FireEye™

Comprehensive Proposal

The FireEye Malware Protection System

2012

The Only U.S. Federal Government-Certified Solution That Delivers Real-Time Analysis and Blocking of Next-Generation Threats

Contents

Executive Summary

Federal government agencies are constantly besieged by advanced malware, zero-day exploits, and targeted advanced persistent threat (APT) attacks—and their existing IT security defenses are failing to guard against these threats.

The cyber threat landscape has changed radically over the last few years. All federal government agencies that are responsible for defending our critical infrastructure are now under constant attack from APTs. Today, cybercriminals are utilizing advanced polymorphic malware and targeted attacks over the Web and email to routinely bypass traditional perimeter security defenses. With increasing regularity, nation-states and cybercriminals are compromising federal agencies' networks and exfiltrating sensitive and classified data.

To mitigate these threats, it is imperative that these advanced attacks are detected and stopped immediately. Traditional signature-based solutions like intrusion prevention systems (IPS), anti-virus (AV), and secure gateways can only identify known threats—but are unable to identify and stop today's zero-day, dynamic malware as well as spear phishing and APTs. Federal agencies now require new technologies that can detect and stop these advanced threats in real time.

The continued perpetration of these attacks presents federal government agencies with an immediate and urgent mandate: security teams have to respond with more advanced, sophisticated defenses. Failure to do so means that sensitive data could be exfiltrated at any time.

"In the not too distant future, we anticipate that the cyber threat will pose the Number 1 threat to our country."

—Robert Mueller, Director of the United States Federal Bureau of Investigation

Why is the Advanced Cyber Threat Problem so Difficult to Solve?

The multi-vector, multi-stage nature of today's APT attacks

APT attacks often use multiple attack vectors to maximize the success of circumventing existing defenses. These advanced attacks are often delivered through legitimate (though compromised) Web sites and spear phishing emails. They can be blended (for example, email-based attacks that contain malicious URLs), and they can use application and OS exploits to maximize the breadth of attacks.

Further, these attacks typically include several distinct, yet coordinated stages. Following is an overview of each:

1. **System exploitation.** Leveraging zero-day exploits or sophisticated, targeted spear phishing tactics, and sometimes both, APT attacks can effectively compromise specific systems, which is the critical first step of the advanced threat.
2. **Malware download and control established.** Once a system has been exploited, the attacker downloads a malicious executable, such as a key logger, Trojan backdoor, password cracker, or file grabber. Just one initial exploit can translate into dozens of infections on the same system. At this point, the criminals have established long-term control over the system. Malware can implement disguises in order to avoid detection during scans. Some will turn off AV scanners, patch the OS to prevent other infections, reinstall missing malware components after a partial cleaning, or lie dormant for days or weeks.
3. **Callback channels opened.** Once the malware is installed, cybercriminals can establish a control point behind your defenses. The malware calls out to criminals' servers for further instructions. By using callbacks that originate from within the trusted network, malware communications are allowed through the firewall and various network defenses.
4. **Data exfiltration.** Next, data acquired from infected servers is staged for exfiltration. Data can be exfiltrated over any of a number of commonly allowed protocol, such as FTP or HTTP. During this process, criminals may use encryption to disguise the assets being transmitted, and send data to another compromised machine outside the targeted organization, for example at a hosting provider, to further disguise their identities and whereabouts making attribution very difficult.
5. **Lateral movement.** During this phase, the criminals work to move beyond the system initially exploited, and begin to move laterally within the target organization, accessing additional systems and gaining elevated access to important user, service, and administrative accounts. To do so, they may leverage automated, self-replicating malware to infect multiple network assets.

FireEye Solution Overview: Next-Generation Threat Protection

Proactive, real-time, and multi-vector protection

FireEye is one of the fastest growing companies in the technology sector, and is the only company in the world today that can deliver a next-generation threat protection platform for guarding against the most advanced attacks being waged today.

FireEye provides the only multi-vector solution that can effectively detect, analyze, and protect against unknown malware and targeted APT attacks, whether they come through the Web, email, file, or blended attack vectors. Only FireEye provides the automated, multi-stage advanced protection needed to address all stages of the attack lifecycle. FireEye spots attacks by recording the initial exploit, analyzing the malware binary, and stopping outbound callbacks to criminal servers.

FireEye products include network appliances called the FireEye Malware Protection System™ (MPS), a Central Management System™ (CMS), and a Malware Analysis System™ (MAS), which enables threat analysts to deeply inspect advanced malware. FireEye also provides a Malware Protection Cloud™ (MPC) service so agencies can take advantage of FireEye's global knowledge base of the latest advanced malware and apply this knowledge for the most efficient, real-time detection and protection against profiled threats.

The FireEye MPS portfolio of products includes the FireEye Web MPS™, the FireEye Email MPS™, and the FireEye File MPS™. Each of these products protects a key attack vector using its built-in, signature-less Virtual Execution (VX) engine™. In addition, they can be combined to offer end-to-end protection as a fully integrated and interoperable system against advanced attacks that blend attack vectors. FireEye MPS appliances can be centrally managed, and share dynamically generated malware intelligence through the global FireEye MPC. All of the FireEye products utilize the FireEye VX engine for real-time malware analysis. They also leverage a callback filter for analyzing and blocking malicious outbound callback traffic.

Gain protection across Web, email, and file attack vectors

With the FireEye MPS, organizations get an integrated, real-time correlated view of all the potential threat vectors that attackers may use, including:

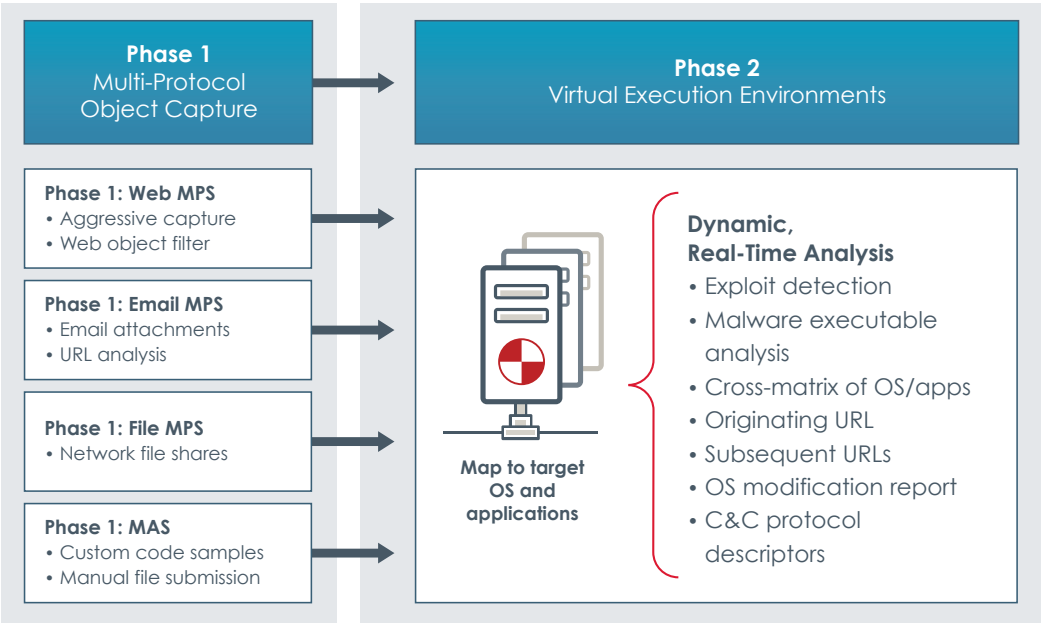
- **Email.** Spear phishing emails represent one of the most common approaches for launching an APT attack on federal agencies. The FireEye Email MPS can block these types of threats, providing real-time analysis of URLs in emails, email attachments, and Web objects to determine whether or not they are malicious.
- **Web.** Browser-based threats and malicious communications can take many forms and move across a range of protocols, including FTP, HTTP, and IRC. The FireEye Web MPS tracks sites and communications in real-time across these different protocols to thwart APT attacks.
- **Files.** Malicious files are used to target application vulnerabilities and can be introduced into a network in any number of ways, whether through a USB drive, mobile device, download from a cloud service, or a host of other means. In addition, these malicious files can be purposely or inadvertently saved to any number of locations throughout an organization, and then lie dormant for a certain period of time before they exhibit their malware behavior. The FireEye File MPS continuously scans and eliminates malware resident on file shares.

The FireEye CMS correlates all of this malware intelligence and shares it across the FireEye deployment. For example, to guard against sophisticated spear phishing attacks, security teams need capabilities for discovering a Web-based attack in real-time, tracing the initial email that lured the user into the attack, and then easily closing the loop to determine if others within the organization have been targeted. By providing this kind of end-to-end protection, the FireEye CMS can deliver timely, actionable information about current threats, and how they can be stopped across the entire organization.

FireEye signature-less, virtual execution technology

FireEye has pioneered the use of virtualization to provide real-time, dynamic protection against advanced malware, zero-day exploits, and targeted APT attacks. Remotely controlled malware is frequently used for exfiltration of data from compromised client machines, sometimes called botnets. The FireEye VX engine uses patented technologies that combine heuristic analyses with deep packet inspection within instrumented virtual machines (see figure). Following is an overview of key capabilities:

The FireEye MPS: Phase 1 and 2 Analysis

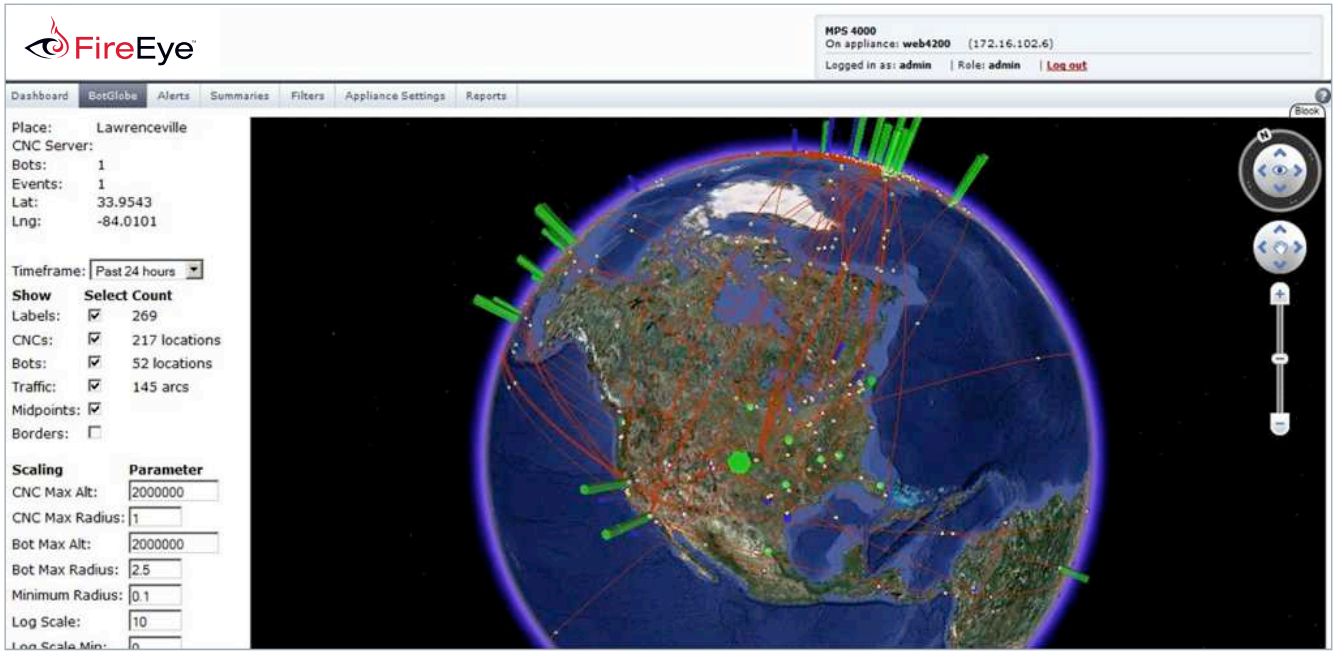


- Phase one is a set of capture heuristics used to identify suspicious network activities. Aggressive heuristics are used to ensure that all potential attacks are identified, thus eliminating false negatives. Output from phase one flows into phase two, the confirmation stage.
- In phase two, network traffic flows are replayed in the proprietary VX engine environment, which validates whether the code is indeed malicious. This environment has instrumented virtual machines to confirm whether or not suspicious code actually infects the system, while also eliminating false positives.
- Aggressive heuristic policies are in place to flag even mildly suspicious network traffic with the understanding that the subsequent VM malware analysis stage would confirm the actual attack traffic and eliminate any false positives.
- This multi-stage analysis enables the programmatic capture, fingerprinting, and blocking of zero-day malware and its unauthorized outbound callbacks to criminal command and control servers—all within seconds.
- Should a customer wish to participate, these callback channels can be shared with the MPC network on an hourly basis. In the MPC network, callback channels are submitted into the network as open signatures, so that other customers can detect callbacks that exhibit the same characteristics in their organizations.

The Web browser is the predominant attack vector used by adversaries as reported in studies by IBM X-Force and ENISA. Consequently, it is now a key requirement to detect and stop Web-based attacks that are disguised through fragmentation or obfuscation techniques. Beyond simple software code emulation, FireEye analyzes threats against the full range of permutations of operating systems, browsers, and plug-in versions to confirm zero-day, unknown malware. The underlying FireEye virtual execution environment that performs the analysis in stage two is configured with the full suite of today's common browsers and plug-ins, such as Internet Explorer, Firefox, Adobe Reader, Adobe Flash Player, Apple QuickTime, Microsoft Office renderers, and RealPlayer.

To assist analysts, these virtual machines are instrumented to provide detailed forensic profiles of identified malware. The forensic data automatically generated includes information about the malware, such as file creation/deletion, registry manipulations, processes that are starting or stopping, memory modifications, MUTEX creation or deletion, PCAP recordings of inbound attacks and outbound callbacks, user or kernel space driver changes, and other alterations that were made to the underlying virtual machine by the malware. Metadata is also provided to the analysts in the form of IP address, ports, VLAN (for multi VLAN interface environments), timestamps, etc. These VMs are then reset back to a pristine state to analyze more user traffic.

Global View of Callback Channels



Why Federal Agencies are Deploying FireEye

Why are so many federal agencies relying on FireEye solutions? FireEye solutions provide the following capabilities:

- Detect and stop Web- and email-based attacks that exploit zero-day vulnerabilities—when they first appear on the network.
- Expose the entire cyber attack lifecycle by correlating intelligence across various threat vectors and callback channels.
- Produce complete cyber forensic details of attacks that exploit Web, email, file, or blended attack vectors.
- Provide a new layer of cyber threat protection that utilizes dynamic, signature-less analysis and yields near- zero false positives.
- Speed the detection of malicious activity and client infections from months and weeks to minutes, providing incident responders with instantaneous event notification.
- Provide continuous monitoring of all incoming Web and email traffic for targeted or non-targeted malware, along with correlating outbound multi-protocol callback traffic.

The bottom line is that with the FireEye MPS, federal agencies get the advanced defense capabilities they need to guard against new sophisticated APT attacks.

Integrated, multi-threat vector and multi-stage protection against advanced attacks

Meeting Federal Cyber Mandates Using the FireEye MPS

FireEye is used by more than 60 U.S. federal government agencies to support continuous monitoring of FISMA security controls. The FireEye signature-less VX engine enables agencies to continuously monitor Web and email vectors for advanced malware, including zero-day exploits and targeted APT attacks. By providing security professionals with rich data on unknown threats, FireEye complements existing signature-based security technologies, such as firewalls, next-generation firewalls, IPS, and AV.

FireEye natively supports FISMA continuous monitoring by providing visibility and protection of data exfiltration through advanced malware—whether it resides physically, virtually, or within a cloud environment. FireEye aligns agency security operations with FISMA NIST 800-53 controls.

FireEye currently addresses the following NIST 800-53 incident response components:

- IR-4: Incident Response—Information Correlation Between Web and Email Attack Vectors
- IR-5: Incident Monitoring
- IR-6: Incident Reporting
- IR-7: Incident Response Assistance

Appendix: Federal Agency Threat Assessment Report

To assess the value of the FireEye MPS, a U.S. federal government agency engaged FireEye for an evaluation. The agency's security team was interested in verifying whether their existing defenses were effectively guarding against ongoing attacks and identifying whether advanced malware resided within their network. FireEye sales and technical teams undertook a 60-day assessment, installing and configuring the FireEye MPS solution on the agency's premises and tracking the details the solution uncovered. In the following sections, we provide a summary of our findings.

Summary of results

During a 60-day customer evaluation, FireEye found hosts infected by 34 distinct variants of malware. It is evident that in some cases hosts were infected by multiple pieces of malware. As a result, malware variants attempted communication to distinct command and control servers spread all over the world. These command and control servers can be used by their controller to perform a large variety of malicious activity, including a distributed attack against specific targets, data harvesting for identity theft, data exfiltration, or espionage. Following is a breakdown of the malware identified:

- 172 malware object downloads including EXE, ZIP, and DLL files
- 126 browser exploits downloaded
- 64 preventable exploit access attempts
- 13 out of 28 DNS lookups were related to known APT activity
- 103 preventable malware callbacks

Technical analysis

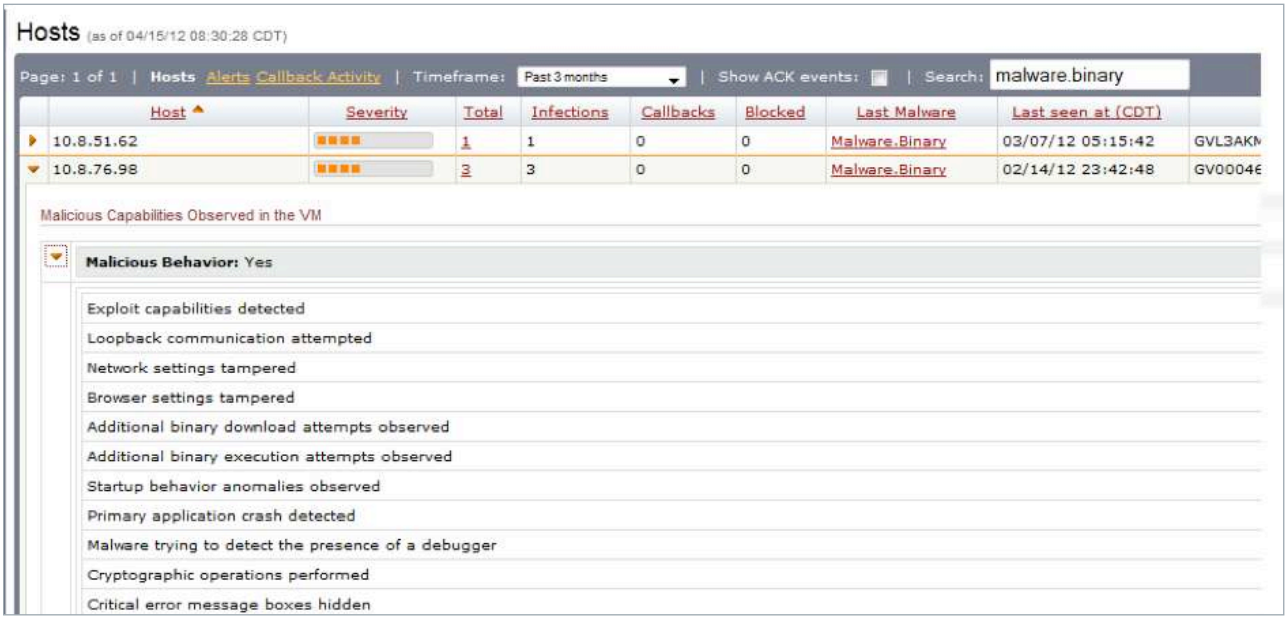
Nation-state advanced persistent threat (APT) confirmed

The presence of an APT was identified on the agency's network and was the most critical of all results discovered through the FireEye evaluation. The APT indicators identified included 13 out of the 28 DNS lookups seen during the evaluation. These DNS lookups are related to known nation-state APT activity. Certain hosts on the agency's network were attempting to locate command and control servers known to have participated in the RSA "Poison Ivy" breach. This command-and-control infrastructure has been associated with the Chinese PLA group known as "Ugly Gorilla". These indicators likely point to a past breach of the agency's networks by one of the most advanced hacking organizations in the world today.

In addition, many other unique malware variants found by the FireEye MPS had characteristics of an APT. FireEye found evidence of data-theft malware with rootkit and backdoor elements. This type of malware is notorious for creating subsequent, multi-faceted infections that are hard to remove and it will typically move laterally in the enterprise. Nation-state and organized crimeware groups typically utilize polymorphism to stay ahead of signature-based security solutions, and subsequently exfiltrate personal credentials and sensitive data.

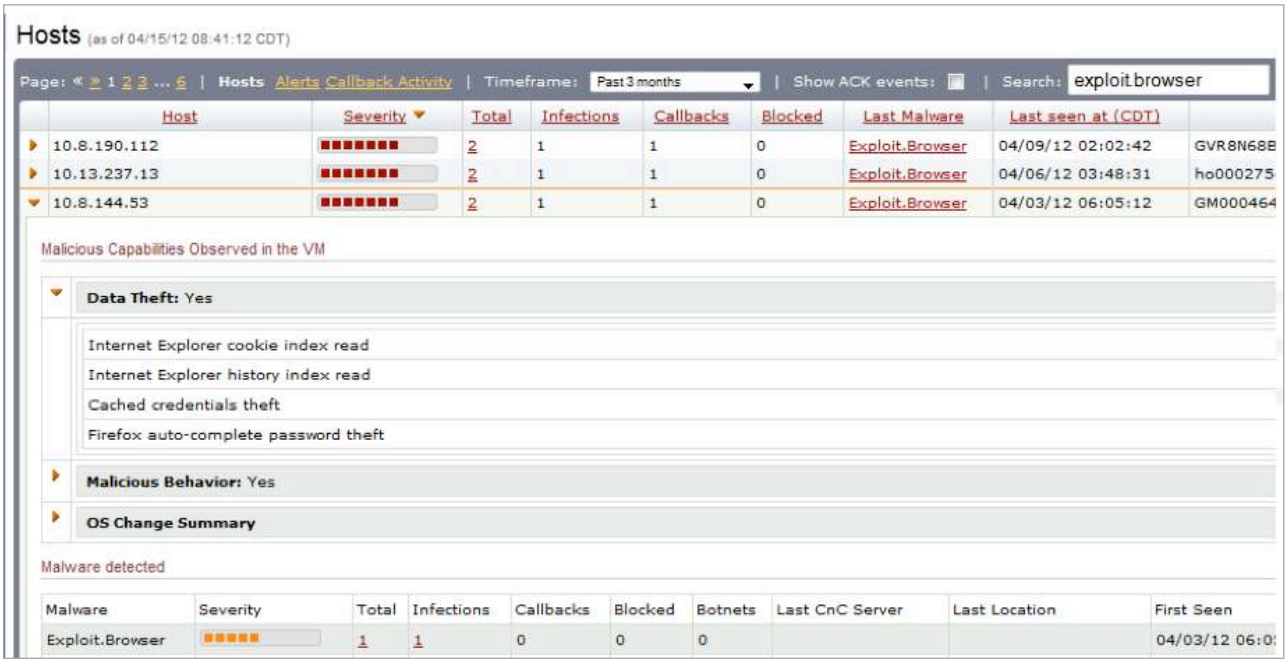
Malware object analysis

During the FireEye MPS federal agency evaluation, 172 malware objects were collected. A malware object file is essentially an executable, archive, or dynamic-link library file that can be used to harbor malicious software. Malicious binaries will typically come in the form of an .exe or obfuscated PDF file. The "malware binary" variants listed below outline the scope of detail and efficacy that is provided by the FireEye MPS and its reporting engine.



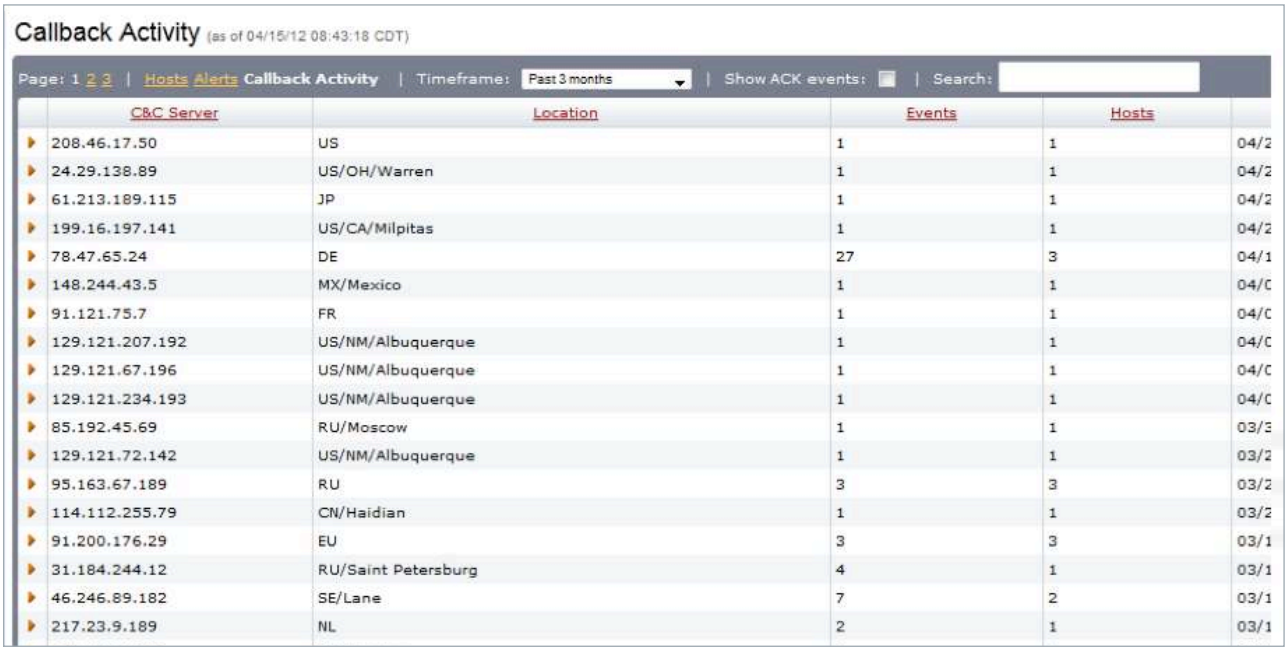
Browser exploit analysis

The FireEye MPS replays all anomalous customer network traffic through the VX engine to execute suspected malware objects in virtual execution environments. 126 browser exploits were detected during the evaluation. The exploit browser events listed below outline the scope of detail and efficacy that is provided by the FireEye MPS.



Callback analysis

The FireEye MPS recorded a significant amount of callback communication events originating from the customer network and sent to 48 distinct locations around the globe. In addition to servers in the United States, callbacks were seen communicating to a number of countries, including Russia, China, Japan, The Netherlands, France, Mexico, Romania, Germany, Latvia, Czech Republic, and Brazil.



Callback Activity (as of 04/15/12 08:43:18 CDT)

Page: 1 2 3 | Hosts Alerts Callback Activity | Timeframe: Past 3 months | Show ACK events: | Search:

C&C Server	Location	Events	Hosts	
208.46.17.50	US	1	1	04/2
24.29.138.89	US/OH/Warren	1	1	04/2
61.213.189.115	JP	1	1	04/2
199.16.197.141	US/CA/Milpitas	1	1	04/2
78.47.65.24	DE	27	3	04/1
148.244.43.5	MX/Mexico	1	1	04/0
91.121.75.7	FR	1	1	04/0
129.121.207.192	US/NM/Albuquerque	1	1	04/0
129.121.67.196	US/NM/Albuquerque	1	1	04/0
129.121.234.193	US/NM/Albuquerque	1	1	04/0
85.192.45.69	RU/Moscow	1	1	03/3
129.121.72.142	US/NM/Albuquerque	1	1	03/2
95.163.67.189	RU	3	3	03/2
114.112.255.79	CN/Haidian	1	1	03/2
91.200.176.29	EU	3	3	03/1
31.184.244.12	RU/Saint Petersburg	4	1	03/1
46.246.89.182	SE/Lane	7	2	03/1
217.23.9.189	NL	2	1	03/1

Determining How Valuable FireEye Can Be To Your Organization

Case study

Architecture: 6 primary Internet egress points (two in the U.S., one in South America, one in EMEA, and two in APAC).

Security Controls: Palo Alto FWs, McAfee AV, TippingPoint IPS, Blue Coat Web proxy, Splunk log correlation/SIEM

[NOTE: TRANSCRIPT TAKEN FROM ACTUAL CUSTOMER-CREATED DOCUMENT FOR INTERNAL BUSINESS COST JUSTIFICATION PURPOSES]

Evaluation deployment overview

- The original working assumption by the agency was that there would be little to no malware in the environment.
- An evaluation was conducted over 60 days in which the FireEye MPS appliance was placed out-of-band at the edge firewall to monitor traffic entering and leaving the network.
- The FireEye appliance was deployed behind other layers of security to focus on malware, zero-day, and targeted APT attacks that bypassed firewalls, IPS, AV, and Web gateways.

Evaluation results

- On day one, unauthorized malware callback communications were discovered that were connecting to multiple command-and-control servers around the world.
- In week one, the FireEye MPS detected malware activity from 11 different hosts that bypassed other layers of defenses.
- After 60 days, malware activity alerts averaged **13 per day**.

Evaluation post-mortem

- The majority of the reported malware issues were with systems in which McAfee AV was installed and updated, but was unable to prevent the infection. The FireEye appliance was able to catch the issue on these systems and likely would have been able to block the initial infection and subsequent command-and-control connections.
- Before FireEye, service desk technicians spent an estimated total of eight days working on the 32 recorded issues over a period of roughly two months.
- Over the 60 day period, FireEye provided 99% accuracy with only one alert that turned out to be a false positive. It was on a high-value system where FireEye took the extra precaution of investigating even though we weren't seeing command-and-control callbacks after the initial infection. Otherwise, every callback event found by FireEye was real.

Customer Purchase: Selected FireEye MPS for global deployment utilizing seven FireEye MPS appliances (one 7300, two 2310s, and three 1310s) and CMS.

"FireEye's return on investment was proven within the 1st hour of connecting the system."

—Director of IT Security at U.S. Federal Government Agency

Conclusion/Next Steps

Learn more about why security-conscious organizations choose FireEye for industry-leading protection against advanced targeted attacks that cut across multiple threat vectors and use multiple stages to systematically bypass traditional defenses. The FireEye MPS supplements traditional and next-generation firewalls, IPS, AV, and gateways whose signatures and heuristics cannot stop this next generation of threats. By combining signature and signature-less detection, and integrating Web, email, and file protection, FireEye stops today's advanced targeted attacks with near-zero false positive rates.

FireEye products range in performance from 10 Mbps to 1 Gbps. All FireEye customers have been able to deploy our next-generation threat protection systems quickly and at very competitive rates. Specific pricing depends on the actual number and size of the systems deployed. FireEye will provide pricing information based upon the configuration your network requires.

Every one of our U.S. federal government customers conducted a free FireEye Security Assessment and found that the cost to purchase, deploy, and manage the FireEye system is dramatically more attractive than the cost of the malware events, data loss, incident responses, remediation, lost productivity, and potential media exposure.

The FireEye Security Assessment is an easy decision:

- There is no cost nor obligation
- FireEye products are extremely easy to install
- Cyber events already in your network will be illuminated
- A total of eight man-hours, on average, is needed for the assessment

Call FireEye, schedule a briefing, conduct a Security Assessment, and start seeing the cyber attacks to which you are blind to today.

Contact Information for Evaluation and Sales:

Dan Brigati
Director of Federal Sales
+1 (703) 462-5450 Work
+1 (703) 370-4056 Mobile
Dan.Brigati@FireEye.com

About FireEye, Inc.

FireEye, Inc. is the leader in stopping advanced cyber attacks that use advanced malware, zero-day exploits, and APT tactics. FireEye solutions supplement traditional and next-generation firewalls, IPS, anti-virus and gateways, which cannot stop advanced threats, leaving security holes in networks. FireEye offers the industry's only solution that detects and blocks attacks across Web and email threat vectors as well as malware resident on file shares. It addresses all stages of an attack lifecycle with a signature-less engine utilizing stateful attack analysis to detect zero-day threats. Based in Milpitas, California, FireEye is backed by premier financial partners including Sequoia Capital, Norwest Venture Partners and Juniper Networks.