Proactive Operations Program Securing Lateral Account Movement

Approach credential theft mitigation with a rational, outcome-based process of slowing down lateral account movement

Proactive Operations Program - Securing Lateral Account Movement (POP-SLAM) is a three-day engagement with a Microsoft Premier Field Engineer working alongside the customer's security and Active Directory staff. The deliverables will consist of training, knowledge transfer and implementation of the recommended mitigations in a customer provided lab. Optionally, a customer may choose to perform a basic implementation in their production environment after testing in a lab environment.

OVERVIEW

As the tools and techniques employed in modern credential theft attacks evolve, attackers are finding it easier to achieve their goals through widely known and commonly used attack vectors. Credential theft and reuse as a means for lateral movement between systems is arguably the most commonly used vector in most organizational compromises. This Proactive Operations Program (POP) will teach attendees a defense-in-depth strategy to guard against lateral traversal, a key aspect of this attack technique

OUTCOMES

The POP-SLAM consists of three major focus areas that will help customers implement critical mitigations for lateral account movement. These mitigations will set customers on the course of mitigating lateral account movement as a means of potentially devastating compromise.

01

UNIQUE LOCAL PASSWORDS

Create unique passwords for local administrators to prevent their credentials from being stolen and reused and enable audit for password access.

02

CREDENTIAL PARTITIONING

Enable secure administrative practices through a process of credential partitioning. Restrict account authentications to a single security tier based on the level of resource trust and value contained in the tier.

03

NETWORK PROTECTION

Windows Firewall configured on end-points to block all non-trusted inbound traffic.

CAPABILITIES

DEFENSE-IN-DEPTH

Multiple layers or protections on end-points mitigations for potentially devastating credential theft attacks

KEY MITIGATIONS

Implementing the core credential theft mitigations, based on data-driven analyses of known attack playbooks

FROM DEV TO PROD

Implementing LAPS, firewall rules, and secure administrative practices, make it significantly more difficult for commodity-style attacks to succeed

Microsoft

SCOPE

POP-SLAM

Scoping

Scoping call and planning

Day 1 Training Modules

Modern Attack Patterns
Modern Defense Patterns
Account Restrictions
Windows Firewall
Local Admin Password Solution (LAPS)

Day 2 Planning and Implementation

LAPS
Modern Authentication
Account Restrictions

Day 3 Audit, Implementation and Review

Windows Firewall Audit
Windows Firewall

SERVICE STATEMENT

The Microsoft Premier POP-SLAM is designed to provide your organization with advanced skills and tools to increase the difficulty for an attacker to move between machines while maintaining manageability. The POP-SLAM draws directly from Microsoft Premier Field Engineer (PFE) experience from the field in order to address real-world blockers and areas of difficulty.

ADDITIONAL DETAILS

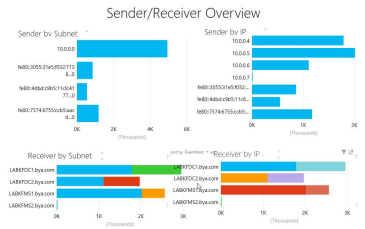
Modules:

The Modern Attack – discuss the current trends observed in today's threat landscape. It will also illustrate what a typical modern attack looks like, what the costs are to an organization as well as an attacker and how a typical attack is carried out against an organization.

The Modern Defense – different mitigations can be used to reduce the risk of Credential Theft Attacks. This includes all current Microsoft recommended mitigations and begin focusing specifically on the topics that will be used for mitigating Lateral Traversal.

Account Restrictions – covers a number of GPO settings supporting the management of highly privileged local groups and restricting a local accounts effectiveness on other client systems within the environment. It will also discuss strategies and features to limit the exposure of highly privileged domain accounts.

Windows Firewall with Advanced Security – effectively using the local firewall on client machines to ensure that client systems within networks do not have connectivity to each other unless specifically allowed. Windows Firewall auditing supports analysis of current traffic patterns for creation of host firewall policies. IPSEC usage for allowing authenticated connections to clients is also discussed.



Local Admin Password Solution (LAPS) utilize the Microsoft LAPS solution for randomizing local administrator passwords and store these passwords in Active Directory with a secure approach.

Customer Requirements:

- Conference room with projection display and whiteboard
- Customer will need to provide an Active Directory lab environment. A minimum 1 Domain Controller, 1 Management Server, and 1 system representing each windows operating system currently used in the environment.

Recommended participants include: Active Directory (AD) and Desktop engineering, IT support staff, security team, staff who share responsibility for active directory, server or workstation endpoint security.