DCSync Attack: The Silent Way Hackers Steal Password Hashes

Key Takeaways

- DCSync attacks exploit Active Directory replication by impersonating domain controllers to steal user credentials, posing a significant security threat.
- DCSync attacks require elevated privileges such as Domain Admin or replication permissions, highlighting the importance of strict access controls.
- Detection is challenging due to the use of legitimate replication processes, but monitoring event logs and network traffic can help identify suspicious activity.
- Restricting replication permissions, enforcing least privilege principles, and regularly auditing privileged accounts are critical defense strategies.
- Advanced detection tools and integrated solutions like Fidelis Active Directory Intercept enhance the ability to detect and respond to DCSync attacks effectively.

You use Active Directory (AD) every day to log in, manage access, and enforce policies. When AD replication runs, it keeps all your domain controllers in sync—but if you're not careful, that same process can be hijacked. If an attacker pretends to be one of your domain controllers, they can quietly pull down password hashes for any user. Understanding how AD replication works—and how it can be weaponized—is the first step to keeping your network safe.

What Exactly Is a DCSync Attack?

A DCSync attack happens when someone tricks AD into treating their system as a trusted domain controller. Once you've given that system the right permissions, it uses the Directory Replication Service Remote (MS-DRSR) protocol to request sensitive data, like password hashes, for any account in AD. Think of it like giving a stranger a master key because they claimed to be a locksmith—you wouldn't do that in your front office, so you shouldn't do it in AD either.

Example: If you grant a service account "Replicate Directory Changes All" and that account gets compromised, the attacker can run Mimikatz's DCSync function to extract the KRBTGT hash. From there, they can forge Golden Tickets and walk right through your network doors.

Why Should You Care About DCSync Attacks?

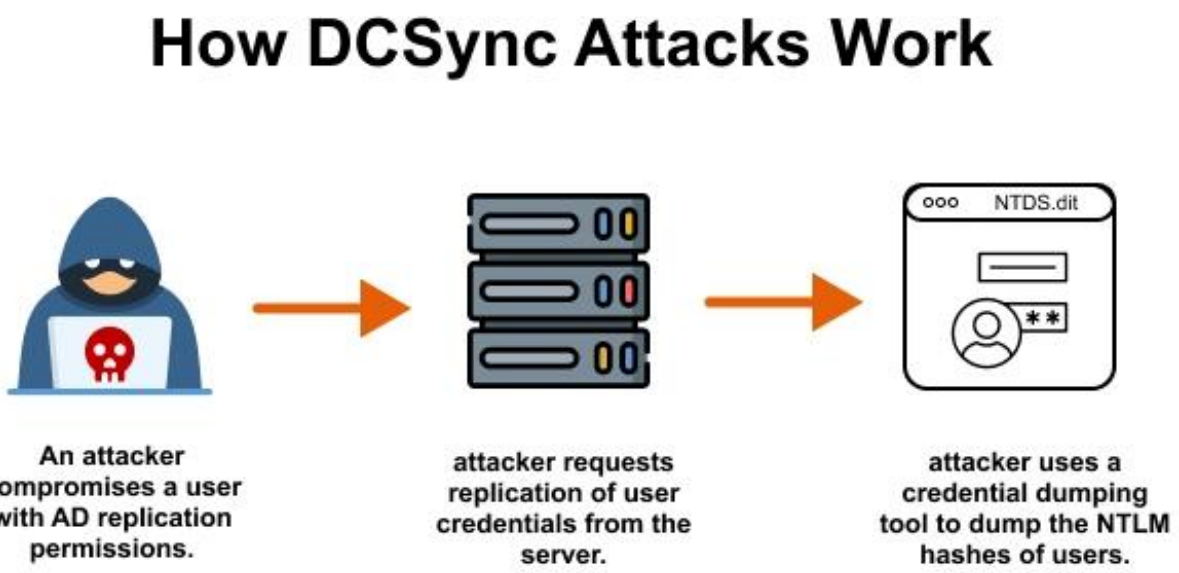
Because these attacks look just like normal replication, they blend into your traffic and audit logs. If you don't know what to watch for, you won't see the danger until it's too late.

- If you ignore replication traffic from non-DC machines, you miss the signs.
- If you trust every successful replication event in your SIEM, you'll never spot the fake ones.

How Do Attackers Carry Out a DCSync Attack?

1. **You give—or they steal—an account with replication rights.** If you've assigned "Replicate Directory Changes" or "Replicate Directory Changes All" too broadly, you've handed them the key.
2. **They pretend to be a domain controller.** With tools like Mimikatz (DsGetNCChanges)

or Windows' own ntdsutil, they spoof a legitimate DC.
3. **They pull down password hashes.** You'll never see them request "normal" data—only the hashes you keep locked down.
4. **They launch follow-on attacks.** Once they have NTLM hashes (especially KRBTGT), they can perform Pass-the-Hash or Golden Ticket attacks to roam freely.



Tip: *If you see RPC calls on port 135 from a workstation, ask yourself: "Why is this non-DC talking replication?" That simple question could stop a breach in its tracks.*

Your Active Directory is Precious! Master strategies and solution to keep it safe with our exclusive whitepaper. Discover:

- Challenge in protecting AD
- How can you get ahead of attackers?
- Setting a proactive AD Defense

[Download the Whitepaper Now!]

How Can You Detect DCSync Activity?

- **If you monitor replication traffic, you'll catch odd requests.** Watch for RPC or LDAP calls that aren't coming from your domain controllers.
- **If you audit your event logs, you'll see strange logon events.** Look at Event IDs 4662 and 4624 for replication activity tied to unexpected accounts.
- **If you baseline permissions, you'll know who really needs those rights.** Conduct regular AD privilege audits to identify which accounts actually require elevated rights.

Perform a permissions assessment to validate whether service accounts truly need replication or other high-level privileges.

Example: You run a permissions assessment and discover a print server with replication privileges. You remove that right, and now attackers can't use that server to sync your AD data.

- Must Read: DCSync Attack Detection using Network Traffic Analysis (NTA)

What Can You Do to Prevent DCSync Attacks?

1. **Enforce least privilege.** Only your domain controllers—and a tiny number of admin accounts—should have replication rights. If you grant that right to anything else, you risk handing attackers the keys to the kingdom.
2. **Harden your high-value accounts.** You must protect Enterprise Admins and the KRBTGT account with MFA and strict login policies. If you don't, attackers will target them first.
3. **Deploy real-time monitoring.** Use AD monitoring tools to alert you when replication traffic looks odd. You want to know immediately if someone's trying to sync hashes.
4. **Test your recovery plan.** Simulate a DCSync breach by rotating your KRBTGT password twice to invalidate any stolen hashes. If you can't recover in your drill, fix your plan before it's too late.

If you practice these steps regularly, you turn AD replication into a controlled process you own—rather than an attack vector you fear.

What Real-World Incidents Teach You About DCSync Risks?

1. **Mustang Panda's Southeast Asia Campaign (2021):**
   When you read about government networks in Southeast Asia, you'll see that Mustang Panda used Mimikatz's DCSync module to harvest domain-admin hashes. They forged Golden Tickets, and no one spotted unusual RPC traffic—because they never thought to look.
2. **APT20's "Operation Wocao" (2019–2023):**
   If you're in healthcare or telecom, know that these sectors were hit by spear-phishing, elevation with Mimikatz, and then DCSync to pull down KRBTGT. You can stop that attack path by running BloodHound audits to remove replication rights from any non-DC principal.
3. **Financial Institution Ransomware (2022):**
   When you tighten replication permissions and set up real-time monitoring, you won't have your trading systems encrypted in hours. That firm lost weeks recovering because they hadn't limited "*Replicate Directory Changes All*" or deployed NDR tools.
4. **Municipal IT Breach via Service Account:**
   If you don't review third-party service accounts, you could miss that a backup account with replication rights is syncing hashes. Enforce MFA on every admin-level account and remove unnecessary rights, and you'll close that blind spot.

DCSync attacks are dangerous because they let attackers quietly extract the keys to your entire Active Directory environment. Once they get domain admin privileges, they can move laterally, create backdoors, and stay hidden for months. You cannot rely on traditional monitoring alone. You need visibility across your network, detection that understands attacker behavior, and automated ways to shut down threats before they spread.

With Fidelis XDR, you get end-to-end coverage that helps you spot unusual replication requests, trace attacker movement, and respond with speed. Instead of chasing alerts, you gain one view

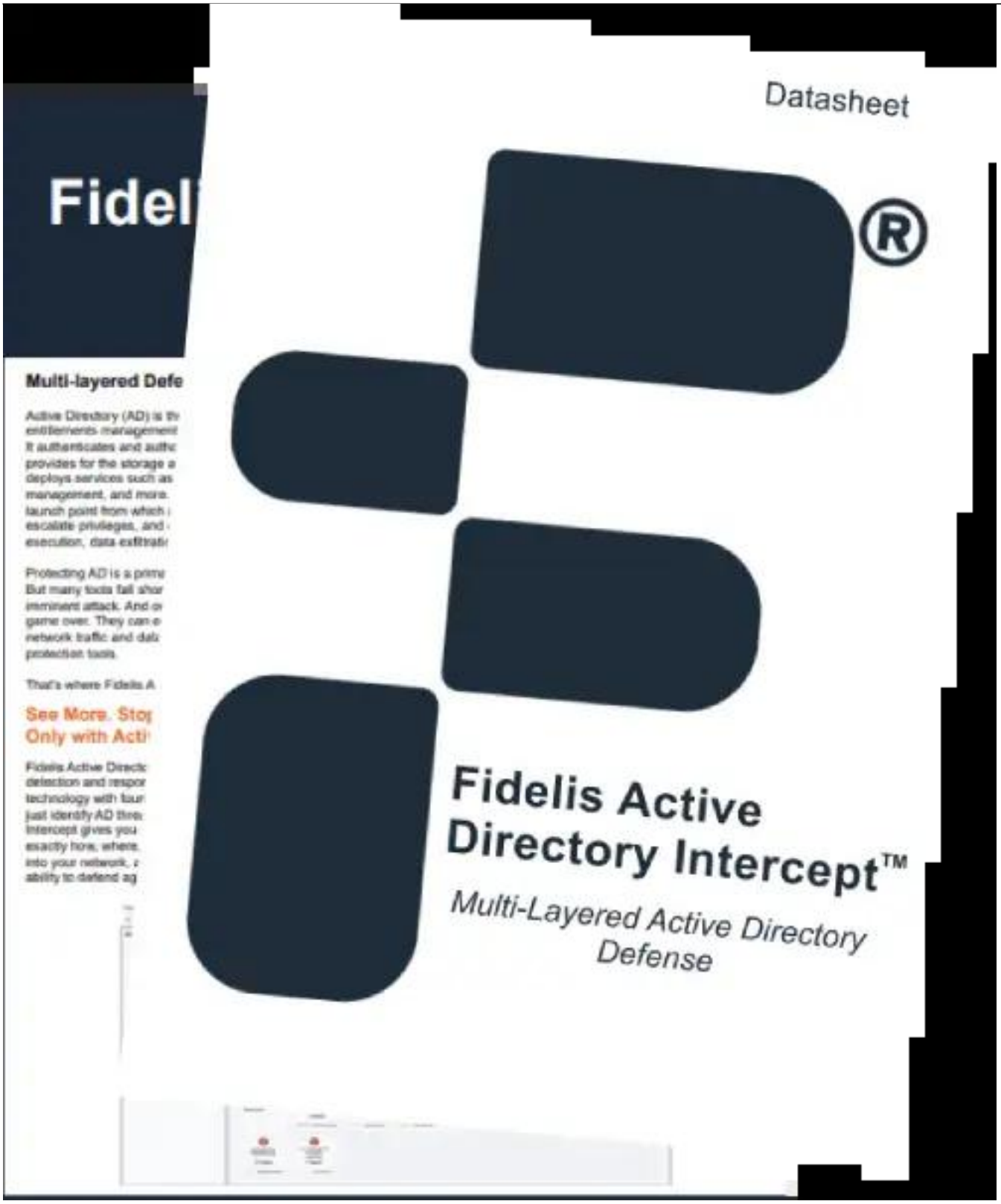
of your environment with the tools to act immediately.

Start today—because the best defense is the one you build before attackers ever knock on your door. Ready to see how Fidelis XDR can help you detect and stop DCSync attacks?

It’s time for Proactive Defense: Real-Time AD Threat Detection Against DCSync

- Defeating advanced AD Attacks and Attempts
- Active Directory Log and Event Monitoring
- How Fidelis Active Directory Intercept™ works

Download Datasheet



Frequently Ask Questions

What is a DCSync attack?

A DCSync attack allows attackers to impersonate domain controllers and extract user credentials from Active Directory by exploiting the Directory Replication Service (DRS) Remote protocol. This technique can significantly compromise an organization’s security.

How can DCSync attacks be detected?

Monitoring event logs, particularly Event ID 4624’s TargetLogonId, along with employing machine learning for anomaly detection in user behavior, is essential for effectively identifying DCSync attacks.

What are the key components targeted in DCSync attacks?

DCSync attacks primarily target domain controllers, domain admins, and sensitive accounts with elevated privileges, such as enterprise admins and service accounts. These components are appealing due to their extensive permissions, making them vital for attackers’ goals.

What steps can be taken to defend against DCSync attacks?

To effectively defend against DCSync attacks, restrict replication permissions to trusted accounts, audit high-privilege Active Directory groups regularly, and implement continuous monitoring to detect unauthorized activities. These measures can significantly enhance the security of your network.

How does Fidelis Active Directory Intercept help in protecting against DCSync attacks?

Fidelis Active Directory Intercept enhances security against DCSync attacks by integrating AD-aware network detection, deception technology, and log monitoring, allowing for swift detection and response to potential threats. This proactive approach significantly strengthens your defenses against unauthorized access and privilege escalation in Active Directory environments.