What is a DCShadow attack?

A DCShadow attack abuses Active Directory replication to inject changes as if they came from a legitimate domain controller. With sufficient rights the attacker temporarily registers a rogue DC, pushes changes (adding SIDHistory, granting DCSync rights, editing group membership), and normal replication distributes them to the real DCs. Because the change does not go through a normal admin action, most auditing misses it, which makes it a stealthy persistence and privilege technique. Defend by restricting replication rights and monitoring for unexpected DC registrations.

HOW IT WORKS

01 How the attack works

With Domain Admin (or equivalent replication rights) the attacker runs `mimikatz lsadump::dcshadow` to register a temporary DC and stage changes, then `lsadump::dcshadow /push` to replicate them. Common payloads are adding SIDHistory of a privileged group to an attacker account, granting DCSync rights on the domain object, or editing primaryGroupID. Once pushed, the rogue DC object is removed, leaving the malicious change behind. Payloads are shown for defensive testing.

SOURCES

[1] MITRE ATT&CK Enterprise Matrix

[2] Microsoft: Active Directory replication concepts

Test your Active Directory before an attacker does.

securelayer7.net/learn/active-directory/dcshadow-attack

Open online