FIREEYE™

SOLUTION BRIEF

Intelligent Server Defense

Counter Advanced Attacks with Both Network and Endpoint Security

HIGHLIGHTS

- Modern attacks target servers with hard to detect methods
- FireEye addresses the threat from the network to the server
- Advanced FireEye threat intelligence allows our solutions to detect attacks others miss

Overview

The average employee operates in a world where mobile devices constantly interact with servers in data centers and in the cloud, sharing all manner of sensitive data as business is more often conducted outside the office than inside. This can leave an open attack path to an organization's crown jewels: the data, customer information and intellectual property stored on their servers.

Servers often run web-facing applications that provide direct attack surfaces from both the Internet and within the managing organization. Threat actors can attack the server directly with an outside-in attack that scans the server and determines what OS, web services and applications are running. They can use this information to identify vulnerabilities or exploits for compromise.

The security industry offers many solutions to protect client endpoints and the network itself, but servers—both Linux and Windows—have different attack surfaces, vulnerabilities and patterns than client endpoints. Attackers stay hidden on the servers; with a median time before attackers are discovered is 78 days; giving attackers time to perform reconnaissance, escalate privileges, steal an organization's most sensitive data and cover their tracks.

How Attackers Approach Servers

The attack on a server is often quite different than a client endpoint. Attackers goal is to stay resident on the system and collecting network reconnaissance data, personal identifiable information or financial transaction information. The longer the attacker can stay hidden, the more value will be gained. Basic attacks such as malware or worms are easily defeated, modern attackers use web shells as a remote access trojan; a few simple lines of code installed on the web server to provide backdoor access or access to the server file system.

These few lines of code look similar to code existent on the server and unless the web shell is active, it is not easy to detect. Using web shells, attackers can modify web servers to redirect search engine requests to a compromised web page. Or present content to the search engine different from what the user sees. Locating a web shell usually requires a user-agent change of the crawler bot.

How Customers Detect Server Attacks Today

Automated tools to detect a web shell attack offer only limited means of detection. Administrators are forced to use indicators to find a web shell attack:

- Abnormally high web server usage (due to heavy downloading and uploading by the attacker)
- Files with an abnormal timestamp (for example, newer than the last modification date)
- Unknown files on server
- Files with dubious references, such as cmd.exe or evals
- Unknown connections in web server logs

Analyzing web server logs could determine the location of the web shell, but the process is time consuming because every suspect log must be reviewed. And during the process, the attack continues.

Traditional security tools are ineffective against modern server attacks. Firewalls and Intrusion Detection Systems typically rely on signatures, which web shells can easily bypass. Secure web gateways and other products may look at content, but web shells can easily fool these scanners because they are legitimate code. Organizations require a solution that can emulate a system completely, interact with code, look for indicators, and only then determine whether code is malicious.

The FireEye Solution

New features in both FireEye Network Security and Endpoint Security detect web shell traffic, determine whether a server has been infected and enable investigation to respond to the attack.

Network Security

For an organization's network traffic, customers can use the FireEye SmartVision engine in the Network Security solution to detect malicious traffic moving between clients and network devices communicating over SMB. With Network Security 8.3, FireEye can detect web shell traffic, determine what the web shell is doing, when it is active and what devices are being used. Incident responders can use this information to determine if an attack is in progress and how to begin an investigation.

Endpoint Security

FireEye Endpoint Security uses four specialized engines to help protect, detect and respond to an attack on clients using Microsoft Windows as well as Windows servers. For Linux servers, Endpoint Security 4.8 provides incident responders with real-time detection and investigation capabilities.

With these two updated solutions, an investigator can use Network Security to determine that a web shell is being used as part of an attack involving servers, and to identify affected servers. The investigator can then use Endpoint Security to perform a deep dive investigation on those servers, determine which web pages or applications have been compromised with the web shell. They can then isolate those web pages or applications, remediate the environment and resume normal operations. Once they determine how the attack occurred, the security team can prevent further infection by resolving vulnerabilities or patching infected systems. Similar proactive fixes can be applied across uninfected servers as a preventative measure.

Better Together

With this combined solution, FireEye cuts the time to detect and resolve attacks from weeks to hours. Dealing with infected files or applications drops from days to minutes. FireEye provides customers with an end-to-end detection and investigation lifecycle for deep data center attacks that no other vendor can match.

To learn more about FireEye, visit: **www.FireEye.com**

FireEye, Inc.
601 McCarthy Blvd. Milpitas, CA 95035
408.321.6300/877.FIREEYE (347.3393)
info@FireEye.com

About FireEye, Inc.

FireEye is the intelligence-led security company. Working as a seamless, scalable extension of customer security operations, FireEye offers a single platform that blends innovative security technologies, nation-state grade threat intelligence, and world-renowned Mandiant® consulting. With this approach, FireEye eliminates the complexity and burden of cyber security for organizations struggling to prepare for, prevent and respond to cyber attacks.

FIREEYE™