What is AdminSDHolder abuse?

AdminSDHolder abuse is a tier-0 persistence technique. The AdminSDHolder object holds a template access control list that a process called SDProp copies onto every protected (privileged) account roughly every 60 minutes. An attacker who writes an ACE, such as GenericAll for their account, onto AdminSDHolder gets that right re-applied to all admin accounts automatically, and it self-heals if a defender removes it from an individual account. Defend by auditing and monitoring the AdminSDHolder ACL.

HOW IT WORKS

01 How the attack works

With write access to the AdminSDHolder object (CN=AdminSDHolder,CN=System,...) the attacker adds an ACE granting their account GenericAll or force-reset-password, using PowerView `Add-DomainObjectAcl` or Impacket `dacledit`. Within about an hour SDProp copies that right onto every protected admin account. If a defender strips the right from one account, SDProp restores it, which is what makes the backdoor durable. Shown for defensive testing.

SOURCES

[1] MITRE ATT&CK Enterprise Matrix

[2] Microsoft: AdminSDHolder, protected groups and SDProp

Test your Active Directory before an attacker does.

securelayer7.net/learn/active-directory/adminsdholder-abuse

Open online