What is trust relationship abuse?

Trust relationship abuse uses Active Directory trusts to escalate across domain and forest boundaries. With control of one domain, an attacker forges an inter-realm ticket using the trust key, or injects a privileged SID (ExtraSids) that SID filtering should strip but often does not within a forest, to gain rights in the trusting domain, commonly climbing from a child domain to Enterprise Admin in the forest root. Defend by enforcing SID filtering on external and forest trusts and treating the forest, not the domain, as the security boundary.

HOW IT WORKS

01 How the attack works

A common chain is child-to-parent: with Domain Admin in a child domain the attacker forges a Golden Ticket that adds the Enterprise Admins SID via ExtraSids (`mimikatz kerberos::golden /sids=<EA SID>` or Rubeus), and because intra-forest SID filtering is off by default, the forged ticket is accepted in the forest root, granting Enterprise Admin. Cross-forest, an attacker with the trust key can forge inter-realm TGTs to move into the trusting forest. Shown for defensive testing.

SOURCES

[1] MITRE ATT&CK Enterprise Matrix

[2] Microsoft: How Active Directory domain trusts work

Test your Active Directory before an attacker does.

securelayer7.net/learn/active-directory/trust-relationship-abuse

Open online