What is timeroasting?

Timeroasting abuses the authenticated NTP (network time) mechanism in Windows: an unauthenticated attacker sends an NTP request referencing a computer account's RID, and the d omain controller replies with a message authentication code derived from that account's password ha sh. The attacker cracks it offline, like Kerberoasting but for machine accounts and with no credentials re quired. Machine passwords are usually long and random, so the practical risk is highest for legacy or manually-set computer accounts. Defend by ensuring strong machine passwords and monitoring.

HOW IT WORKS

01 How the attack works

The attacker queries the DC's NTP service f or many RIDs with a tool such as `timeroast.py <dc-ip>`, collecting one crackable hash per computer account. They then run the hashes through an offline cracker. Machine accounts normally use 120-character random passwords that resist cracking, so the win is on accounts with weak or manually-set passwords (legacy devices, appliances, misconfigured joins). Shown for defensive testing.

SOURCES

[1] MITRE ATT&CK Enterprise Matrix

[2] MITRE ATT&CK: Steal or Forge Kerberos Tickets

Test your Active Directory before an attacker does.

securelayer7.net/learn/active-directory/timeroasting

Open online