

DECLARATION OF FRANK JAS

I, Frank Jas, declare as follows:

1. I have personal knowledge of the facts set forth in this declaration, and I could and would testify competently thereto if called upon to do so.

2. I am a Distinguished Engineer with Juniper Networks, Inc. ("Juniper"). Prior to working at Juniper, I was Chief Technology Officer with Cyphort Inc. ("Cyphort"). Cyphort was acquired by Juniper in September 2017 and the Cyphort product catalog was rebranded in March 2018 to Juniper Advanced Threat Protection Appliance (collectively, "ATP Appliance"). During my time with Juniper and Cyphort, I have been responsible for the development of various different components of the ATP Appliance, and I understand how the ATP Appliance operates.

3. The ATP Appliance is a passive device that connects to a network to observe traffic. To do this, the ATP Appliance sets up "collectors" at various points in the network either virtually or physically (such as a gateway or switch). The ATP Appliance does not interrupt or block network traffic, but instead analyzes copies files have been sent to it while those files continue on to their destination.

4. During collection, the ATP Appliance performs MD5, SHA1, and SHA256 hashes on the copied files as they are received to perform a hash look up. The ATP Appliance does not inspect the file to identify whether there are any referenced software components contained in it. Nor does it fetch or retrieve any components that are referenced in the file before the file is hashed. The ATP Appliance also does not wait to receive anything that is referenced in the file before it processes the file. If the ATP Appliance were to separately receive a file's referenced components (because, for example, the end user clicked on them or initiated a separate request for them), it would treat them as a separate file sample. Thus, ATP Appliance hashes the file by itself and not together with any other file or component. Nowhere in ATP Appliance is there any function that hashes the contents of a file together with the contents of any other files.

5. After a file is copied and hashed at the collection point, the copied file is sent to ATP Appliance's pipeline analysis, which includes, among other things: (1) static analysis, and (2) dynamic analysis.

DECL. OF FRANK JAS ISO
JUNIPER'S MOTION FOR SUMMARY JUDGMENT

6. As part of static analysis, ATP Appliance uses rules and signatures to identify known threats and malware. During static analysis, ATP Appliance does not identify a file's referenced software components; nor does it fetch any referenced components. In addition, the static analysis engine does not perform any hashing functions.

7. As part of dynamic analysis, a file is executed in a sandbox environment for ATP Appliance to observe its behavior. During this analysis, the file is unaltered. If the file being analyzed is programmed to do so, it is allowed to obtain components referenced in the file as part of its execution, although ATP Appliance itself does not fetch or retrieve those components. In the event that a file obtains any referenced software components during execution in the sandbox, those software components are not hashed. The dynamic analysis engine does not perform any hashing functions.

8. I understand that Finjan cites to a document titled Vandelay-ThreatAssessment-2015 in its infringement contentions to support an allegation that ATP Appliance fetches and generates the hash value for dropped files that are detected during dynamic analysis. ATP Appliance has no such functionality. The Vandelay-ThreatAssesment-2015 document does not describe the functionality of ATP Appliance. Rather, this document is an exemplary report that the Threat Research team at Cyphort would manually assemble to describe threat detections at customer deployments.¹

//

Executed this 14th day of February, 2019, at Sunnyvale, CA

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.


Frank Jas

¹ "Vandelay Industries" is actually a reference to a fictional company in the sitcom Seinfeld where George Costanza pretends to have interviewed at "Vandelay Industries" as a latex salesman.