What is a skeleton key attack?

A Skeleton Key attack patches the LSASS process on a domain controller in memory so that a single attacker-chosen master password authenticates as any account, while real passwords keep working so nothing looks broken. It is a stealthy domain-wide backdoor that needs Domain Admin to deploy and is cleared by a reboot. Defend by protecting LSASS (RunAsPPL), restricting Domain Admin, and monitoring DCs for the in-memory patch.

HOW IT WORKS

01 How the attack works

With Domain Admin on a DC the attacker runs `mimikatz misc::skeleton`, which patches the running LSASS so the master password (a known default in the public tool) authenticates as any account. The attacker can then log in as any user with that one password. Because it lives only in memory, a reboot removes it, so attackers pair it with other persistence. Shown for defensive testing.

SOURCES

[1] MITRE ATT&CK Enterprise Matrix

[2] Microsoft: Configuring additional LSA protection (RunAsPPL)

Test your Active Directory before an attacker does.

securelayer7.net/learn/active-directory/skeleton-key-attack

Open online