Account Discovery: Local Account, Sub-technique T1087.001 - Enterprise

Archived: 2026-04-05 15:40:47 UTC

G0018 admin@338

admin@338 actors used the following commands following exploitation of a machine with LOWBALL malware to enumerate user accounts: `net user >> %temp%\download` `net user /domain >> %temp%\download` [5]

S0331 Agent Tesla

Agent Tesla can collect account information from the victim's machine.[6]

G0006 APT1

APT1 used the commands `net localgroup` , `net user` , and `net group` to find accounts on the system.[1]

G0022 APT3

APT3 has used a tool that can obtain info about local and global group users, power users, and administrators.[7]

G0050 APT32

APT32 enumerated administrative users using the commands `net localgroup administrators` .[8]

G0096 APT41

APT41 used built-in `net` commands to enumerate local administrator groups.[9]

G1044 APT42

APT42 has used the PowerShell-based POWERPOST script to collect local account names from the victim machine.[10]

S0239 Bankshot

Bankshot gathers domain and account names/information through process monitoring.[11]

S0534 Bazar

Bazar can identify administrator accounts on an infected host.[12]

S0570 BitPaymer

BitPaymer can enumerate the sessions for each user logged onto the infected host.[13]

S0521 BloodHound

BloodHound can identify users with local administrator rights.[14]

G0114 Chimera

Chimera has used `net user` for account discovery.[15]

S0244 Comnie

Comnie uses the `net user` command.[16]

S0038 Duqu

The discovery modules used with Duqu can collect information on accounts and permissions.[17]

S1159 DUSTTRAP

DUSTTRAP can enumerate local user accounts.[18]

S0081 Elise

Elise executes `net user` after initial communication is made to the remote server.[19]

S0363 Empire

Empire can acquire local and domain user account information.[20]

S0091 Epic

Epic gathers a list of all user accounts, privilege classes, and time of last logon.[21]

G0117 Fox Kitten

Fox Kitten has accessed ntuser.dat and UserClass.dat on compromised hosts.[22]

S0049 GeminiDuke

GeminiDuke collects information on local user accounts from the victim.[23]

S0537 HyperStack

HyperStack can enumerate all account names on a remote share.[24]

S1245 InvisibleFerret

InvisibleFerret has queried the victim device using Python scripts to obtain the User and Hostname.[25][26]

S0260 InvisiMole

InvisiMole has a command to list account information on the victim's machine.[27]

S0265 Kazuar

Kazuar gathers information on local groups and members on the victim's machine.[28]

G0004 Ke3chang

Ke3chang performs account discovery using commands such as `net localgroup administrators` and `net group "REDACTED" /domain` on specific permissions groups.[29]

S0236 Kwampirs

Kwampirs collects a list of accounts with the command `net users`.[30]

G0030 Lotus Blossom

Lotus Blossom has used commands such as `net` to profile local system users.[31]

G1051 Medusa Group

Medusa Group has leveraged `net user` for account discovery.[32]

S1146 MgBot

MgBot includes modules for identifying local administrator accounts on victim systems.[33]

S1015 Milan

Milan has run `C:\Windows\system32\cmd.exe /c cmd /c dir c:\users\ /s 2>&1` to discover local accounts.[34]

S0084 Mis-Type

Mis-Type may create a file containing the results of the command `cmd.exe /c net user {Username}`.[35]

G1009 Moses Staff

Moses Staff has collected the administrator username from a compromised host.[36]

S0233 MURKYTOP

MURKYTOP has the capability to retrieve information about users on remote hosts.[37]

S0039 Net

Commands under `net user` can be used in Net to gather information about and manipulate user accounts.[38]

G0049 OilRig

OilRig has run `net user` , `net user /domain` , `net group "domain admins" /domain` , and `net group "Exchange Trusted Subsystem" /domain` to get account listings on a victim.[39]

C0012 Operation CuckooBees

During Operation CuckooBees, the threat actors used the `net user` command to gather account information.[40]

S0165 OSInfo

OSInfo enumerates local and domain users[7]

S0598 P.A.S. Webshell

P.A.S. Webshell can display the /etc/passwd file on a compromised host.[41]

S1145 Pikabot

Pikabot will retrieve the name of the user associated with the thread under which the malware is executing.[42]

S0453 Pony

Pony has used the `NetUserEnum` function to enumerate local accounts.[43]

G0033 Poseidon Group

Poseidon Group searches for administrator accounts on both the local victim machine and the network.[44]

S0378 PoshC2

PoshC2 can enumerate local and domain user account information.[45]

S0194 PowerSploit

PowerSploit's `Get-ProcessTokenGroup` Privesc-PowerUp module can enumerate all SIDs associated with its current token.[46][47]

S0223 POWERSTATS

POWERSTATS can retrieve usernames from compromised hosts.[48]

S0196 PUNCHBUGGY

PUNCHBUGGY can gather user names.[49]

S0192 Pupy

Pupy uses PowerView and Pywerview to perform discovery commands such as net user, net group, net local group, etc.[50]

S1242 Qilin

Qilin can list all local users found on a targeted system.[51]

S1148 Raccoon Stealer

Raccoon Stealer checks the privileges of running processes to determine if the running user is equivalent to `NT Authority\System`.[52]

S0241 RATANKBA

RATANKBA uses the `net user` command.[53]

G1039 RedCurl

RedCurl has collected information about local accounts.[54][55]

S1240 RedLine Stealer

RedLine Stealer has collected account information from the victim's machine.[56][57]

S0125 Remsec

Remsec can obtain a list of users.[58]

S0085 S-Type

S-Type has run the command `net user` on a victim.[35]

S0063 SHOTPUT

SHOTPUT has a command to retrieve information about connected users.[59]

S0649 SMOKEDHAM

SMOKEDHAM has used `net.exe user` and `net.exe users` to enumerate local accounts on a compromised host.[60]

S0516 SoreFang

SoreFang can collect usernames from the local system via `net.exe user`.[61]

S0603 Stuxnet

Stuxnet enumerates user accounts of the local host.[62]

G0027 Threat Group-3390

Threat Group-3390 has used `net user` to conduct internal discovery of systems.[63]

S0266 TrickBot

TrickBot collects the users of the system.[64][65]

G0010 Turla

Turla has used `net user` to enumerate local accounts on the system.[66][67]

S0452 USBferry

USBferry can use `net user` to gather information about local accounts.[68]

S0476 Valak

Valak has the ability to enumerate local admin accounts.[69]

G1017 Volt Typhoon

Volt Typhoon has executed `net user` and `quser` to enumerate local account information.[70]
