Valid Accounts: Domain Accounts, Sub-technique T1078.002 - Enterprise

Archived: 2026-04-05 12:54:38 UTC

G1030 Agrius

Agrius attempted to acquire valid credentials for victim environments through various means to enable follow-on lateral movement.[3]

G0022 APT3

APT3 leverages valid accounts after gaining credentials for use within the victim domain.[4]

G1023 APT5

APT5 has used legitimate account credentials to move laterally through compromised environments.[5]

G0143 Aquatic Panda

Aquatic Panda used multiple mechanisms to capture valid user accounts for victim domains to enable lateral movement and access to additional hosts in victim environments.[6]

G1043 BlackByte

BlackByte captured credentials for or impersonated domain administration users.[7][8]

G0114 Chimera

Chimera has used compromised domain accounts to gain access to the target environment.[9]

G1021 Cinnamon Tempest

Cinnamon Tempest has obtained highly privileged credentials such as domain administrator in order to deploy malware.[10]

S0154 Cobalt Strike

Cobalt Strike can use known credentials to run commands and spawn processes as a domain user account.[11][12][13]

S1024 CreepySnail

CreepySnail can use stolen credentials to authenticate on target networks.[14]

C0029 Cutting Edge

During Cutting Edge, threat actors used compromised VPN accounts for lateral movement on targeted networks.[15]

G0119 Indrik Spider

Indrik Spider has collected credentials from infected systems, including domain accounts.[16]

C0049 Leviathan Australian Intrusions

Leviathan compromised domain credentials during Leviathan Australian Intrusions.[17]

G0059 Magic Hound

Magic Hound has used domain administrator accounts after dumping LSASS process memory.[18]

G0019 Naikon

Naikon has used administrator credentials for lateral movement in compromised networks.[19]

C0002 Night Dragon

During Night Dragon, threat actors used domain accounts to gain further access to victim systems.[20]

G0049 OilRig

OilRig has used an exfiltration tool named STEALHOOK to retreive valid domain credentials.[21]

C0012 Operation CuckooBees

During Operation CuckooBees, the threat actors used compromised domain administrator credentials as part of their lateral movement.[22]

C0023 Operation Ghost

For Operation Ghost, APT29 used stolen administrator credentials for lateral movement on compromised networks.[23]

C0048 Operation MidnightEclipse

During Operation MidnightEclipse, threat actors used a compromised domain admin account to move laterally.[24]

C0014 Operation Wocao

During Operation Wocao, threat actors used domain credentials, including domain admin, for lateral movement and privilege escalation.[25]

G1040 Play

Play has used valid domain accounts for access.[26]

S0446 Ryuk

Ryuk can use stolen domain admin accounts to move laterally within a victim domain.[27]

C0059 Salesforce Data Exfiltration

During Salesforce Data Exfiltration, threat actors used compromised credentials for lateral movement.[28][29]

G0034 Sandworm Team

Sandworm Team has used stolen credentials to access administrative accounts within the domain.[30][31]

S0140 Shamoon

If Shamoon cannot access shares using current privileges, it attempts access using hard coded, domain-specific credentials gathered earlier in the intrusion.[32][33]

C0024 SolarWinds Compromise

During the SolarWinds Compromise, APT29 used domain administrators' accounts to help facilitate lateral movement on compromised networks.[34]

S0603 Stuxnet

Stuxnet attempts to access network resources with a domain account’s credentials.[35]

G0092 TA505

TA505 has used stolen domain admin accounts to compromise additional hosts.[36]

G0028 Threat Group-1314

Threat Group-1314 actors used compromised domain credentials for the victim's endpoint management platform, Altiris, to move laterally.[37]

G1022 ToddyCat

ToddyCat has used compromised domain admin credentials to mount local network shares.[38]

G1017 Volt Typhoon

Volt Typhoon has used compromised domain accounts to authenticate to devices on compromised networks.[39][40][41]

G0102 Wizard Spider

Wizard Spider has used administrative accounts, including Domain Admin, to move laterally within a victim network.[42]

Source: https://attack.mitre.org/techniques/T1078/002