System Network Connections Discovery, Technique T1049 - Enterprise

Archived: 2026-04-05 18:24:17 UTC

G0018 admin@338

admin@338 actors used the following command following exploitation of a machine with LOWBALL malware to display network connections: `netstat -ano >> %temp%\download` [6]

G0138 Andariel

Andariel has used the `netstat -naop tcp` command to display TCP connections on a victim's machine.[7]

G0006 APT1

APT1 used the `net use` command to get a listing on network connections.[8]

G0022 APT3

APT3 has a tool that can enumerate current network connections.[9][10][11]

G0050 APT32

APT32 used the `netstat -anpo tcp` command to display TCP connections on the victim's machine.[12]

G0082 APT38

APT38 installed a port monitoring tool, MAPMAKER, to print the active TCP connections on the local system. [13]

G0096 APT41

APT41 has enumerated IP addresses of network resources and used the `netstat` command as part of network reconnaissance. The group has also used a malware variant, HIGHNOON, to enumerate active RDP sessions.[14] [15]

G1023 APT5

APT5 has used the BLOODMINE utility to collect data on web requests from Pulse Secure Connect logs.[16]

S0456 Aria-body

Aria-body has the ability to gather TCP and UDP table status listings.[17]

S0638 Babuk

Babuk can use "WNetOpenEnumW" and "WNetEnumResourceW" to enumerate files in network resources for encryption.[18]

G0135 BackdoorDiplomacy

BackdoorDiplomacy has used NetCat and PortQry to enumerate network connections and display the status of related TCP and UDP ports.[19]

S1081 BADHATCH

BADHATCH can execute `netstat.exe -f` on a compromised machine.[20]

S0089 BlackEnergy

BlackEnergy has gathered information about local network connections using netstat.[21][22]

S0335 Carbon

Carbon uses the `netstat -r` and `netstat -an` commands.[23]

G0114 Chimera

Chimera has used `netstat -ano | findstr EST` to discover network connections.[24]

S0154 Cobalt Strike

Cobalt Strike can produce a sessions report from compromised hosts.[25]

S0244 Comnie

Comnie executes the `netstat -ano` command.[26]

S0575 Conti

Conti can enumerate routine network connections from a compromised host.[27]

S0488 CrackMapExec

CrackMapExec can discover active sessions for a targeted system.[28]

S0625 Cuba

Cuba can use the function `GetIpNetTable` to recover the last connections to the victim's machine.[29]

S0567 Dtrack

Dtrack can collect network and active connection information.[30]

S0038 Duqu

The discovery modules used with Duqu can collect information on network connections.[31]

G1006 Earth Lusca

Earth Lusca employed a PowerShell script called RDPConnectionParser to read and filter the Windows event log "Microsoft-Windows-TerminalServices-RDPClient/Operational"
(Event ID 1024) to obtain network information from RDP connections. Earth Lusca has also used netstat from a compromised system to obtain network connection information.[32]

S0554 Egregor

Egregor can enumerate all connected drives.[33]

S0363 Empire

Empire can enumerate the current network connections of a host.[34]

S0091 Epic

Epic uses the `net use` , `net session` , and `netstat` commands to gather information on network connections.[35][36]

G1016 FIN13

FIN13 has used `netstat` and other net commands for network reconnaissance efforts.[37]

S0696 Flagpro

Flagpro has been used to execute `netstat -ano` on a compromised host.[38]

S1144 FRP

FRP can use a dashboard and U/I to display the status of connections from the FRP client and server.[39]

C0007 FunnyDream

During FunnyDream, the threat actors used netstat to discover network connections on remote systems.[40]

G0093 GALLIUM

GALLIUM used `netstat -oan` to obtain information about the victim network connections.[41]

S0237 GravityRAT

GravityRAT uses the `netstat` command to find open ports on the victim’s machine.[42]

G1001 HEXANE

HEXANE has used netstat to monitor connections to specific ports.[43]

G1032 INC Ransom

INC Ransom has used RDP to test network connections.[44]

S0283 jRAT

jRAT can list network connections.[45]

G0004 Ke3chang

Ke3chang performs local network connection discovery using `netstat`.[46][47]

S0356 KONNI

KONNI has used `net session` on the victim's machine.[48]

S1075 KOPILUWAK

KOPILUWAK can use netstat, Arp, and Net to discover current TCP connections.[49]

S0236 Kwampirs

Kwampirs collects a list of active and listening connections by using the command `netstat -nao` as well as a list of available network mappings with `net use`.[50]

G0032 Lazarus Group

Lazarus Group has used `net use` to identify and establish a network connection with a remote host.[51]

S0681 Lizar

Lizar has a plugin to retrieve information about all active network sessions on the infected server.[52]

G0030 Lotus Blossom

Lotus Blossom has used commands such as `netstat` to identify system network connections.[53]

S0532 Lucifer

Lucifer can identify the IP and port numbers for all remote connections from the compromised host.[54]

S1141 LunarWeb

LunarWeb can enumerate system network connections.[55]

S1060 Mafalda

Mafalda can use the `GetExtendedTcpTable` function to retrieve information about established TCP connections.[56]

G0059 Magic Hound

Magic Hound has used quser.exe to identify existing RDP connections.[57]

S0449 Maze

Maze has used the "WNetOpenEnumW", "WNetEnumResourceW", "WNetCloseEnum" and "WNetAddConnection2W" functions to enumerate the network resources on the infected machine.[58]

G0045 menuPass

menuPass has used `net use` to conduct connectivity checks to machines.[59]

S0443 MESSAGETAP

After loading the keyword and phone data files, MESSAGETAP begins monitoring all network connections to and from the victim server. [60]

G0069 MuddyWater

MuddyWater has used a PowerShell backdoor to check for Skype connections on the target machine.[61]

G0129 Mustang Panda

Mustang Panda has used `netstat -ano` to determine network connection information.[62]

S0102 nbtstat

nbtstat can be used to discover current NetBIOS sessions.

S0039 Net

Commands such as `net use` and `net session` can be used in Net to gather information about network connections from a particular host.[63]

S0104 netstat

netstat can be used to enumerate local network connections, including active TCP connections and other network statistics.[64]

S0198 NETWIRE

NETWIRE can capture session logon details from a compromised host.[65]

G0049 OilRig

OilRig has used `netstat -an` on a victim to get a listing of network connections.[66]

S0439 Okrum

Okrum was seen using NetSess to discover NetBIOS sessions.[67]

C0012 Operation CuckooBees

During Operation CuckooBees, the threat actors used the `net session`, `net use`, and `netstat` commands as part of their advanced reconnaissance.[68]

C0014 Operation Wocao

During Operation Wocao, threat actors collected a list of open connections on the infected system using `netstat` and checks whether it has an internet connection.[69]

S0165 OSInfo

OSInfo enumerates the current network connections similar to `net use`.[9]

S1091 Pacu

Once inside a Virtual Private Cloud, Pacu can attempt to identify DirectConnect, VPN, or VPC Peering.[70]

S0013 PlugX

PlugX has a module for enumerating TCP and UDP network connections and associated processes using the `netstat` command.[71]

G0033 Poseidon Group

Poseidon Group obtains and saves information about victim network interfaces and addresses.[72]

S0378 PoshC2

PoshC2 contains an implementation of netstat to enumerate TCP and UDP connections.[73]

S0184 POWRUNER

POWRUNER may collect active network connections by running `netstat -an` on a victim.[74]

S1228 PUBLOAD

PUBLOAD has used several commands executed in sequence via `cmd` in a short interval to gather information on network connections.[75]

S0192 Pupy

Pupy has a built-in utility command for `netstat`, can do net session through PowerView, and has an interactive shell which can be used to discover additional information.[76]

S1032 PyDCrypt

PyDCrypt has used netsh to find RPC connections on remote machines.[77]

S0650 QakBot

QakBot can use `netstat` to enumerate current network connections.[78][79]

S0458 Ramsay

Ramsay can use `netstat` to enumerate network connections.[80]

S0241 RATANKBA

RATANKBA uses `netstat -ano` to search for specific IP address ranges.[81]

S0153 RedLeaves

RedLeaves can enumerate drives and Remote Desktop sessions.[82]

S0125 Remsec

Remsec can obtain a list of active connections and open ports.[83]

G0034 Sandworm Team

Sandworm Team had gathered user, IP address, and server data related to RDP sessions on a compromised host. It has also accessed network diagram files useful for understanding how a host's network was configured.[84][85]

S1085 Sardonic

Sardonic has the ability to execute the `netstat` command.[86]

S0445 ShimRatReporter

ShimRatReporter used the Windows function `GetExtendedUdpTable` to detect connected UDP endpoints.[87]

S0063 SHOTPUT

SHOTPUT uses netstat to list TCP connection status.[88]

S0589 Sibot

Sibot has retrieved a GUID associated with a present LAN connection on a compromised machine.[89]

S0633 Sliver

Sliver can collect network connection information.[90]

S0533 SLOTHFULMEDIA

SLOTHFULMEDIA can enumerate open ports on a victim machine.[91]

S0374 SpeakUp

SpeakUp uses the `arp -a` command. [92]

S0018 Sykipot

Sykipot may use `netstat -ano` to display active network connections.[93]

G0139 TeamTNT

TeamTNT has run `netstat -anp` to search for rival malware connections.[94] TeamTNT has also used `libprocesshider` to modify `/etc/ld.so.preload`.[95]

G0027 Threat Group-3390

Threat Group-3390 has used `net use` and `netstat` to conduct internal discovery of systems. The group has also used `quser.exe` to identify existing RDP sessions on a victim.[96]

G1022 ToddyCat

ToddyCat has used `netstat -anop tcp` to discover TCP connections to compromised hosts.[97]

S0678 Torisma

Torisma can use `WTSEnumerateSessionsW` to monitor remote desktop connections.[98]

S0094 Trojan.Karagany

Trojan.Karagany can use netstat to collect a list of network connections.[99]

G0081 Tropic Trooper

Tropic Trooper has tested if the localhost network is available and other connection capability on an infected system using command scripts.[100]

G0010 Turla

Turla surveys a system upon check-in to discover active local network connections using the `netstat -an`, `net use`, `net file`, and `net session` commands.[35][101] Turla RPC backdoors have also enumerated the IPv4 TCP connection table via the `GetTcpTable2` API call.[102]

S0452 USBferry

USBferry can use `netstat` and `nbtstat` to detect active network connections.[100]

G1047 Velvet Ant

Velvet Ant has enumerated existing network connections on victim devices.[103]

S0180 Volgmer

Volgmer can gather information about TCP connection state.[104]

G1017 Volt Typhoon

Volt Typhoon has used `netstat -ano` on compromised hosts to enumerate network connections.[105][106]

S0579 Waterbear

Waterbear can use API hooks on `GetExtendedTcpTable` to retrieve a table containing a list of TCP endpoints available to the application.[107]

S0251 Zebrocy

Zebrocy uses `netstat -aon` to gather network connection information.[108]
