DCSync, Golden and Silver tickets.

These three techniques mark full domain compromise. DCSync abuses the replication right that Domain Controllers use to sync with each other: an attacker who holds it asks a real DC to hand over any account's password hash, including the KRBTGT account that signs all Kerberos tickets. With the KRBTGT hash, an attacker forges a Golden Ticket, a self-made TGT that grants access as anyone, to anything, for as long as they like. A Silver Ticket is the narrower version: a forged service ticket for one specific service, using that service account's hash. They are detection-evasive and persistent, which is why reaching this stage means a domain rebuild, not just a password reset.

HOW IT WORKS

01 Golden Tickets: forging trust itself

Every Kerberos TGT is signed with the password hash of one special account, KRBTGT. The whole domain trusts anything signed with that key.

Once an attacker has the KRBTGT hash (usually via DCSync), they can forge their own TGT, a Golden Ticket, that claims to be any user, in any group, including Domain Admins. The Domain Controllers accept it because it is signed with the key they trust. A Golden Ticket can grant access to everything, can be made valid for years, and survives the compromised user changing their password, because it does not depend on that user's password at all. It is the ultimate persistence.

02 Silver Tickets: the quieter cousin

A Silver Ticket is more surgical. Instead of forging a TGT signed by KRBTGT, the attacker forges a service ticket (TGS) for one specific service, signed with that service account's hash.

The trade-off: a Silver Ticket only opens one service (say, a specific file server or database), but it is quieter, because it never contacts the Domain Controller to request the ticket. For a targeted, low-noise foothold on a particular system, it is the preferred forgery.

03 Why this means rebuild, and how to delay it

Reaching DCSync and Golden Tickets is full compromise. Because a Golden Ticket is independent of normal passwords, the only complete remediation is to reset the KRBTGT

SOURCES

[1] MITRE ATT&CK Enterprise Matrix

[2] Microsoft: Kerberos Authentication Overview

[3] NIST SP 800-115 Technical Guide to Security Testing

account password twice (to invalidate forged tickets) and, in serious cases, rebuild trust from clean ground.

To make attackers' lives harder before that point:

- Restrict replication rights. Audit who holds DS-Replication-Get-Changes-All; it should be almost no one.
- Protect Tier 0. Domain Admin credentials should never land on ordinary machines where they can be dumped to enable DCSync in the first place.
- Rotate KRBTGT regularly so any unknown Golden Ticket has a shorter shelf life.
- Monitor for replication requests from anything that is not a Domain Controller, which is a strong DCSync signal.

> THE HARD TRUTH
>
> *Everything earlier in this section, Kerberoasting, relay, ACL abuse, AD CS, exists to reach this stage. The defensive goal is to make the chain to DCSync long and loud, because once an attacker is here, recovery means a KRBTGT double-reset and often a domain rebuild.*

Test your Active Directory before an attacker does.
securelayer7.net/learn/active-directory/dcsync-golden-silver-tickets

Open online