SOLUTION BRIEF

FireEye

FireEye SmartVision

Detect suspicious lateral movements within an enterprise network

HIGHLIGHTS

- Detects formerly undetectable suspicious lateral movements
- Delivers visibility into suspicious network traffic within the network
- Employs an advanced network event correlation and analytics engine, machine-learning technology and more than 120 intrusion detection rules
- Supports a variety of deployments as part of FireEye Network Security

Today's changing threat landscape

Today's threat landscape continues to evolve, making preventive measures less and less reliable for thwarting sophisticated attackers. The days of "smash-and-grab" attacks are over. Once inside the network, today's attackers are likely to remain active in the breached environment, conducting stealthy internal reconnaissance in order to accomplish their mission: stealing your valuable information.

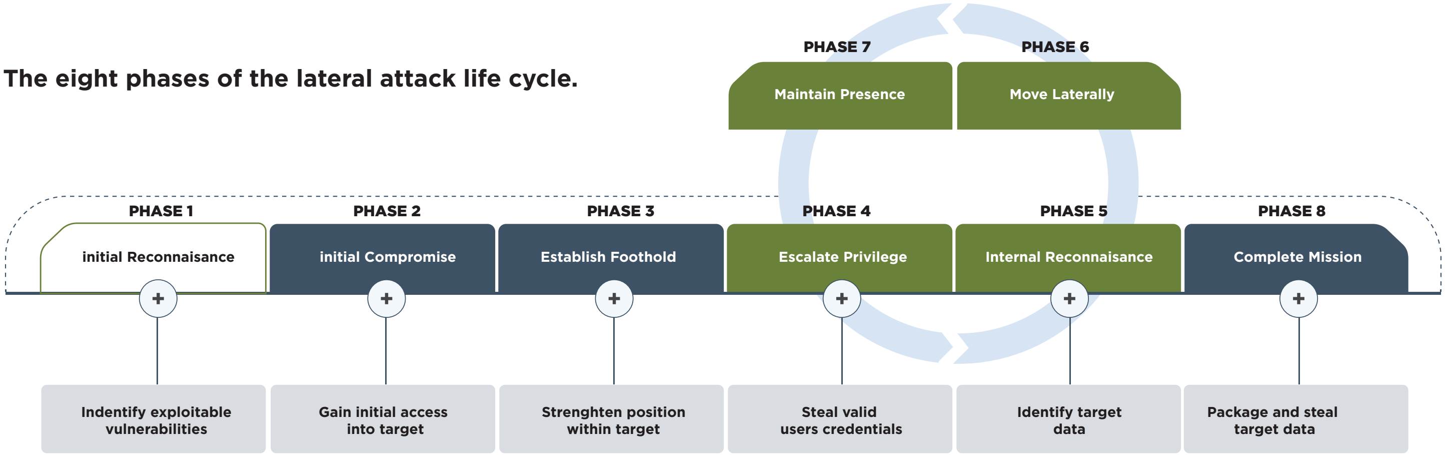
Meanwhile, improved counter-forensic techniques allow attackers to mask their lateral "East-West" movements and hide their electronic tracks. These cyber criminals often load custom backdoors with unique configurations for each compromised system so that they can maintain future entry and network access.

Post-Breach Detection Challenges

Unfortunately, the tools available today for detecting post-breach, lateral activities have limitations or simply can't detect such activities at all. For example, due to their cumbersome set up and complex management, security information and event management systems (SIEMs) often miss lateral movements, or worse, generate a myriad of false positive alerts, overloading security teams.

Many organizations deploy multiple firewall deployments to limit attackers' movement and contain damage to a limited network segment. In addition to the high cost and complexity of this approach, firewalls often fail to detect and stop suspicious lateral movement because the attacker has already gained some level of trusted, credentialed access, thus bypassing the firewalls altogether.

The eight phases of the lateral attack life cycle.



FireEye SmartVision

FireEye has identified several unique indicators and actions that denote inside efforts to steal data. Armed with this intelligence, FireEye developed FireEye SmartVision™, a new capability for detecting formerly undetectable lateral attack movements.

When used in conjunction with the FireEye Network Security platform, SmartVision allows security administrators to detect a variety of suspicious lateral movements, giving newfound visibility into suspicious network traffic across the perimeter as well as within the network core and servers.

Core components of SmartVision include:

- An advanced correlation and analytics engine
- A machine-learning module that detects data exfiltration attempts
- More than 120 intrusion detection rules that identify weak indicators of compromise (IOCs)

How SmartVision Detects the Undetectable

SmartVision detects a myriad of malicious activities within the enterprise network. Because of the unique characteristics exhibited by attackers' movements during the lateral attack lifecycle, SmartVision can key in on specific activities to trigger an alert.

Privilege escalation phase

During this phase, SmartVision identifies:

- **"Pass the hash":** This hacking technique allows an attacker to authenticate to a remote server or service by using the underlying NTLM or LanMan hash of a user's password.
- **File-less malware:** SmartVision detects file-less malware like "mimikatz," a well-known tool for extracting plain text passwords, hash, PIN codes and Kerberos tickets.

Internal reconnaissance phase

During this phase, FireEye Network SmartVision identifies:

- **Network Mapping:** Attackers may use SNMP-based approaches, active probing or route analytics to discover devices on the network such as endpoints and servers, their operating system information and their state of connectivity.
- **Host and Service Enumeration:** Attackers use discovery tools to gather information about user names, work groups, shared resources, open ports, remote hosts and other network services.
- **User Hunting:** To determine who has administrative rights, attackers employ tools that use WinAPI calls, which provide information about user accounts on a server, Active Directory, domain controllers and endpoints.

Lateral movement phase

During this phase, SmartVision identifies traffic over SMB protocols where attackers use the SMB and SMB2 protocol to transfer malware, files, and in particular, password dumpers.

Data exfiltration phase

During this phase, SmartVision detects unusual file transfers associated with data theft via its machine learning, data exfiltration module.

Deployment of SmartVision

As part of a FireEye Network Security environment, SmartVision can be deployed in a number of ways to best meet any combination of network designs and requirements. FireEye Network Security sensors are typically installed behind internal firewalls on server-facing traffic. This allows the sensors to capture traffic between clients and servers or between peer systems.

SmartVision supports in-line and out-of-band deployments, and can be used for on-premise, and network packet broker/TAP environments.

In summary

The threat landscape continues to evolve, making preventive measures less and less reliable for thwarting sophisticated attackers. Because of this, breach detection is becoming more and more critical, especially as threat actors improve on their abilities to stealthily move through networks at ease.

The anatomy of the lateral attack lifecycle present numerous challenges that existing security solutions cannot completely address. However, FireEye has identified unique indicators and actions that denote inside efforts to steal data.

Armed with this intelligence, FireEye developed SmartVision as an innovative solution to detect what used to be undetectable — lateral attack movements. And now, as part of the FireEye Network Security platform, SmartVision can be deployed in a variety of network architectures, giving enterprises visibility into lateral threat actions, helping businesses stay secure when threats go sideways.

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

SB.FSV.US-EN-032018