DATASHEET

FireEye 4200

Web Malware & Botnet Security System

KEY FEATURES & BENEFITS

- Stops data loss and intellectual property thefts
- Real-time detection of zero-day Web malware & botnets
- In-bound attack security & out-bound call-back protection
- Near-zero false positives using virtual machine analysis
- Deploys out-of-band; Web & CLI management

FireEye offers a blended defense against zero-day Web malware and botnets, preventing data loss and intellectual property theft. There has been a rapid rise in Web-based malware that uses techniques like malicious, obfuscated JavaScript code to exploit client browsers and operating systems. FireEye security appliances detect blended-attack Web malware and botnets by using the best of network-based signature, heuristic, and virtual victim machine analyses.

FireEye Appliances:

1) **Identify** potentially malicious inbound & outbound traffic using signatures & behavioral heuristics
2) **Confirm** the attack & eliminate false positives using virtual 'victim' machine analysis
3) **Fingerprint** the attack and record unauthorized outbound destinations
4) **Share** intelligence to the FireEye MAX Network

The Web is the Primary Infection Vector

Criminals now aggressively use the Web to deliver malicious code (malware) and infect PCs. A European Union study indicated that the Web is utilized 65% of the time to deliver malware. Using a variety of techniques from social engineering to code obfuscation, criminals infect PCs that visit infectious Web sites, blogs, or simply load a malicious JPG, which exploits browser and OS vulnerabilities. Accurately finding today's modern malware is the chief challenge facing IT organizations because it is straightforward for malicious code developers to circumvent traditional detection techniques.

Legacy Security Has Been Bypassed

Traditional security techniques do not accurately detect zero-day modern Web malware. Legacy security technologies rely on detection techniques such as pattern matching (signatures) and anomaly detection (heuristics) that are easily bypassed. As a result, there is a proliferation of remote control malware targeted at enterprises for the purpose of cybercrime. Malware now utilize obfuscation techniques where it is encoded to obscure the text and intent of the code. JavaScript, for example, can be restructured or hidden making it nearly impossible to detect via traditional means. Obfuscated Web code and exploits easily bypass technologies such as intrusion prevention systems (IPSs) and URL filtering.

Detecting Stealth Malware Without False Positives

FireEye security appliances increase network security and restore IT control over the network by uncovering zero-day Web malware and data-stealing outbound malware communications. Stealth malware is created by criminal enterprises seeking to exploit your resources, valuable data, and intellectual property. Modern malware disrupts client security, bypasses network filters, and avoids anomaly detectors to infiltrate your network. FireEye prevents data loss due to modern malware by using its patent-pending FACT engine to identify compromised PCs and to prevent new machines from being taken over.

FireEye Analysis & Control Technology (FACT)

FireEye appliances use a multi-stage analysis engine called the FireEye Analysis and Control Technology, or FACT for short. FACT detects zero-day Web malware and botnets by analyzing real-time Web and network traffic flows. When malware is confirmed within a virtual victim machine, FireEye appliances alert administrators about attack details and repel attacks via integration with existing security enforcement infrastructure.

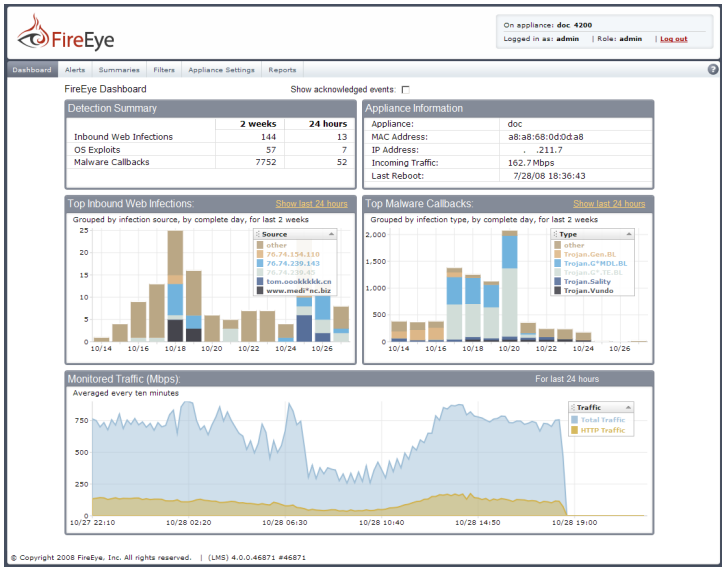
The FACT Engine features:

- Multi-stage detection eliminates false positives
- Virtual victim machine analysis
- Fingerprints malware & outbound call-backs

First, FireEye identifies potentially malicious code using signatures, outbound call-back coordinates, advanced heuristics, and anomaly detection to cast the widest net possible.

Next, FireEye appliances confirm malware and eliminate false positives using virtual victim machines to 'taste test' network traffic.

FireEye virtual victim machines are transparent to attackers, as the appliance is deployed out-of-band while capturing and replaying live network activity in an isolated environment.



IT administrators get an instant view into Web malware infection types and frequency

Virtual victim machines combine virtualization with patent-pending instrumentation to analyze memory, CPU, network interface, and other aspects of control flow within the virtual PC. Parallel virtual victim machines operate to analyze for zero-day Web malware and botnets and run on Microsoft® Windows® operating systems.

Finally, FireEye appliances alert administrators and can optionally share the malware intelligence data gathered via the FireEye Malware Analysis & Exchange (MAX) Network. Members receive zero-day malware signatures, call-back coordinates, and botnet intelligence for more efficient FACT engine performance.

FireEye 4200	
Form Factor	1U Rack-Mount
Weight	32lbs, (16.78kg)
Dimensions	17.25"W x 21.75"D x 1.75"H (43.8 x 55.3 x 4.5 cm)
Enclosure	Fits 19-Inch Rack
Interfaces	(6)10/100/1000 BASE-T Ports
Performance Rating	200 Mbps of Web traffic
AC Input Voltage	100 ~ 240 VAC Full Range
AC Input Current	4.8 - 2.0 A
Frequency	50-60Hz
AC Power	400 W Max
Ambient Temp	40 °C

About FireEye, Inc.

FireEye, Inc. is the leader in anti-malware and anti-botnet protection, enabling organizations to protect critical intellectual property, computing resources, and network infrastructure against Web malware and botnet infiltration. Today's most damaging attacks are perpetrated through Web malware that forms into highly organized botnets, or networks of remotely controlled, compromised machines. FireEye delivers a complete solution that is designed from the ground up to detect and protect organizations from advanced Web malware and botnets through global and local intelligence and analysis. The company is backed by Sequoia Capital, Norwest Venture Partners, JAFCO, SVB Capital, DAG Ventures, and Juniper Networks.

www.fireeye.com

FireEye, Inc.
1390 McCarthy Blvd
Milpitas, CA 95035
+1 (877) FIREEYE (347.3393) info@fireeye.com