What is a Golden gMSA attack?

A Golden gMSA attack recovers the KDS root key, the domain secret that derives every group Managed Service Account (gMSA) password. With the key and a target account's attributes, the attacker computes the gMSA password offline, at any time, with no further contact with a DC, similar to a Golden Ticket but for service accounts. It is a durable persistence technique because rotating a gMSA password does not help while the root key is known. Defend by protecting the KDS root key as tier-0.

HOW IT WORKS

01 How the attack works

With rights to read the KDS root key (Domain Admin, or a principal with access to the Key Distribution Service object) the attacker extracts it and the target gMSA's attributes, then computes the password offline with a tool such as `GoldenGMSA`. The recovered password (or its hash) is then used to authenticate as the service account. Because the computation is offline, it leaves no authentication trail until the derived credential is used.

SOURCES

[1] MITRE ATT&CK Enterprise Matrix

[2] Microsoft: Group Managed Service Accounts overview

Test your Active Directory before an attacker does.

`securelayer7.net/learn/active-directory/golden-gmsa-attack`

Open online