

Malware Protection Cloud

A real-time global exchange of threat data helps preempt emerging, zero-day attacks

The FireEye Malware Protection Cloud connects FireEye Web and Email Malware Protection Systems (MPS) into a real-time exchange of malware intelligence and threat data on confirmed, emerging attacks.

This Internet cyber crime watch system provides subscribers the latest intelligence on inbound zero-day malware attacks and unauthorized outbound callback destinations, such as botnet command and control centers. It helps prevent system compromises and data exfiltration, alteration and destruction.

Global Network to Share Local Malware Intelligence

The FireEye Malware Protection Cloud (MPC) interconnects FireEye appliances deployed within customer networks, technology partner networks and service providers around the world. This worldwide cloud efficiently shares auto-generated malware security intelligence, such as covert callback channels, as well as new threat findings from the FireEye Malware Intelligence Lab.

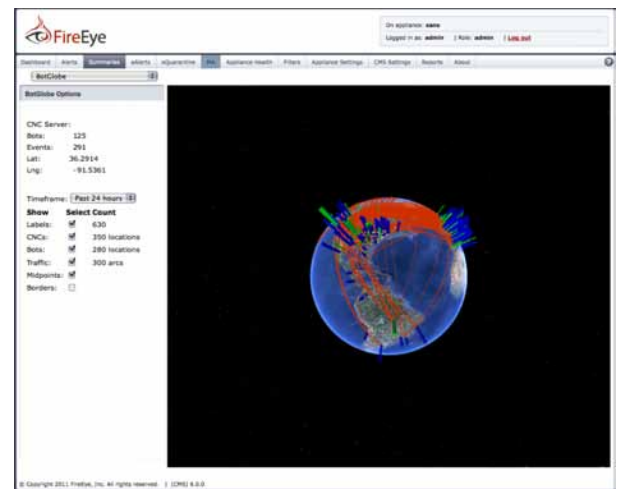
FireEye appliances also share breaking news about other criminal activities, such as new malware profiles, vulnerability exploits and obfuscation tactics, which cybercriminals use to hide from traditional security technologies. Through these constant communications, FireEye appliances can detect both emerging, unknown zero-day malware as well as the personalized, highly targeted attacks used in cybercrime, cyber espionage and cyber reconnaissance.

How it Works: Disrupting Zero-day Threats

FireEye Email and Web MPS appliances inspect for and filter out malware attacks within inbound traffic and also block malware callbacks within outbound traffic. They inspect across multiple protocols including HTTP, IRC, FTP and SMTP.

Highlights

- Global sharing of anonymized intelligence on emerging Web- and email-enabled threats
- Appliances can pull data feeds on Trojans, bots and advanced persistent threats to prevent malware infiltrating the network
- Ongoing callback destination updates block botnet communications, malware transmissions and data exfiltration
- Subscription and publishing of threat intelligence are optional, so sites can decide how much to share



The FireEye Malware Protection Cloud helps share dynamic threat intelligence between FireEye researchers and appliances

“Within seconds of a potential compromise the FireEye appliance tells us exactly what we need to know, and it allows us to focus our resources on what is important. The benefits, not only to my own organization but to all the scientists and engineers, have been invaluable.”

— Lead Analyst, Cyber Defense, Government Agency

The FireEye Virtual Execution (VX) engine has two stages that work together to identify suspicious traffic and test it to assess if it is indeed malicious. This integrated approach enables the most comprehensive protection against known and zero-day malware that attacks across multiple vectors. FireEye appliances supplement their real-time local detections by subscribing to the global FireEye Malware Protection Cloud to learn from the ongoing discoveries of other FireEye appliances.

Detailed Intelligence on Breaking Threats

When an appliance confirms an attack locally, it generates a dynamic and anonymized signature of the attack and distributes it through the Cloud to warn other users. Threat intelligence includes:

- Malware attack profiles (MD5s of malware code, network behaviors, obfuscation tactics) that identify confirmed and known attacks
- Analysis of email attachments and URLs
- 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

Blocks Based on Facts to Avoid False Positives and Negatives

Unlike reputation and risk-based threat intelligence networks, which make assumptions about potentially risky code and broadcast signatures that may either falsely block or falsely allow traffic, FireEye systems confirm malicious activity. The assessments captured by the FireEye systems are conclusive, because suspicious code is fully tested in a virtual execution environment.

A botnet example demonstrates the invaluable impact of these ongoing intelligence updates:

1. A FireEye appliance identifies a malicious IP address serving as a command and control (C&C) system and begins to block outbound calls to that address
2. The appliance automatically notifies the FireEye MPC of the destination IP address, port and malware protocol used in the attempted connection

3. MPC subscribers' FireEye appliances pull down regular updates and block connections to that IP address that use the same port and malware protocol
4. Compromised systems at all MPC subscriber sites are cut off from contacting the botnet C&C system
5. By seeing which hosts contact that C&C IP address, the system administrators at each site can know which systems are infected and what data was being targeted for theft

About FireEye

FireEye is the leading provider of next-generation threat protection focused on combating advanced malware, zero-day and targeted APT attacks. FireEye's solutions supplement security defenses such as next generation and traditional Firewalls, IPS, AV and Web gateways, which can't stop advanced malware. These technologies leave significant security holes in the majority of corporate networks. FireEye's Malware Protection Systems feature both inbound and outbound protection and a signature-less analysis engine that utilizes the most sophisticated virtual execution engine in the world to stop advanced threats that attack over Web and email. Our customers include enterprises and mid-sized companies across every industry as well as Federal agencies. Based in Milpitas, California, FireEye is backed by premier financial partners.