What is SID history injection?

SID history injection abuses the sIDHistory attribute, which lets a migrated account retain the access of its old identity. An attacker writes a privileged SID (Domain Admins, Enterprise Admins, or a target domain's admin) into an account's sIDHistory, so the account inherits those rights while looking ordinary. It is used for stealthy persistence and for escalation across domain and forest trusts. Defend by monitoring sIDHistory changes, enabling SID filtering on trusts, and treating it as tier-0.

HOW IT WORKS

01 How the attack works

With sufficient rights (Domain Admin, or via DCShadow / a directory-level write) the attacker adds a privileged SID to a target account's sIDHistory, using tools such as mimikatz `sid::add` or DSInternals `Add-ADDBSidHistory`. Injecting the Enterprise Admins SID, or an admin SID from another domain in the forest, escalates the account across the boundary, since SID filtering often does not apply within a forest. Shown for defensive testing.

SOURCES

[1] MITRE ATT&CK Enterprise Matrix

[2] Microsoft: Security identifiers and SID history

Test your Active Directory before an attacker does.

securelayer7.net/learn/active-directory/sid-history-injection

Open online