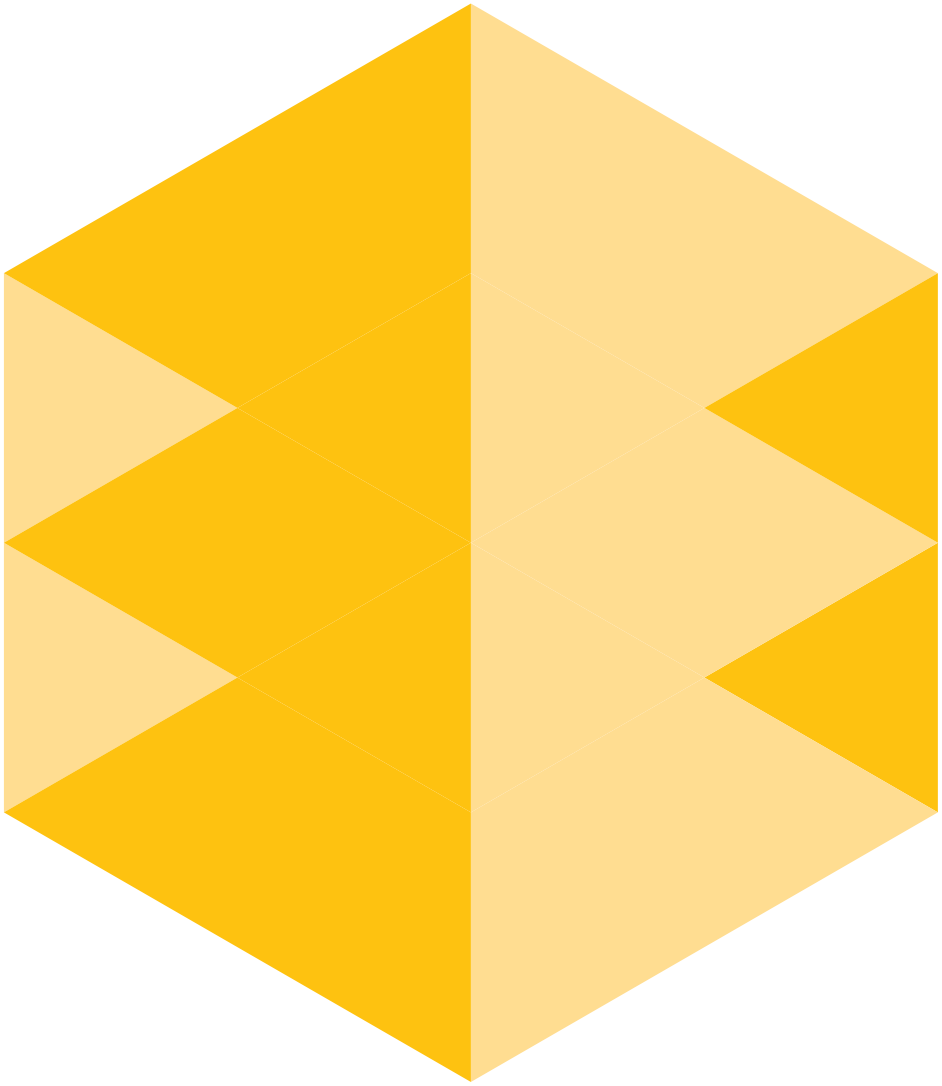


Ten Active Directory Misconfigurations that Lead to Total Domain Compromise

WHITE PAPER

Symantec™

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 admin 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; AD authorizes users (whether legitimate or nefarious) to use its built-in query capability to locate sensitive information.

Unfortunately, AD may also 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.

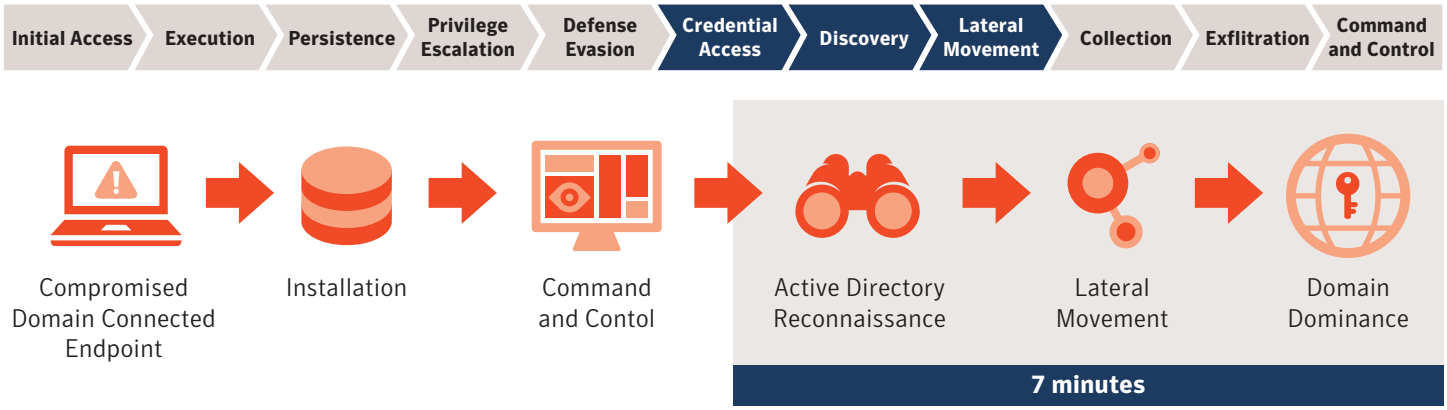
This ability to stealthily access network resources explains why many attackers prefer AD reconnaissance over network scans. And it explains why attackers eagerly exploit the default AD query capability. See attacks documented by MITRE below:

Active Directory Is a Basic Building Block of APTs*

Group Name	Alias	Credential Theft	Active Directory 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

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

Attackers Start on an Endpoint



Anatomy of an Active Directory 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.

Once attackers compromise an endpoint, they need just seven minutes to totally dominate a domain, establish persistence, and begin stealing or encrypting sensitive data.

Active Directory misconfigurations open the door to attackers

As your organization evolves its Active Directory 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 these 10 Active Directory 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 admin 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 was added to the domain replication object, an attacker accesses all 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 Admin 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—which gives that unprivileged user the ability to add themselves 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 Active Directory 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 Active Directory when Directory Services are down—to leave hidden administrator privileges, via 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 Admin 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—and pass the local admin long-term key to a remote endpoint to authenticate itself.

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

Next steps: Protect your organization from Active Directory threats

Complimentary security assessment

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

Request a complimentary Active Directory threat assessment from your Symantec account team.

Continuous assessment

Active Directory is a critical attack surface that needs continuous monitoring for misconfigurations, vulnerabilities, and attack persistence. Symantec Endpoint Threat Defense for Active Directory includes a built-in threat assessment service that provides ongoing analysis of every component of the domain and Active Directory structure. Endpoint Threat Defense for Active Directory 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 Active Directory, visit https://www.symantec.com/products/endpoint-threat-defense-for-active-directory

About Symantec

Symantec Corporation (NASDAQ: SYMC), the world's leading cyber security company, helps organizations, governments and people secure their most important data wherever it lives. Organizations across the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across endpoints, cloud and infrastructure. Likewise, a global community of more than 50 million people and families rely on Symantec's Norton and LifeLock product suites to protect their digital lives at home and across their devices. Symantec operates one of the world's largest civilian cyber intelligence networks, allowing it to see and protect against the most advanced threats. For additional information, please visit www.symantec.com, subscribe to our blogs, or connect with us on Facebook, Twitter, and LinkedIn.

Symantec

350 Ellis St., Mountain View, CA 94043 USA | +1 (650) 527 8000 | 1 (800) 721 3934 | www.symantec.com

19D219637_WP_Ten_AD_Misconfigurations_EN