

Malware Analysis System

Next generation forensic analysis of advanced malware, zero-day and targeted APT attacks

The FireEye Malware Analysis System gives threat analysts hands-on control over a powerful auto-configured test environment where they can deeply inspect advanced malware, zero-day and targeted APT attacks embedded in common file formats, email attachments and Web objects.

As criminals tailor attacks to penetrate a specific business, user account or system, analysts need easier-to-use forensic tools that can help them test, replay, characterize and document very customized malicious activities. The FireEye Malware Analysis System (MAS) analyzes advanced malware, zero-day and targeted APT attacks that aggressively evade signature-based defenses and compromise a majority of corporate networks.

Assess OS, Browser and Application Attacks

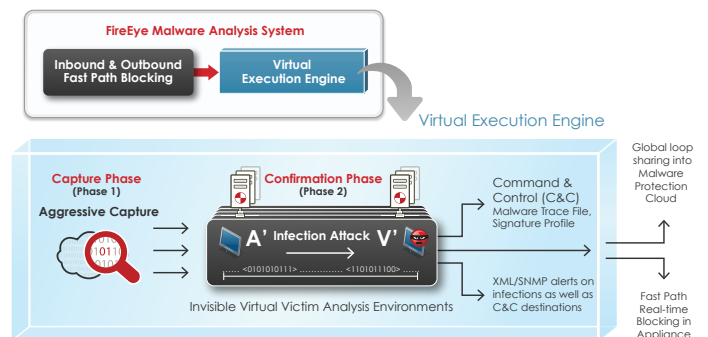
FireEye empowers in-house analysts with a full 360-degree view of an attack, from the initial exploit and malware execution path to callback destinations and follow-on malware download attempts. Through a pre-configured, instrumented Windows virtual execution engine, the FireEye system fully executes suspicious code to allow deep inspection of the advanced attacks embedded in common file formats, email attachments and Web objects. FireEye inspects single files or batches of files for malware and tracks outbound connection attempts across multiple protocols. It provides not only a confirmation of malware, but also a full understanding of the intent of the malicious software.

Spend Time Analyzing, not Administering

The FireEye Virtual Execution (VX) engine features virtualized PC hardware running full-fledged versions of Microsoft operating systems as well as browsers, plug-ins and other third-party applications. With the convenience of a true appliance, these systems free administrators from time-consuming setup, baselining and restoration of the virtual machine environments used in manual malware analysis.

Highlights

- Streamlines and batches analysis of suspicious files, Web code and executables
- Reports in-depth on system-level OS and application changes to file systems, memory and registries
- Offers sandbox or live-mode analysis to confirm zero-day exploits
- Shows the intent of malware with details on the attack, system changes and outbound transmissions
- Eliminates deployment headaches and tuning with a pre-configured environment, plus automated setup and teardown of virtual test images
- Dynamically generates malware intelligence for immediate local protection
- Captures packets to allow analysis of malicious URL session and code execution



Inside the FireEye Virtual Execution Engine

“One of the big attractions of the FireEye solution is that analysis is performed in a virtual execution environment to determine if a flagged piece of code actually is a threat. The detailed information that is generated allows us to pinpoint the optimal option for resolving an issue. It puts us in the position of knowing exactly how to react.”

— Director of Cyber Security, Energy Sector

Choose Sandbox or Honeypot Analysis Modes

FireEye offers both a sandbox mode and live, on-network “honeypot” mode for malware analysis. In sandbox mode, researchers can witness the execution path of particular malware samples. When the MAS confirms malicious software, it generates a dynamic and anonymized profile of the attack and can distribute it through the Central Management System to other FireEye Web and Email Malware Protection System appliances. The threat intelligence dynamically generated includes:

- Malware attack profiles, including identifiers of malware code, exploit URLs and other sources of inbound infections and attacks
- Fully qualified malware callback destinations (Destination IP address, protocols used, ports used) that identify malicious websites and email sources
- Malware communication protocol characteristics, such as custom commands used to instantiate transmission sessions

In addition to offline analysis in a secure, encapsulated sandbox, FireEye offers a live, on-network “honeypot” mode for full malware lifecycle analysis. Today’s stealth malware has circumvented conventional security technologies by unfolding in multiple stages. The first vulnerability exploit stage simply establishes a beachhead for criminals to fully own the endpoint.

FireEye integrates inbound and outbound inspections across multiple protocols for comprehensive threat analysis of OS, Web-based, email and application threats that attack across multiple vectors. For example, after confirming a heap spray exploit used to facilitate arbitrary code execution, the honeypot-mode MAS would connect outbound and download additional malware. The heap spray, memory locations corrupted and other malware forensics are catalogued, as are malware outbound destinations, for use by researchers and analysts.

Global Malware Protection Network

Customers using the FireEye Web or Email Malware Protection Systems can automatically load malware forensics data into their appliances via the FireEye Central Management System to block outbound data exfiltration attempts and stop inbound known attacks. Analysts can also share this data with the FireEye Malware Protection Cloud. This Internet cyber crime watch system provides subscribers the latest intelligence on inbound attacks and unauthorized outbound callback destinations in real time.

With pre-configured virtual execution engines eliminating the need for tuning heuristics, the FireEye Malware Analysis System saves administrators setup time and configuration headaches. This is an easy-to-manage, cost effective solution that helps threat researchers analyze next generation threats without adding network and security management overhead.

Technical Specifications		
	FireEye MAS 4310	FireEye MAS 7300
Form Factor	1U Rack-Mount	1U Rack-Mount
Weight	30lbs (13.6kg)	30lbs (13.6kg)
Dimensions	17.2" x 25.6" x 1.7" (43.7 x 65.0 x 4.3 cm)	17.2" x 25.6" x 1.7" (43.7 x 65.0 x 4.3 cm)
Enclosure	Fits 19-Inch Rack	Fits 19-Inch Rack
Monitoring Interfaces	(4)10/100/1000 BASE-T Ports	(4)10/100/1000 BASE-T Ports
Management Interfaces	(2)10/100/1000 BASE-T Ports	(2)10/100/1000 BASE-T Ports
Performance Rating	Up to 250 Mbps	Up to 1 Gbps
AC Input Voltage	100 ~ 240 VAC Full Range	100 ~ 240 VAC Full Range
AC Input Current	8.5 - 6 A	8.5 - 6 A
Power Supply/RAID	Dual / 2 SAS HDD in HW RAID1	Dual / 2 SAS HDD in HW RAID1
Frequency	50-60Hz	50-60Hz
AC Power	700 W Max	700 W Max
Ambient Temp	40 °C	40 °C

© 2011 FireEye, Incorporated. All rights reserved. FireEye and the FireEye logo are trademarks or registered trademarks of FireEye, Inc. in the United States and/or other countries. All other brands, products or service names are or may be trademarks or service marks of their respective owners. DS.MAS.122011