The FireEye MAX Cloud is a real-time exchange for malware threat data to maximize preemptive protection against broad and targeted attacks.

FireEye Malware Analysis & Exchange Cloud Intelligence Network

Malware Protection System

The FireEye Malware Analysis & Exchange (MAX) Cloud Intelligence network is a real-time exchange for malware threat data to maximize preemptive protection against a dynamic cyber threat. Within locally deployed FireEye appliances, the Malware-VM™ and Malware-Callback™ filters automatically generates real-time malware intelligence to protect the local network against zero-day malware and advanced persistent threats. The Malware-VM filter fingerprints zero-day malware and captures its callback IP address, communication protocol(s), port(s), and other details. Through the MAX Cloud, subscribers get real-time updates of global threats to their local network.

Global Network to Share Local Malware Intelligence

The FireEye MAX Cloud Intelligence network is formed from interconnected FireEye appliances deployed within customer networks, technology partner networks, and service providers around the world. FireEye has built a worldwide cloud to share and efficiently distribute the auto-generated malware security intelligence, such as its covert callback channels. The MAX Cloud is essentially an Internet cyber crime watch system to provide subscribers the latest intelligence on inbound attacks and unauthorized outbound callback destinations to prevent data exfiltration, alteration, and destruction. Real-time blocking of inbound targeted attacks take place in the local FireEye network appliances. It blocks outbound callback transmissions based on its local callback database and further maximizes the blocking of modern malware infections by subscribing to the global MAX Cloud.

KEY FEATURES & BENEFITS

- Global distribution of modern malware intelligence
- Pull-based data feed on Trojans, bots, and advanced persistent threats
- Prevents modern malware infiltration within the network
- Real-time updates to block malware transmissions and stop data exfiltration

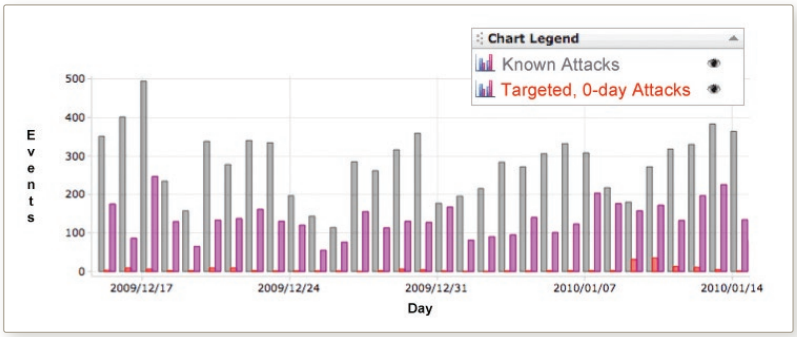
FireEye®

Understanding the Malware Intelligence Service

The global MAX Cloud network is a service providing subscribers with the latest malware intelligence produced by the Malware-VM engine complementing on-premise anti-malware FireEye security appliances. The MAX Cloud provides subscribers:

- Modern malware attack profiles (MD5's of malware code, network behaviors, obfuscation tactics)
- Fully qualified malware callback destinations (IP address, protocol, ports)
- Malware communication protocol characteristics

This maximizes FireEye's ability to accurately block stealth malware that have circumvented conventional security technologies and to stop the proliferation of modern malware targeted at your organization for the purpose of cybercrime, cyber espionage, and cyber reconnaissance.



MAX Network attack graph for a customer site over a one-month period

Disrupting the Modern Malware Lifecycle

FireEye inspects for and filters out malware attacks within inbound traffic as well as malware callbacks within outbound traffic across multiple protocols to identify compromised systems transmitting your data to criminal servers. This integrated approach enables the most comprehensive threat protection against modern malware that attack across multiple vectors to penetrate the network. The initial compromise of a system could be a social engineering attack like a spear-phish email with a URL or malicious PDF. Once the dropper malware is installed, it calls back out to upload stolen data and download further malware payloads. With both inbound and outbound threat protection, FireEye can protect against the entire modern malware lifecycle and goes beyond simple signature matching or rudimentary packet/DNS analysis.

With the MAX Cloud Intelligence network, FireEye security appliances address the operational concerns of IT security by providing additional accurate, real-time malware blocking to help restore IT control over the network while eliminating the headaches associated with false positive analysis. The MAX Network completes the story for an easy-to-manage, cost effective solution that maximizes modern malware protection without adding network and security management overhead.

About FireEye, Inc.

FireEye, Inc. is the leader in malware protection systems and next generation network threat prevention solutions that safeguard valuable data and networks against Modern Malware infiltration and theft in commercial enterprises, higher education, and government institutions. The FireEye Malware Protection System is the industry's first solution that completely breaks the Modern Malware infection lifecycle by stopping inbound, zero hour, targeted attacks, outbound data exfiltration callbacks, and dynamically inoculating networks from future attacks through both local and global intelligence. FireEye finds and blocks the 90% of Modern Malware attacks that conventional defenses miss, at network speeds and near-zero false positive rates, delivering an extremely low security TCO. FireEye is based in Milpitas, Calif. and backed by Sequoia Capital, Norwest Venture Partners, JAFCO Ventures, DAG Ventures, Juniper Networks, and In-Q-Tel. For more information, contact (408) 321-6300 or email: info@fireeye.com. Visit us at www.FireEye.com.

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

www.FireEye.com