Trellix SmartVision

Detect suspicious lateral movements within an enterprise network

The changing threat landscape

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

Additionally, improved counter-forensic techniques allow attackers to mask their lateral movements and hide their electronic tracks. Cybercriminals often load custom backdoors with unique configurations for each compromised system so they can maintain future entry and network access.

Post-breach detection challenges

Unfortunately, the tools available today have limitations or can't detect post-breach, lateral activities at all. For example, due to cumbersome setup and complex management, security information and event management systems (SIEMs) often miss lateral movements—or worse, generate false positive alerts that overload security teams.

Many organizations deploy multiple firewalls to limit attackers' movements and contain damage to a limited network segment. But, in addition to high costs and complexity, this approach often fails to detect and stop suspicious lateral movement because the attacker has already gained some level of trusted, credentialed access, bypassing the firewalls altogether.

Highlights

- Detects previously undetectable suspicious lateral movements
- Delivers visibility into suspicious traffic within the network, including JA3 (encrypted communication) and web shell (web server attacks) detection
- Employs an advanced network event correlation and analytics engine, machine-learning technology, and more than 180 rules
- Maps adversarial techniques with the MITRE ATT&CK framework
- Provides layer 7 context around every real-time alert
- Supports a variety of deployments as part of Trellix Network Security

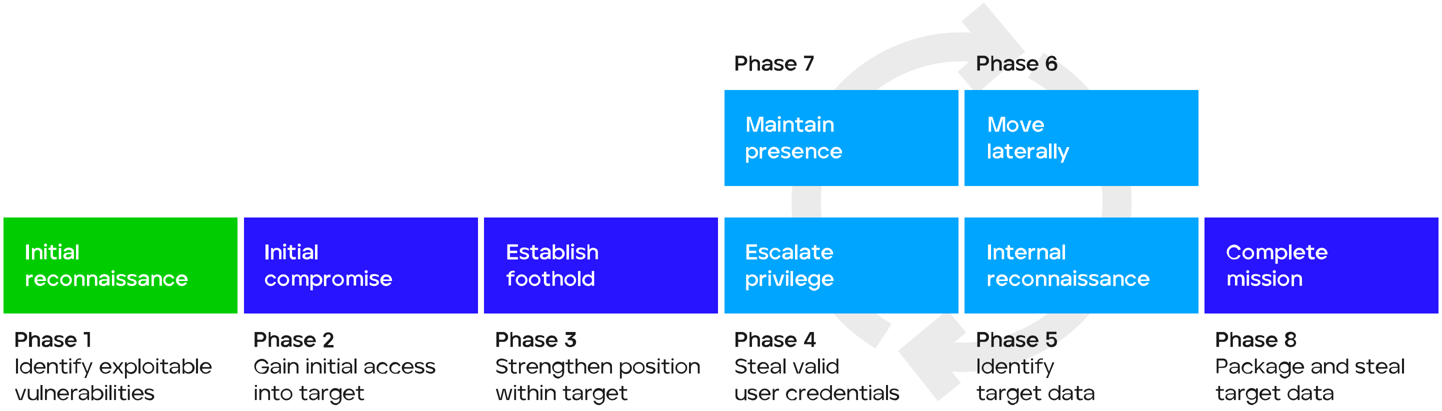

Figure 1. The eight phases of the lateral attack life cycle

Trellix SmartVision

Trellix identifies several unique indicators and actions that denote inside efforts to steal data. Using this intelligence, our Trellix SmartVision capability detects formerly undetectable lateral attack movements.

Included with Trellix Network Security, SmartVision allows your security administrators to detect a variety of suspicious lateral movements, giving you newfound visibility into suspicious network traffic across your hybrid environment.

Core components of SmartVision include:

- An advanced correlation and analytics engine
- A machine-learning module that detects data exfiltration attempts
- More than 180 rules that identify weak indicators of compromise (IOCs)

How SmartVision detects the undetectable

SmartVision detects many malicious activities within your 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.
- **Fileless malware.** SmartVision detects fileless malware like Mimikatz, a well-known tool for extracting plain text passwords, hash, PIN codes, and Kerberos tickets.

Internal reconnaissance phase

During this phase, 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 usernames, 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.

Deploying SmartVision

As part of Trellix Network Security, SmartVision mode can be deployed multiple ways to best meet many combinations of network designs and requirements. 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-premises, virtual, and network packet broker/TAP environments.

Summary

As the threat landscape continues to change and preventive measures become less reliable, breach detection is becoming more critical—especially as threat actors improve their ability to stealthily move through networks.

The anatomy of the lateral attack lifecycle presents many challenges that existing security solutions can't completely address. But Trellix has identified unique indicators and actions that denote inside efforts to steal data.

Trellix used this intelligence to develop SmartVision to detect what used to be undetectable—lateral attack movements. And included with Network Security, SmartVision can be deployed in a variety of network architectures, giving your enterprise visibility into lateral threat actions and helping your business stay secure when threats go sideways.

To learn more about Trellix, visit trellix.com.

Trellix
6220 American Center Drive
San Jose, CA 95002
www.trellix.com