Network Share Discovery, Technique T1135 - Enterprise

Archived: 2026-04-05 16:57:18 UTC

S1129 Akira

Akira can identify remote file shares for encryption.[3]

G0006 APT1

APT1 listed connected network shares.[4]

G0050 APT32

APT32 used the `net view` command to show all shares available, including the administrative shares such as `C$` and `ADMIN$`.[5]

G0082 APT38

APT38 has enumerated network shares on a compromised host.[6]

G0087 APT39

APT39 has used the post exploitation tool CrackMapExec to enumerate network shares.[7]

G0096 APT41

APT41 used the `net share` command as part of network reconnaissance.[8][9]

S0640 Avaddon

Avaddon has enumerated shared folders and mapped volumes.[10]

S1053 AvosLocker

AvosLocker has enumerated shared drives on a compromised network.[11][12]

S0638 Babuk

Babuk has the ability to enumerate network shares.[13]

S0606 Bad Rabbit

Bad Rabbit enumerates open SMB shares on internal victim networks.[14]

S1081 BADHATCH

BADHATCH can check a user's access to the C$ share on a compromised machine.[15]

S0534 Bazar

Bazar can enumerate shared drives on the domain.[16]

S0570 BitPaymer

BitPaymer can search for network shares on the domain or workgroup using `net view`.[17]

G1043 BlackByte

BlackByte enumerated network shares on victim devices.[18]

S1181 BlackByte 2.0 Ransomware

BlackByte 2.0 Ransomware can identify network shares connected to the victim machine.[19]

S1180 BlackByte Ransomware

BlackByte Ransomware can identify network shares connected to the victim machine.[20]

S1068 BlackCat

BlackCat has the ability to discover network shares on compromised networks.[21][22]

C0015 C0015

During C0015, the threat actors executed the PowerView ShareFinder module to identify open shares.[23]

G0114 Chimera

Chimera has used `net share` and `net view` to identify network shares of interest.[24]

S0660 Clambling

Clambling has the ability to enumerate network shares.[25]

S0611 Clop

Clop can enumerate network shares.[26]

S0154 Cobalt Strike

Cobalt Strike can query shared drives on the local system.[27]

S0575 Conti

Conti can enumerate remote open SMB network shares using `NetShareEnum()`.[28][29]

S0488 CrackMapExec

CrackMapExec can enumerate the shared folders and associated permissions for a targeted network.[30]

S0625 Cuba

Cuba can discover shared resources using the `NetShareEnum` API call.[31]

G0105 DarkVishnya

DarkVishnya scanned the network for public shared folders.[32]

S0616 DEATHRANSOM

DEATHRANSOM has the ability to use loop operations to enumerate network resources.[33]

S0659 Diavol

Diavol has a `ENMDSKS` command to enumerates available network shares.[34]

G0035 Dragonfly

Dragonfly has identified and browsed file servers in the victim network, sometimes , viewing files pertaining to ICS or Supervisory Control and Data Acquisition (SCADA) systems.[35]

S1159 DUSTTRAP

DUSTTRAP can identify and enumerate victim system network shares.[36]

S1247 Embargo

Embargo has searched for folders, subfolders and other networked or mounted drives for follow-on encryption actions.[37]

S0367 Emotet

Emotet has enumerated non-hidden network shares using `WNetEnumResourceW` . [38]

S0363 Empire

Empire can find shared drives on the local system.[39]

G1016 FIN13

FIN13 has executed net view commands for enumeration of open shares on compromised machines.[40][41]

S0618 FIVEHANDS

FIVEHANDS can enumerate network shares and mounted drives on a network.[42]

S0696 Flagpro

Flagpro has been used to execute `net view` to discover mapped network shares.[43]

S0617 HELLOKITTY

HELLOKITTY has the ability to enumerate network resources.[33]

S0483 IcedID

IcedID has used the `net view /all` command to show available shares.[44]

G1032 INC Ransom

INC Ransom has used Internet Explorer to view folders on other systems.[45]

S1139 INC Ransomware

INC Ransomware has the ability to check for shared network drives to encrypt.[46]

S0260 InvisiMole

InvisiMole can gather network share information.[47]

S0250 Koadic

Koadic can scan local network for open SMB.[48]

S1075 KOPILUWAK

KOPILUWAK can use netstat and Net to discover network shares.[49]

S0236 Kwampirs

Kwampirs collects a list of network shares with the command `net share`.[50]

S1160 Latrodectus

Latrodectus can run `C:\Windows\System32\cmd.exe /c net view /all` to discover network shares.[51][52]

C0049 Leviathan Australian Intrusions

Leviathan scanned and enumerated remote network shares in victim environments during Leviathan Australian Intrusions.[53]

S1199 LockBit 2.0

LockBit 2.0 can discover remote shares.[54]

S1202 LockBit 3.0

LockBit 3.0 can identify network shares on compromised systems.[55]

S1141 LunarWeb

LunarWeb can identify shared resources in compromised environments.[56]

G1051 Medusa Group

Medusa Group has identified network shares using `cmd.exe /c net share`.[57]

S1244 Medusa Ransomware

Medusa Ransomware has identified networked drives.[58][59][60]

S0233 MURKYTOP

MURKYTOP has the capability to retrieve information about shares on remote hosts.[61]

S0039 Net

The `net view \remotesystem` and `net share` commands in Net can be used to find shared drives and directories on remote and local systems respectively.[62]

S0365 Olympic Destroyer

Olympic Destroyer will attempt to enumerate mapped network shares to later attempt to wipe all files on those shares.[63]

C0012 Operation CuckooBees

During Operation CuckooBees, the threat actors used the `net share` command as part of their advanced reconnaissance.[64]

C0014 Operation Wocao

During Operation Wocao, threat actors discovered network disks mounted to the system using netstat.[65]

S0165 OSInfo

OSInfo discovers shares on the network[66]

S0013 PlugX

PlugX has a module to enumerate network shares.[67][68]

S0192 Pupy

Pupy can list local and remote shared drives and folders over SMB.[69]

S0650 QakBot

QakBot can use `net share` to identify network shares for use in lateral movement.[70][71]

S1242 Qilin

Qilin has the ability to list network drives.[72][73]

S0686 QuietSieve

QuietSieve can identify and search networked drives for specific file name extensions.[74]

S0458 Ramsay

Ramsay can scan for network drives which may contain documents for collection.[75][76]

S1212 RansomHub

RansomHub has the ability to target specific network shares for encryption.[77]

S1073 Royal

Royal can enumerate the shared resources of a given IP addresses using the API call `NetShareEnum`.[78]

S1085 Sardonic

Sardonic has the ability to execute the `net view` command.[79]

S0444 ShimRat

ShimRat can enumerate connected drives for infected host machines.[80]

S0692 SILENTTRINITY

SILENTTRINITY can enumerate shares on a compromised host.[81]

G0054 Sowbug

Sowbug listed remote shared drives that were accessible from a victim.[82]

S0603 Stuxnet

Stuxnet enumerates the directories of a network resource.[83]

G0131 Tonto Team

Tonto Team has used tools such as NBTscan to enumerate network shares.[84]

S0266 TrickBot

TrickBot module shareDll/mshareDll discovers network shares via the WNetOpenEnumA API.[85][86]

G0081 Tropic Trooper

Tropic Trooper used `netview` to scan target systems for shared resources.[87]

S0612 WastedLocker

WastedLocker can identify network adjacent and accessible drives.[88]

S0689 WhisperGate

WhisperGate can enumerate connected remote logical drives.[89]

G0102 Wizard Spider

Wizard Spider has used the "net view" command to locate mapped network shares.[90]

S0251 Zebrocy

Zebrocy identifies network drives when they are added to victim systems.[91]

Source: https://attack.mitre.org/techniques/T1135