Account Discovery: Domain Account, Sub-technique T1087.002 - Enterprise

Archived: 2026-04-05 13:39:29 UTC

S0552 AdFind

AdFind can enumerate domain users.[2][3][4][5][6]

G0096 APT41

APT41 used built-in `net` commands to enumerate domain administrator users.[7]

S0239 Bankshot

Bankshot gathers domain and account names/information through process monitoring.[8]

S0534 Bazar

Bazar has the ability to identify domain administrator accounts.[9][10]

G1043 BlackByte

BlackByte has used tools such as AdFind to identify and enumerate domain accounts.[11]

S1068 BlackCat

BlackCat can utilize `net use` commands to identify domain users.[12]

S0521 BloodHound

BloodHound can collect information about domain users, including identification of domain admin accounts.[13]

S0635 BoomBox

BoomBox has the ability to execute an LDAP query to enumerate the distinguished name, SAM account name, and display name for all domain users.[14]

G0060 BRONZE BUTLER

BRONZE BUTLER has used `net user /domain` to identify account information.[15]

S1063 Brute Ratel C4

Brute Ratel C4 can use LDAP queries, `net group "Domain Admins" /domain` and `net user /domain` for discovery.[16][17]

G0114 Chimera

Chimera has has used `net user /dom` and `net user Administrator` to enumerate domain accounts including administrator accounts.[18][19]

S0154 Cobalt Strike

Cobalt Strike can determine if the user on an infected machine is in the admin or domain admin group.[20]

S0488 CrackMapExec

CrackMapExec can enumerate the domain user accounts on a targeted system.[21]

G0035 Dragonfly

Dragonfly has used batch scripts to enumerate users on a victim domain controller.[22]

S0105 dsquery

dsquery can be used to gather information on user accounts within a domain.[23][24]

S1159 DUSTTRAP

DUSTTRAP can enumerate domain accounts.[25]

S0363 Empire

Empire can acquire local and domain user account information.[26][27]

G1016 FIN13

FIN13 can identify user accounts associated with a Service Principal Name and query Service Principal Names within the domain by utilizing the following scripts: `GetUserSPNs.vbs` and `querySpn.vbs`.[28][29]

G0037 FIN6

FIN6 has used Metasploit's PsExec NTDSGRAB module to obtain a copy of the victim's Active Directory database.[30]

G0046 FIN7

FIN7 has used the PowerShell script 3CF9.ps1 and the executable WsTaskLoad to enumerate domain administrations by executing `net group "Domain Admins" /domain`.[31] FIN7 has also used csvde.exe, which is a built-in Windows command line tool, to export Active Directory information.

G0117 Fox Kitten

Fox Kitten has used the Softerra LDAP browser to browse documentation on service accounts.[32]

S1022 IceApple

The IceApple Active Directory Querier module can perform authenticated requests against an Active Directory server.[33]

S0483 IcedID

IcedID can query LDAP and can use built-in `net` commands to identify additional users on the network to infect.[34][35]

G1032 INC Ransom

INC Ransom has scanned for domain admin accounts in compromised environments.[36]

G0004 Ke3chang

Ke3chang performs account discovery using commands such as `net localgroup administrators` and `net group "REDACTED" /domain` on specific permissions groups.[37]

G1004 LAPSUS$

LAPSUS$ has used the AD Explorer tool to enumerate users on a victim's network.[38][39]

S1160 Latrodectus

Latrodectus can run `C:\Windows\System32\cmd.exe /c net group "Domain Admins" /domain` to identify domain administrator accounts.[40]

G0030 Lotus Blossom

Lotus Blossom has used `net` commands and tools such as AdFind to profile domain accounts associated with victim machines and make Active Directory queries.[41][42]

G0045 menuPass

menuPass has used the Microsoft administration tool csvde.exe to export Active Directory data.[43]

S1146 MgBot

MgBot includes modules for collecting information on Active Directory domain accounts.[44]

G0069 MuddyWater

MuddyWater has used `cmd.exe net user /domain` to enumerate domain users.[45]

G0129 Mustang Panda

Mustang Panda has utilized AdFind to identify domain users.[46]

S0039 Net

Net commands used with the `/domain` flag can be used to gather information about and manipulate user accounts on the current domain.[47]

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.[48]

C0012 Operation CuckooBees

During Operation CuckooBees, the threat actors used the `dsquery` and `dsget` commands to get domain environment information and to query users in administrative groups.[49]

C0022 Operation Dream Job

During Operation Dream Job, Lazarus Group queried compromised victim's active directory servers to obtain the list of employees including administrator accounts.[50]

C0014 Operation Wocao

During Operation Wocao, threat actors used the `net` command to retrieve information about domain accounts.[51]

S0165 OSInfo

OSInfo enumerates local and domain users[52]

G0033 Poseidon Group

Poseidon Group searches for administrator accounts on both the local victim machine and the network.[53]

S0378 PoshC2

PoshC2 can enumerate local and domain user account information.[54]

S0184 POWRUNER

POWRUNER may collect user account information by running `net user /domain` or a series of other commands on a victim.[55]

G1039 RedCurl

RedCurl has collected information about domain accounts using SysInternal’s AdExplorer functionality .[56][57]

G0034 Sandworm Team

Sandworm Team has used a tool to query Active Directory using LDAP, discovering information about usernames listed in AD.[58]

G1015 Scattered Spider

Scattered Spider has enumerated legitimate domain accounts which are used in the targeted environment.[59][60][61][62]

S0692 SILENTTRINITY

SILENTTRINITY can use `System.Security.AccessControl` namespaces to retrieve domain user information.[63]

C0024 SolarWinds Compromise

During the SolarWinds Compromise, APT29 used PowerShell to discover domain accounts by exectuing `Get-ADUser` and `Get-ADGroupMember`.[1][64]

S0516 SoreFang

SoreFang can enumerate domain accounts via `net.exe user /domain`.[65]

G1053 Storm-0501

Storm-0501 has utilized an obfuscated version of the Active Directory reconnaissance tool ADRecon.ps1 (obfs.ps1 or recon.ps1) to discover domain accounts.[66]

G1046 Storm-1811

Storm-1811 has performed domain account enumeration during intrusions.[67]

S0603 Stuxnet

Stuxnet enumerates user accounts of the domain.[68]

S0018 Sykipot

Sykipot may use `net group "domain admins" /domain` to display accounts in the "domain admins" permissions group and `net localgroup "administrators"` to list local system administrator group membership.[69]

G1022 ToddyCat

ToddyCat has run `net user %USER% /dom` for account discovery.[70]

G0010 Turla

Turla has used `net user /domain` to enumerate domain accounts.[71]

S0476 Valak

Valak has the ability to enumerate domain admin accounts.[72]

G1017 Volt Typhoon

Volt Typhoon has run `net group /dom` and `net group "Domain Admins" /dom` in compromised environments for account discovery.[73][74]

G0102 Wizard Spider

Wizard Spider has identified domain admins through the use of `net group "Domain admins" /DOMAIN`. Wizard Spider has also leveraged the PowerShell cmdlet `Get-ADComputer` to collect account names from Active Directory data.[10][75]
