Permission Groups Discovery: Local Groups, Sub-technique T1069.001 - Enterprise

Archived: 2026-04-05 14:54:52 UTC

G0018 admin@338

admin@338 actors used the following command following exploitation of a machine with LOWBALL malware to list local groups: `net localgroup administrator >> %temp%\download` [1]

S0521 BloodHound

BloodHound can collect information about local groups and members.[2]

C0015 C0015

During C0015, the threat actors used the command `net localgroup "adminstrator"` to identify accounts with local administrator rights.[3]

S0572 Caterpillar WebShell

Caterpillar WebShell can obtain a list of local groups of users from a system.[4]

G0114 Chimera

Chimera has used `net localgroup administrators` to identify accounts with local administrative rights.[5]

S0154 Cobalt Strike

Cobalt Strike can use `net localgroup` to list local groups on a system.[6]

S0082 Emissary

Emissary has the capability to execute the command `net localgroup administrators` .[7]

S0091 Epic

Epic gathers information on local group names.[8]

S1179 Exbyte

Exbyte checks whether the process is running with privileged local access during execution.[9]

S0696 Flagpro

Flagpro has been used to execute the `net localgroup administrators` command on a targeted system.[10]

S0381 FlawedAmmyy

FlawedAmmyy enumerates the privilege level of the victim during the initial infection.[11][12]

S1198 Gomir

Gomir checks the effective group ID of its process when initially executed to determine if it is in group 0, denoting superuser privileges in Linux environments.[13]

S0170 Helminth

Helminth has checked the local administrators group.[14]

G1001 HEXANE

HEXANE has run `net localgroup` to enumerate local groups.[15]

S0201 JPIN

JPIN can obtain the permissions of the victim user.[16]

S0265 Kazuar

Kazuar gathers information about local groups and members.[17]

S0236 Kwampirs

Kwampirs collects a list of users belonging to the local users and administrators groups with the commands `net localgroup administrators` and `net localgroup users`.[18]

S1141 LunarWeb

LunarWeb can discover local group memberships.[19]

S0039 Net

Commands such as `net group` and `net localgroup` can be used in Net to gather information about and manipulate groups.[20]

G0049 OilRig

OilRig has used `net localgroup administrators` to find local administrators on compromised systems.[21][22]

C0012 Operation CuckooBees

During Operation CuckooBees, the threat actors used the `net group` command as part of their advanced reconnaissance.[23]

C0014 Operation Wocao

During Operation Wocao, threat actors used the command `net localgroup administrators` to list all administrators part of a local group.[24]

S0165 OSInfo

OSInfo has enumerated the local administrators group.[25]

S0378 PoshC2

PoshC2 contains modules, such as `Get-LocAdm` for enumerating permission groups.[26]

S0184 POWRUNER

POWRUNER may collect local group information by running `net localgroup administrators` or a series of other commands on a victim.[27]

S0650 QakBot

QakBot can use `net localgroup` to enable discovery of local groups.[28][29]

S0692 SILENTTRINITY

SILENTTRINITY can obtain a list of local groups and members.[30]

S0060 Sys10

Sys10 collects the group name of the logged-in user and sends it to the C2.[31]

G0131 Tonto Team

Tonto Team has used the `ShowLocalGroupDetails` command to identify administrator, user, and guest accounts on a compromised host.[32]

G0010 Turla

Turla has used `net localgroup` and `net localgroup Administrators` to enumerate group information, including members of the local administrators group.[33]

G1017 Volt Typhoon

Volt Typhoon has run `net localgroup administrators` in compromised environments to enumerate accounts.[34]
