What is RID hijacking?

RID hijacking is a Windows persistence technique that edits an account's relative identifier (RID), the tail of its security identifier, so a low-privilege account is treated as another, usually the built-in Administrator (RID 500). An attacker with SYSTEM modifies the account's RID in the SAM registry; the account then logs in normally but with administrator privileges, a stealthy backdoor that survives password changes. Defend by protecting SYSTEM access, monitoring SAM changes, and detecting RID anomalies.

HOW IT WORKS

01 How the attack works

With SYSTEM on a host the attacker edits the target account's F value in the SAM registry (HKLM\SAM) to set its RID to 500, using a tool such as `mimikatz misc::rid` or a direct registry edit. The low-privilege or even disabled account can then be used to log in with full administrator privileges. Because the change is in the SAM and survives reboots and password resets, it is durable local persistence. Shown for defensive testing.

SOURCES

[1] MITRE ATT&CK Enterprise Matrix

[2] Microsoft: Security identifiers

Test your Active Directory before an attacker does.

securelayer7.net/learn/active-directory/rid-hijacking

Open online