WHITEPAPER

Attivo NETWORKS

DEFENDING AGAINST CREDENTIAL-BASED ATTACKS – PROTECTING THE KEYS TO THE FRONT DOOR

Giving the right user secure access to a system, resource, application, or network hinges on one thing – accurately confirming the user's identity. Organizations often 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 the organization would never know. Since the credential is valid, the attacker gains access to everything the legitimate user has access to. If attackers steal credentials that have higher privileges to resources in the network, they can cause much 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 bridge with Deception 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) secures, controls, manages and monitors these privileged accounts to prevent misuse.

PAM works by storing these privileged account credentials inside a secure repository (vault), isolating their use to reduce the risk of theft. Systems administrators must check out the privileged credential from the PAM to use it, and has a limited duration or set of uses before the PAM invalidates the credential. The PAM authenticates and logs their access and alerts on suspicious behavior. When the administrator checks the privileged credential back in, the PAM resets it 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 for MFA to work with. To compensate for this, the underlying Windows OS reverts to passwords or hashes that it loads into memory to authenticate with these resources. Attackers can steal these in-memory access tokens with applications like Mimikatz and use them to access the network and spread to other systems.

Windows systems also use an authentication mechanism called a Kerberos ticket to avoid storing passwords locally or transmitting them for authentication. In summary, this method uses symmetric-key cryptography to grant and verify session-specific tokens for access. Every time 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. Attackers can steal these Kerberos tickets and reuse them for access to the network resource.

With PAM holding all the privileged accounts, the organization must protect it as carefully as it does 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 such as those for Remote Desktop Protocol 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 gain access to the original user's system.

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 allow attackers to query the AD database and map user accounts, privileges associated with groups, and other account-related information. They can use Bloodhound to find overlapping rights based on group memberships and inherited permissions. They can 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.

CLOSING THE GAPS WITH ADSECURE AND THREATSTRIKE®

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 the openness of AD to data gathering and offline analysis for attackers to find overlapping permissions and privileges the organization is unaware of. Organizations that implement both still must contend with these coverage gaps, but implementing the Attivo Endpoint Detection Net (EDN) Suite, as a part of the ThreatDefend Platform, can strengthen endpoint defenses against credential-based exploitation.

The Endpoint Detection Net (EDN) Suite is designed for the benefit of ambushing attackers at the endpoint. The suite of products includes the ThreatStrike solution, which creates and stores fake credentials on user systems and servers, both in credential storage and within memory. These deceptive breadcrumbs include credentials (such as local or domain administrator accounts), as well as decoy hashes, access tokens, and Kerberos tickets. The solution also maps fake file shares that lead to decoy servers on the network. When attackers steal the locally stored credentials using Mimikatz or a similar tool, they will also take the fake credentials, which lead to decoys on the network. If they follow the credentials, they will engage with the decoys, which generates an alert while recording all of their activities for developing adversary intelligence.

The other offering within the EDN Suite is the ADSecure solution, which 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 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 the deception environment.

The vital thing to note is that these solutions do not impact the production environment. The mapped shares point to decoys. The credentials are only valid within the deception environment. The ADSecure solution adjusts the results reported to the unauthorized queries without interfering with legitimate queries or touching the AD controllers directly. They also do not interfere with existing endpoint security solutions such as Endpoint Protection Platforms or Endpoint Detection and Response solutions, nor do they affect current PAM or MFA solutions within the organization. In fact, both the ADSecure solution and the ThreatStrike solution 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 and ADSecure solutions are both sold as add-on licenses to the ThreatDefend platform. Additionally, the ADSecure solution can be deployed in a standalone configuration.

SUMMARY

MFA and PAM are effective technologies for defending against credential-based endpoint attacks, particularly when used jointly, but they don't cover all such activities. Deploying the ThreatDefend Platform's EDN suite, particularly the ThreatStrike and ADSecure solutions, significantly increases endpoint security against credential-based attacks and provides the best possible defense at the endpoint.

ABOUT ATTIVO NETWORKS®

Attivo Networks®, the leader in deception technology, provides an active defense for early detection, forensics, and automated incident response to in-network attacks. The Attivo ThreatDefend Deception Platform offers comprehensive and accurate threat detection for user networks, data centers, clouds, and a wide variety of specialized attack surfaces. A deception fabric of network, endpoint, application, and data deceptions efficiently misdirect and reveal attacks from all threat vectors. Advanced machine-learning simplifies deployment and operations for organizations of all sizes. Automated attack analysis, forensics, actionable alerts, and native integrations accelerate and streamline incident response. The company has won over 130 awards for its technology, innovation and leadership.

Learn more : www.attivonetworks.com