? Sorry.

20 MR. PRICE: Yes.

21 Pedro, you can answer the questions. I'll
22 tell you if a question comes up that --

23 THE WITNESS: Okay. Yes. Sorry.

24 Yesterday, sir.

25 BY MR. DONOVAN:

1 Q. Is that the only time?

2 A. It was the only time.

3 Q. And about how long did you meet for?

4 A. About two hours.

5 Q. Did you review any documents during that
6 meeting?

7 A. Yes, sir.

8 Q. What documents did you review?

9 A. The one you just showed with the description
10 of the rules.

11 Q. Anything else?

12 A. Not that I can remember.

13 Q. Did you meet with anyone other than your
14 attorneys to prepare for this deposition?

15 A. To prepare for the deposition, no.

16 Q. Did you meet with anyone other than your
17 attorneys to prepare the declaration? And that was
18 Exhibit 2031.

19 A. No. To prepare this, no. They send me a --
20 I'm not going to say, but just I wrote it, I send it
21 to them, and deposed, and then we met only yesterday.

22 MR. DONOVAN: All right. I have no more
23 questions. I appreciate your time today.

24 THE WITNESS: Thank you, Mr. Donovan and Jeff
25 Price for your time, and I hope that I helped because

1 as I said, I'm very worried with people thinking that
2 we can prevent data exfiltration with just an IPS
3 system.

4 That is not true, and I'm worried about that,
5 and we need to make sure that we know what the systems
6 can and cannot do. And if it cannot do what we need
7 it to do, we need to better develop systems.

8 So I appreciate it. I hope I helped, and
9 yeah, this is all I got.

10 MR. PRICE: I just have a very short
11 redirect.

12

13 EXAMINATION

14 BY MR. PRICE:

15 Q. Do you need a break or -- Pedro, I'm just
16 going to ask you maybe a few questions.

17 A. Go ahead, yes.

18 Q. Yes. Do you recall when counsel was asking
19 you questions -- any questions about a rule with the
20 password file?

21 A. The rule with the pass- -- yes.

22 Yes, I remember.

23 Q. And can you explain what information is
24 included in a Linux password file?

25 A. The Linux password file is a file that we

Page 123

1 hold the -- it's like a reference to another file. It
2 doesn't have the passwords, first of all, because we
3 might think that the password file has the actual
4 passwords, and it doesn't. The password file doesn't
5 have the passwords. It has the lines with the users,
6 like all of the users.

7 Let's suppose we have a Linux running in the
8 Oracle database. We have the user Oracle. We have
9 the user Apache HTTP server. We have the hooch user
10 and all of that. And this file, the past DD file, it
11 gives an indication of the users that has on a Linux
12 system. That's what it does, yes, sir.

13 Q. So the system passwords are not included in
14 is that password file; correct?

15 A. That's correct, sir. Yes.

16 MR. PRICE: Okay. I have no questions.

17

18 FURTHER EXAMINATION

19 BY MR. DONOVAN:

20 Q. And just to -- I think this was explained,
21 but it does include the information about the user
22 accounts, just not the passwords in the password file;
23 is that right?

24 A. That is right, sir, yes.

25 MR. DONOVAN: I have no more questions.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

(Witness excused.)

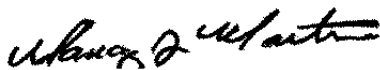
(Deposition concluded at 1:18 p.m.)

Page 125

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

C E R T I F I C A T E

I do hereby certify that the aforesaid testimony was taken before me, pursuant to notice, at the time and place indicated; that said deponent was by me duly sworn to tell the truth, the whole truth, and nothing but the truth; that the testimony of said deponent was correctly recorded in machine shorthand by me and thereafter transcribed under my supervision with computer-aided transcription; that the deposition is a true and correct record of the testimony given by the witness; and that I am neither of counsel nor kin to any party in said action, nor interested in the outcome thereof.



Nancy J. Martin, RMR, CSR

Dated: 1/28/24

(The foregoing certification of this transcript does not apply to any reproduction of the same by any means, unless under the direct control and/or supervision of the certifying shorthand reporter.)

INSTRUCTIONS TO WITNESS

Please read your deposition over carefully and make any necessary corrections. You should state the reason in the appropriate space on the errata sheet for any corrections that are made.

After doing so, please sign the errata sheet and date it. You are signing same subject to the changes you have noted on the errata sheet, which will be attached to your deposition. It is imperative that you return the original errata sheet to the deposing attorney within thirty (30) days of receipt of the deposition transcript by you. If you fail to do so, the deposition transcript may be deemed to be accurate and may be used in court.

- - - - -

E R R A T A

- - - - -

[illegible]

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

ACKNOWLEDGMENT OF DEPONENT

I, PEDRO MARINHO, do hereby certify that I have read the foregoing pages, _____ to _____, and that the same is a correct transcription of the answers given by me to the questions therein propounded, except for the corrections or changes in form or substance, if any, noted in the attached Errata Sheet.

DATE SIGNATURE

Subscribed and sworn to before me this _____ day of _____, 20__.

My commission expires: _____.

Notary Public

&	120:11	19 112:7	66:12
	1000 3:9	118:10	2010220 65:13
	10036 3:4	1:18 125:2	2010234 110:15
0	1020 4:9 8:20	2	2010630 56:22
0 80:20	48:14,16 56:21	2 9:25 12:21	56:24 59:24
00 76:21 77:6	62:22 65:11	50:13 51:7	2011 63:14
77:20 79:3,6	66:16	52:15 53:2,2	2011232 62:25
97:11	1024 51:15	56:7 75:10	2012 80:1,22
00's 55:21	73:7 76:1	20 9:20 46:17	2016 23:6
000 53:16	77:25 78:16,22	46:23 129:17	31:12 46:25
00101238 100:8	78:25 79:11	20005 3:10	2019 10:1
002034 100:3	115 62:23,24	2001 13:7,7,8	202 3:10
008806 56:5	63:4	17:4	2023 9:20
01 52:16 53:11	116 62:24 63:5	2002034 98:18	2024 1:16 2:13
03 76:21 77:6	1177 3:3	2002526 79:18	5:1
77:20 79:3,6	11:00 48:9	2003021 72:19	2031 4:10 8:21
0b 52:16 53:11	11:08 48:10	2005319 104:25	9:8,9,17 70:15
1	123 4:4	2008 14:13	96:20 122:18
1 1:25 53:2	124 4:5	26:22	212 3:4
67:6 110:19	126 65:11	2008389 66:17	22 119:7
1,000 41:8	129 1:25	70:11	23 1:16 2:13
1.2 93:23	12:28 96:17	2008805 48:23	5:1
1/28/24 126:17	12:36 96:18	2008806 56:7	23rd 80:1,22
10 46:24 79:17	13 18:10 66:14	2010 12:23	28805 53:6
85:12 95:18	96:21	13:7,8 14:11	3
10,567,343 1:7	1301 3:9	14:13,13 17:3	3 23:3 31:9
2:7	14 66:14 100:7	17:4 19:9	53:2 73:8,15
100 41:8 47:6,7	16 53:2	22:19,23 23:6	78:15 79:9
61:22 74:5,8	162 48:15	23:9 26:23	93:12,18,23
74:22 82:4	17 76:21 77:6	31:11,12 32:7	94:1,2
95:23,23 99:14	77:20 79:3,6	33:23 34:2,4	30 127:12
99:15 101:18	104:22	34:16 37:17,24	3128 67:7,10
113:25 116:10	177 66:16	38:16 39:13	68:11
116:11 118:13	18 110:14	43:6,7 46:10	
118:20 119:1,3		46:25 57:24	

[4 - affirmed]

4	9		
4 43:14 53:2 60:25 63:21 69:13,20 76:21 77:20 414-9200 3:10 43 56:21 443 108:25 48 4:9	9 4:10 78:12 80:20 9504 1:24 975 126:15 9:57 2:16 5:2	accuracy 61:22 74:5 101:18 118:13,20 119:1 120:11 accurate 74:9 89:18 99:14 113:25 116:12 119:4 127:14 accurately 83:23 acknowledg... 129:1 acrobat 83:20 act 29:11 action 29:18,19 29:20,23,24 31:1,1 35:15 60:4 113:2 126:12 activate 71:8 79:22 activated 51:21 activity 85:14 118:12 actor 32:25 33:2 88:1 actual 81:5 124:3 actually 11:16 29:4,13,24 30:6 33:14 34:22 60:13 62:23 82:11 110:11	added 100:19 120:12 addition 28:20 42:18 additional 68:3 70:12 address 25:12 31:20 59:21 60:6 addresses 11:1 25:10 35:20 60:3 addressing 72:18 79:18 100:8 administration 94:23 administrator 41:25 53:10 54:12 84:22 87:1 109:15 117:15 administrators 36:18 111:9 adobe 83:20 92:1 advance 116:8 advantage 33:1 advertisements 113:11 adware 57:9,10 57:15 affected 94:7,8 affirmed 5:5
5	a a.m. 2:16 5:2 48:9,10 ability 34:9 able 19:18,20 19:23 33:15 45:9,12 49:1 50:19,23 63:15 65:24 83:23,24 84:17 90:16 95:15 96:4 108:20 above 53:5 78:25 accepted 22:25 47:23 access 33:3 37:6 41:22 86:17,21,21,24 87:2,9,11 88:10 105:10 accessed 75:2 accesses 108:2 accessing 31:19 64:23 65:3 98:6 111:1,8 accounts 124:22		
6			
6 53:2 70:18 64 73:11 64,000 73:11 65,000 77:5 65535 76:1 77:25 78:16,22 79:12			
7			
7 67:2,3 68:13 68:18 69:16,21 71:12 715-7502 3:4			
8			
8 72:18 80 106:24 805 56:11,16,17 806 56:10,16			

[aforesaid - attached]

aforesaid 126:2 agent 49:4 63:17,19,20 64:3,7,17,19,21 64:25 65:5 66:1 ago 18:10,10 63:14 66:14,14 ahead 72:13 85:11 96:22 123:17 aided 126:9 alarms 25:4 50:15 108:6 alert 29:9,10,17 29:21,21 30:3 30:7,23,24 31:1 33:17 36:12 60:4,19 60:20,22 64:16 67:14,16,22 68:1,6 70:23 70:24 71:1 75:25 78:13 79:12,22 83:3 84:21 94:22 98:20,24 99:4 99:19 102:19 104:7,9,13,18 105:16 108:1 109:19 111:4,9 113:2 114:2 115:6,24,24 116:6 117:20 118:1	alerting 51:20 67:5 99:25 alerts 35:15 50:16 53:25 54:4 67:21 75:3 80:25 99:13 103:14 108:6 align 108:4 alive 51:1 all.rules. 45:18 allow 58:19 allows 33:2 americas 3:3 ampersand 61:17 analysis 31:10 32:1 43:16 analyst 10:2,10 23:5 analysts 11:20 analytic 100:4 analyze 37:7 40:20 71:16,20 anjuan 11:9 annotation 71:6,9 answer 6:24 8:2 15:11,22 16:10 28:15 34:14 42:14 60:15 72:2,10 72:14 86:5 89:4 91:16 92:25 102:1	114:24 119:24 119:25 120:21 121:2,4,12,19 121:21 answering 14:22 16:16,18 25:4 75:9 answers 7:9 16:1 129:6 antivirus 111:13 anymore 14:5 66:11 apache 124:9 appeal 1:3 2:3 appear 66:19 appeared 2:18 appears 66:21 appliance 27:10,11 28:9 application 12:17,19 33:2 35:17 53:18 61:8 62:6,19 64:14,22 65:2 66:4 68:19 69:13 76:2,6 77:20 78:21 83:5,17 89:1 90:15 91:20,25 92:13,16 94:12 95:6 106:7 107:4 108:8 115:7,8,15 120:5	applications 61:25 65:6,22 78:22 79:11 applies 76:3 apply 126:22 appreciate 122:23 123:8 appropriate 127:5 april 80:1,22 archived 45:18 asked 22:23 37:3 75:9 88:22 asking 15:10 16:17 37:2 47:11 56:1 72:6,7 90:24 93:16 107:12 120:23,24 121:7 123:18 aspect 31:24 aspects 40:22 assisting 39:25 associated 80:12 assume 49:17 49:19,20 101:17 108:18 112:11 117:22 assuming 57:18 65:20 attached 127:10 129:8
--	---	--	---

[attack - bytes]

attack 74:21 97:2 98:22 100:4 attacks 32:20 43:18 attempt 7:4 32:12,14,22,22 33:15,18 36:10 103:7 attempting 61:3 89:25 101:7 105:10 105:21 106:4 attend 13:3,5 attended 42:8 43:4 attention 58:25 attorney 127:12 attorneys 122:14,17 authored 46:17 46:21 63:9 66:7 authorities 55:5 59:11 85:1 90:19 91:8 available 9:10 46:13 48:17 avenue 3:3 aware 17:25 26:14,20,22 42:2,7,15 93:5	b bachelor's 12:23 back 12:21 26:21,22 27:4 33:23 35:9 38:11 39:20 42:7 45:2 54:18 58:22 62:22 64:5 70:15 85:12 96:20 98:6 102:1 114:23 114:25 bad 24:19,20 39:4 80:14,15 81:17 based 37:10,11 75:19,20 118:13 basically 10:19 52:20 80:19 107:1,22,24 109:14 110:1 becoming 37:16 beginning 2:16 67:2 belief 119:10 believe 18:4,11 19:8 20:1,4,21 20:22 47:21 54:16 70:2 93:9,11,19 94:2 97:19	101:19 believed 119:10 belo 5:1 best 30:21 119:12,14 better 85:3,3 123:7 beyond 112:19 big 40:25 79:4 79:5 114:21 bigger 105:12 billions 114:7 binary 81:25 82:1 83:14 85:23 89:15,16 90:15 bit 43:16 79:25 106:20 bits 69:13,16 69:20,21 77:20 bizconcept.info 109:6 bleeding 18:8,9 18:11,11,11,14 18:14,18,18 22:9,9 93:9,14 blend 68:23 block 99:23 101:10 109:21 113:6,7 115:25 blocking 99:22 105:17 112:25 bnm 49:4,4 board 1:3 2:3	body 63:4 bold 96:24 booby 59:2 bottom 48:24 63:3 65:12 66:17 brazil 5:1 14:4 break 7:25 8:3 48:1,4,6,12 96:9 123:15 breaks 7:24 88:14 briefly 35:12 bring 9:7 48:14 48:15,19 broader 69:15 69:18 browser 64:24 64:24,25 build 118:24 built 44:3 bulletproof 113:24 bunch 39:3 53:12 107:23 business 109:13 buy 58:12 byte 33:7 bytes 50:13 51:7 52:15 53:2,3 56:7 67:2 68:18 70:2 73:8,15 79:3,6 85:23

[bytes - coming]

89:17 106:6,25	certainly 96:13	86:14,14 91:22	88:24 91:4
c	certification	91:23 92:8,11	93:16 107:12
c 3:1 26:11	126:21	92:12 111:12	120:23
126:1,1	certified 2:17	111:12	cleaninternet
call 50:6,7,9	certify 126:2	checkin 109:6	10:17
58:10 59:18	129:3	checking 25:10	clear 5:14
71:6 74:17	certifying	51:9 53:1	33:19 54:15
77:5	126:24	62:16 64:7,10	55:20 88:18
called 10:24	challenging	65:7,8 66:4,25	114:22
14:4 18:8	23:1	68:10,19 69:11	clickadsbyie
23:11 64:12	chance 98:12	69:12,16,20	66:2
calls 22:3 71:24	114:21	70:12 73:18	clicking 11:15
capable 101:18	chances 113:15	76:1,6,7,13,16	20:8
capture 110:9	116:15	91:19,21 94:11	client 11:21
careful 30:12	change 30:22	105:5,23	65:6
carefully 127:3	30:24 49:4	106:14 110:25	clients 10:12,17
carry 118:22	62:2 70:24,25	111:24 112:2	10:23
case 8:16,18	77:12 114:14	115:1	close 68:24
10:3 49:20	114:15,15,17	checks 83:25	69:7
55:14 60:10,14	118:23 128:4	89:19 92:16	code 33:1,3,4,6
61:6 63:24	changed 22:8	choose 30:19	33:8 35:4 55:7
64:16 65:4	22:14 53:5	71:20	57:10 91:25
cases 33:10	changes 26:6	circumstances	92:1,2
category 43:18	127:9 129:7	52:3	collect 110:12
109:10	channel 51:2	cited 71:13	college 17:3
catholic 12:24	channels	claim 74:15	column 97:11
cause 99:23	108:22,24	clarification	combination
causes 62:9	character	27:17 120:17	75:3,4 94:21
73:18	80:20	clarifies 79:16	come 13:18
caution 121:1	charges 54:24	84:25 98:15	comes 114:17
center 118:3	check 12:8	114:3	121:22
centripetal 1:9	25:11 56:2	clarify 47:10	comfortable
2:9 10:2,2,5,8	59:25 60:1	55:3,18 56:15	50:8
11:17 12:22	62:15 64:6	58:20 69:17	coming 36:3
	73:4 74:25	72:6 85:1	98:6

[command - content]

command 24:4 51:10,22 117:1 117:6 118:3,6 118:17 commanding 116:18 comment 39:6 63:3 70:3 79:20 100:21 102:5,5 commented 25:2,8,16 50:14 52:1 53:22 54:4 71:5 73:1 101:4 comments 49:15 commission 129:20 committed 63:10 common 32:4 36:9 51:2,11 51:16 62:5 67:9 74:10 105:22 110:8 110:10 111:1 116:5 117:8 118:14 communicate 6:4,9 105:22 117:8 118:6 communicated 40:20 67:9	communicates 51:10 110:25 116:17 communicating 6:6 31:20 117:1,5 communication 31:25 40:22 50:25 57:13,16 89:21 116:5 121:8 communicati... 9:2 71:25 72:1 72:3,12 120:24 121:3 community 17:8 21:23 40:24 41:4 company 14:4 14:5,8 22:15 23:10 26:21 27:6,7,9 38:22 compatible 104:19 complete 6:11 7:13,17,20 11:8 105:6,11 114:9 completely 90:11 complex 85:8 87:11 91:3 108:13 complicated 30:16 51:4	55:7 85:10 compress 85:21 85:22 compressed 19:16 53:15 77:7 82:2,2,5 83:15,22 84:3 85:20 compromise 10:24,25 11:6 11:7 computational 90:2 computer 6:1,2 6:7 12:23 35:3 80:9 109:25 126:9 computer's 32:24 concentrate 87:17 concepts 32:17 concluded 125:2 condition 32:25 94:22 conditions 33:7 conference 42:4,6,8,12,21 42:21 conferences 42:2,15,25 43:3,5 73:13 confidential 43:22,22	configuration 15:13 confirm 5:13 6:2,6 18:12 49:13 conjunction 87:7,17 connection 29:12,12,12 64:16 84:16 109:15 111:5 connections 95:13 108:21 108:23 109:21 consider 43:24 consistent 88:23 consumption 80:9 contact 6:13 26:15 39:21 contain 116:10 contained 35:12 content 36:13 36:14,15 50:13 51:6 52:14 53:2,19 56:6 60:24 61:13 62:15,17 64:6 66:4 68:13 73:20 76:20 77:19 80:4,5 106:2,18,19 107:13,13,14
--	--	---	--

[content - data]

108:4,7,16,18 108:19 111:2 112:5,8 113:14 115:10,16 116:13 content.info. 109:13 contents 121:3 121:8 context 56:16 97:7 112:11 116:24 continue 59:18 contractor 22:25 23:7,10 23:15 31:13 37:16 46:3,15 contribute 34:3 control 51:2,10 51:11,16,22 52:6 67:9 73:8 105:22 110:9 110:11 111:1 116:18 117:2,6 117:9 118:3,7 118:17 126:23 controlled 52:24 controller 68:15 controls 57:15 116:5 convince 54:22 copied 88:4	copies 108:14 108:14 copy 23:22 24:3 48:22 copying 99:10 correct 12:18 12:20 13:1,2 13:11 15:1 16:12,15 17:12 20:12 25:21 27:22,24 31:8 37:18 38:7 44:8 45:14,15 49:9 60:17 64:8,9 65:10 66:3,6 68:2,7,8 69:22 71:11 75:23 76:3,8 76:18,22 77:16 77:22 78:8,11 83:6 91:18 92:10 93:4 98:19,20,23 100:20 104:7 104:10,15 106:1,16 107:9 111:20,23 115:12,18 117:2,3 118:4 118:5,8 124:14 124:15 126:10 129:5 corrections 127:4,6 129:7	correctly 12:7 51:19 126:7 correlate 11:2 36:19 54:12 84:23 94:23 correlated 92:21 cost 73:17 81:12 90:2,2 counsel 3:5,11 6:22 9:3 71:21 72:4,7,9,16 119:19,20 120:6,24 121:8 123:18 126:11 country 119:13 couple 15:24 course 7:12 27:10 57:4 111:6 courses 13:13 court 127:15 cpt 60:4 cpu 24:14 80:9 create 32:11,13 32:19 33:14 41:25 64:16 87:8,10 90:21 created 42:24 47:3 77:16 87:19 111:16 118:11 creates 90:20 creating 31:22 32:21 54:23	credentials 43:25 critical 74:18 74:19 criticality 32:5 cross 30:12 crosstalk 19:10 41:14 110:3 csr 1:24 126:15 cto 49:23 curate 38:16 curated 38:12 current 110:18 custom 70:4,7 customer 30:11 99:23 cve 36:9 cyber 43:18 <tr> <td colspan="4">d</td></tr> <tr> <td colspan="4"> d 4:1 d.c. 3:10 d3 76:23 daily 58:22 dangerous 58:9 113:10 114:5 dash 102:23 103:1 104:7,11 dashes 101:14 101:21 102:25 data 35:5,6,8 43:22,24 52:12 53:15,17 54:10 54:21 55:12,15 57:21 58:2,7 58:13,17 59:12 </td></tr>	d				d 4:1 d.c. 3:10 d3 76:23 daily 58:22 dangerous 58:9 113:10 114:5 dash 102:23 103:1 104:7,11 dashes 101:14 101:21 102:25 data 35:5,6,8 43:22,24 52:12 53:15,17 54:10 54:21 55:12,15 57:21 58:2,7 58:13,17 59:12			
d											
d 4:1 d.c. 3:10 d3 76:23 daily 58:22 dangerous 58:9 113:10 114:5 dash 102:23 103:1 104:7,11 dashes 101:14 101:21 102:25 data 35:5,6,8 43:22,24 52:12 53:15,17 54:10 54:21 55:12,15 57:21 58:2,7 58:13,17 59:12											

[data - developed]

59:14,16 73:13 74:14,23 75:7 76:13 77:24 78:4,9,10,25 85:5,6,9 86:12 89:25 90:25 94:17,25 95:3 96:7 101:15 104:4 107:21 108:5,13,20 109:3,21 111:2 111:6 112:18 112:22 113:17 113:20,22 114:15,18 115:10 116:11 116:18 117:6 118:7 123:2 database 124:8 date 127:8 129:12 dated 126:17 day 37:2 129:16 days 127:12 dd 97:23,24 98:11,13 99:5 99:8,15 124:10 december 46:10 declaration 8:17 9:19 23:3 31:9 43:14 70:16 75:11 85:13 96:20	104:23 119:7 119:17,20 122:17 declarations 120:12 declare 119:8 decompress 82:8,13 84:4 86:3 89:25 90:1 decompresses 83:18 decrypt 57:24 84:17 deemed 127:14 default 50:18 53:23 71:5 100:22 defect 77:17 83:11 defender 87:1 defending 58:24 defense 55:11 demand 88:12 demands 86:8 95:18 demonstrative 28:14 depending 67:7 85:18 98:4 deponent 126:4 126:6 129:1 deposed 6:16 122:21	deposing 127:11 deposition 1:15 2:15 5:11 6:3,5 6:7,10,19 7:25 8:16,25 9:4 120:20 121:11 122:14,15 125:2 126:9 127:3,10,13,14 depth 60:25 63:21 67:2,3 68:13 76:21 106:3 describe 50:22 description 122:9 designed 30:6 52:2 54:6,8,9 54:21 74:4 77:4,11,13,14 81:22 92:7,8 92:11 94:20 96:25 109:11 109:20,22 110:11 111:4 116:2,4,25 117:23 118:1 designing 99:20,20 destination 60:14 details 31:17 detect 25:24 33:11 50:24,25	63:16 74:4 77:18 80:24 81:21 82:23,24 83:7 84:11,12 86:12 87:13 88:3 96:25 101:17 107:10 107:15,19 108:5,9,12,20 109:12 115:20 116:2,4 118:13 120:10 detected 10:14 32:6,7,8 74:12 95:20 detecting 56:9 56:15 63:17 95:5 97:22 107:23 108:7 detection 13:22 21:1,4 28:21 28:24 detects 118:1 determine 60:8 76:2,20 94:25 116:8 determined 38:9 develop 37:21 40:13 46:2 85:3,3 91:10 123:7 developed 27:3 27:6
--	---	--	--

[developers - e]

developers 15:21,21 development 43:8 device 51:23 difference 28:23 29:1,6 29:25 44:18,21 45:10 90:10 different 18:6 36:14 52:12 53:13 61:24 78:22 82:1 86:4 89:13,14 89:15 90:11 92:22,22 98:7 113:19 difficult 69:9 74:5,8 91:6 direct 55:5 126:23 directed 78:15 direction 35:21 35:25 56:18 60:8 95:2 101:23 103:22 directory 23:23 24:3 disable 25:18 54:1 disabled 50:11 50:17 53:23 71:5 100:22 104:14	discard 39:5 discuss 14:19 42:12,24 45:3 discussed 31:12 42:3,7,9,16,18 42:20 43:3,16 discussing 48:12 104:25 118:15 discussions 72:7 distinction 61:15 divulge 72:3,11 121:3 dns 49:4 document 5:22 9:14,23 46:18 46:20 48:22 80:25 82:7 85:18 90:9 94:19 120:12 120:13 documents 5:19 8:10,11 8:14,15,23 9:4 34:21 39:4 85:15 122:5,8 doing 5:25 6:1 36:23 50:22 58:14,15 66:2 67:12 69:1 102:22 105:20 117:23 127:7	dollar 60:5 domain 11:1 donovan 3:7 4:3,5 5:9,11 9:7,12 12:5 13:17 17:11 19:12 22:7 40:15 41:15 47:25 48:8,11 48:18 72:5,17 91:14 96:8,13 96:19 103:19 110:4 116:22 119:23 120:3 120:16,22 121:5,15,25 122:22,24 124:19,25 double 98:13 download 19:3 19:13 20:2,8,9 20:10 23:20 24:5 28:13 44:17,24 45:7 45:9,13,20 54:3 97:1,22 downloader 49:4 downloading 19:16 20:5,7 23:18 41:19 downloads 41:23 driver's 8:13	drop 29:3,13 29:15,17,23,23 29:24 30:4,6,9 30:13,14,19,23 30:24 31:2 32:15 35:15 50:19 54:6,9 54:19,20 60:21 60:23 62:9,12 70:22,25 71:1 74:2 77:13,13 78:13 99:6,7 99:21 100:1 103:4,17,17 105:16,19,20 112:9,13,24 113:1,7 114:6 114:11 115:23 117:21 dropbox 88:3,4 88:4,5,15 dropped 103:18 dropping 29:5 29:7 30:10 50:20 74:2 114:2 drops 30:1 duly 126:4
			e
			e 3:1,1 4:1 15:9 16:8,9 17:13 17:16 108:15 126:1,1 128:2

[earlier - evaluate]

earlier 56:1,8 56:13 70:20 76:25 93:1 early 94:3 easier 5:20 6:15 48:20 easiest 9:14 east 3:9 59:8 easy 20:8 35:2 81:23 82:23 83:1 85:4,4 echanblard 63:17,18 64:13 64:18 65:4 edge 18:8,11,12 18:14,18 effective 111:11 efficient 75:8 efficiently 59:20 eight 48:24 either 18:17 22:8 29:17 104:18 eligible 112:24 emerging 13:13 13:15,18,23,25 14:15,21,24 16:3,13,16,19 16:22,25 17:6 17:14,21,25 18:3,7,15,19,23 18:24 19:4,4 19:14 20:6,11	20:13,18,19 22:9,12,16,22 22:23 23:4,7 23:11,14,16 24:9 25:6 26:5 27:25 28:3,6 28:16 31:10,16 34:4,6,8,11,15 34:17 36:24,25 37:3,11,15,21 38:1,5,8,15 39:12,14,16,17 39:20,23 40:1 40:4,23,24 41:3,10,20 42:3,5,6,9,12 42:16 44:4,14 44:15,16,19 45:1,12,17,18 45:20,24 46:6 46:9,13,14 47:12,15,16 48:13,15 49:22 70:22 71:4,13 93:2 100:16 emergingthre... 18:4 emit 36:17 60:22 64:24 80:25 94:22 111:4 116:6 emits 29:10 64:22 emitted 11:19 92:22	emitting 67:22 109:19 employ 86:9 employee 22:16 22:20,21,22 47:16 enable 24:13 25:13,22,23,24 31:23 33:7 52:5,24 100:24 102:8,13,15,17 102:21 104:16 104:17 108:11 enabled 54:2 75:14 80:13 103:12 enables 32:25 encountered 55:2 encrypted 58:4 58:5 65:23,25 77:24 78:14 84:15,16,19 87:21,22,23,25 88:7 89:9,10 89:21 90:1 95:12,13,15 96:1,3,5 103:20 108:3 108:16,17,22 108:24 109:1,3 109:3 111:5,6 117:11 encryption 88:5,6 96:2	ends 48:23 enemies 58:10 58:14 74:21 engine 39:7 43:1 engineers 90:24 english 50:6 55:23 94:9 98:11 102:14 entire 10:6 61:21,21 101:20 118:22 119:2 120:13 enumeration 32:4 36:10 74:10 environment 10:14 37:6 52:6,25 98:8 equal 114:17 equals 61:17 64:17 112:19 113:17,20,22 114:15 115:10 errata 127:5,7 127:9,11 129:9 especially 47:20 91:5,7 esq 3:2,7,8 estimate 41:6,7 et 109:6 110:17 evaluate 34:11 73:22
---	---	--	---

[event - extent]

event 11:19,19 36:18,19 54:12 92:20,20 108:1 events 10:13 11:21 36:8 54:13 67:6 75:4 87:5 92:22 94:24 101:8 103:5 107:23,25 110:18 117:17 eventually 45:5 everybody 17:16 39:24 evidence 11:20 54:11 86:19,25 87:5 111:14 evidences 111:16 exact 22:6 30:14 99:14 exactly 17:2 18:9 34:1 36:22 46:24 50:22 59:12 78:6 79:13 85:1 91:8 93:24 97:8 99:3 102:21,22 112:14 examination 5:8 123:13 124:18 examined 5:6	example 11:14 11:15 24:22 35:22 36:10 53:22 62:6 64:23 77:8 78:23 84:12 87:21 88:13 98:5 99:11 101:4 examples 34:23 46:18 excel 89:14 except 129:7 exclusively 42:12 excuse 103:2 109:13 excused 125:1 execute 32:18 33:3 37:7 40:12,18 executing 31:17 40:17 execution 31:18 40:19 exfiltrate 95:10 110:12 116:18 117:6 118:7 exfiltrated 58:13 90:23 exfiltrating 77:24 78:4,9 78:10 116:1 exfiltration 35:6,7,8 43:18	43:20,21 44:1 54:11,21 55:6 55:13,15 58:2 58:7,17 59:12 59:14,16 74:14 74:24 75:7 80:25 81:21 83:11 85:5,7,9 86:8,13 87:14 88:12,25 89:20 90:25 91:19 92:14,18,19 94:13,17,25 95:3,20 96:7 98:10 99:8,8 101:16 104:4 107:10,15,21 108:5,9,12,13 108:20 109:21 115:20 116:2,3 116:11 123:2 exfiltrations 83:3,8 exhibit 4:9,10 5:18 8:20,21 9:8,9,17 48:14 48:16 56:21 62:22 65:11 66:16 70:15 90:17 96:20 122:18 exhibited 83:19 exhibits 4:7 5:17	exist 14:5 54:11 expanded 18:21 expansive 24:14 25:12 81:10 expect 22:1 96:13 112:12 expected 96:15 experience 31:6 47:22 expires 129:20 explain 35:12 50:23 67:17,18 69:9 78:7 81:24 123:23 explained 6:23 124:20 explaining 12:7 explanation 112:10 120:9 exploit 32:12 32:14,23 33:16 33:18 36:8 exploits 32:17 expression 80:5 80:6,8,10,16 81:8,12,13 82:25 100:19 101:11,21 103:8,10 104:2 expressions 102:24 104:1 extent 71:24 72:11
--	--	---	--

[external - flag]

external 35:23 35:25 36:1 51:14,23 56:3 56:9,14,18 60:11 65:9,19 68:11 73:6 75:25 76:10 80:8 105:24 111:18 112:1 115:3 extract 82:9 83:24 86:1 89:12 90:3,5 92:5 extracting 31:18 extreme 66:1 extremely 83:8	58:11,18 62:7 62:11 65:23 67:21 74:1 76:25 77:1,2 77:10,15,18 78:6 80:25 81:20 82:19 83:3,9 84:9,10 85:16,17 90:20 90:21 95:8 97:10,17,18,19 97:21,23 98:2 98:10,13,24 99:17,21 105:14,17 107:7,8 108:6 112:8 113:6,13 113:15,23,25 114:22 115:21 115:23 116:15 familiar 43:17 45:23 46:5,8 feel 59:1 97:5 feeling 59:5 fid 61:17 field 59:25 60:1 62:19 64:21 65:8 66:1 76:2 76:6,7 84:4,5 89:1 91:20 92:9,12,17 94:12 95:6,6 106:7 107:4 108:8 109:5 115:14,16	fields 36:16 82:1,2,5 83:16 83:18,22 85:19 86:4 file 19:16 20:10 78:24 79:2,3,4 79:4,4,8 81:21 81:25 82:1,2,3 82:4,6,8,9,10 82:11,11,12,13 82:24 83:12,12 83:13,13,14,16 83:17,17,19,21 83:22,23,24 84:1,1,2,14,14 84:19 85:19,20 85:24 86:1,1,5 86:8,16,17,21 87:2,4,13,15,19 87:20,20 88:2 88:2,4,12,15 89:7,12,12,15 90:1,3,3,4,5,6,7 90:8,9,10,11,12 90:13,13,16,17 90:17 91:24 92:5,6 94:19 94:19,19 95:10 95:11,11,14,25 97:1,23,24 98:11,13,21,25 99:2,5,7,8,15 100:4 108:14 108:15 110:10 115:25 116:2,3	123:20,24,25 123:25 124:1,3 124:4,10,10,14 124:22 files 19:17 25:3 25:16 43:22 75:1,2 81:25 82:5 83:16 84:4 86:15,24 87:8,10,12 88:10 89:14 90:14,22 92:2 92:23 98:7 find 12:1,9 19:18,20,23,24 82:14 87:18 101:11 113:7 finding 16:1 98:9 fine 5:13 first 6:21 9:7 9:25 13:18 19:7 23:14 68:18 69:13,20 69:21 70:2 72:21,23 75:24 77:20 78:12 90:3 106:5,25 109:10 124:2 five 106:5,5 flag 13:24 33:15,17 67:22 67:23,25 68:4 68:5
f			
f 42:22 126:1 fact 57:22 fail 127:13 fair 23:12,13 83:2 115:19 fakealert 110:18 fakeav 110:18 falls 24:24 67:4 false 21:19 24:12,21 25:4 25:20 30:8,17 30:20 46:4 50:15,15,18 53:21,23,25 54:4,23,24			

[flagged - great]

flagged 52:7 flagging 92:20 flowbit 67:11 67:11 flowbits 67:5 67:15,19,22,23 73:18 focus 75:9 focusing 81:5 85:12 follow 47:14 followed 67:1 68:16,17,17 69:3 70:2 102:25 follows 5:6 foregoing 126:21 129:4 form 13:14 17:10 43:25 129:8 format 83:13 83:17 89:13,14 90:14 formats 89:15 90:11 forth 98:6 115:14 forward 81:3 found 12:15 13:22,23 14:25 15:19 38:11 46:18 foundation 12:3 40:10	42:22,23,23 founded 27:7,8 fourth 66:17 fragmented 79:4,7 90:4 frame 26:23 frankel 3:3 fraudpack 110:18 free 37:4,12,15 37:21 45:7 97:5 ftp 78:24 79:2,8 87:22 95:25 ftps 95:25 full 22:24 23:9 46:3 fully 58:2 fun 22:25 function 61:4 functionalities 86:8 88:12 functionality 71:15 95:19 96:4 functions 59:13 117:7 further 124:18	generate 24:12 24:21 30:8 53:20,25 54:3 62:11 67:4,6 73:25 81:20 97:18,19,21 99:17 101:8 103:5 105:16 108:6 111:9 113:25 generates 24:23 30:16 50:15 67:20 generating 25:3 107:23 114:22 gerais 12:24 gerard 3:7 5:10 gestures 7:10 give 7:13,17,19 16:8 54:11 59:4 given 126:10 129:6 gives 124:11 glad 55:2 91:3 gmail 108:14 go 8:1 19:24 32:16 33:16 42:10 45:12 48:8,23 55:19 56:20,21 58:21 58:22 62:22,22 65:11 66:16 70:15,18 72:13	72:18 75:7 78:12 79:17 80:15 81:16,24 85:11 90:13 96:11,22 98:16 100:1,7 104:22 110:14 117:16 119:6 123:17 goal 100:6 going 5:17 6:23 30:22 36:7 38:24 47:25 48:2,3 54:3,18 59:1 62:23 71:3 73:9,15 80:7,17 86:6 91:6,7 95:3 96:8,11 101:6 101:8,16 103:9 103:13,17 105:23 111:18 111:25 113:20 118:15,16 121:6 122:20 123:16 good 5:10 16:19 34:12 53:22 84:6,7 96:11 99:11 gpl 44:23 graphic 28:10 great 6:8 8:9 12:25 30:18 32:6,9 33:10 37:13 57:22
	g		
	gain 33:3 gateway 10:15 gdonovan 3:11 generally 49:14 100:22 102:2		

65:21 73:18 108:21,23,25 114:21 greater 113:15 116:14 grid 74:20 grouped 32:3 guess 21:7 33:21 52:18 56:20 68:5 guxx.dload 110:18 guy 27:8 88:14 108:14 guys 8:19 34:10 50:6 53:9,9,10 54:7,16,16,19 55:1,4,10 58:15,19 59:2 74:4 82:16 90:23 101:25	happened 11:22 22:12 42:13 43:8 87:2,14 116:9 117:17 120:9 happening 36:12 37:9 59:8,9,10 69:10 85:7 94:25 108:23 117:19 happens 33:9 52:15 77:6 79:3,6 86:20 108:25 113:18 hard 93:11 harden 87:9 hardware 57:13 harper 100:12 100:13 102:9 hash 50:7 71:6 71:9 75:13,15 75:17 79:21 102:19 104:8 104:10,11,13 104:17 hashtag 50:5,9 50:10 header 12:16 12:18 25:11 35:20,21 59:25 60:1,12 61:9 62:18,19 63:18 63:19 65:8	66:5 68:20 69:13 76:2,6,7 76:9,13,14,15 76:16,17 77:21 89:1,10 91:20 92:9,12,13,17 94:12,16 95:2 95:6,6 103:21 106:7 107:4 108:8 111:24 112:2 115:2,4 115:5,7,8,14,15 headers 60:13 89:8 hear 5:13,14 heard 13:25 27:2 42:4,5,11 heart 93:13 help 36:18 55:18 80:24 81:20 82:22 87:1 92:19 helped 122:25 123:8 helpful 33:20 helps 88:24 hey 41:23 64:25 65:5 94:17 109:14 high 50:18 53:21 hit 68:3,6 hits 69:24 hoizonte 5:1	hold 71:23 124:1 holding 61:24 home 20:2 35:22,24 36:2 51:15 60:3,5 60:11 65:9,18 68:10 73:6 75:25 76:10 80:7 105:24 111:18 115:2 honor 119:13 hooch 97:11,12 97:12,12 124:9 hope 58:21 74:16 79:15 81:2 84:25 88:17 114:3,22 122:25 123:8 hopefully 5:20 9:13 48:20 hospital 52:11 88:1,14 host 111:11,13 hour 48:1 67:6 96:9,14 hours 122:4 http 12:12,14 12:16,19 61:4 61:5,8 62:18 63:18,19,20,23 63:25 64:3,7 64:17,19,21 65:20,25 66:4 68:19,21,23,25
h			
h 3:2 61:10 104:13,13 half 83:21 handles 45:2 hands 58:10,14 happen 25:25 53:12,13,14,15 61:23 73:12,14 89:20 91:12 95:4 101:14 106:17 108:22 112:20 114:11			

69:5,8,12 70:3 70:8,10,11 80:12 89:1,19 91:19 92:14 94:16 105:24 106:4,8,15,24 107:3,11,16,19 108:7,19 109:1 110:19 111:3,5 111:19,22 112:2 115:3 117:9 124:9 https 65:22 88:16 89:8,22 108:3 117:9 huge 61:16 80:8 82:3 83:22 90:2 huh 7:2 48:25 97:8 human 90:14 97:13,14 humans 112:16 hundreds 66:10	24:6 25:7,19 26:6,8 29:4,22 30:19 32:7,13 33:12,14,17 34:24 35:9 37:19 39:7 50:5 61:20 65:23 74:12 81:11 86:9,20 88:7,16 89:19 91:2 94:21 95:19,24 96:3 109:2 111:6,7 117:10 118:24 idses 13:21,24 21:10,13,17 26:13 28:20 31:7 37:25 82:18 ignore 113:17 iis 36:9 imagine 52:18 82:16 112:19 immediately 36:11 83:15 89:17 impact 30:11 79:14 imperative 127:10 implanted 30:2 implement 26:6 30:4 important 61:15	impossible 6:13 104:3 improved 18:21 inaccurate 79:13 94:15 inbound 36:2 include 34:12 115:9,10 124:21 included 85:15 115:15 123:24 124:13 includes 76:20 indexed 32:4 indicate 49:14 63:22 indicated 126:4 indicating 95:7 indication 124:11 indicator 11:7 indicators 10:24,25 11:1 11:5 indiscernible 19:10 41:14 110:3 inevitable 30:17 inexperienced 47:20 infiltrated 88:1 inform 14:15	information 15:18 31:18,23 38:21 42:23 64:22 65:2 83:19 110:12 119:10 123:23 124:21 initial 79:6 106:5 initiate 116:7 inside 77:6 inspecting 23:25 65:18 76:19 install 28:13 57:10 installation 99:11 installed 109:25 installed.php 57:12,16 instructions 127:1 integrity 75:1 intelligence 10:9,10,15,18 11:10,11,13 intend 66:23 intended 50:24 50:25 63:16 66:24 81:22 83:2 105:4 109:19
i			
idea 21:25 22:14 41:24 64:13 85:25 ideas 40:21 73:22 identified 53:6 identify 90:12 ids 19:1 21:15 21:21 23:1,23			

[intensive - know]

intensive 83:8 intent 77:3 intention 84:6 84:7 100:2 interested 126:12 interface 28:10 intern 37:25 39:11,11,15 internal 38:23 38:24 51:23 56:3,10,14,18 112:1 internally 100:23 101:24 102:3 interned 14:10 internet 15:17 43:25 56:18,19 internship 13:21 14:2,3 15:16 19:8 20:25 21:9 37:19 interpreted 53:18 interval 76:11 intrusion 13:21 15:4 18:25 21:1,4 27:13 27:15,16,18,19 28:19,21,24,24 29:2 31:4 investigated 92:21	investigation 36:19,21 54:14 75:5 84:24 109:20 111:10 111:15 116:7 117:15 invited 34:6 involved 41:3 ip 25:10,11,12 25:17 31:19 35:19 52:13 53:14 60:2,3,6 60:7,12 73:12 76:14,17 77:7 77:9 111:24 ipr2023-00446 1:6 2:6 ips 27:10,13 28:7 29:3,4,13 30:4 33:12 55:16 57:25 58:8 59:13,13 60:2,7 74:24 86:9 89:10,23 90:22 91:2,23 92:3 94:20,21 95:10,13,19,24 101:9 109:1 111:16 123:2 ipses 28:19 issue 104:6 issues 59:21 73:19	j j 1:23 2:16 126:15 january 1:16 2:13 5:1 23:6 31:12 jeff 122:24 jefferey 3:2 jeffrey 121:14 job 22:25 31:3 40:13 41:24,25 jobs 33:25 46:2 john 3:8 96:22 join 14:23 34:6 joined 13:7 36:24 38:13,15 39:23 40:24 41:2 46:3 47:12 joining 12:22 jonkman 49:4 49:18,21,22 100:12,18 102:10 jprice 3:5 k k 3:9 keep 48:2,3 51:1 57:20 58:6 59:20 89:8 keeps 48:20 keysight 1:6 2:6	keysight's 71:14 keyword 29:19 29:20,21 30:25 31:1 67:3 70:23 99:19 kin 126:11 kind 8:13 31:21 52:7 54:5 86:22 90:7 99:6 knew 26:24,25 27:9 know 5:22 7:4 7:20 8:1 9:2,5 9:23 15:25 20:23 21:3,5,7 21:23 22:6,8 22:11 24:18 29:16 30:20 36:11 38:8 39:23 40:23,25 41:2,8,9,19,21 42:21 43:5 45:1 46:7,20 47:8 49:2 51:19 52:7,18 53:9 55:1,10 57:12 59:11 60:8 64:10 65:21 69:8 70:3 74:4 82:21 87:25 90:23 91:8,24 96:15,24 97:8
--	---	---	--

[know - lottery]

99:10 100:13 102:2,7 105:7 112:14 123:5 knowledge 30:21 119:9,12 119:14 known 20:19 43:18 kramer 3:3 kramerlevin.... 3:5	left 13:7 legal 8:24 legitimate 30:10 78:16,19 79:10 105:20 length 116:14 116:14 level 86:21,23 87:3 88:10 117:17 levin 3:3 license 8:13 44:23 45:8 life 22:14 103:13 likely 73:2 limitations 84:21 limited 31:6 62:1 line 30:13 35:4 35:4,11 55:6 75:15 128:4 lines 86:6 91:24 92:1,2 118:10 124:5 link 11:15,16 20:2,8 linux 28:14 98:22 123:24 123:25 124:7 124:11 list 14:17,18,20 14:24 15:5,7,9 15:15,19 16:4	16:7,11,13,14 16:16 17:7,13 17:16,19,22 21:6,12,14,20 21:24 34:8,9 34:10 37:1 38:6,10 39:1 45:3,24 47:16 lists 17:20 little 43:16 49:2 79:24 106:20 live 52:8,22 59:6 llp 3:3,8 load 23:24 25:6 27:25 28:3,15 28:16,17 39:7 75:18,21 102:19 104:18 loaded 24:8 50:5 102:23 103:12 loading 23:24 25:19 71:9 logs 40:18 41:22 75:2 84:23 86:22 87:18 111:12 116:7 117:16 long 18:10 63:13 72:3 122:3 longer 96:10,15 look 50:12 59:8 59:9,9 70:8	73:5 82:14 97:14,25 109:17 111:10 113:4 looking 10:12 11:20 34:23 50:2 57:7 59:23 63:15 64:2 66:23 75:10 90:8 looks 59:6 63:7 68:23 69:8 lose 87:23 loses 95:13 96:3 109:2 lot 24:17 25:2,3 41:11,12,13 47:1,2,3 50:15 51:8 52:16 53:17 58:13,23 69:25 73:15 74:19 83:9 98:5 104:2,3 112:22 113:18 113:19 115:20 lots 21:14,17 24:12 30:16 43:2 46:7,7 50:15 53:19 83:25 86:13 90:3 95:3 105:9 lottery 52:17 52:19
l			
l 55:23,23 lab 98:6 large 21:23 40:23 launch 33:5 layer 35:17 53:18 lead 75:4 leak 43:21 learn 13:18 15:14 20:15 34:20 37:4,22 38:16 learned 16:12 16:21,25 20:13 35:10 learning 37:12 leaving 80:11 81:14 85:15 98:21 99:5,15 100:5 106:23 107:20 115:13			

[loud - match]

loud 5:14 love 23:1 lube 53:17 lubes 53:16,16 53:19,20 lunch 96:12 lying 119:15	108:21,23,25 make 5:20 7:8 7:11 8:4 26:5 39:1,9 47:17 51:17 53:17 54:15 55:3 56:23 59:10,19 61:15 62:3 64:18 65:15 67:12,17,24 74:15,16 81:16 86:1 91:7,12 91:16 101:3 102:4 103:13 104:5 105:6 111:25 112:3 117:21 123:5 127:4 makes 6:15 8:5 24:16 48:20 55:10,17 80:14 88:22 112:23 119:3 making 14:3 59:3 malicious 10:19,21 11:22 33:5,6,7 49:5 57:14 malware 23:4 31:10,17,18,19 31:24 32:1 37:7,8,20 40:17,17,19,22 43:15 49:5	51:6,10,15,22 52:7 57:21 62:6 67:8 68:22 69:1 70:4 77:23 78:9 105:18,21 109:6,11,16,24 110:1,2,25 111:11 116:4 116:17,25 117:4,8 118:2 118:6,12,17,25 malwares 57:23 70:6 117:8 manage 10:17 10:20 13:21 15:17 21:12 25:20 28:10 managed 21:1 21:3,15,17 31:3 managing 21:10 31:6 37:25 march 10:1 marinhi 63:7 marinho 1:15 2:15 4:2 5:4,10 48:11,19 49:1 49:3 62:14 63:1 84:9 91:15 96:19 119:6 129:3	mark 112:18 112:22 113:17 113:20,22 marked 4:7 9:9 48:16 marketing 22:13 marking 5:17 martin 1:23 2:16 27:7 126:15 match 24:15 25:17 29:14 31:24 32:11,13 32:20,22 36:2 36:16,17 40:21 50:13 51:7,8 51:12 52:12,14 52:16 56:6 57:13 58:3,4 60:12 61:4,13 61:14,20,21 62:1,4 63:19 65:24 73:8,9 73:15,15,16,20 73:21 74:6 77:2,4,4,5,11 77:19 79:13 80:4,5,21 81:7 81:10 82:6 83:23 84:5,18 85:24 87:24 88:7,16 89:9 92:5 95:2,11 95:11,14,15
m			
mac 65:1 machine 126:7 made 9:9 15:24 38:10 47:9,10 47:19 48:16 53:7 115:23,24 119:8,9 127:6 magic 35:5 mail 16:8 17:16 108:15 mailing 14:17 14:18,20,24 15:5,7,9,14,19 16:4,7,11,13,14 16:16 17:7,13 17:16,18,19,20 17:21 21:6,12 21:14,20,24 34:8,9,10 37:1 38:6,10,25 45:3 mails 15:9 16:9 17:13 main 45:9 majority 30:18 32:6,9 33:10 57:22 65:21			

[match - monitoring]

96:4,5 99:9,12 99:14,16 101:22 104:1,2 105:9,10,21 106:4,23 107:1 108:4,7,16,16 108:19,19 109:3 111:2,6 111:7 112:6,8 113:15,21 114:18,20 115:2,5,7 116:13 117:12 118:14,16 119:1,2,2 matched 77:6 92:13 98:25 115:14 matches 11:18 29:9,15 34:25 36:13,14,15 51:3 53:19 57:11 60:7 66:5 73:23 80:16 101:12 101:13 102:25 117:10 matching 24:1 30:15 51:5,13 52:14,21 57:9 57:20 60:14 61:3 63:23 64:15 65:25 68:15,16 69:2 70:1 74:14	78:14 80:19 81:12 84:13,13 86:4,9 89:1 94:15 95:21 101:5,5,11,21 101:22 103:23 103:24,25,25 107:3 113:9 118:20,21 material 42:19 matt 49:3,18,21 49:22 100:12 100:18 matter 103:8 mean 8:13 10:20 20:21 21:6,16,18 22:20 26:2 32:21 39:21 41:16 42:11 45:24 46:24 49:19 50:4,19 57:3,19 59:1 67:13 68:14 69:17 70:5,6 73:3,11 74:3,9 74:13,15 77:23 84:6 86:11,14 88:3 97:5 99:13 100:18 101:2,8,25 102:7,18 103:11 106:3 106:24 108:1,3 109:9 112:24	113:23 117:11 117:13 120:14 means 35:24 36:2,12 50:11 60:19 97:9 102:2,21,22 126:23 mechanics 35:1 meet 29:9 120:19,25 121:10,18 122:3,13,16 meeting 122:6 megabytes 82:4 member 17:18 17:20 mention 113:3 118:25 mentioned 61:6 79:15 108:11 mentioning 63:24 114:8 merit 2:17 message 36:7 36:11 51:1 109:5,14 110:17 met 100:14 122:21 method 61:4,7 61:8 63:23,24 68:20 69:2 70:12 89:1 91:20 92:14 94:16 106:5	107:11,16 108:11 111:3 111:22 115:9 methods 61:6 microsoft 36:9 82:12 83:13,20 84:1 86:2 90:9 91:24,25 middle 59:8 96:23 million 67:6 103:5 minas 12:24 mind 48:5 57:20 58:6 minutes 103:5 miracles 84:20 mistake 53:7 63:11 mistaken 14:6 18:5 misworded 76:4 modifiers 36:14,15 modify 26:1,2,3 29:11 modifying 30:5 money 54:25 58:12 monitor 62:13 77:14 88:9 118:12 monitoring 29:4,6,8,22
---	---	--	--

[monitoring - november]

86:23 88:9 monitors 29:25 months 72:24 72:25 morning 5:10 move 59:19 81:3 multiple 68:4 90:4	necessary 59:14 127:4 need 7:25 9:2 9:15,22 30:12 35:8 36:17 48:21 54:15 58:6 59:10,14 59:15 70:25 74:22,24,25,25 75:2 84:25 85:2,3 86:13 86:14,17 87:13 90:13 91:7,10 91:10,12 95:4 97:6 105:6 117:21 123:5,6 123:7,15 needed 15:25 needs 91:22 92:21 94:23 negative 30:11 65:24 79:14 84:9,10 negatives 85:17 neither 126:11 net 35:22 36:2 40:9,11,16 52:5,25 56:3,3 56:9,10,14,14 60:5 65:9,9,18 65:19 68:10,11 73:6,6 75:25 75:25 76:10,10 105:24,24 111:18,18	112:1,1 115:2 115:3 network 10:12 10:23 11:2,18 11:22 23:25 24:1,16 29:9 29:11,15 30:11 30:15 31:21,25 32:19 33:9,11 34:25 35:23,24 35:24,25 36:1 36:3,16,18 37:8 40:20 51:8,14,15,23 51:23 52:10,23 53:10,13 54:2 54:12,13 59:15 60:3,7,11,11,17 62:15 67:7 74:6,7,14 77:24 80:7,8 80:11 81:14 82:10,24 83:25 84:15,22 85:15 86:10 87:1,5 87:13,16,21 88:15 89:11 90:6 92:4 94:23 98:3,21 100:5,23 101:7 101:24 102:3,6 103:24 106:24 107:11,15,20 109:14 111:9 115:13 116:1	117:5,15 networks 1:9 2:9 10:2 58:24 99:24 never 20:7 27:11 28:11,18 42:4,5,8,10,10 42:11 43:4 50:19 52:8,11 53:10 54:5 58:3,3 60:22 65:24 74:2 82:18,18,22 83:4 95:15 100:14 108:16 113:6 new 3:4,4 91:10 nightmare 101:6 103:14 nine 13:10 noalerts 67:5 nods 7:9 noise 108:6 noisy 67:3,20 normal 53:24 107:21 nos 55:22 notary 129:23 note 70:21 71:3 noted 127:9 129:8 notice 126:3 november 23:5 23:9 31:11 34:16 37:17
n			
n 3:1 4:1 15:1 55:22,23 60:17 n.w. 3:9 naftalis 3:3 naive 55:17 85:8 90:18 name 5:10 14:6 14:7 18:6,7 22:8,14 26:8 40:12 44:12 49:5 63:8,11 66:21,21 93:9 109:12 names 11:1 40:3 nancy 1:23 2:16 7:7 126:15 navigate 5:21 9:22 navigated 11:14 navigating 19:15			

38:15 39:13 nsi 57:12,16 nuances 94:18 nullify 55:25 nulls 55:24 number 4:8 22:6 52:19 53:21,23 61:19 78:15 101:12 101:17 102:25 103:1,15,22 104:8 112:18 numbers 52:18 52:20 101:14 101:21 114:14 118:23	okay 5:23 6:22 7:22 9:11,16 9:22 22:19 28:19 48:7 49:14 52:1 53:7,8 60:16 70:19 72:14 84:13 86:5 87:18 93:16 97:15 98:1 110:14 112:17 121:23 124:16 old 66:12 once 41:2 65:23 68:4 87:23 95:12 96:3 ones 27:3 46:24 open 42:21,22 42:22 44:19,21 44:23 45:4,6 45:14 47:23 83:14 90:2,6 openly 44:25 operation 117:17 operational 31:22 86:15,16 86:20,23 87:3 87:6 88:10 92:23 opportunity 37:13 opposed 7:9 opposite 56:17	optimized 44:4 option 29:3 67:21 73:23 105:16 options 29:20 36:4,5,13 oracle 124:8,8 order 36:6,17 44:17 54:14 59:16 70:24 82:6,10 83:22 84:5,18,23 85:23 86:4,12 87:13 94:24 104:17 115:6 117:18 origin 99:5 original 127:11 os 65:1 outbound 35:25 60:10 63:20 64:16 65:8,19 68:10 103:9 109:15 111:5,21 117:1 117:5 118:2 outcome 126:13 outside 20:18 100:23 101:23 102:3,6 outstanding 8:3 overall 80:15 81:16	overwhelmed 92:4 own 44:24 70:5 70:7 owner 1:10 2:10 3:5
o			p
o 15:1 42:22 55:22 oath 8:6 objection 12:3 13:14 17:10 22:3 40:10 71:22,24 89:3 116:19 119:22 120:7 observed 11:12 57:16 obtained 12:22 october 9:20 offered 46:21 office 1:1 2:1 officially 22:13 oisf 42:25			p 3:1,1 p.m. 96:17,18 125:2 package 76:13 packet 12:14 12:17 59:25 60:1,20,21,23 61:8 65:7 66:5 67:2 68:6,18 68:20 73:17 76:7,9,16,17 77:7,21 78:14 80:7,11 81:14 92:9,12 94:16 95:5 103:8,9 104:1 106:8,15 106:25 107:4 108:8 111:24 112:2 115:2,7 115:8,13,14 packet's 106:6 packets 29:13 65:8 76:3 79:5 79:7 90:3,4 105:23 115:1 page 4:2,8 20:3 48:15,21 56:21 56:23 62:23

63:4,5 65:11 65:15 66:16 75:10 86:6 128:4 pages 1:25 62:24 129:4 papers 8:17 paragraph 9:25 12:21 23:3 31:9 43:10,14 45:16 45:16 70:18 71:12 72:18 78:12 79:17 85:12 95:18 96:21,23 100:7 104:22 110:14 112:7 118:10 119:7 parameters 61:16,25 114:13,13,19 118:23 paraphrasing 32:23 pardon 16:23 parenthesis 36:5 parse 90:1,12 90:16 91:23 92:2,6 parsing 82:13 90:13 94:18 part 59:24 61:11,14 63:21	65:7 69:3 90:13 102:4,14 105:5,11 106:10 participate 6:3 15:8,20 34:6 participated 14:18,20 45:3 participation 16:13 38:13 parties 2:18 parts 62:1 64:17 96:14 party 20:15,20 22:21 126:12 pass 123:21 passed 61:24 114:19 passing 114:13 114:14 118:23 password 87:11 97:1 98:21 100:4 123:20,24,25 124:3,4,14,22 passwords 124:2,4,5,13,22 past 97:23,24 98:11 124:10 patent 1:1,3,7 1:10 2:1,3,7,10 3:5 path 98:13 99:5 99:8,15	patrick 100:11 100:13 pattern 53:11 97:20 98:1 101:11 105:13 105:21 114:9 pause 48:4 pay 44:16 45:8 54:25 58:11 payload 33:5 68:18 106:6 107:1 pcre 81:6,6,9 100:12,18 pdf 62:23 81:25 82:2,4,11,11 83:12 84:1 85:19 86:2 89:14 90:9 94:19 peace 58:14 pedro 1:15 2:15 4:2 5:4 49:3 63:7 71:23 72:1 121:21 123:15 129:3 pedromarinho 49:7 peer 64:12,12 64:14,14 65:6 65:6 98:7,7 people 14:19,21 15:7,10,21 16:15 17:6 21:3,5,12,14,17	21:20 22:2 30:18 32:18 39:17,19,21,22 40:3 41:3,8,8,9 41:11,12,19,21 44:23,24,25 45:2 52:23 54:1,22 81:21 102:11 123:1 percent 61:22 74:5,8,22 95:23,23 99:14 99:15 101:18 113:25 116:10 116:11 118:13 118:20 119:1,4 120:11 perfect 6:15 113:24 118:18 118:19 performance 24:20,21 25:13 39:5 46:4 73:2 73:19,21 80:3 80:14,15 81:1 81:16,19 103:6 performed 37:12 persistent 89:24 person 21:9 100:14 petition 71:14 petitioner 1:7 2:7 3:11
---	---	--	---

[phishing - prevent]

phishing 11:15 11:16 phone 6:10,12 6:13 phonetic 11:9 97:11 php 112:18,22 113:17,19,22 phrase 98:15 102:14 pick 83:13 picked 72:15 piece 33:4 57:13 86:19,25 110:25 pieces 11:20 90:17 place 87:18 126:4 plays 58:9,13 please 6:17 7:8 7:15 9:4 55:19 56:12 59:18 64:4 75:7 85:11 98:15 100:1 116:21 120:2 127:3,7 plenty 32:2 plus 67:1 68:17 69:3,21 70:13 point 86:18 88:24 pointed 53:4 policies 10:17 10:20,22,23	pontifical 12:23 poor 73:21 94:9 port 67:10 68:11 76:1,11 77:5,25 78:15 101:23 103:2 103:22 105:24 106:24,24 108:25 portal 5:18 portion 5:21 9:23 32:10,13 33:13 62:4,16 68:9,14 74:11 75:24 97:6 106:14,18,19 112:6 114:8,20 118:21 119:3 ports 51:14 60:14 65:19 67:7,8 73:7,7 73:11,12,14 76:15 78:21,23 78:24,25 80:11 105:25 109:1 111:19 115:3 position 31:14 positions 20:25 positive 30:8 76:25 77:1,10 85:16 97:17,18 97:24 98:10 105:14 112:8	113:6,23 positives 21:19 24:12,21,24 25:20 30:17,20 46:4 50:18 53:21,24 62:7 62:11 67:4 74:1 77:2,15 77:18 78:6 81:20 82:19 83:4,10 95:8 97:10,20,21 98:2,14,25 99:17,22 105:17 107:7,8 113:13,16 114:1,22 115:21,23 116:15 possibility 77:15 possible 32:11 85:24 89:18 103:6 possibly 88:3 post 61:5 67:1 68:13,15,16,20 68:21 69:2,4 69:11,13,20,21 70:1,2,3,5,9,12 89:19 106:3,5 106:25 107:2,4 107:11,16 108:4,7,11,16 108:19,19	110:19 111:3 111:22 112:3 115:9,16 potential 11:3 13:25 33:15,18 84:22 92:20 94:22 96:24 97:1,9,9,22 98:12 99:21 112:25 113:13 116:4 118:12 potentially 40:21 pound 50:6,7 75:15,17 power 74:20 80:10 81:13 89:24 117:22 practically 83:5 precautions 95:1 preceded 50:10 precedes 75:14 precise 114:10 predated 94:1 prepare 120:19 121:10 122:14 122:15,17,19 pretty 59:20 prevent 35:5,6 35:8 54:10,21 55:5,12 58:2,7 58:17 59:12,14 59:16 67:15
--	---	--	--

[prevent - question]

74:13,23 75:6 85:9 88:25 89:20 90:25 91:19 92:14,17 92:19 94:13,17 95:1,3 96:6 101:15 104:3 108:5,20 109:20 115:25 116:3 120:10 123:2 prevented 95:24 preventing 85:5 86:7 88:11 109:21 prevention 15:4 27:15,16 27:18,20 28:20 28:24 29:2 31:4 previously 4:7 9:9 48:16 price 3:2 4:4 12:3 13:14 17:10 22:3 40:10 48:5 54:24 58:11 71:22 72:10 89:3,5 96:10 116:19 119:22 120:1,7 121:1 121:13,20 122:25 123:10 123:14 124:16	principal 80:20 prior 37:16,24 43:6,7 45:11 112:11 privileged 71:25 72:2,3 72:12 pro 44:5,14,15 44:22 45:8 probably 7:24 42:20,24 49:11 49:12 50:1 57:5,6,9,14 63:10,11 66:9 66:12,22 67:8 70:9,10,11,14 problem 7:3 14:9 33:1 55:16 73:24 85:8 86:7 88:11 91:2 95:18 problems 25:13 62:9 99:23 proceeding 9:1 proceedings 1:14 process 23:24 24:4 38:23 111:14 processes 31:21 38:21,24 processing 73:17 80:10 81:13	processor 83:4 program 57:14 project 18:14 22:15 23:11 40:9,11 promote 77:12 promoting 62:8 prone 53:20 pronounced 12:25 proof 32:17 propounded 129:7 proprietary 38:21 protect 10:23 101:7 protecting 52:10 74:19,20 74:20 protection 18:25 27:14 87:8 protections 87:7 protocol 12:12 12:14,19 35:16 35:17 36:16 60:4 61:5 63:25 64:21 69:5,12 70:4,5 70:7 78:25 79:8 80:12 87:20 93:21,24 94:6 96:2	115:5 protocols 53:14 53:16,17 89:21 prove 55:12 59:3 74:17 provide 34:9 46:18 71:14 88:13 95:19 provided 11:9 provider 11:12 20:20 providers 11:10,13 20:15 public 129:23 pull 96:22 pursuant 126:3 push 58:7 90:19 put 5:18 55:9 61:5 90:16 puts 58:18 putting 5:19
			q
			qa 46:5 question 6:17 7:4,15 8:2 12:4 12:9 28:2,15 71:19 72:2,11 75:9 76:5 104:5 112:18 112:22 113:17 113:20,22 116:21 119:24 121:2,22

[questions - removing]

questions 6:24 6:25 14:20,22 15:10,11,20,23 15:24 16:2,9 16:10,10,16,17 21:18,22 37:2 44:25 55:19 56:1 59:2,18 59:20 81:3 96:14 121:7,21 122:23 123:16 123:19,19 124:16,25 129:6 queue 29:11 quick 48:1,5	real 52:8,22 reality 61:23 84:7 85:6 114:12 realized 16:18 really 24:20 41:21 54:15,18 58:21 80:15 81:16,17 reason 7:13,17 7:19 50:12,14 58:1 99:18 112:14 116:17 117:4 127:5 reasons 73:2 118:5,9 reassemble 90:5 recall 14:9,12 16:21,25 17:2 19:18,22,23 20:3 26:25 40:6 49:19 57:7 63:12 64:1 72:21 93:22 94:3 123:18 recap 75:20 receipt 127:12 receive 15:9 received 17:19 receiving 16:9 17:12,16 recess 48:9 96:17	recognize 9:19 46:12 57:1 recollection 93:18 record 6:11 8:1 48:8 126:10 recorded 126:7 red 59:9 redirect 123:11 reed 3:8 reedsmith.com 3:11 refer 9:3,15 15:5 reference 45:17 46:9 48:15,21 52:23 70:22 71:4 124:1 referred 16:3 76:25 79:20 104:7 referring 9:5 45:19 55:21 78:20 79:21 98:17 104:8 106:13 refers 45:16 regard 56:10 regarding 15:12 register 59:17 registered 2:17 regular 80:5,6 80:8,10,16 81:8,12,13	82:25 100:19 101:10,21 102:24 103:7 103:10 104:1,2 related 13:13 62:5 relating 8:15 relation 8:18 remain 68:5 remained 10:5 remember 14:4 14:7 18:9 20:17 25:23 40:2,5,8 46:22 46:23 47:1 49:11,13 57:3 57:5 63:13 64:14 66:9,11 66:13 70:8 72:23 93:8,9 93:12,13,15,20 93:24 94:5,6 122:12 123:22 remote 1:14 2:15 remotely 2:18 5:12,25 22:22 remove 71:9 75:13 102:18 104:17 106:19 removed 79:21 80:2,23 81:2 81:18 106:18 removing 102:22 107:13
r			
r 3:1 15:1 26:11 126:1 128:2,2 raises 67:23 raising 67:21 range 60:2 76:1 78:15 rates 32:5 rather 69:21 read 23:23 49:1 90:6 127:3 129:4 readable 90:15 reader 83:20 83:20 92:1 reading 34:21 102:13 120:13 reads 83:17 96:25			

[repeat - rule]

repeat 6:17 7:15 12:4 28:2 56:12 64:4 116:21 repeated 80:18 repetition 80:18 rephrase 6:18 7:5 replace 30:25 replies 17:19 reply 17:15,17 51:11 replying 21:6 report 10:16 11:21 reported 1:23 reporter 2:17 2:18 126:24 reporting 10:13 reports 57:10 reproduction 126:22 request 64:3,7 64:20 107:20 require 24:15 58:25,25 research 31:11 37:11,20 43:15 researcher 23:5 33:25 93:2 researching 15:17	reset 29:12 residing 92:24 resolve 55:16 91:2 responding 17:7,8 response 51:3,3 51:4,12,14,15 51:21 restart 90:7 result 97:1 98:21 return 127:11 reveal 38:22 review 5:19 97:6 122:5,8 reviewed 8:17 71:12 72:21,23 110:24 114:4 119:20 120:5 right 6:13 7:6 14:4 16:4 17:5 17:9,15 18:16 19:21 20:11,12 21:22 22:17,18 23:16,17 24:7 27:20 28:1,5 33:22 34:18,19 37:1 38:2,3 39:12 44:13,20 45:22 46:10 48:11 49:8 51:24,25 56:5 56:11,16,17 59:4,10 60:18	60:21 62:14 64:6 65:9,21 66:8 68:12 69:16 70:1 71:1,2,6,7,10 73:7 75:19 76:11,17,21,24 78:5,18 79:23 79:24 80:1 81:9 83:10 85:13 91:5 92:9 93:3,13 93:22 94:1 96:19 97:14,15 98:18 99:1,11 100:7,17 104:14,19,20 105:25 106:8,9 106:15 107:5,6 111:19,22 112:3,4 115:3 115:4,11,17 116:24 117:25 118:3 121:6 122:22 124:23 124:24 risk 99:22 rmr 1:24 126:15 roesch 27:8 role 10:5,8,10 31:14,15 43:17 93:1 rpr 1:24	rule 19:17 24:23 25:24 26:3,4,6 29:16 29:21,22,24,25 30:2,3,5,22,23 30:23,24,24,25 32:11 33:14,17 34:11,12,21,24 35:3,6,11,13,21 36:4,5,7 39:7 44:10,12,16 47:8,23 48:23 49:10,17,20,24 50:2,3,4,11,12 50:13,17,19 51:13,13 52:5 52:8,11,13,20 53:4,5,8,21,22 53:25 54:3,4 54:22 56:5,10 56:13,16,21 57:1,4,7,12 59:23,24,25 60:19,25 61:12 62:17,24 63:4 63:9,12,15,16 63:22 64:2,10 65:7,12,18 66:2,3,5,7,17 66:19,23 67:13 67:20,20,25 68:3,6,9 69:15 69:16,19,24 70:11 72:19,22 73:1,4,5,9,15
--	---	--	--

[rule - s]

73:24 74:3 75:10,11,14,14 75:19,24 76:3 76:19 77:3,4 77:12,16 78:1 78:2,4,8,13 79:7,12,13,18 79:22 80:13,23 81:5,10,11,22 82:16,20,22 83:2,7 84:5,8 84:11,12,17 85:5,12,14 89:19 90:25 91:3 92:12,13 95:14 97:8 98:9,17,20,24 98:25 99:6,14 100:3,6,8,16,19 100:21,22 101:4,9,15,16 101:18,19,20 101:20 102:10 102:18,20 103:4,11,17,20 103:21 104:3,4 104:14,17,25 105:2,4,5,10,13 105:18 106:2 106:10,17,20 107:10,15 109:11 110:15 110:17,23,24 111:3,17 112:11,13	113:7,23 114:4 114:18,25 115:1,5,6,15,17 115:19 116:1,6 116:25 117:25 118:1,24 123:19,21 rules 8:25 14:19,19 15:12 18:24 19:25 20:1,1,6,10,14 20:16,20 21:19 23:1,15,18,20 23:22,23,25 24:2,5,8,9,11 24:12,13,13,15 24:17,17,19,22 25:2,5,7,9,10 25:11,14,15,16 25:17,18,22,23 26:1,2 27:23 27:25 28:1,3,4 28:10,16 29:14 29:19 30:7,14 30:19 32:13 33:22 34:1,3,7 34:10,16,20,22 35:2,10 36:24 37:5,10 38:4,9 38:10,12,14,16 38:17,25 39:1 39:2,3,3,6,6,8,9 39:10 40:4 41:9,13,20 42:1,3,5,6,9,13	42:16,25 43:1 43:3 44:7,23 44:24 45:4,4,5 45:9,13,14,19 45:24 46:1,2,4 46:5,6,7,8,10 46:12,17,20,22 46:24 47:1,1,2 47:2,3,4,9,11 47:15,17,21,21 47:23 48:13 49:12,12,14,23 50:10,21 51:9 54:5,7,8,10,11 54:17,18,19 55:3,11 57:5 57:19,20 58:1 58:15,16,20,22 59:3 61:20 62:3,8,10,12,12 66:10,11 67:15 70:21,22,23,24 70:25 71:4,8 71:13,16,18,20 72:15 73:16,19 73:20,25 75:6 77:2,11 79:25 80:1,22 81:2 81:18 82:19 84:20 85:9 98:2,3 99:7,19 99:20,25 100:15 105:7,8 105:15 109:18 109:22 112:15	112:16,23,24 113:1,12 114:1 114:6,11 115:23 117:14 117:22 119:3 120:10 122:10 ruleset 13:23 18:17,20,22,23 18:24 19:4,13 20:6,14 24:10 25:6 27:7 34:4 34:17 38:10,17 39:1,10 45:6 45:19 47:9,18 47:23 50:11 80:2,23 81:18 rulesets 16:11 34:13 run 24:15 28:13 33:8 80:6,10 81:13 83:7 98:3 100:23 101:23 102:3,6 103:7 103:9 running 65:1 98:4 111:13 124:7 runs 78:21,23 79:11 s s 3:1 15:1 26:11 42:22 55:23 80:18 104:13
---	---	--	--

[safari - shipped]

safari 64:25 samples 83:18 san 40:9,16 52:5,25 sand 40:11 saw 14:17,21 26:4 saying 37:8 54:19 55:22 60:17 69:9 87:25 91:18 96:6 112:12 117:13 says 9:25 12:21 35:21 43:14 44:3 46:17 49:7 51:1 63:7 75:25 78:13 81:6 100:11,21 102:8 104:16 106:2,10 109:5 110:17 118:11 science 12:23 35:3 screen 5:15,20 5:22 9:13 48:20 110:8 screenshot 110:8 scroll 106:20 sea 59:9 second 56:22 secret 24:22 82:7,14 84:13 84:14,14,18	85:16 secretly 80:17 secure 31:17 37:6,7 90:22 95:25 security 10:1 40:13 42:22,22 54:23,24 58:11 58:18 90:20,21 92:20 101:12 101:17 103:15 see 5:15,16 6:1 9:17,18 12:11 12:13 17:17 32:18 34:24,24 36:7 51:18 52:16 56:24,25 60:25 61:16 63:1 64:16 66:5 69:24 70:9 72:19,20 73:8 80:4,17 81:6 82:14,19 83:14 89:17 96:24 97:3,14 97:16 100:9,10 100:25 101:1 103:14 105:2,8 106:10,20 109:5,7 110:15 110:16,20,21 111:5 seeing 91:5 seen 16:15 17:13 27:11	28:9 93:19,21 93:25 94:5 109:15 select 71:16,18 selected 72:8,8 semm.php 115:10 send 57:21,23 60:20 67:14 68:1,22,24 69:7 110:8,10 122:19,20 sending 31:20 32:18 67:16 108:15 118:1 118:25 sends 51:11 111:2 senior 10:1 senn 113:21 sense 7:11 8:4,5 51:17 54:23,24 58:11,18 64:18 67:12,24 74:15 74:16 88:22 90:20,21 101:3 102:4 sensitive 43:24 sent 8:25 11:10 77:17 sentence 78:13 96:25 118:11 sentinel 10:11 sequence 101:13	series 87:12 serious 88:18 server 36:9 51:10,11,22,22 53:16 57:14 64:23,24 65:3 67:9 105:22 110:9,11 116:5 116:18 117:2,6 117:9 118:7,17 124:9 set 18:24 25:15 50:19 62:11,12 67:15,19,25 68:4,5,5 73:18 99:6 100:16 101:20 103:17 112:9 113:6 114:5 115:14 sets 67:23 setting 67:11 seven 86:6 118:10 seventh 65:12 several 71:13 share 8:20 shared 8:20 9:13 sharing 9:11 sheet 127:6,7,9 127:11 129:9 ship 39:6 105:15 shipped 113:2 114:1
--	---	---	---

[ships - sorry]

ships 50:17 shoot 10:18,21 short 51:7,7 52:15 73:20,23 94:14 96:9 112:8 114:5,21 116:13 123:10 shorter 113:14 116:13,14 shorthand 2:17 126:7,24 shortly 46:13 show 58:16 59:1 showed 122:9 showing 104:14 shows 45:18 sic 66:24 102:23 112:21 sid 48:23 53:6 56:5,22 59:24 62:24 65:13 66:17 98:18 100:3,8 104:25 110:15 side 32:15,16 sign 11:13 39:6 50:6,7,7 60:5 67:1 68:17 69:3 75:13,16 75:17 79:21 102:23 104:8,8 104:10,13,18 120:13,15 127:7	signal 117:14 117:14 signals 59:15 signature 29:8 31:23 32:19,21 37:21 44:6,12 96:25 118:11 126:15 129:12 signatures 15:12 16:20 19:1 44:4 86:10 95:21 112:7 signed 9:20 119:21 120:6 signing 127:8 simple 55:16 82:24 89:7 91:1,2 simply 20:23 30:16 single 57:21 73:16 80:6,11 103:1,25 107:1 107:19 120:9 sip 88:13 sir 5:14,24 6:12 7:2 8:5,8 9:6 9:18,24 10:4 11:6 12:20 13:2,9 15:2 19:21 21:2,11 23:8 24:7 25:21 26:12,19 27:24 28:22	29:18 31:5 34:19 35:10,14 37:14,18 41:18 42:17 43:11,13 43:19 44:2,8 44:20 45:22 49:6,9 51:25 55:25 56:25 59:22 61:1 63:13 66:6,15 66:18 69:14 70:17 75:23 77:22 78:11 79:19,24 83:6 92:10 93:4,15 97:4 98:19 100:10,17,20 104:10,15,24 106:1 109:7 110:21 111:20 112:14 115:12 115:18 118:8,9 119:11 120:18 121:4,9,17,24 122:7 124:12 124:15,24 sites 24:14 situation 59:6 65:17 114:4 six 46:25 size 51:6 53:17 116:12,13 slash 67:1 68:17 69:3,25 70:13	small 32:10,13 33:13 49:2 74:11 114:20 119:2 smaller 85:23 smith 3:8 snort 8:25 14:17,18,19 15:1,3,4,5,8,10 15:11,13,14,17 15:20,22 16:7 16:14,17 17:7 17:8,13,19,21 18:14,18 19:1 20:14,15,20 21:19,24 22:9 25:13 26:18 27:3,6,7,12,18 27:23 28:8,8 28:12,13,16,19 28:20 33:21 35:13,17 38:4 44:4,6,7,12,12 70:23 71:10 75:19,20,21 104:18 social 101:12 101:17 103:15 solemnity 119:11 somebody 75:11 sorry 8:16 11:23 13:8 14:7 19:22
---	--	--	--

[sorry - sure]

24:25 27:19 28:2 35:18 41:16 43:12 53:6 62:8 63:2 64:4 71:23 76:4,14 88:5 88:20 94:8,10 96:16 103:3 104:10 106:24 116:14 121:19 121:23 sort 33:14 54:10 87:8 108:5 source 33:1 60:2,7 sourcefire 26:20,21,22 27:2,5,19,21 28:1,4,6,7,8,17 space 67:1 68:16 127:5 spans 62:24 speak 41:16 specific 25:24 59:21 93:17 specified 115:16 speculation 22:4 spy 110:12 spyware 109:6 109:12,23,24 110:6,7	spywares 110:11 ssl 76:23 77:17 77:24 78:14 79:9,13,15 92:17 93:5,7 93:10,12,18,20 94:1,2,6,11 95:7,10,12,16 96:1 standard 69:12 stands 27:13 start 15:17 16:8 23:25 24:3 33:21 35:1 36:6,19 36:20 51:2 54:14 84:24 86:4 109:19 111:10,15 112:23 117:15 started 23:14 23:15 33:23,24 34:15 36:23 37:10 39:13 46:14 starting 23:9 51:1 75:4 113:21 starts 35:14 63:3 69:25 state 13:4 71:12 127:4 statements 119:8,9	states 1:1 2:1 51:2 55:2,4 59:11 85:1 90:19 119:13 stealing 43:23 43:24 stop 29:12 80:17 89:11 92:5 stored 86:15,16 story 79:25 stream 52:12 64:25 65:2 street 3:9 strike 76:4 string 97:11 strong 84:21 student 35:3 37:23,24 students 98:6 subject 127:8 submission 41:13 submit 40:4 44:24 45:4 57:4 submitted 34:16 38:5,9 41:9 45:5 47:9 47:11,15,22 48:12 57:2 100:11 submitting 34:7 36:25 37:10 38:25	100:15 subpattern 57:11 subscribe 15:8 15:19 16:8 subscribed 129:16 subscription 44:17 subset 44:15,17 substance 129:8 substream 105:9 successful 97:2 98:22 100:4 sudden 54:2 suite 3:9 summary 71:14 supervision 126:8,24 suppose 84:12 88:1 124:7 supposed 50:21 99:23 103:18 113:8 sure 6:18,22 7:8,16 12:6 28:3,17 33:19 39:19 40:2 41:5 47:5 55:3 55:20 56:13,23 59:11,19 64:5 65:15 66:14 67:17 68:21
---	---	--	---

[sure - things]

69:4 74:22 86:1 91:8,16 98:17 104:5 105:6 107:14 111:25 112:3 116:23 117:21 123:5 suricata 18:25 26:10,18 42:24 42:25 43:1,3,7 44:4 75:21 suspicious 109:16 swear 119:11 sworn 5:5 126:5 129:16 symbol 102:23 syntax 34:21 35:12 59:24 70:20 81:5 114:25 system 10:22 11:17 14:6 15:4 18:25 23:23 24:6,9 25:22 27:10,14 27:15,16,18,20 28:14,24,25 29:2 31:22 33:4,5,8 40:12 40:14,16 41:22 41:25 55:12,16 58:8 59:13 71:10 75:1,19 75:22 80:15	81:16 83:9 86:15,16,18,20 86:23 87:3,6,9 88:10,20,25 91:18 92:11,16 92:23 95:10 98:22 100:5 101:9 102:19 104:19 110:12 111:16 117:1,4 117:18 123:3 124:12,13 systems 13:22 19:1 21:1,4 28:20,21 31:4 36:20,20 54:13 59:15 74:18,25 74:25 84:23 85:2,3,4 87:16 88:9 92:3,7,8 92:23 94:24 116:8 123:5,7 t t 15:1 26:11 126:1,1 128:2 table 40:17 take 7:24 8:3 26:4 30:3 32:25 48:1,4 96:9 110:7 taken 6:19 48:9 96:15,17 126:3 talk 38:20,23 talked 23:18	talking 44:7 56:2,8 62:14 70:20 76:9 81:9 85:7 87:4 87:5 93:1 target 33:8 tasks 58:22 tcp 35:16,18 60:13 68:10 75:25 76:14,15 76:17 78:14 103:24 105:23 115:2,5 team 8:24 15:11,11 16:17 17:14 18:13 technologies 1:6 2:6 91:9 technology 91:11 tell 6:11 7:20 50:2 53:8 63:16 64:1 69:23 79:24 121:22 126:5 tended 113:1 terminology 33:22 39:12 terms 24:14 44:11 86:9 terrible 80:3 81:1,19 test 46:4 98:2 105:8 112:16	tested 44:3 82:18 testified 5:6 56:13 testimony 4:2 7:14,18,20 56:4 59:5 94:11 126:2,6 126:10 testing 42:1 text 83:15,15 85:15,21,22 110:10 thank 7:6,22 9:7 27:16 55:24,25 59:19 104:12,21 114:23 120:17 122:24 thanks 47:14 thereof 126:13 thing 29:2 44:11 91:4 things 5:20 34:8 50:20 52:12 54:8 58:23 73:10,10 74:6,19,20 79:15 80:16 82:15 86:13 87:12 91:22,22 95:4 96:5 98:10 99:4,7,9 99:12,16 105:17 110:1,6
--	---	--	--

[things - trademark]

113:7,11,12 think 20:17 27:8 29:1 33:20 42:13 47:19 55:17,21 63:10 67:13 69:10 85:8 88:23,23 89:6 90:18,19 91:15 92:15 94:10 96:8,11 97:13 97:16,21,25 99:11 101:16 102:15 103:19 104:5,6 112:16 113:3,16 114:10 124:3 124:20 thinking 102:10 123:1 third 20:15,20 22:21 thirty 127:12 thought 14:23 37:13 53:6 thousand 41:23 thousands 22:1 74:10,11 92:1 threat 10:9,13 10:15,18 11:3 11:10,11,12 29:11,15,22 32:25 33:2 52:9 53:13 65:25 88:1	89:10 108:15 threats 10:19 10:21 13:13,15 13:19,23,25 14:1,16,21,24 16:3,13,16,19 16:22 17:1,6 17:14,21,25 18:3,7,15,19,23 18:24 19:4,4 19:14 20:6,11 20:13,18,19 22:9,10,12,16 22:22,23 23:4 23:7,11,14,16 24:10 25:6 26:5 27:25 28:4,6,16 31:10,16 34:4 34:6,8,11,15,17 36:24,25 37:3 37:11,16,21 38:1,5,8,15 39:12,14,17,18 39:20,23 40:1 40:4,23,24 41:3,10,20 42:3,5,6,9,12 42:16 44:5,14 44:15,16,19 45:2,12,17,21 45:24 46:6,9 46:13,14 47:12 47:16,17 48:13 48:15 49:23	70:22 71:4,13 92:4 93:2 three 29:20 39:21 time 6:21 7:25 10:6 15:22 18:10 20:20 22:24 23:10,10 24:6 26:14,23 27:1 31:13 35:9 37:19 38:4,11 39:20 40:1 42:7,10 45:2 46:3 49:23 52:15 53:12 58:25 63:13 67:23 68:1 73:9 75:2 81:14 89:23,24 91:6 96:11 99:15 102:1 103:16 108:2 114:15 118:24 122:1,2,23,25 126:3 times 68:4 80:19 tiny 50:13 62:4 63:2 73:20 title 82:7,14 84:2,3 89:17 tls 57:23,24 58:3 73:10 77:8 84:19 88:5,5,15 89:9	89:21 92:17 93:23 94:1,3 94:11 95:7 96:1 today 5:11,18 6:23 7:7,14,18 8:7 9:4 32:8 41:23 45:1 58:24 75:8 120:20 122:23 together 73:5 90:16 told 51:6 66:10 74:9 83:12 88:17 89:7 90:20 91:23 94:18 102:24 103:7 116:12 118:22 ton 73:25 113:21 tons 54:3 top 24:22 56:22 82:7,14 84:13 84:14,14,18 85:16 86:7 topic 91:16 topics 15:12 43:2 tower 3:9 tracker 12:12 89:9 trademark 1:1 2:1
---	--	--	--

[traffic - understand]

traffic 11:2,18 12:1,8,9,11 24:1,1,16 29:3 29:5,7,10,17,17 29:24 30:1,4,6 30:9,10,15,19 31:21 34:25 35:22 36:1,3 36:16 50:20 51:5,8 54:6,9 54:20,20 56:9 56:15 57:18,21 57:25 60:9,10 62:9,12,16 63:20 65:18,19 65:20 68:3,10 69:19 74:2,3,7 74:14 76:19,23 77:3,14,14,17 77:19 78:3,10 82:10 83:25 84:18 86:10 87:24 88:7 89:11 90:6 95:15 96:1 98:3,5 99:21 99:22 100:1 103:4,18,23,24 105:19,20 107:22 109:2 111:17,21,25 112:25 115:24 117:21 118:2 118:16	transcribed 126:8 transcript 7:8 55:20 60:16 126:21 127:13 127:14 transcription 126:9 129:5 transfer 78:24 79:8 87:20 89:7 95:25 transferred 53:15 84:15 87:4,19,20,22 transferring 79:2 transfers 73:13 78:25 88:15 transformed 85:22 transiting 82:24 84:19 87:16 translation 104:6 transmit 79:5 trap 59:2 travel 42:11 treats 100:16 trial 1:3 2:3 trigger 69:19 77:25 78:2,4 79:8,12 99:3,4 99:13 115:17	triggered 60:20 64:2 68:1 76:23 78:9 85:14 100:3 111:17 116:25 trouble 20:5,7 true 58:8 74:16 89:6 90:23 116:16 119:9 119:10,15,16 120:15 123:4 126:10 trust 104:2 truth 126:5,5,6 truthful 7:14 7:18 truthfully 6:25 try 54:21 59:20 75:9 90:18 92:5 trying 24:15 32:19 34:22 51:12 54:7,16 54:17 58:16 59:1 68:23 74:6 78:7 92:4 111:4 tuesday 1:16 2:13 5:1 tunnel 59:2 tuple 56:2 68:9 turn 9:25 12:21 52:8,11 69:24 98:9	turned 6:12 turning 96:20 114:23,25 two 26:15,18 29:20 39:21 52:17,20 90:10 122:4 type 86:1 90:8 109:24 110:1 types 11:5 88:8 116:7 117:16 typing 110:10 typo 63:8
u			
u 26:11 55:23 u.s. 1:7 2:7 91:8 udp 35:16,18 103:25 uh 7:2 48:25 97:8 ultimately 54:5 54:9 unacceptable 81:15 unauthorized 33:3 43:21 86:21 87:2 uncomfortable 55:18 59:5 under 8:6 43:8 44:23 126:8,23 understand 7:1 8:6,8 27:4 34:23 51:18 53:1 55:4,5			

[understand - validates]

56:4 63:8 64:6 67:17 71:19 87:1 91:17 101:2,25 102:6 102:9,13,17 109:8 116:20 116:24 117:18 117:25 understanding 7:3 35:1 100:2 110:22 understood 12:7 91:15 94:10 unencrypt 89:11 117:11 unencrypted 57:19,20,22 65:20 111:7,8 unfortunately 28:11 51:4 52:14 82:23 97:10 unintelligible 48:25 65:16 unique 97:15 97:17,21 98:1 112:17 113:5 united 1:1 2:1 55:2,4 59:11 85:1 90:19 119:13 units 10:25 universe 114:6	university 12:24 13:3,6 13:10,12,20 37:25 98:4,5 unix 28:14 unprecise 94:15 unusable 24:16 unviable 81:10 uploaded 88:2 upside 59:7 uri 57:11,15 61:14,14 62:15 62:16,18 106:18,19 107:13,13,14 111:2 112:5 115:10,16 uricontent 61:11,13 106:11 uris 61:15 url 11:5,7,8,8 11:17 12:2,8 12:10,15 19:25 31:19 45:18 57:11,11 61:14 61:21,22,23 62:1,4 69:4 105:5,6,6,10,11 106:14 109:16 111:1,8 112:6 112:8,17 113:16,20,21 114:5,8,9,12,12	114:20 116:12 118:14,21,22 118:25 119:2,3 urls 11:2,4,9,12 11:14,17,18,25 12:11,13 62:5 69:25 105:9,12 105:13 112:18 112:22 113:3,9 113:10,19 114:6,7,20,21 118:22 use 6:2,3 11:2 19:2 23:20 24:9,23 25:5,7 25:16 27:22,23 28:1,4,19 40:14,16 52:22 53:16,17 62:10 70:23 74:1 75:11,19 102:20 103:2,4 108:3 used 10:21 13:21 18:8 21:7,24 24:6 32:16 39:5 40:3 41:12 44:25 46:3 49:23 52:2 67:14 83:5 84:21 88:5,5 93:8 94:12 101:9 108:8 110:6 112:15	115:19 127:15 useful 13:24 16:1 100:24 102:8,10,12,14 102:15,18,18 103:13 104:16 user 40:14 63:17,18,20 64:3,7,17,19,21 64:24 65:4 66:1 86:17 87:10,11,18,19 124:8,9,9,21 users 15:8 52:4 124:5,6,11 uses 15:7 78:17 78:19 83:4 using 6:7 10:18 23:14 30:19 55:11 78:14 88:15 96:2 105:22 107:11 107:15 111:2 usual 116:9 usually 12:11 30:7 36:6 79:1 v v 1:8 2:8 v3 77:17,24 93:5,7 validate 60:6 82:10 94:23 105:8 validates 89:12
---	--	---	--

[validating - work]

validating 90:7 value 61:9,18 61:18 62:20 89:2 91:20 92:13 94:12 95:7 106:7 107:5 108:8 values 25:12 36:17 59:25 60:1 61:24 63:18 65:8 76:2,7,7,16 92:9,12,17 95:6 111:25 112:2 115:2,8 115:14,16 variable 60:3,5 variables 97:12 variety 109:25 110:5 various 48:13 verbal 7:9 veritext 8:20 version 65:1 78:15 79:9,14 92:17 93:12,18 93:20,23,24 94:1,2,6,11 95:7 versions 94:3,7 vetting 38:14 46:5 video 73:13 77:5	view 31:23 114:18 115:21 viewable 81:11 viewed 10:22 visibility 87:24 109:2 vobfus 110:19 voice 52:13 53:14 73:12 77:7,9 volunteer 37:4 39:15,16 40:4 47:13 volunteering 34:7 37:20 38:1 volunteers 39:25 40:6 vulnerabilities 32:2,3,5,6,9,10 32:14 33:11,13 74:11,12,13 93:6,7,10,11,18 93:19,21,25 94:4,5,7,8 vulnerability 23:5 31:11 32:2,4,12,16,23 32:24 33:16,19 33:25 36:10 43:15 74:10 93:2,13,17 vulnerable 33:6	w w 60:17 80:18 80:19 walk 89:16 wan 60:2,7,17 want 5:21 48:1 48:2,3,4 50:21 52:6 59:4 91:4 91:16 96:9 118:19 wanted 5:12 22:24 37:3 56:15 75:11 wants 52:24 wars 91:7 washington 3:10 waste 89:24 103:16 watch 10:10 watching 10:12 way 16:1 31:16 31:17 37:7 57:24 88:8 120:8 we've 47:25 96:8 weak 117:14 web 64:23 107:21 113:12 website 11:16 18:1,3 19:5,15 19:19,20,23 23:19 45:12,21 46:13 108:2	websites 113:11 weight 80:9 went 91:16 whichever 50:8 win 85:4 windows 36:9 99:10 winners 52:19 wish 55:9 59:17 witness 9:10,11 12:4 13:15 19:11 22:5 40:11 48:3,7 48:17 72:14 89:4,6 96:16 116:20 119:25 120:2,8,21 121:2,4,12,14 121:19,23 122:24 125:1 126:11 127:1 word 82:12 83:13,20 84:1 86:2 90:9 91:24,25 94:19 96:24 98:12 104:9 words 7:9 work 10:9 11:8 11:11 15:21 20:14 21:8,20 22:11,12,13,24 26:16 28:7 30:18 34:22,24
---	---	--	---

[work - zuzu.php.]

35:2 37:4,15 39:12,17,22 40:9 45:11 65:22 84:7,8 91:12 105:7 113:4 worked 21:10 23:4 27:11 28:8,11,12 31:10 37:19 39:19 40:7 43:15 46:1 49:24 53:10 82:18 working 22:21 26:9 46:14,25 47:12 112:15 world 59:7,10 91:5 worobij 3:8 worried 55:10 88:18,19 123:1 123:4 worst 101:19 101:19 103:6 write 23:1 33:17 34:1,20 35:3,10 37:5 40:21 49:23,24 102:5 119:17 119:18 writing 16:19 33:21 36:24 47:20,22 61:20 63:12 85:5	120:11 written 29:16 30:3,7 49:3 57:4 120:9 wrong 51:19 67:16 wrote 34:17 38:4 46:7,22 47:2 49:10,13 49:15,18 57:6 57:8 66:10,11 66:20 119:21 120:6,14 122:20	z z 80:20 zeros 53:12,20 80:18 zoom 5:15 zpack 110:19 zuzu.php 106:11 zuzu.php. 105:9
	x	
	x 4:1 xyz 65:1	
	y	
	yeah 20:18 25:2,24 44:10 48:5 52:20 95:16 96:10 102:4 110:16 123:9 year 17:2 19:9 years 13:3,5,10 14:9 18:10 43:8 46:24 47:1 66:14,14 yep 66:14 yesterday 121:24 122:21 york 3:4,4	