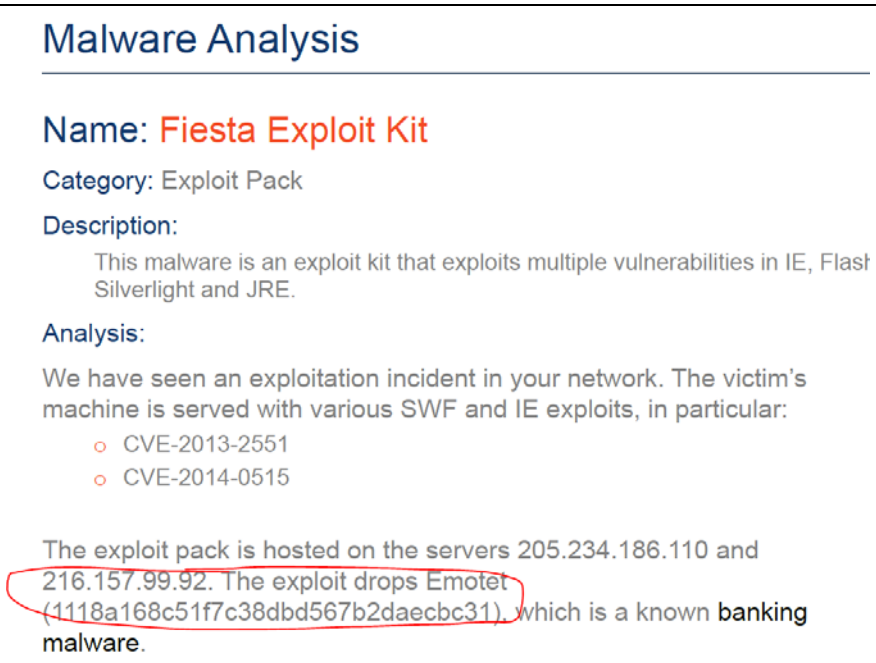
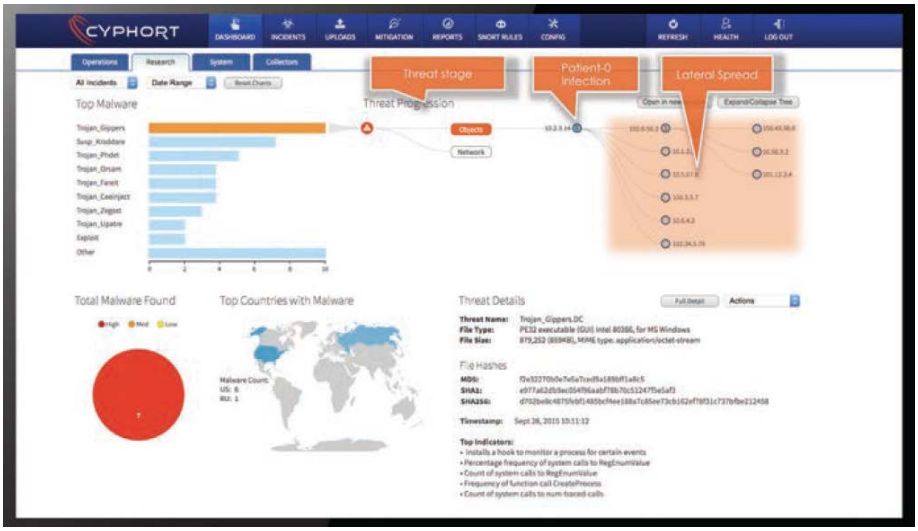
EXHIBIT 5

<table>
<tr><td></td><td>


Vandelay-ThreatAssessment-2015 (emphasis added) (showing fetching an component and creating a hash value for that dropped file).



Cyphort DataSheet (showing MD5, SHA1, and SHA256 hashes).</td></tr>
<tr><td>Claim 9</td><td></td></tr>
<tr><td>9a. A system for generating a Downloadable ID to identify a Downloadable, comprising:</td><td>ATP Appliance meets the recited claim language they provide a system for generating a Downloadable ID to identify a Downloadable.

ATP Appliance meet the recited claim language because ATP Appliance is a system which generates a Downloadable ID by creating malware attack profiles which include a hash to identify a Downloadable such as malware. The analysis includes scanning the Downloadables which include references to software</td></tr>
</table>

components required to be executed by the Downloadable (e.g., suspicious web page content containing HTML, PDFs, JavaScript, drive-by downloads, obfuscated code, or other blended web malware).

ATP Appliance is a system which obtains a Downloadable then generates a profile that includes generating a Downloadable ID (e.g., the SHA-256 hash) to identify a Downloadable and to determine whether it is malicious and to return a risk score or verdict.

Malware Analysis

Name: Fiesta Exploit Kit

Category: Exploit Pack

Description:

This malware is an exploit kit that exploits multiple vulnerabilities in IE, Flash Silverlight and JRE.

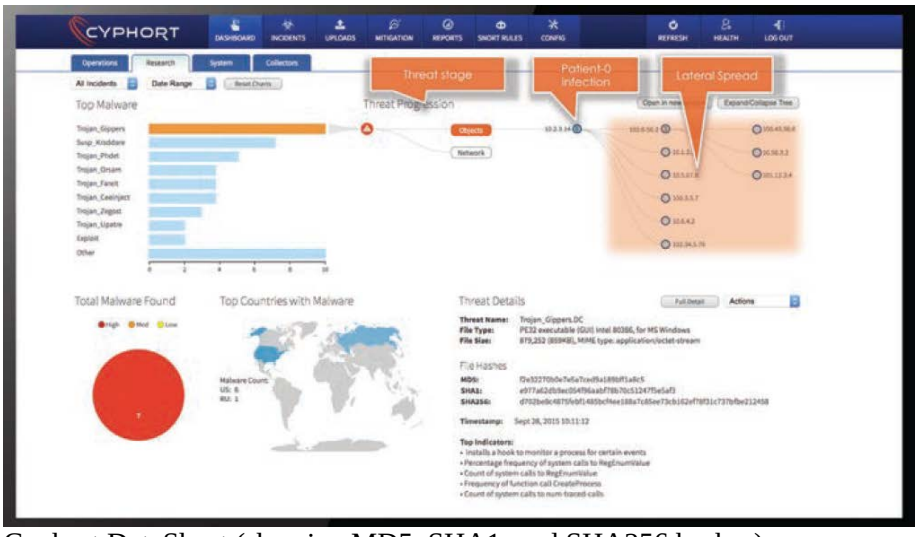
Analysis:

We have seen an exploitation incident in your network. The victim's machine is served with various SWF and IE exploits, in particular:

- CVE-2013-2551
- CVE-2014-0515

The exploit pack is hosted on the servers 205.234.186.110 and 216.157.99.92. The exploit drops Emotet (1118a168c51f7c38dbd567b2daecbc31), which is a known **banking malware**.

Vandelay-ThreatAssessment-2015 (emphasis added) (showing fetching an component and creating a Downloadable ID for that dropped file).



Cyphort DataSheet (showing MD5, SHA1, and SHA256 hashes).

9b. a communications engine for obtaining a Downloadable that includes one or more references to software components required to be executed by the Downloadable; and	ATP Appliance meets the recited claim language because they provide a communications engine for obtaining a Downloadable that includes one or more references to software components required to be executed by the Downloadable. ATP Appliance meet the recited claim language because ATP Appliance is a system which includes a communications engine (e.g., network interface and corresponding proxy software) which obtains suspicious traffic flows for analysis that include Downloadables such as web page content and/or email attachments. These Downloadables include references to software components required to be executed by the Downloadable (e.g., suspicious web page content containing HTML, PDFs, JavaScript, drive-by downloads, obfuscated code, or other blended web malware). Downloadables that includes one or more references to software components required to be executed by the Downloadable include a web page that includes references to JavaScript, visual basic script, ActiveX, injected iframes; and a PDF that includes references to JavaScript, swf files or other executables. Typically, Juniper characterizes them as drive-by-downloads or droppers as such Downloadables are usually programmed to take advantage of a browser, application, or OS that is out of date and has a security flaw. The initial downloaded code is often small enough that it wouldn't be noticed, since its job is often simply to contact another computer where it can pull down the rest of the code on to the computer. In particular, such software components are usually programmed to be downloaded and run in the background in a manner that is invisible to the user - and without the user taking any conscious actions as just the act of viewing a web-page that harbors this malicious code is typically enough for the download and execution to occur. ATP Appliance includes a communications engine (e.g., network interface and corresponding proxy software) to obtain Downloadables for scanning. ATP appliance scans Downloadables that may include malware embedded in images, JavaScript, text and Flash files. As shown below, ATP Appliance obtains and conducts analysis on Downloadables such as Executable files (e.g., ".bin, .com, .dat, .exe, .msi, .msm, .mst"), PDF files, Java (e.g., ".class, .ear, .jar, .war"), MS Office file types, Flash and Silverlight applications, Script files, and installer files through an application program interface. The ATP Appliance performs behavioral analysis such as potential dropper infection for Downloadables. Potential dropper infections are references to software components required to be executed by the Downloadable. As shown below, the ATP Appliance uses behavior inspection and dynamic detection to find dropper files and to perform hashing functions on them.

Dynamic Detection™

Machine Learning + Behavioral Inspection = Dynamic Detection™

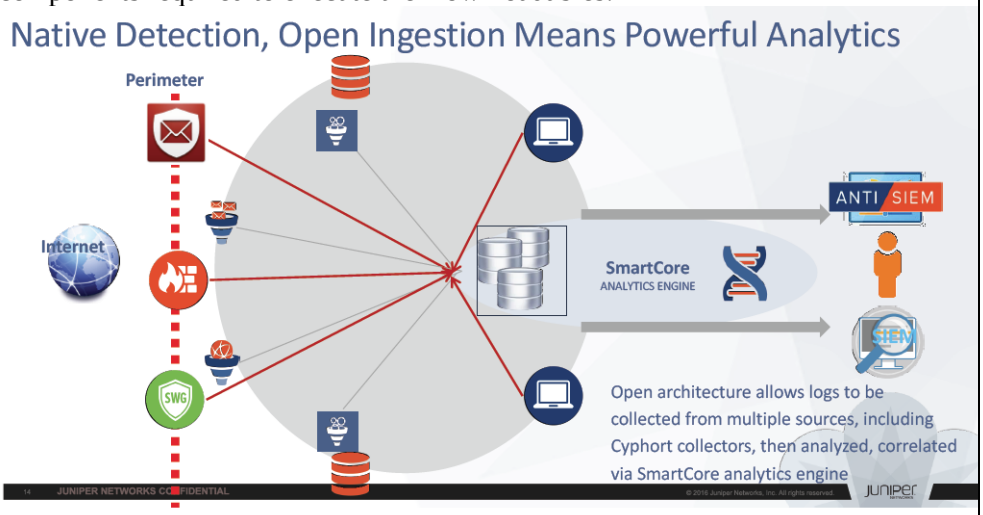
Unlike 1st generation behavioral systems that leverage heuristics based analysis for threat detection, Cyphort's innovative Dynamic Detection™ method utilizes a Machine Learning engine combined with Behaviorial Inspection analytics to adapt to evolving malware and new threat techniques, including evasion tactics.

Defeat evasion with adaptive sandbox array

Cyphort's Array of Sandboxes including virtualization and system emulation combined with a deep understanding of evasion and cloaking techniques allows the detection of evasion by ensuring that malicious code elicits enough behavior to make a determination.

Cyphort Datasheet

As shown below, ATP Appliance will obtain Downloadables, as well as components required to execute the Downloadables.



Redimadrid_Journadas-Sky ATP Enhancements.pdf at page 14.

Single Event

A threat evolves along well-understood phases – reconnaissance, weaponization, delivery, exploitation, malware installation, command and control callback and payload drop, and execution of hostile actions (e.g., exfiltration of digital assets and IP) – as depicted in Figure 5 in the context of a kill chain. A single-event methodology is typically focused only on malware delivery. As previously mentioned, the first few phases of an attack are designed to obtain control of an employee's device and malware delivery may not always occur inside the enterprise's boundaries. In any event, most advanced single-event solutions are focused only on detecting the exploit and are therefore ineffective against all attack vectors at all attack stages.

Cyphort WP Security 2.0

DOCKET ALARM

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.