SOLUTION BRIEF

LEVERAGING MITRE ATT&CK AND SHIELD TO PROTECT ACTIVE DIRECTORY

Most enterprise networks use Active Directory 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 Shield 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 SHIELD

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, MITRE Shield is a free, publicly available knowledge base that captures and organizes data from active defense and adversary engagements. MITRE Shield helps organizations take proactive steps to defend their networks and assets. 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 Shield matrix lists the capabilities a defender must build for an Active Defense and adversary engagement in a post-breach situation. MITRE Shield outlines tactics and techniques fundamental to building an active defense strategy that can derail attack activities targeting AD.

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

MITRE TECHNIQUES	MITRE SUB-TECHNIQUES	MITRE TACTICS	SHIELD ACTIVE DEFENSE TECHNIQUES
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 and 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	**DTE0012 - Decoy Credentials** A defender can seed systems with decoy credentials in various locations and establish alerting that will trigger if an adversary harvests the credentials and attempts to use them.
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. Organizations can assign network logon scripts using Active Directory or Group Policy Objects, which run with the privileges of the user to which they are assigned. 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	**DTE0006 - Baseline** A defender can revert a system to a verified baseline on a frequent, recurring basis to remove adversary persistence mechanisms.
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	**DTE0036 - Software Manipulation** A defender could manipulate a system's software to alter the results of an adversary enumerating permission group information.
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	**DTE0010 - Decoy Account** A defender can create decoy user accounts to make a decoy system or network look more realistic. **DTE0012 - Decoy Credentials** A defender can seed systems with decoy credentials in various locations and establish alerting that will trigger if an adversary harvests the credentials and attempts to use them. **DTE0008 - Burn-In** A defender can prepare a Decoy System by logging in to the Decoy Account and using it in ways consistent with the deception story, creating artifacts in the system that make it look legitimate.

MITREV TECHNIQUES	MITRE SUB-TECHNIQUES	MITRE TACTICS	SHIELD ACTIVE DEFENSE TECHNIQUES
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	**DTE0036 - Software Manipulation** A defender could alter the output from account enumeration commands to hide accounts or show the presence of accounts that do not exist. **DTE0010 - Decoy Account** During an adversary engagement operation, a defender can utilize decoy accounts to provide content to an adversary and encourage additional activity. **DTE0013 - Decoy Diversity** A defender can make various decoy accounts and see if the adversary seems to be drawn to accounts of a specific type, with specific permissions, group access, etc.
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. To create or manipulate accounts, the adversary must already have sufficient permissions on systems or the domain.	Persistence	**DTE0010 - Decoy Account** **A defender can use decoy accounts and monitor them for any activity that might reveal adversary manipulation.**
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 knowing the password for an account, an adversary may 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 consider the target's policies on password complexity or use policies that may lock accounts out after several failed attempts.	Credential Access	**DTE0034 - System Activity Monitoring** A defender can monitor for user login activity that may reveal an adversary leveraging brute force techniques.

MITRE TECHNIQUES	MITRE SUB-TECHNIQUES	MITRE TACTICS	SHIELD ACTIVE DEFENSE TECHNIQUES
T1110 - Brute Force (cont.)	**T1110.002 - Password Cracking** Adversaries may use password cracking to recover usable credentials, such as plaintext passwords, when they obtain credential material such as password hashes. OS Credential Dumping is used to obtain password hashes, and 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. They may use the resulting plaintext password resulting from a successfully cracked hash 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	**DTE0034 - System Activity Monitoring** A defender can monitor for user login activity that may reveal an adversary leveraging brute force techniques.
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. Windows security uses SIDs 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	**DTE0036 - Software Manipulation** A defender could feed or redirect requests for credentials with false data to direct an adversary into a decoy network or system. **DTE0007 - Behavioral Analytics** A defender could implement behavioral analytics that detects common access token manipulation techniques and denies these actions.
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, an adversary can use the "net user /add /domain" command to create a domain account.	Persistence	**DTE0033 - Standard Operating Procedure** A defender can detect user accounts created outside the acceptable process.

MITRE TECHNIQUES	MITRE SUB-TECHNIQUES	MITRE TACTICS	SHIELD ACTIVE DEFENSE TECHNIQUES
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	**DTE0007 - Behavioral Analytics** A defender can implement behavioral analytics, which would indicate activity on or against a domain controller. Activity that is out of sync with scheduled domain tasks or results in an uptick in traffic with a particular system on the network could indicate malicious activity.
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 to escalate 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	**DTE0034 - System Activity Monitoring** A defender could monitor for directory service changes using Windows event logs, which can alert to the presence of an adversary in the network.
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 place of login credentials. **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. Adversaries can use Kerberos authentication as the first step to lateral movement to a remote	Defense Evasion Lateral Movement	**DTE0007 - Behavioral Analytics** Defenders can look for anomalies where an account is authenticating and the resource it is authenticating with to detect potentially malicious intent.

MITRE TECHNIQUES	MITRE SUB-TECHNIQUES	MITRE TACTICS	SHIELD ACTIVE DEFENSE TECHNIQUES
T1558 - Steal or Forge Kerberos Tickets	**T1558.001 - Golden Ticket** Adversaries with 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 pre-authentication by Password Cracking Kerberos messages.	Credential Access	**DTE0025 - Network Diversity** A defender can set up networks that use Kerberos authentication with systems that authenticate using it, giving a chance to see if an adversary can steal or forge Kerberos tickets for lateral movement. **DTE0032 - Security Controls** A defender can secure Kerberos to prevent an adversary from leveraging the tickets to authenticate or move laterally, which may result in the adversary exposing additional TTPs.

CONCLUSION

Leveraging the MITRE ATT&CK matrix to understand the tactics attackers use to compromise AD and the corresponding Shield tactics that counter 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 Shield Active Defense techniques listed, identify gaps, and find controls that bridge them.

Deception technology has a reputation for its ability to create an Active Defense. However, unlike other solutions, the Attivo Networks ThreatDefend® platform provides extensive attack prevention and detection capabilities covering many decoy techniques and other methods. Those familiar with Attivo Networks know that it provides extensive coverage for MITRE Shield. There are currently 33 Shield Techniques and 190 use cases covered in the MITRE Shield documentation. The Attivo Networks ThreatDefend platform covers 27 of the Shield Techniques and 123 use cases and efficiently protects against tactics common to attackers targeting Active Directory.

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. Attivo has 150+ awards for technology innovation and leadership. www.attivonetworks.com