Attivo NETWORKS
A SentinelOne Company

LATERAL MOVEMENT DEFENSE

Prevent In-Network Attacker Lateral Movement

Attackers have proven they can evade the perimeter to establish a beachhead inside a network from which they can laterally move while remaining undetected, often for months or years. Traditional security controls do not stop the in-network tactics that attackers use to elude detection while traversing the network. The Attivo Networks ThreatDefend® platform prevents, detects, and reveals these tactics while denying attackers visibility and access to sensitive or critical data to exploit.

UNDERSTANDING ADVANCED ATTACKS

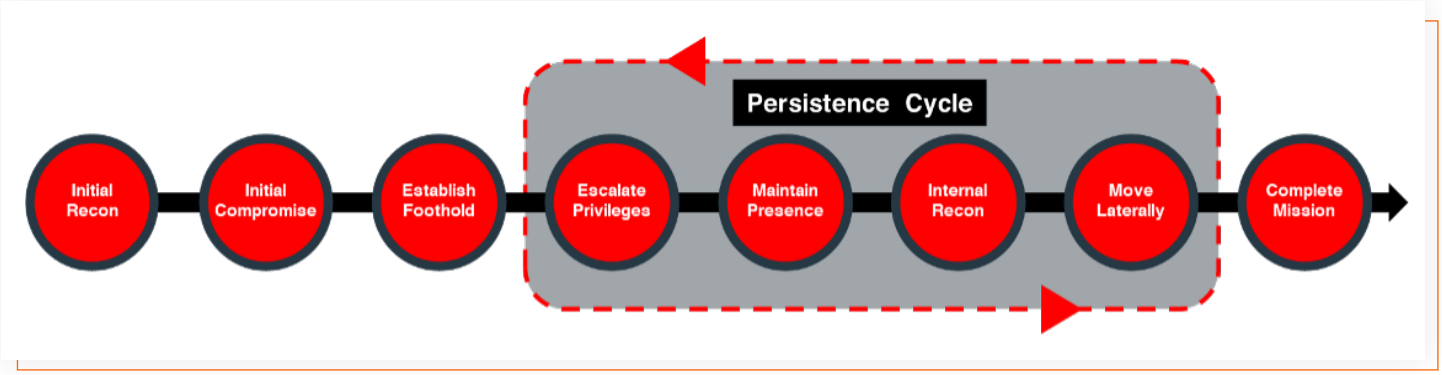

Fig. 1 - A typical attack cycle

The first system an attacker compromises from outside is just a beachhead, usually accomplished using social engineering (such as phishing emails) or exploiting externally vulnerable services.

Once an attacker compromises a host inside the network and establishes a foothold, they must ensure that they can always return to continue their attacks. They install back doors and remote access tools to establish persistence mechanisms, using covert communications channels to remain hidden. They must then break out from this initially compromised system to move around.

Many recent attacks involved attackers compromising Active Directory for lateral movement.

In the next attack stage, they conduct discovery activities to identify subsequent targets. They search the local system for data and credentials they can steal to progress their attacks. They also query Active Directory (AD) from a domain-joined system and extract sensitive information, such as domain administrator accounts, domain controller addresses, service principal names, or Kerberos tickets. They can use this data to find targets, compromise systems, and elevate privileges. Many recent attacks involved attackers compromising Active Directory for lateral movement.

Once they identify their next targets, they fingerprint the systems for any open ports or services to exploit or use the data they gathered from AD to compromise them. They then move laterally to the target and install their persistence mechanisms.

Next, they look for sensitive or critical data to either use to further their attacks or exploit for gain. They repeat this cycle of discovery, credential theft, privilege escalation, lateral movement, and data collection until they complete their mission. These steps can occur in any order and often do.

PROVIDING IN-NETWORK DEFENSES WITH THE THREATDEFEND PLATFORM

Security solutions deployed inside the network, such as IDPS, segmentation firewalls, EDR, and EPP, are good at preventing known attacks from an initial compromise. However, these security controls can do little to detect in-network threat activity because attackers use native tools and advanced tactics to remain hidden. The Attivo Networks ThreatDefend platform takes a different approach, providing visibility and prevention against actions attackers must perform to conduct discovery, credential theft, privilege escalation, lateral movement, and data collection.

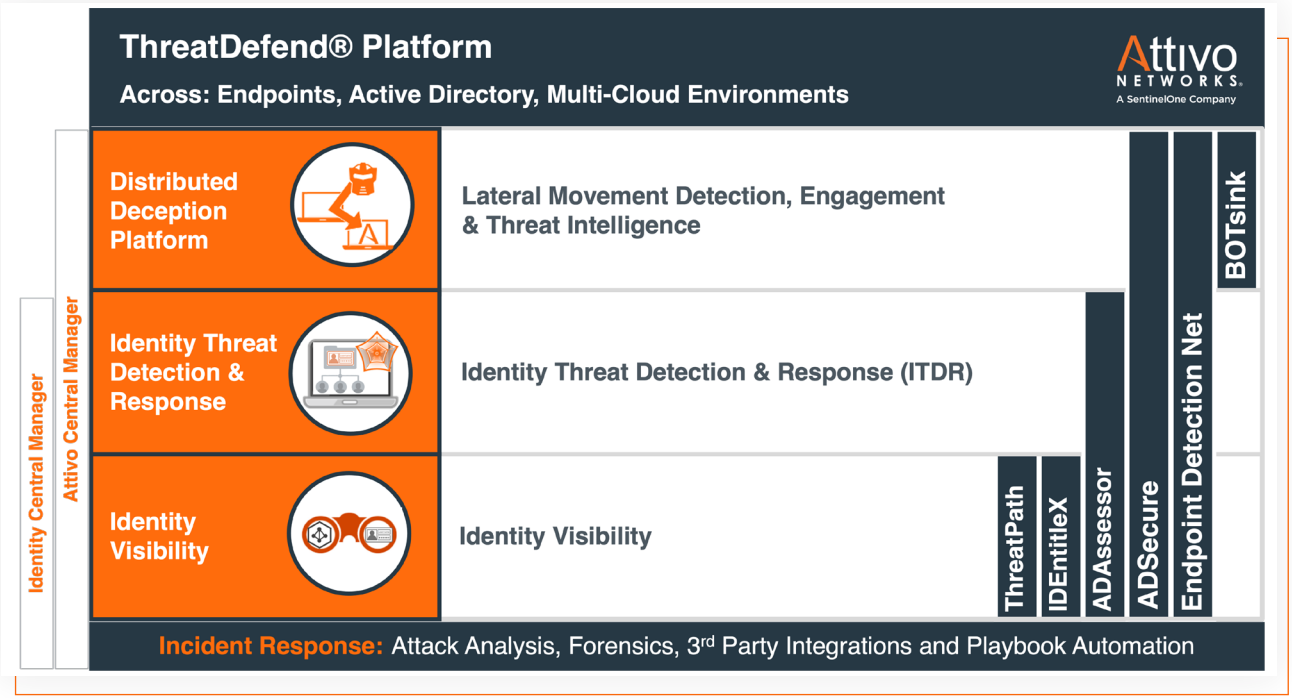

Fig. 2 –Attivo Networks ThreatDefend Platform

The Attivo Networks ThreatDefend® platform provides a customer-proven innovative defense against identity compromise, privilege escalation, and lateral movement attacks. The platform's visibility programs deliver insight into credential and attack path vulnerabilities and Active Directory domain, user, and device-level exposures for organizations seeking increased security based on least privilege access. The ThreatDefend platform's concealment technology derails attackers as they can no longer find or access the data, files, AD objects, and credentials they seek.

Additionally, the solution's decoys obfuscate the attack surface, collect forensic data, automatically analyze attack data, and automate incident response through its 30 native integrations. The platform provides the most comprehensive in-network detection solution, providing a detection fabric that scales to on-premises, cloud, remote worksites, and specialty environments such as IoT, SCADA, POS, SWIFT, and network infrastructure.

The ThreatDefend Platform includes several modular components. The ADAssessor solution identifies AD exposures and alerts on attacks targeting it. The Endpoint Detection Net (EDN) suite consists of the ThreatStrike® credential lures endpoint module, ThreatPath® for attack path visibility, ADSecure for Active Directory defense, the Cloaking function to hide and deny access to sensitive data and credentials, and the Deflect function to redirect malicious connection attempts to decoys for engagement. The Attivo BOTsink® deception server provides decoys, gathers attacker threat intelligence, and automates incident response with orchestration playbooks. Joining the EDN suite, the ADSecure solution, and ADAssessor solutions as part of Attivo's identity security offerings, the IDEntitleX solution reduces the attack surface by providing visibility to cloud identity entitlement exposure. The ThreatDirect deception forwarders support remote and segmented networks. Attivo Central Managers are available as management consoles.

The ThreatDefend platform enhances existing security controls by efficiently adding internal network visibility, prevention, and detection for those tactics that attackers use to bypass traditional defenses, move laterally through the network, and escalate privileges.

DENYING, DETECTING, AND DERAILING LATERAL MOVEMENT

The ThreatDefend platform provides visibility into and protection against attacker lateral movement across the network, as highlighted below:

DETECTING CREDENTIAL EXPOSURES

- Find exposed lateral movement paths using the ThreatPath solution and remediate them
- Analyze the presence of new user accounts, privilege accounts, or service accounts on endpoints, Active Directory using the ThreatPath solution

DENYING CREDENTIAL STEALING

- Deploy lures across all endpoints, raising alerts on theft and leading attackers to decoys
- Bind application credential stores on endpoints to the applications that own them, preventing other processes from accessing or seeing the stored credentials.

DENYING ACTIVE DIRECTORY DATA HARVESTING AND PRIVILEGE ESCALATION

- Prevent and detect kerberoasting attacks with the ADSecure solution by hiding the service accounts, thereby mitigating the risk of kerberoasting and silver ticket attacks while alerting in real-time
- Analyze the presence of attackers on domain-connected endpoints discovering privileges in Active Directory while getting real-time visibility into domain enumeration
- Detect and prevent attacker lateral movement from a domain-connected system

DENYING ACCESS TO DATA

- Deploy SMB mapped shares to decoys
- Apply concealment policies to restrict access to production network file shares, OneDrive mapped drives, or other sensitive storage from attacker tools
- Apply concealment policies to restrict access to data documents on endpoints from attacker tools

DERAILING INTERNAL DISCOVERY

- Deploy decoys mimicking critical servers, code repositories, databases, file servers, and other deceptive assets
- Deploy ThreatDirect (TD) forwarders, either TD-VM or TD-EP, across all subnets and expand deception coverage
- Deploy the ThreatDefend® Deflect function to detect port and service discovery activities – the Deflect function turns every endpoint into a decoy and engages attackers as they fingerprint and discover network services

CONCLUSION

The Attivo Networks ThreatDefend platform is customer-proven to reduce dwell times with early lateral movement detection. No other platform provides a cohesive detection fabric covering the enterprise on-premises, in the cloud, and at remote sites across the network, on endpoints, and in Active Directory. Security teams can benefit from the integration, visibility, information, and early detections that the platform provides to existing security controls.

Organizations gain the means to protect themselves against attacker lateral movement and privilege escalation tactics. The platform's unique functionality significantly enhances existing security controls. It serves as a critical defense layer to detect attackers conducting credential access, discovery, lateral movement, and collection activities. Investigators attribute the success of many recent high-profile security breaches to gaps in in-network lateral movement detection and protection. Organizations deploying the ThreatDefend platform will gain an efficient and powerful internal security control for closing these detection gaps and the time an attacker can remain undetected within their networks.

ABOUT ATTIVO NETWORKS®

Attivo Networks®, a SentinelOne company, provides Identity Threat Detection and Response (ITDR) and cyber deception solutions for protecting against identity compromise, privilege escalation, and lateral movement attacks. Through data cloaking, misdirection, and cyber deception, the platform efficiently prevents attacks across Active Directory, cloud environments, and devices.

ANSB050222
www.attivonetworks.com