EXHIBIT 5

Finjan v. Juniper

Nagarajan, Chandra (Vol. 01) - 05/31/2018

1 CLIP (RUNNING 00:31:58.496)

Plaintiff's Deposition Designations for Chandra Nagarajan - Accepted Counters, Juniper's Counters, and Finjan's Counters (05-31-

CN0531-CC **72 SEGMENTS (RUNNING 00:31:58.496)**

1. PAGE 10:05 TO 10:20 (RUNNING 00:00:47.877)

CHANDRA NAGARAJAN,
the witness herein, having been first duly sworn, was examined and testified as follows:

EXAMINATION

BY MR. LEE:

Q Where do you work?

A I work in Juniper Networks.

Q What's your position at Juniper Networks?

A My position is a senior director in the security business group.

Q What are your responsibilities?

A I manage a team of engineers and -- I'm responsible for the engineering delivery of the product. So I ensure we get the right specifications for the product, and then we execute the schedule we come up with for the features requested.

2. PAGE 11:21 TO 12:20 (RUNNING 00:01:32.753)

Q What is Sky ATP?

A Sky ATP is a cloud-delivered advanced threat prevention service. It -- it works directly with SRX and then try -- it tries to get files out of the network, whatever is going through the network and makes a determination, to the best of its ability, what the threat level of those files are. And it's -- it's basically a SAS type of product where the most of the functionalities reside in the cloud and the user itself logs into the cloud and most of the input -- input on the user interface is on the cloud site.

Q What does Sky ATP stand for?

A Sky is, I guess, is just a brand name, and the A. T. P. is for advanced threat prevention.

Q What is advanced threat prevention?

A What is advanced -- so the advanced threat prevention, the name mainly comes because in the market, there are a lot of AVs which can detect if something is -- is good or bad based on what they know. But advanced threat prevention is something even if you get a file, which it doesn't know about, it tries to evaluate to the best of its capability and determines the threat level.

Q So advanced threat prevention is for unknown threats?

3. PAGE 12:22 TO 12:23 (RUNNING 00:00:06.646)

A Advanced threat protection is both for known threats and also for unknown threats.

4. PAGE 12:24 TO 12:24 (RUNNING 00:00:03.404)

Q What are the key components of Sky ATP?

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
Trial Exhibit 496
Case No. 17-CV-05659-WHA
Date Entered: __________ By: __________
Deputy Clerk

5. PAGE 13:01 TO 13:19 (RUNNING 00:01:16.038)

A So the key components of Sky ATP is there is a module in SRX which -- which analyzes a protocol, and if there is a -- is a particular file is fetched by the client, it determines the file category of it. And then if the user has configured that category to be analyzed, it takes the file, sends it to the cloud. Okay. And that's the first part of it.

And then the action mostly moves the cloud where we have a set of adapters which inspects these files and -- there are a series of adapters which inspects these files, tries to get the behaviors of these files, and then it tries, to the best of its ability, to determine the threat level to this file. And the threat level can be -- the user can choose to do what with the threat level. They can try -- they can configure policies to let it go or just -- just log or they can configure policies to block it, or they can even configure to just to analyze these files without doing anything.

6. PAGE 17:02 TO 17:14 (RUNNING 00:00:45.557)

Q All right. In the collection of behaviors and the threat levels, are they stored anywhere?

A The collection of behaviors is -- for a particular file is stored in -- in a file in S3, and -- but the mapping of the behavior to the threat level is not stored. It's -- it's on a machine-learning algorithm. Even we don't -- even we're not able to clearly explain how that maps to the threat level. It's something which is a learned behavior by the machines.

Q Is there -- strike that.

Did you say the collection of behaviors is stored in S3?

A Yes.

7. PAGE 17:24 TO 18:14 (RUNNING 00:01:05.733)

How do you know which file performed the collection of behaviors?

A Oh, I see. Okay.

So whenever each file is given to the Sky ATP, we calculate a SHA-256. It's -- it's really a unique identifier to identify that file. And the collection of whatever behaviors of all the adapters which we store in S3 is linked to that -- the SHA-256 ID.

Q How is it linked to the SHA-256 ID?

A So we store the ID in the DynamoDB of AWS, and then from there, there's a link to the S3 for that sample, which -- which has all this -- all the results of the various adapters stored in a file in some unstructured format. It's a JSON format, and it has various sections where all the -- it has information of the behaviors from various adapters.

8. PAGE 18:16 TO 18:20 (RUNNING 00:00:15.892)

So the collection of behaviors is stored in DynamoDB, and there's a -- a link --

A Not -- the collection of behaviors is not stored in the DynamoDB. The collect -- the SHA ID and the link to the behaviors are stored in the DynamoDB.

9. PAGE 18:21 TO 19:01 (RUNNING 00:00:18.968)

Q When you say the "link to the behaviors," can you elaborate? Is that two -- the SHA-256?

A No. The -- the actual behaviors are stored in the S3. Once you look up a SHA-256, somehow you were to get to that file where all this information is stored. That's why I call it as a link.

10. PAGE 19:02 TO 19:05 (RUNNING 00:00:16.312)

Q And you say a link. Is it like a hyperlink?

A I haven't exactly looked at the source code, so I won't be able to authoritatively state how it looks like. I think the answer should be in the source code.

11. PAGE 19:06 TO 19:17 (RUNNING 00:00:46.087)

Q What is DynamoDB?

A The DynamoDB is an Amazon-provided service. And it is a -- it is a new class of schema LS database where you can store some key-value files in the -- in the DynamoDB. And it's very -- very efficient. They provide a higher availability in all those things.

Q What do you mean by key-value pairs?

A The key-values -- for example, the SHA-256, that's a key for us to locate the -- all this information of the various adapters. And the value I would say what I would call is the link to get the behaviors.

12. PAGE 19:18 TO 19:19 (RUNNING 00:00:06.223)

Q Is anything else stored in DynamoDB other than the SHA-256 and the link to the behaviors?

13. PAGE 19:21 TO 20:01 (RUNNING 00:00:20.601)

A So I -- I would say since my involvement is at the -- the secondary level, I haven't looked at the source code. So I would say maybe the threat level is stored, if I were to guess, here. I think the source code would be the most authoritative. But I would -- it's possible that the threat level is stored there.

14. PAGE 23:07 TO 23:14 (RUNNING 00:00:29.248)

Q Are these characteristics stored anywhere?

A Again, the characteristics are stored in the file, whatever we mentioned before. That is a file where it's an unstructured format in JSON. It has the results of the adapters. Whatever characteristics we -- we get out of this greyduckling is again stored as a result in that file as a -- as an analysis of the greyduckling adapter.

15. PAGE 23:15 TO 23:16 (RUNNING 00:00:03.640)

Q Is there a name for this file that contains the results?

16. PAGE 23:18 TO 24:03 (RUNNING 00:00:34.043)

A So it is -- I'm not aware of any name. So we -- we -- I think in the code maybe it is referred as a results database, where it has the identifier with the links we set to the results of all the adapters of the file.

Q Just to be clear, I'm asking about the -- the file that contains all the results.

A Uh-huh.

Q You said it's a JSON file?

A Yes.

Q Is there a name for that file?

17. PAGE 24:05 TO 24:10 (RUNNING 00:00:23.551)

A There's a -- is there a technical name? It's just a -- it is just a -- it's -- you can call it results -- adapter results file, but I don't think we call it in -- a specific name for that file. Maybe the file name is usually identified as a ID, dot, something, the name of the file itself, the way it is stored.

18. PAGE 24:11 TO 24:15 (RUNNING 00:00:17.963)

Q Is this JSON fail -- file stored in results database?

A So the JSON file is stored in S3. And the -- the DynamoDB links the -- the identifier for the file to the results file.

19. PAGE 24:18 TO 24:23 (RUNNING 00:00:21.147)

Q Did you mention a results database?

A So in the -- in the -- technically internal to the team, we refer to it as a results database. In the code maybe there is reference to the results database, but the -- the way it works is we're using the DynamoDB and the JSON file.

20. PAGE 24:24 TO 25:11 (RUNNING 00:00:56.249)

Q What is the results database?

A I'll -- I'll repeat one more time since the question is the same. So the results database, whatever you see in the code is just your DynamoDB, which has a key as the SHA-256 as an identifier. And from there you can directly link to the JSON file, which has all the behaviors of the adapter, and the JSON file is stored in S3.

Q So the results database is a combination of DynamoDB and S3?

A Yes. It's a combination of the -- the DynamoDB and the -- and the information in S3.

Q What's the purpose of the results database?

21. PAGE 25:13 TO 25:20 (RUNNING 00:00:35.438)

A The purpose of the -- the DynamoDB is -- is when you get a file from the SRX, the cloud calculates the ID using the SHA-256 column, and it looks up the DynamoDB and then gets the threat level. And if the file existed, you'll immediately get the threat level. If it doesn't exist, then the code allows it to go through the rest of the adapters to get the file -- file analysis more.

22. PAGE 32:17 TO 33:02 (RUNNING 00:00:41.285)

Q Previously, I asked you what are the key components for Sky ATP. Do you recall that?

A Uh-huh.

Q I think you mentioned SRX adapters and policies?

A Uh-huh. I -- okay. That's correct. There are some modules in SRX to get the files.

Q So why are the adapters a key component?

A The adapters are a key component because the adapters determine the threat level for the file, which is the primary -- primary goal of this ATP product.

23. PAGE 35:20 TO 35:20 (RUNNING 00:00:02.751)

Q Why was Sky ATP developed?

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.

WHAT WILL YOU BUILD? | **sales@docketalarm.com** | **1-866-77-FASTCASE**

fastcase®
Smarter legal research.