FEDERAL SUMMARY

*"Protecting [our digital] infrastructure will be a national security priority. We will ensure that these networks are secure, trustworthy and resilient. We will deter, prevent, detect, and defend against attacks…"*

– President Barack Obama's Remarks on Securing Our Nation's Cyber Infrastructure

# FIGHTING CYBER TERRORISM REQUIRES DYNAMIC MALWARE PROTECTION

Yesterday's security solutions do not protect your agency from today's Modern Malware. Today, cyber terrorists are routinely bypassing conventional perimeter security solutions.

## Sophisticated Malware Is The Top Cyber Threat To Federal Agencies

Organized groups of attackers are able to extract sensitive and mission critical data through the use of targeted malware, commonly called "botnets". The most sophisticated attacks are targeting the US Federal Government and are having great success exploiting unknown, zero-day vulnerabilities.

## Protecting Critical Infrastructure and Information Demands A Better Solution

Given the magnitude of targeted malware attacks, and the success that customized malware achieves bypassing pattern matching technologies, it is imperative that Federal Security professionals identify whether or not their network has been compromised. If these targeted attacks go undetected and unblocked, a data breach is essentially inevitable.

The FireEye MPS blocks Modern Malware, which has no discernible pattern and is predicated upon using a zero-day exploit. The FireEye MPS breaks the malware infection lifecycle stopping zero-day (customized) attacks and the outbound callbacks used to exfiltrate sensitive data.

## FIREEYE'S UNIQUE APPROACH

- Patent-pending, integrated Malware-VM™ and Malware-Callback™ filters to block known targeted attacks, detect zero-day malware, and stop malware transmissions that exfiltrate sensitive data
- Up to 76% of modern malware goes undetected on a compromised end-user system*
- FireEye blocks the 90% of Modern Malware attacks that conventional defenses miss
- Near-zero false positive rates ensures your IT team can focus their response efforts on real attacks
- The FireEye MAX Cloud Intelligence network gives subscribers real-time intelligence on malware threats (collected through the global MPS network)
- The FireEye system is the only solution that passes suspicious code through a "virtual victim machine", executes it, and determines conclusively if the code is malicious. It offers an extremely accurate method for detecting known and zero-day malware so that customers can shut the backdoors into their network (aka infected PCs.)

* Mandiant, *Advanced Persistent Threat Report*, 2010

FREE SECURITY AUDIT AND ANALYSIS
FireEye is offering a free Modern Malware security analysis of the network. This is a limited time offer, so contact us today!

+1 (877) FIREEYE (347.3393)
+1 (703) 956.3017
info@fireeye.com

## Conventional intrusion detection systems are not able to detect & block these targeted exploits reliably

Attackers target browser and Web 2.0 vulnerabilities to bypass IDS/IPS. Why? Most IDS technologies use pattern matching for detecting exploits (aka signatures, which require prior knowledge of attack characteristics) and some employ heuristics (a statistical analysis applied to network traffic, which is not an accurate nor precise technique to pinpoint today's targeted attacks).

Both methods are fundamentally blind to the threat of custom, never before seen Modern Malware. Specifically, signature-based systems cannot react in time to zero-day exploits leading to an increasing false negative (missed attack) problem. Layering in heuristics is an attempt to compensate but leads to false positives since heuristics require baselining of historical traffic trends as well as tuning overhead by network security & IT operations staff.

## 0-day Malware Protection at Near-zero False Positives

FireEye achieves near-zero false positives wit its multi-phase malware analysis engine that identifies targeted, zero-day attacks. Known and zero-day attacks (as well as its outbound callbacks) are blocked preventing data theft, alteration, and destruction.

In addition to blocking known attacks, FireEye stops zero-day attacks using a malware inspection engine that features advanced capture heuristics coupled with virtual machine technology to confirm if the suspicious traffic infects the virtual machine. The engine is a cyber Petri dish to confirm the presence of malware. Zero-day malware inside the virtual machine is then analyzed to create a full malware profile including dynamic signatures, callback destinations across protocols, and malware commands issued.

## Global Network to Share Local Malware Intelligence

Customers share and add to their local malware intelligence by tying into the Malware Analysis and Exchange (MAX) Network. Auto-generated security intelligence is distributed to subscribers worldwide to stop global attacks targeted at their local network.

## Security Without Operational Trade-offs

With FireEye, IT administrators have a clientless solution that deploys in 30 minutes and requires absolutely no tuning. It deploys in several modes, including out-of-band monitoring via a SPAN port, inline monitoring, or inline active blocking to stop attacks and outbound transmissions.

## Integrated Security To Stop Malicious Data Theft

FireEye accurately protects systems against inbound infection and stops unauthorized data transmissions to criminal servers. This integrated approach enables the most comprehensive threat protection against modern threats that attack across multiple vectors. FireEye's unique multi-phase inspection engine pinpoints zero-day, targeted attacks that continue to bypass conventional security. With FireEye, it is possible to stop the proliferation of cybercrime, cyber espionage, and cyber reconnaissance attacks.

## KEY TECHNOLOGY DIFFERENTIATORS

- Accurate inbound attack detection using a multi-phase malware inspection engine
- Outbound filtering of malware transmissions to prevent data theft
- Global network to share malware intelligence and callback destinations
- Only solution to stop network- and application-based exploits in content, such as HTML, PDF, and Flash

## KEY BUSINESS DIFFERENTIATORS

- Prevents data, identity, and resource theft due to targeted malware
- Stops targeted attacks like Aurora, bots, and Trojans that IPS & antivirus miss
- Protects against zero-day inbound malware at near-zero false positive rates
- Real-time intelligence network to prevent global threats against the local network

FireEye®

FireEye, Inc.
1390 McCarthy Blvd
Milpitas, CA 95035

+1 (877) FIREEYE (347.3393)
info@fireeye.com

www.FireEye.com