What is the KRBTGT account?

KRBTGT is a built-in, disabled Active Directory service account that the Key Distribution Center uses to encrypt and sign every Kerberos ticket in the domain. Its password hash is the master key of Kerberos: any Ticket Granting Ticket (TGT) is valid only because it is signed with the KRBTGT hash. If an attacker steals that hash, usually through DCSync after reaching Domain Admin, they forge a Golden Ticket that impersonates any user for as long as they want. That is why recovering from a KRBTGT compromise means resetting its password twice and treating the domain as fully breached.

HOW IT WORKS

01 The attack it enables: Golden Ticket

Because the domain trusts anything signed with the KRBTGT hash, an attacker who holds that hash can forge their own TGT, a Golden Ticket, that claims to be any account in any group, including Domain Admins.

The Domain Controllers accept it without question. A Golden Ticket grants access to everything, can be set to remain valid for years, and keeps working even after the impersonated user changes their password, because it never depended on that password. This makes KRBTGT theft the most durable persistence in Active Directory.

02 How the attack runs

First the attacker steals the KRBTGT hash, typically with a DCSync request once they hold Domain Admin rights:

- `lsadump::dcsync /domain:corp.local /user:krbtgt` (Mimikatz)
- `secretsdump.py corp.local/admin@dc -just-dc-user krbtgt` (Impacket)

Then they forge the ticket and inject it into their session:

- `kerberos::golden /user:Administrator /domain:corp.local /sid:<domain-SID> /krbtgt:<hash> /ptt` (Mimikatz)
- `Rubeus.exe golden /rc4:<krbtgt-hash> /user:Administrator /domain:corp.local /sid:<domain-SID>`

HOW TO DEFEND

- Protect Tier 0. A Golden Ticket needs the KRBTGT hash, which needs Domain Admin first. Keep privileged credentials off ordinary machines so attackers cannot reach DCSync.
- Rotate the KRBTGT password on a schedule, and crucially reset it twice (with a delay) after any suspected compromise, because a single reset leaves forged tickets temporarily valid.
- Monitor for DCSync: replication requests from anything that is not a Domain Controller are a strong signal someone is reaching for the KRBTGT hash.
- Watch for ticket anomalies, such as TGTs with unusual lifetimes, a hallmark of Golden Tickets.

SOURCES

[1] Microsoft: Kerberos Authentication Overview

[2] MITRE ATT&CK Enterprise Matrix

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

From that moment the attacker acts as a Domain Admin on demand. These are published, well-documented techniques shown here for defenders to recognise.

Test your Active Directory before an attacker does.

securelayer7.net/learn/active-directory/what-is-krbtgt

Open online