DEFENDING AGAINST CREDENTIAL-BASED AND PRIVILEGE ESCALATION ATTACKS
INTRODUCTION

Giving the right user secure access to a system, resource, application, or network goes beyond confirming the user’s identity based on their authorization and authentication. It must also include accurately making sure that the tools they use are entitled to this access. Without this additional layer of protection, threat actors can masquerade as real users and gain unwarranted access. Most organizations rely on directory services such as Active Directory (AD) to authorize account access verifying a username and password combination. The problem is that attackers can steal and misuse these credentials for malicious purposes, and it becomes very challenging for the organization to know. With a valid credential, the attacker gains access to everything that AD authorizes the legitimate user. If attackers steal credentials that have higher privileges to the network’s resources, they can use these to escalate their attack and cause more material damage.

To protect against credential-based attacks, organizations have implemented solutions, such as Multifactor Authentication or Privileged Access Management, that seek to curtail unauthorized access. However, these solutions still have gaps that an organization can close with Attivo Networks technology.

MULTIFACTOR AUTHENTICATION AND PRIVILEGED ACCESS MANAGEMENT

Multifactor Authentication (MFA) aims to prevent unauthorized access by requiring at least two independent forms of verification. The logic is that legitimate users will have both authentication factors to verify identity while illegitimate users will not. These factors include:

- something one knows – password, security question
- something one has – token, authentication app
- something one is – biometrics
- somewhere one is – geofencing, location-aware apps
- something one does – typing speed, gestures

The system will only grant access when the user presents both elements at the time of login.

Regular user accounts have limited rights to access organizational resources or critical assets, as average users will not have the knowledge or training to manage these resources effectively. Users whose duties require managing and maintaining these network assets use system administrator accounts, service accounts, or other accounts with elevated rights and access to administer them. Privileged Access Management (PAM) solutions secure, control, manage, and monitor these privileged accounts to prevent misuse.
PAM solutions store privileged account credentials inside a secure repository (vault), isolating their use to reduce the risk of theft. System administrators must check out the privileged credential from the vault to use it for elevated access; this credential is typically restricted in the scope of uses and valid for limited duration. The PAM solution authenticates, logs their access and alerts on suspicious behavior. When the administrator checks the privileged credential back in or if the allotted time has expired, the PAM solution resets the credential to prevent reuse.

While these solutions are effective at their intended purpose, especially when used together, attackers have methods that can bypass their protection.

**GETTING PAST MFA AND PAM**

Attackers know that while MFA works for interactive logins, it does not protect against non-interactive resource access. For example, when a user logs into a Windows system that is part of a domain and uses a smartcard as the second factor after the password, MFA works to protect that initial login. However, as the system reconnects to the network, it will map existing network shares, reconnect to the user’s email account on the server, or reestablish connections to a database. These activities still need to send authentication information to the network resources they are accessing, but there is no interactive login to work with MFA. The underlying Windows OS reverts to passwords or hashes that it loads into memory to authenticate with these resources to compensate for this lack of functionality. The risk here is that attackers can steal these in-memory access tokens with applications like Mimikatz and use them to access the network and move laterally to other systems.

Windows systems also use an authentication mechanism called a Kerberos ticket to avoid storing passwords locally or transmitting them for authentication. Basically, this method uses symmetric-key cryptography to grant and verify session-specific tokens for access. Whenever a user logs in or tries to access a network resource, a Kerberos server provides authentication tokens that validate the user, the session, and the length of time the access is valid. While much more secure than just relying on sending passwords (since the entire token exchange is encrypted, as well as the storage of the access keys), Kerberos tickets still reside in memory and can do so for up to ten hours. This memory residence creates an ideal opportunity for attackers to steal these Kerberos tickets and reuse them to access the network resource.

With PAM holding all the privileged accounts, the organization must protect the PAM server as carefully as a Directory Controller. If not, attackers can compromise the PAM server to access the privileged accounts. However, most attackers will not need to go so far as they can take advantage of stored credentials for Remote Desktop Protocol and other services to gain access to systems. Additionally, if a user uses RDP to connect to another computer that attackers then compromise, they can reuse the credentials to access the original user’s system. Many organizations still do not mandate multifactor authentication for RDP.
Once attackers have access to a system that is part of the AD domain, they can use it to move laterally to other systems using the information and connections it has. Tools like Bloodhound, Mimikatz, Powerview, and Nishang allow attackers to query the AD database and map user accounts, privileges associated with groups, and other account-related information. They can use these tools to find overlapping rights based on group memberships and inherited permissions. Next, they leverage these connections to elevate privileges from a standard account by mapping the different credentials and AD objects they would need to compromise to get to a Domain Administrator account. With automated attack tools and scripts, attackers can gain persistent AD Domain Administrator access in as little as five minutes.

ADVANCED ATTACKS ON AD: TOOLS & TECHNIQUES

CLOSING CREDENTIAL SECURITY GAPS

PAM and MFA are valuable for their intended uses, but they are not a panacea for all credential-related compromises. MFA covers the initial login but can not secure non-interactive logins or deal with memory-resident theft of access tokens or hashes. PAM protects privileged accounts but can’t protect against Active Directory’s susceptibility to data gathering and offline analysis for attackers to find overlapping permissions and privileges unidentified by the organization.

By implementing the Attivo Networks ThreatDefend platform’s Endpoint Detection Net (EDN) Suite or the Attivo Identity Visibility Bundle, which includes end-to-end visibility from endpoints to Active Directory to the cloud, organizations can strengthen defenses against credential-based attacks, exploitation of excess entitlements, and unauthorized privilege escalation.
The Endpoint Detection Net (EDN) Suite prevents lateral movement from the endpoint by anticipating attack techniques and ambushing the attacker’s every move. The product suite includes the ThreatStrike solution, which protects credentials at the endpoint by hiding and binding them to prevent unauthorized access, and misdirecting the attacker with fake credentials. Plus, deceptive credentials serve as breadcrumbs stored on user systems and servers, both in credential storage and memory. These deceptive breadcrumbs also include local or domain administrator accounts, decoy hashes, access tokens, and Kerberos tickets, and more. Additionally, fake file shares lead to decoy servers on the network. When attackers attempt to steal the locally stored credentials using Mimikatz or a similar tool, they will take the fake credentials, which lead to decoys on the network. If they follow the credentials, they will engage with the decoys, which generate alerts while recording their activities to develop adversary intelligence.

The Threatpath solution reduces the endpoint attack surface and proactively increases security by identifying misconfigurations and credential exposures that create attack paths for attackers to move laterally. A topographical visualization and attack path associations provide a straight-forward view of how attacks can elevate their privileges and reach their target.

The ADSecure solution, available as part of the EDN suite or as a standalone solution, detects and alerts on unauthorized AD queries from such tools as PowerShell or Bloodhound. When the AD controller replies with the query results, the ADSecure solution raises an alert and replaces the critical accounts and objects with fake data that leads to the decoys. These AD objects include user accounts, groups, service accounts, or Service Principal Names to counter activities like Kerberoasting. When the attackers follow this data, they will land in an engagement server where critical company-centric attack data can be collected and correlated.

- The ADSecure solution only responds to unauthorized queries and will not interfere with legitimate ones or cause any impact to the AD controllers.

Organizations that want to gain a continuous assessment across endpoints, AD, and cloud vulnerabilities and gain live AD attack detection can add the Attivo Identity Visibility bundle, which includes IDEntitleX and ADAssessor along with ThreatPath. This bundled solution evaluates endpoint attack paths and the data within AD, identifying user account exposures such as vulnerable policies, exposed accounts, endpoint attack paths and inadequate security settings. Organizations can then remediate these vulnerabilities so attackers can’t exploit them as part of an attack. Furthermore, the solution continually assesses AD for any new exposures that arise as AD teams make periodic changes as part of day-to-day operations that may inadvertently introduce new vulnerabilities. The vital thing to note is that these solutions do not impact the production environment and do not require privileged access to function.
• The IDEntitleX provides cloud identity and entitlement visibility

• The ADAssessor installs on a single endpoint without requiring extra privileges

The ThreatStrike, ThreatPath, ADSecure, and Identity Visibility bundle solutions act as force multipliers to existing security controls to create a more robust security posture at the endpoint. By providing visibility and detection capabilities to these solutions, the organization closes the lingering coverage gaps left by existing controls to protect endpoints better.

Configuration Options

The ThreatStrike, ThreatPath, and ADSecure solutions are part of the Endpoint Detection Net Suite software license. Additionally, the ADSecure solution can be deployed in a standalone configuration. The Identity Visibility bundle is comprised of ThreatPath, ADAssessor and IDEntitleX. ADAssessor is also offered as a separate software license.

SUMMARY

MFA and PAM are effective technologies for defending against credential-based endpoint attacks, particularly when used jointly but have protection gaps related to misused credentials and entitlement for privileged access. Deploying the EDN suite for credential theft and privilege escalation prevention significantly increases an organization’s overall protection of identities and entitlements. Moreover, they achieve this without disrupting or needing access that could create additional risk to operations.

ABOUT ATTIVO NETWORKS®

Attivo Networks®, the leader in identity detection and response, delivers a superior defense for preventing privilege escalation and lateral movement threat activity. Customers worldwide rely on the ThreatDefend® Platform for unprecedented visibility to risks, attack surface reduction, and attack detection. The portfolio provides patented innovative defenses at critical points of attack, including at endpoints, in Active Directory, and cloud environments. Data concealment technology hides critical AD objects, data, and credentials, eliminating attacker theft and misuse, particularly useful in a Zero Trust architecture. Bait and misdirection efficiently steer attackers away from production assets, and deception decoys obfuscate the attack surface to derail attacks. Forensic data, automated attack analysis, and automation with third-party integrations serve to speed threat detection and streamline incident response. ThreatDefend capabilities tightly align to the MITRE ATT&CK Framework and deception and denial are now integral parts of NIST Special Publications and MITRE Shield active defense strategies. Attivo has 150+ awards for technology innovation and leadership. www.attivonetworks.com