SOLUTION BRIEF

LEVERAGING MITRE ATT&CK AND ENGAGE TO PROTECT ACTIVE DIRECTORY

Most enterprise networks use Active Directory (AD) as their primary authentication and authorization service. Unfortunately, while they focus on operations, they seldom go beyond basic best practices to secure AD, and this lack of security is why attackers consider it a high-value target. Attackers know that they can use the data in AD to identify sensitive or critical assets to target. If they can compromise AD by stealing credentials, moving laterally, and elevating privileges, they can access any resource on the network.

Understanding how attackers compromise AD can aid organizations in defending against them. The following analysis uses the MITRE ATT&CK and Engage matrices to identify adversary tactics, techniques, and procedures (TTPs) that target AD and the steps organizations can take to mitigate them.

MITRE ATT&CK AND ENGAGE

MITRE ATT&CK is an adversary model and framework for describing an adversary's actions to compromise and operate within an enterprise network. It details the TTPs they use to gain access and execute their objectives while operating inside a network. Organizations can use the model to characterize and describe post-compromise adversary behavior better. MITRE ATT&CK documents many of the TTPs attackers use to compromise AD.

As a complement to ATT&CK, the MITRE Engage framework emphasis is on tactics the defender can implement to engage adversaries and implement an active defense. From a defender's perspective, the ATT&CK matrix provides a data model of how one should protect their enterprise against cybersecurity threats. Meanwhile, the Engage matrix list informed by adversary behavior observed in the real world and is intended to drive strategic cyber outcomes. Engage was created to help the private sector, government, and vendor communities to plan and execute the use of adversary engagement strategies and technologies.

The table below identifies the most common MITRE TTPs targeting AD that attackers use. It then outlines the Engage tactics that defenders can use to protect themselves.

TECHNIQUE	SUB-TECHNIQUES	TACTICS	MITRE ENGAGE ACTIVITIES
T1003 - OS Credential Dumping	**T1003.003 - NTDS** Adversaries may attempt to access or create a copy of the Active Directory domain database to steal credential information, as well as obtain other information about domain members such as devices, users, and access rights. By default, the NTDS file (NTDS.dit) is located in %SystemRoot%\NTDS\Ntds.dit of a domain controller.	Credential Access	**EAC0005 - LURES** A defender can utilize Lures to enable or block the adversary's intended actions. Defenders can deploy Lures in various forms, including credentials, domain accounts, Active Directory objects, files, folders, network directories, etc. Lures allow the defender to drive adversary behavior in ways that align with operational outcomes.
T1037 - Boot or Logon Initialization Scripts	**T1037.003 - Network Logon Script** Adversaries may use network logon scripts automatically executed at logon initialization to establish persistence. Network logon scripts can be assigned using Active Directory or Group Policy Objects. These logon scripts run with the privileges of the user they are assigned to. Depending on the systems within the network, initializing one of these scripts could apply to more than one or potentially all systems.	Persistence Privilege Escalation	**EAC0014 - SOFTWARE MANIPULATION** A defender can manipulate software by changing the output of commonly used discovery commands to hide legitimate systems and reveal deceptive artifacts and systems. Alternatively, the defender can change the output for an adversary attempting to harvest credentials from SYSVOL share and Netlogon folders.
T1069 - Permission Group Discovery	**T1069.002 - Domain Groups** Adversaries may attempt to find domain-level groups and permission settings. The knowledge of domain-level permission groups can help adversaries determine which groups exist and which users belong to a particular group. Adversaries may use this information to determine which users have elevated permissions, such as domain administrators.	Discovery	**EAC0015 - INFORMATION MANIPULATION** A defender can conceal facts and fiction such as accounts, credentials, groups, decoy files, and high-value assets. It will affect the adversary's sense of uncertainty to support the operational objectives like escalating privileges and maintaining persistence.
T1078 - Valid AccountAs	**T1078.002 - Domain Accounts** Adversaries may obtain and abuse credentials of a domain account as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion. Domain accounts are those managed by Active Directory Domain Services, where access and permissions are configured across systems and services that are part of that domain. Domain accounts can cover users, administrators, and services. **T1078.004 - Cloud Accounts** Adversaries may obtain and abuse credentials of a cloud account as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion. Cloud accounts are those an organization creates and configures for use by users, remote support, services, or for administration of resources within a cloud service provider or SaaS application. In some cases, cloud accounts may be federated with a traditional identity management system, such as Window Active Directory.	Defense Evasion Persistence Privilege Escalation Initial Access	**EAC0008 - BURN-IN** A defender can engage with the environment to produce the Burn-In artifacts, such as when the defender logs into a decoy account or accesses a decoy website to generate session cookies and browser history. The artifacts generated during the Burn-In process can reassure the adversary of the environment's legitimacy by creating an environment that more closely resembles a real, lived-in system or network. **EAC0022 - ARTIFACT DIVERSITY** A defender can present multiple network and system artifacts to the adversary, including a diverse set of domain and cloud accounts, and then monitor to determine which accounts the adversary targets in the future.

TECHNIQUE	SUB-TECHNIQUES	TACTICS	MITRE ENGAGE ACTIVITIES
T1087 - Account Discovery	**T1087.002 - Domain Accounts** Adversaries may attempt to get a listing of domain accounts. This information can help adversaries determine which domain accounts exist to aid in follow-on behavior. **T1087.004 - Cloud Account** Adversaries may attempt to get a listing of cloud accounts. Cloud accounts are those created and configured by an organization for use by users, remote support, services, or for administration of resources within a cloud service provider or SaaS application.	Discovery	**EAC0014 - SOFTWARE MANIPULATION** A defender can manipulate software by changing the output of commonly used discovery commands to hide legitimate systems and reveal deceptive artifacts and systems. Alternatively, the defender can change the output of the password policy description for an adversary attempting to brute-force credentials. **EAC0022 - ARTIFACT DIVERSITY** A defender can present multiple network and system artifacts to the adversary, including a diverse set of domain and cloud accounts, and then monitor to determine which accounts the adversary targets in the future.
T1098 - Account Manipulation	Adversaries may manipulate accounts to maintain access to victim systems. Account manipulation may consist of any action that preserves adversary access to a compromised account, such as modifying credentials or permission groups. These actions could also include account activity designed to subvert security policies, such as performing iterative password updates to bypass password duration policies and preserve the life of compromised credentials. In order to create or manipulate accounts, the adversary must already have sufficient permissions on systems or the domain.	Persistence	**EAC0014 - SOFTWARE MANIPULATION** **A defender can manipulate software by changing the output of commonly used discovery commands to hide legitimate systems reveal deceptive artifacts and systems. Alternatively, the defender can change the output of the password policy description for an adversary attempting to brute-force credentials.**
T1110 - Brute Force	**T1110.001 - Password Guessing** Adversaries with no prior knowledge of legitimate credentials within the system or environment may guess passwords to attempt access to accounts. Without knowledge of the password for an account, an adversary may opt to systematically guess the password using a repetitive or iterative mechanism. An adversary may guess login credentials without prior knowledge of system or environment passwords during an operation by using a list of common passwords. Password guessing may or may not take into account the target's policies on password complexity or use policies that may lock accounts out after a number of failed attempts.	Credential Access	**EAC0022 - ARTIFACT DIVERSITY** A defender can include a diverse set of accounts and credentials and then monitor to determine which accounts the adversary targets in the future. **EAC0003 - SYSTEM ACTIVITY MONITORING** A defender can use system logging to study and collect first-hand observations about the adversary's actions and tools. This solution can send data to a centralized collection location for further analysis.

TECHNIQUE	SUB-TECHNIQUES	TACTICS	MITRE ENGAGE ACTIVITIES
T1110 - Brute Force (cont.)	**T1110.002 - Password Cracking** Adversaries may use password cracking to attempt to recover usable credentials, such as plaintext passwords, when credential material such as password hashes are obtained. OS Credential Dumping is used to obtain password hashes; this may only get an adversary so far when Pass the Hash is not an option. Techniques to systematically guess the passwords used to compute hashes are available, or the adversary may use a pre-computed rainbow table to crack hashes. Cracking hashes is usually done on adversary-controlled systems outside of the target network. The plaintext password resulting from a successfully cracked hash may be used to log into systems, resources, and services in which the account has access. **T1110.003 - Password Spraying** Adversaries may use a single or small list of commonly used passwords against many different accounts to attempt to acquire valid account credentials. Password spraying uses one password (e.g. 'Password01') or a small list of commonly used passwords, that may match the complexity policy of the domain. Logins are attempted with that password against many different accounts on a network to avoid account lockouts that would normally occur when brute forcing a single account with many passwords.	Credential Access	
T1134 - Access Token Manipulation	**T1134.005 - SID-History Injection** Adversaries may use SID-History Injection to escalate privileges and bypass access controls. The Windows security identifier (SID) is a unique value that identifies a user or group account. SIDs are used by Windows security in both security descriptors and access tokens. An account can hold additional SIDs in the SID-History Active Directory attribute, allowing inter-operable account migration between domains (e.g., all values in SID-History are included in access tokens).	Defense Evasion Privilege Escalation	**EAC0003 - SYSTEM ACTIVITY MONITORING** A defender can capture system logging to study and collect first-hand observations about the adversary's actions and tools. **EAC0014 - SOFTWARE MANIPULATION** A defender can manipulate software by changing the output of commonly used discovery commands to hide legitimate systems reveal deceptive artifacts and systems. Alternatively, the defender can change the output of the password policy description for an adversary attempting to brute-force credentials.

TECHNIQUE	SUB-TECHNIQUES	TACTICS	MITRE ENGAGE ACTIVITIES
T1136 - Create Account	**T1136.002 - Domain Account** Adversaries may create a domain account to maintain access to victim systems. Domain accounts are those managed by Active Directory Domain Services where access and permissions are configured across systems and services that are part of that domain. Domain accounts can cover user, administrator, and service accounts. With a sufficient level of access, the net user /add /domain command can be used to create a domain account.	Persistence	**EAC0022 - ARTIFACT DIVERSITY** A defender can include a diverse set of accounts and credentials and then monitor to determine which accounts the adversary targets in the future.
T1207 - Rogue Domain Controller	Adversaries may register a rogue Domain Controller to enable manipulation of Active Directory data. DCShadow may be used to create a rogue Domain Controller (DC). DCShadow is a method of manipulating Active Directory (AD) data, including objects and schemas, by registering (or reusing an inactive registration) and simulating the behavior of a DC. [1] Once registered, a rogue DC may be able to inject and replicate changes into AD infrastructure for any domain object, including credentials and keys.	Defense Evasion	**EAC0008 - BURN-IN** A defender can engage with the environment to produce the Burn-In artifacts, such as when the defender logs into a decoy account or accesses a decoy website to generate session cookies and browser history. The artifacts generated during the Burn-In process can reassure the adversary of the environment's legitimacy by creating an environment that closely resembles a real, lived-in system or network.
T1484 - Domain Policy Modification	**T1484.001 - Group Policy Modification** Adversaries may modify Group Policy Objects (GPOs) to subvert the intended discretionary access controls for a domain, usually with the intention of escalating privileges on the domain. Group policy allows for centralized management of user and computer settings in Active Directory (AD). GPOs are containers for group policy settings made up of files stored within a predicable network path \<DOMAIN>\SYSVOL\<DOMAIN>\Policies\.	Defense Evasion Privilege Escalation	**EAC0005 - LURES** A defender can utilize Lures to enable or block the adversary's intended actions. Defenders can deploy Lures in various forms, including credentials, domain accounts, Active Directory objects, files, folders, network directories, etc. Lures allow the defender to drive adversary behavior in ways that align with operational outcomes.
T1550 - Use Alternate Authentication Material	**T1550.001 - Application Access Token** Adversaries may use stolen application access tokens to bypass the typical authentication process, and access restricted accounts, information, or services on remote systems. These tokens are typically stolen from users and used in lieu of login credentials.	Defense Evasion Lateral Movement	**EAC0023 - INTRODUCED VULNERABILITIES** A defender can attempt to motivate the adversary to target specific resources. This targeting may move the adversary towards a particular resource or away from another resource. The defender may introduce vulnerabilities to encourage the adversary to reveal targeting preferences available capabilities or even influence future targeting decisions.

TECHNIQUE	SUB-TECHNIQUES	TACTICS	MITRE ENGAGE ACTIVITIES
T1550 - Use Alternate Authentication Material (cont.)	**T1550.002 - Pass the Hash** Adversaries may "pass the hash" using stolen password hashes to move laterally within an environment, bypassing normal system access controls. Pass the hash (PtH) is a method of authenticating as a user without having access to the user's cleartext password. This method bypasses standard authentication steps that require a cleartext password, moving directly into the portion of the authentication that uses the password hash. **T1550.003 - Pass the Ticket** Adversaries may "pass the ticket" using stolen Kerberos tickets to move laterally within an environment, bypassing normal system access controls. Pass the ticket (PtT) is a method of authenticating to a system using Kerberos tickets without having access to an account's password. Kerberos authentication can be used as the first step to lateral movement to a remote system.	Defense Evasion Lateral Movement	**EAC0022 - ARTIFACT DIVERSITY** A defender can present multiple network and system artifacts to the adversary, including a diverse set of domain and cloud accounts, and then monitor to determine which accounts the adversary targets in the future.
T1558 - Steal or Forge Kerberos Tickets	**T1558.001 - Golden Ticket** Adversaries who have the KRBTGT account password hash may forge Kerberos ticket-granting tickets (TGT), also known as a golden ticket. Golden tickets enable adversaries to generate authentication material for any account in Active Directory. **T1558.002 - Silver Ticket** Adversaries who have the password hash of a target service account (e.g. SharePoint, MSSQL) may forge Kerberos ticket granting service (TGS) tickets, also known as silver tickets. Kerberos TGS tickets are also known as service tickets. **T1558.003 - Kerberoasting** Adversaries may abuse a valid Kerberos ticket-granting ticket (TGT) or sniff network traffic to obtain a ticket-granting service (TGS) ticket that may be vulnerable to Brute Force. **T1558.004 - AS-REP Roasting** Adversaries may reveal credentials of accounts that have disabled Kerberos preauthentication by Password Cracking Kerberos messages.	Credential Access	**EAC0022 - ARTIFACT DIVERSITY** A defender can present multiple network and system artifacts to the adversary, including a diverse set of domain user and computer service accounts, and then monitor to determine which accounts the adversary targets in the future. **EAC0006 - APPLICATION DIVERSITY** A defender can install one or more applications with various patch levels to see how the adversary's response differs across versions. Additionally, a diverse set of applications provides a variety of avenues for the defender to present additional information throughout an operation. It can also introduce additional attack surfaces, motivate or demotivate the adversary, or further the engagement narrative.

CONCLUSION

Leveraging the MITRE ATT&CK matrix to understand the tactics attackers use to compromise AD and the corresponding Engage tactics that address them gives defenders the means to protect an organization from the catastrophic loss of domain control. Organizations should examine their security infrastructure to determine if they can implement the Engage activities listed to improve their defenses. Deception technology has a reputation for its ability to alert early in the attack cycle. However, unlike other solutions, the Attivo Networks ThreatDefend® platform provides extensive attack prevention, detection, concealment, misdirection, and engagement capabilities covering many decoy techniques and other methods. Those familiar with Attivo Networks know that it provides extensive coverage for MITRE ATT&CK and Engage and efficiently protects against tactics common to attackers targeting Active Directory.

ABOUT ATTIVO NETWORKS®

Attivo Networks®, the identity detection and response leader, delivers a superior defense to prevent privilege escalation and lateral movement. 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 attack points, 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 Engage adversary engagement strategies. Attivo has 180+ awards for technology innovation and leadership. www.attivonetworks.com