Symantec by Broadcom

WHITE PAPER

Ten Active Directory Misconfigurations that Lead to Total Domain Compromise

WHITE PAPER

Ten Active Directory Misconfigurations that Lead to Total Domain Compromise

Symantec by Broadcom

TABLE OF CONTENTS

Introduction: Active Directory Security Risks

Why is Microsoft Active Directory (AD) the business world's most targeted asset? Because with just a few queries to AD from a compromised endpoint, attackers obtain all the information they need to steal domain administrator credentials and move laterally to high-value assets. Put another way: Attackers gain control of an organization's vital assets simply by compromising a single domain-connected endpoint. The AD database exposes all identities and resources on the corporate network to any domain-connected user, and AD authorizes users (whether legitimate or nefarious) to use its built-in query capability to locate sensitive information.

Unfortunately, AD also may be the least protected asset in your company. Nine out of ten companies around the world use AD to control and maintain internal resources, but most companies focus on defending endpoints, applications, servers, mobile devices, and networks, leaving AD dangerously unguarded.

YOU CANNOT DISABLE THE AD QUERY CAPABILITY, NOR DETECT USERS MAKING THE QUERIES.

This ability to stealthily access network resources explains why many attackers prefer AD reconnaissance over network scans. And it explains why attackers eagerly exploit the default AD query capability. See the following table with attacks documented by MITRE.

AD Is a Basic Building Block of APTs[a]

Group Name	Alias	Credential Theft	AD Enumeration	Timeframe	Origin
APT 3	Boyusec, UPS	Yes	Yes	Ongoing	China
APT 10	Stone Panda	Yes	Yes	Ongoing	China
APT 28	Sofacy, Fancy Bear	Yes	Yes	Ongoing	Russia
APT 29	Cozy Duke, Cozy Bear	Yes	Yes	Ongoing	Russia
APT 32	OceanLotus	Yes	Yes	Ongoing	Vietnam
APT 33	Charming Kitten	Yes	Yes	Ongoing	Iran
APT 34	Twisted Kitten	Yes	Yes	Ongoing	Iran
APT 35	Newscaster Team	—	—	Ongoing	Iran
Turla	Snake, Uroburos	Yes	Yes	Last Seen in 2017	Russia
Shell_Crew	Deep Panda	Yes	Yes	Last Seen in 2017	China
Dark Seoul	Lazarus Group, Hidden Cobra	Yes	Yes	Ongoing	North Korea

a. https://attack.mitre.org/groups/G0022

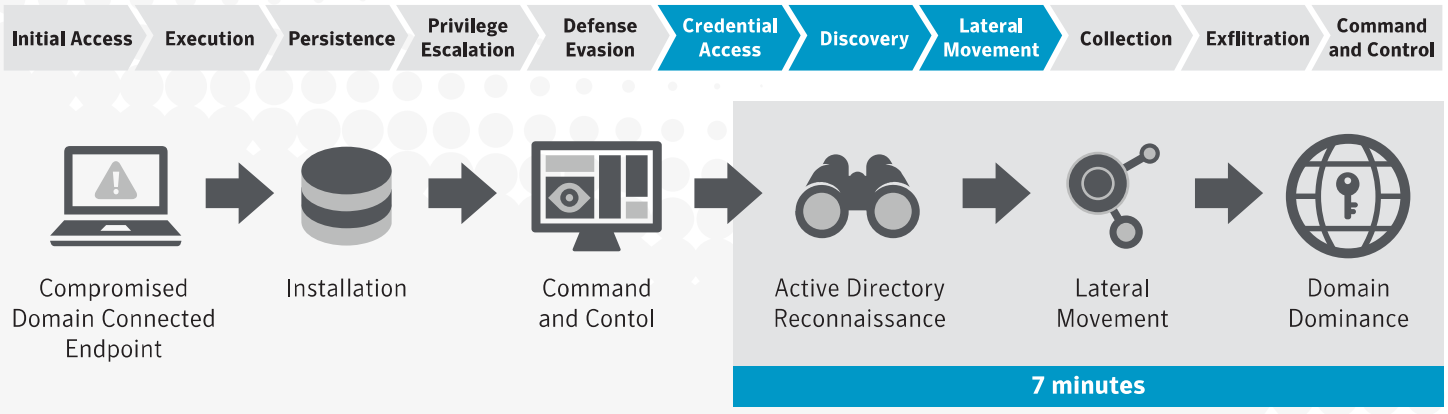
Anatomy of an AD Attack

Given a foothold on a domain-connected endpoint, attackers perform AD reconnaissance into your organizational resources. From the compromised endpoint, they generate and send queries to AD, uncovering the information they need to locate and access sensitive data. They easily learn about all your employees (including their identities, roles, and privileges) and the applications running on databases, servers, storage, and internal security components. Then they steal domain credentials and spider out laterally.

ONCE ATTACKERS COMPROMISE AN ENDPOINT, THEY NEED JUST SEVEN MINUTES TO TOTALLY DOMINATE THE DOMAIN (FULL-FLEDGED NETWORK BREACH). HIDING AMONG THE AUTHORIZED USER POPULATION, THEY APPEAR AS NORMAL USERS.

Domain-connected endpoints are a higher security risk than other devices because just one compromised device jeopardizes the entire organization. You must protect AD at compromised endpoints to stop attackers in their tracks.

Attackers Start on an Endpoint



AD Misconfigurations Open the Door to Attackers

As your organization evolves its AD implementation over time, your IT group may not properly maintain its configuration settings or implement security enhancements. Attackers lie in wait; as vulnerabilities appear on the domain and in AD services, they pounce. They also install backdoors and persistence hooks, enabling them to come back at any time.

Symantec believes that these ten AD misconfigurations create the greatest risk.

1. Group Policy Preferences Visible Passwords

Attack explanation: Administrators use Group Policy Preferences (GPPs) to configure local administrator accounts, schedule tasks, and mount network drives with specified credentials when a user logs on. They write GPPs to the SYSVOL share of domain controllers. Attackers access the GPP XML files inside the SYSVOL share and extract the specified credentials stored in the GPP.

Potential threat: Attackers gain the same account privileges they extract from the GPPs. Accounts with GPPs typically have local administrator user rights for every endpoint.

2. Hidden Security Identifier (SID)

Attack explanation: Attackers use the Security Identifier (SID) History object to inherit permissions from other high-privileged SID accounts or groups without any trace of additional group membership for the user.

Potential threat: Using a SID attribute indicates the attacker is trying to hide high-privileged group membership (for example, domain admins) in a low-privileged account to conceal a post-exploitation domain backdoor.

3. Golden Ticket

Attack explanation: Attackers with the long-term key for the *krbtgt* account forge a logon ticket (TGT) with any user rights. The ticket contains a fictitious username with domain admin membership (or any other membership the attackers choose).

Potential threat: Attackers gain privileges for any service or endpoint on the network and use it everywhere. These privileges persist until administrators reset the *krbtgt* account.

4. Domain Replication Backdoor

Attack explanation: If a low-privileged user were added to the domain replication object, an attacker accesses all of the domain sensitive data (for example, user hashes in the domain) without being a high-privileged user. Because some domain services require domain replication capabilities, replication permissions must be assigned to AD objects.

Potential threat: Attackers gain full access to the entire company domain database.

5. Unprivileged Administrator Holder ACL

Attack explanation: Attackers exploit AdminSDHolder ACLs, such as adding an unprivileged user to the AdminSDHolder security object with full control or write permissions. The unprivileged user now has the ability to add themself or other users to powerful groups, such as domain admins, without having high privileges.

Potential threat: Attackers that enable and modify this feature leave hidden administrator privileges on the domain controller without using domain accounts.

6. Power User Enumeration

Attack explanation: Authenticated users enumerate any object in the domain. Enumerating users whose passwords never expire reveals high-privileged users in the domain.

Potential threat: With these credentials, attackers gain access to high privileges in the network that last indefinitely.

7. Silver Ticket

Attack explanation: Users request service tickets, encrypted with the service account's long-term key, to any service in the domain. Attackers gather service tickets and attempt local brute-force attacks on the long-term key.

Potential threat: Attackers obtain fully privileged access to the endpoints running the service account.

8. Anonymous LDAP Allowed

Attack explanation: Unmanaged endpoints query AD, and without authentication, gather information on the domain environment.

Potential Threat: Attackers view the entire directory structure and permissions from an unauthenticated user and computer with a network connection.

9. DSRM Login Enabled

Attack explanation: Attackers enable and modify DSRM (a special boot mode for repairing or recovering AD when Directory Services are down) to leave hidden administrator privileges, through a backdoor, on the domain controller without using any domain accounts.

Potential threat: Attackers gain full control of, and access to, your organization's domain controllers.

10. Local Administrator Traversal

Attack explanation: Attackers steal local administrator credentials from a local computer in the network. Many companies use imaging software, so the local administrator password is frequently the same across the entire enterprise. The attackers pass the local administrator long-term key to a remote endpoint to authenticate.

Potential threat: Attackers obtain local administrator credentials on one machine, then move laterally and obtain access to every endpoint in the network.

Next Steps: Protect Your Organization from AD Threats

Complimentary Security Assessment

Symantec offers a complimentary, software-driven AD threat assessment. It automatically scans for, and detects, misconfigurations in AD and the entire domain environment. The output includes best-practices remediation recommendations.

Continuous Assessment

AD is a critical attack surface that needs continuous monitoring for misconfigurations, vulnerabilities, and attack persistence. Symantec® Endpoint Threat Defense for AD includes a built-in threat assessment service that provides ongoing analysis of every component of the domain and AD structure. Endpoint Threat Defense for AD looks for misconfigurations and backdoors left behind by attackers and, when it identifies one, it alerts the central console with prescriptive remediation recommendations.

To learn more about Symantec Endpoint Threat Defense for AD, visit www.broadcom.com/info/endpoint-security/threat-defense-for-active-directory

BROADCOM® connecting everything®

For more information, visit our website at: www.broadcom.com

Copyright © 2023 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

TAD-MIS-WP100 August 15, 2023