System Network Configuration Discovery, Technique T1016 - Enterprise

Archived: 2026-04-02 12:30:18 UTC

S1028 Action RAT

Action RAT has the ability to collect the MAC address of an infected host.[4]

S0552 AdFind

AdFind can extract subnet information from Active Directory.[5][6][7]

G0018 admin@338

admin@338 actors used the following command after exploiting a machine with LOWBALL malware to acquire information about local networks: `ipconfig /all >> %temp%\download` [8]

S0331 Agent Tesla

Agent Tesla can collect the IP address of the victim machine and spawn instances of netsh.exe to enumerate wireless settings.[9][10]

S0092 Agent.btz

Agent.btz collects the network adapter's IP and MAC address as well as IP addresses of the network adapter's default gateway, primary/secondary WINS, DHCP, and DNS servers, and saves them into a log file.[11]

S1025 Amadey

Amadey can identify the IP address of a victim machine.[12]

S0504 Anchor

Anchor can determine the public IP and location of a compromised host.[13]

S0622 AppleSeed

AppleSeed can identify the IP of a targeted system.[14]

G0006 APT1

APT1 used the `ipconfig /all` command to gather network configuration information.[15]

G0073 APT19

APT19 used an HTTP malware variant and a Port 22 malware variant to collect the MAC address and IP address from the victim's machine.[16]

G0022 APT3

A keylogging tool used by APT3 gathers network information from the victim, including the MAC address, IP address, WINS, DHCP server, and gateway.[17][18]

G0050 APT32

APT32 used the `ipconfig /all` command to gather the IP address from the system.[19]

G0096 APT41

APT41 collected MAC addresses from victim machines.[20][21]

G1044 APT42

APT42 has used malware, such as GHAMBAR and POWERPOST, to collect network information.[22]

S0456 Aria-body

Aria-body has the ability to identify the location, public IP address, and domain name on a compromised host.[23]

S0099 Arp

Arp can be used to display ARP configuration information on the host.[24]

S0373 Astaroth

Astaroth collects the external IP address from the system. [25]

S0640 Avaddon

Avaddon can collect the external IP address of the victim.[26]

S0473 Avenger

Avenger can identify the domain of the compromised host.[27]

S0344 Azorult

Azorult can collect host IP information from the victim's machine.[28]

S0414 BabyShark

BabyShark has executed the `ipconfig /all` command.[29]

S0093 Backdoor.Oldrea

Backdoor.Oldrea collects information about the Internet adapter configuration.[30][31]

S0245 BADCALL

BADCALL collects the network adapter information.[32]

S0642 BADFLICK

BADFLICK has captured victim IP address details.[33]

S0234 Bandook

Bandook has a command to get the public IP address from a system.[34]

S0534 Bazar

Bazar can collect the IP address and NetBIOS name of an infected machine.[35]

S0268 Bisonal

Bisonal can execute `ipconfig` on the victim’s machine.[36][37][38]

G1043 BlackByte

BlackByte used tools such as Arp to pull system network information and identify connected devices.[39][40]

S0089 BlackEnergy

BlackEnergy has gathered information about network IP configurations using ipconfig.exe and about routing tables using route.exe.[41][42]

S0520 BLINDINGCAN

BLINDINGCAN has collected the victim machine's local IP address information and MAC address.[43]

S0657 BLUELIGHT

BLUELIGHT can collect IP information from the victim’s machine.[44]

S1184 BOLDMOVE

BOLDMOVE enumerates network interfaces on the infected host.[45]

S0486 Bonadan

Bonadan can find the external IP address of the infected host.[46]

S0651 BoxCaon

BoxCaon can collect the victim's MAC address by using the `GetAdaptersInfo` API.[47]

S0252 Brave Prince

Brave Prince gathers network configuration information as well as the ARP cache.[48]

C0015 C0015

During C0015, the threat actors used code to obtain the external public-facing IPv4 address of the compromised host.[49]

C0017 C0017

During C0017, APT41 used `cmd.exe /c ping %userdomain%` for discovery.[50]

C0018 C0018

During C0018, the threat actors ran `nslookup` and Advanced IP Scanner on the target network.[51]

S0274 Calisto

Calisto runs the `ifconfig` command to obtain the IP address from the victim's machine.[52]

S0335 Carbon

Carbon can collect the IP address of the victims and other computers on the network using the commands: `ipconfig -all` `nbtstat -n`, and `nbtstat -s`.[53][54]

S0261 Catchamas

Catchamas gathers the Mac address, IP address, and the network adapter information from the victim's machine.[55]

S0572 Caterpillar WebShell

Caterpillar WebShell can gather the IP address from the victim's machine using the IP config command.[56]

S1204 cd00r

cd00r can discover the IP for the network interface on the compromised device.[57]

S0674 CharmPower

CharmPower has the ability to use `ipconfig` to enumerate system network settings.[58]

G0114 Chimera

Chimera has used ipconfig, Ping, and `tracert` to enumerate the IP address and network environment and settings of the local host.[59]

S0667 Chrommme

Chrommme can enumerate the IP address of a compromised host.[60]

S0660 Clambling

Clambling can enumerate the IP address of a compromised machine.[61][62]

S0154 Cobalt Strike

Cobalt Strike can determine the NetBios name and the IP addresses of targets machines including domain controllers.[63][64]

S0244 Comnie

Comnie uses `ipconfig /all` and `route PRINT` to identify network adapter and interface information.[65]

S0575 Conti

Conti can retrieve the ARP cache from the local system by using the `GetIpNetTable()` API call and check to ensure IP addresses it connects to are for local, non-Internet, systems.[66]

S0488 CrackMapExec

CrackMapExec can collect DNS information from the targeted system.[67]

S1024 CreepySnail

CreepySnail can use `getmac` and `Get-NetIPAddress` to enumerate network settings.[68]

S0115 Crimson

Crimson contains a command to collect the victim MAC address and LAN IP.[69][70]

S0625 Cuba

Cuba can retrieve the ARP cache from the local system by using `GetIpNetTable`.[71]

S0687 Cyclops Blink

Cyclops Blink can use the Linux API `if_nameindex` to gather network interface names.[72][73]

G0012 Darkhotel

Darkhotel has collected the IP address and network adapter information from the victim's machine.[74][75]

S1052 DEADEYE

DEADEYE can discover the DNS domain name of a targeted system.[50]

S0354 Denis

Denis uses `ipconfig` to gather the IP address from the system.[19]

S0659 Diavol

Diavol can enumerate victims' local and external IPs when registering with C2.[76]

S0472 down_new

down_new has the ability to identify the MAC address of a compromised host.[27]

G0035 Dragonfly

Dragonfly has used batch scripts to enumerate network information, including information about trusts, zones, and the domain.[77]

S0567 Dtrack

Dtrack can collect the host's IP addresses using the `ipconfig` command.[78][79]

S0038 Duqu

The reconnaissance modules used with Duqu can collect information on network configuration.[80]

S1159 DUSTTRAP

DUSTTRAP can enumerate infected system network information.[81]

S0024 Dyre

Dyre has the ability to identify network settings on a compromised host.[82]

G1006 Earth Lusca

Earth Lusca used the command `ipconfig` to obtain information about network configurations.[83]

S0605 EKANS

EKANS can determine the domain of a compromised host.[84]

S0081 Elise

Elise executes `ipconfig /all` after initial communication is made to the remote server.[85][86]

S0082 Emissary

Emissary has the capability to execute the command `ipconfig /all`.[87]

S0363 Empire

Empire can acquire network configuration information like DNS servers, public IP, and network proxies used by a host.[88][89]

S0091 Epic

Epic uses the `nbtstat -n` and `nbtstat -s` commands on the victim's machine.[90]

S0569 Explosive

Explosive has collected the MAC address from the victim's machine.[91]

S0181 FALLCHILL

FALLCHILL collects MAC address and local IP address information from the victim.[92]

S0512 FatDuke

FatDuke can identify the MAC address on the target computer.[93]

S0171 Felismus

Felismus collects the victim LAN IP address and sends it to the C2 server.[94]

S0267 FELIXROOT

FELIXROOT collects information about the network including the IP address and DHCP server.[95]

G1016 FIN13

FIN13 has used `nslookup` and `ipconfig` for network reconnaissance efforts. FIN13 has also utilized a compromised Symantec Altiris console and LanDesk account to retrieve network information.[96][97]

S0696 Flagpro

Flagpro has been used to execute the `ipconfig /all` command on a victim system.[98]

C0001 Frankenstein

During Frankenstein, the threat actors used Empire to find the public IP address of a compromised system.[89]

S1044 FunnyDream

FunnyDream can parse the `ProxyServer` string in the Registry to discover http proxies.[99]

C0007 FunnyDream

During FunnyDream, the threat actors used ipconfig for discovery on remote systems.[99]

G0093 GALLIUM

GALLIUM used `ipconfig /all` to obtain information about the victim network configuration. The group also ran a modified version of NBTscan to identify available NetBIOS name servers.[100]

S0049 GeminiDuke

GeminiDuke collects information on network settings and Internet proxy settings from the victim.[101]

S0588 GoldMax

GoldMax retrieved a list of the system's network interface after execution.[102]

S1198 Gomir

Gomir collects network information on infected systems such as listing interface names, MAC and IP addresses, and IPv6 addresses.[103]

S1138 Gootloader

Gootloader can use an embedded script to check the IP address of potential victims visiting compromised websites.[104]

S0531 Grandoreiro

Grandoreiro can determine the IP and physical location of the compromised host via IPinfo.[105]

S0237 GravityRAT

GravityRAT collects the victim IP address, MAC address, as well as the victim account domain name.[106]

S0690 Green Lambert

Green Lambert can obtain proxy information from a victim's machine using system environment variables.[107] [108]

S0632 GrimAgent

GrimAgent can enumerate the IP and domain of a target system.[109]

G0125 HAFNIUM

HAFNIUM has collected IP information via IPInfo.[110]

S1229 Havoc

Havoc has a module for network enumeration including determining IP addresses.[111]

G1001 HEXANE

HEXANE has used Ping and `tracert` for network discovery.[112]

S1249 HexEval Loader

HexEval Loader has leveraged server-side client configurations to identify the public IP of the victim host.[113]

G0126 Higaisa

Higaisa used `ipconfig` to gather network configuration information.[114][115]

S0431 HotCroissant

HotCroissant has the ability to identify the IP address of the compromised machine.[116]

S0203 Hydraq

Hydraq creates a backdoor through which remote attackers can retrieve IP addresses of compromised machines.[117][118]

S1022 IceApple

The IceApple ifconfig module can iterate over all network interfaces on the host and retrieve the name, description, MAC address, DNS suffix, DNS servers, gateways, IPv4 addresses, and subnet masks.[119]

S0483 IcedID

IcedID used the `ipconfig /all` command and a batch script to gather network information.[120]

S0101 ifconfig

ifconfig can be used to display adapter configuration on Unix systems, including information for TCP/IP, DNS, and DHCP.

S0278 iKitten

iKitten will look for the current IP address.[121]

S0604 Industroyer

Industroyer's 61850 payload component enumerates connected network adapters and their corresponding IP addresses.[122]

S1245 InvisibleFerret

InvisibleFerret has collected the local IP address, and external IP.[123][124]

S0260 InvisiMole

InvisiMole gathers information on the IP forwarding table, MAC address, configured proxy, and network SSID.[125][126]

S0100 ipconfig

ipconfig can be used to display adapter configuration on Windows systems, including information for TCP/IP, DNS, and DHCP.

S0015 Ixeshe

Ixeshe enumerates the IP address, network proxy settings, and domain name from a victim's system.[127]

S1203 J-magic

J-magic can compare the host and remote IPs to check if a received packet is from the infected machine.[128]

S0044 JHUHUGIT

A JHUHUGIT variant gathers network interface card information.[129]

S0201 JPIN

JPIN can obtain network information, including DNS, IP, and proxies.[130]

S0283 jRAT

jRAT can gather victim internal and external IPs.[131]

S0265 Kazuar

Kazuar gathers information about network adapters.[132]

G0004 Ke3chang

Ke3chang has performed local network configuration discovery using `ipconfig`.[133][134][135]

S0487 Kessel

Kessel has collected the DNS address of the infected host.[46]

S1020 Kevin

Kevin can collect the MAC address and other information from a victim machine using `ipconfig/all`.[112]

S0387 KeyBoy

KeyBoy can determine the public or WAN IP address for the system.[136]

S0271 KEYMARBLE

KEYMARBLE gathers the MAC address of the victim’s machine.[137]

G0094 Kimsuky

Kimsuky has used `ipconfig/all` and web beacons sent via email to gather network configuration information.[138][139] Kimsuky has also identified Host IP addresses leveraging the WMI class `Win32_NetworkAdapterConfiguration`.[140]

S0250 Koadic

Koadic can retrieve the contents of the IP routing table as well as information about the Windows domain.[141][142]

S0641 Kobalos

Kobalos can record the IP address of the target machine.[143]

S0356 KONNI

KONNI can collect the IP address from the victim’s machine.[144]

S1075 KOPILUWAK

KOPILUWAK can use Arp to discover a target's network configuration setttings.[145]

C0035 KV Botnet Activity

KV Botnet Activity gathers victim IP information during initial installation stages.[146]

S0236 Kwampirs

Kwampirs collects network adapter and interface information by using the commands `ipconfig /all`, `arp -a` and `route print`. It also collects the system's MAC address with `getmac` and domain configuration with `net config workstation`.[147]

S1160 Latrodectus

Latrodectus can discover the IP and MAC address of a targeted host.[148][149]

G0032 Lazarus Group

Lazarus Group malware IndiaIndia obtains and sends to its C2 server information about the first network interface card’s configuration, including IP address, gateways, subnet mask, DHCP information, and whether WINS is available.[150][151]

S0395 LightNeuron

LightNeuron gathers information about network adapters using the Win32 API call `GetAdaptersInfo`.[152]

S0513 LiteDuke

LiteDuke has the ability to discover the proxy configuration of Firefox and/or Opera.[93]

S0681 Lizar

Lizar has retrieved network information from a compromised host, such as the MAC address.[153][154]

S0447 Lokibot

Lokibot has the ability to discover the domain name of the infected host.[155]

G0030 Lotus Blossom

Lotus Blossom has used commands such as `ipconfig` and `netstat` to gather network information on compromised hosts.[156]

S0451 LoudMiner

LoudMiner used a script to gather the IP address of the infected machine before sending to the C2.[157]

S0532 Lucifer

Lucifer can collect the IP address of a compromised host.[158]

S1143 LunarLoader

LunarLoader can verify the targeted host's DNS name which is then used in the creation of a decyrption key.[159]

S1141 LunarWeb

LunarWeb can use shell commands to discover network adapters and configuration.[159]

S0409 Machete

Machete collects the MAC address of the target computer and other network configuration information.[160][161]

S1016 MacMa

MacMa can collect IP addresses from a compromised host.[162]

S1060 Mafalda

Mafalda can use the `GetAdaptersInfo` function to retrieve information about network adapters and the `GetIpNetTable` function to retrieve the IPv4 to physical network address mapping table.[163]

G0059 Magic Hound

Magic Hound malware gathers the victim's local IP address, MAC address, and external IP address.[164][165][166]

S1182 MagicRAT

MagicRAT collects system network information using commands such as `ipconfig /all`.[167]

S1156 Manjusaka

Manjusaka gathers information about current network connections, local and remote addresses associated with them, and associated processes.[168]

G1051 Medusa Group

Medusa Group has obtained host network details utilizing the command `cmd.exe /c ipconfig /all`.[169]

G0045 menuPass

menuPass has used several tools to scan for open NetBIOS nameservers and enumerate NetBIOS sessions.[170]

S1015 Milan

Milan can run `C:\Windows\system32\cmd.exe /c cmd /c ipconfig /all 2>&1` to discover network settings.[171]

S0084 Mis-Type

Mis-Type may create a file containing the results of the command `cmd.exe /c ipconfig /all`.[172]

G1036 Moonstone Sleet

Moonstone Sleet has gathered information on victim network configuration.[173]

S0149 MoonWind

MoonWind obtains the victim IP address.[174]

S0284 More_eggs

More_eggs has the capability to gather the IP address from the victim's machine.[175]

G1009 Moses Staff

Moses Staff has collected the domain name of a compromised network.[176]

S0256 Mosquito

Mosquito uses the `ipconfig` command.[177]

G0069 MuddyWater

MuddyWater has used malware to collect the victim’s IP address and domain name.[178]

G0129 Mustang Panda

Mustang Panda has used `ipconfig` and `arp` to determine network configuration information.[179] Mustang Panda has also utilized SharpNBTScan to scan the victim environment.[180]

S0205 Naid

Naid collects the domain name from a compromised host.[181]

G0019 Naikon

Naikon uses commands such as `netsh interface show` to discover network interface settings.[182]

S0228 NanHaiShu

NanHaiShu can gather information about the victim proxy server.[183]

S0336 NanoCore

NanoCore gathers the IP address from the victim's machine.[184]

S0590 NBTscan

NBTscan can be used to collect MAC addresses.[185][186]

S0102 nbtstat

nbtstat can be used to discover local NetBIOS domain names.

S0691 Neoichor

Neoichor can gather the IP address from an infected host.[135]

S0198 NETWIRE

NETWIRE can collect the IP address of a compromised host.[187][188]

S1106 NGLite

NGLite identifies the victim system MAC and IPv4 addresses and uses these to establish a victim identifier.[189]

S1147 Nightdoor

Nightdoor gathers information on victim system network configuration such as MAC addresses.[190]

S1100 Ninja

Ninja can enumerate the IP address on compromised systems.[191]

S0359 Nltest

Nltest may be used to enumerate the parent domain of a local machine using `/parentdomain`.[192]

S0353 NOKKI

NOKKI can gather information on the victim IP address.[193]

S0346 OceanSalt

OceanSalt can collect the victim's IP address.[194]

S0340 Octopus

Octopus can collect the host IP address from the victim's machine.[195]

G0049 OilRig

OilRig has run `ipconfig /all` on a victim.[196][197]

S0439 Okrum

Okrum can collect network information, including the host IP address, DNS, and proxy information.[198]

S0365 Olympic Destroyer

Olympic Destroyer uses API calls to enumerate the infected system's ARP table.[199]

C0012 Operation CuckooBees

During Operation CuckooBees, the threat actors used `ipconfig` , `nbtstat` , `tracert` , `route print` , and `cat /etc/hosts` commands.[200]

C0014 Operation Wocao

During Operation Wocao, threat actors discovered the local network configuration with `ipconfig` .[201]

S0229 Orz

Orz can gather victim proxy information.[183]

S0165 OSInfo

OSInfo discovers the current domain information.[17]

S0352 OSX_OCEANLOTUS.D

OSX_OCEANLOTUS.D can collect the network interface MAC address on the infected host.[202][203]

S0556 Pay2Key

Pay2Key can identify the IP and MAC addresses of the compromised host.[204]

S1050 PcShare

PcShare can obtain the proxy settings of a compromised machine using `InternetQueryOptionA` and its IP address by running `nslookup myip.opendns.comresolver1.opendns.com\r\n`.[99]

S0587 Penquin

Penquin can report the IP of the compromised host to attacker controlled infrastructure.[205]

S1145 Pikabot

Pikabot gathers victim network information through commands such as `ipconfig` and `ipconfig /all`.[206]

S1031 PingPull

PingPull can retrieve the IP address of a compromised host.[207]

S0501 PipeMon

PipeMon can collect and send the local IP address, RDP information, and the network adapter physical address as a part of its C2 beacon.[208]

S0124 Pisloader

Pisloader has a command to collect the victim's IP address.[209]

S0254 PLAINTEE

PLAINTEE uses the `ipconfig /all` command to gather the victim’s IP address.[210]

G1040 Play

Play has used the information-stealing tool Grixba to enumerate network information.[211]

S0013 PlugX

PlugX has captured victim IP address details of the targeted machine.[212][213]

S0378 PoshC2

PoshC2 can enumerate network adapter information.[214]

S0139 PowerDuke

PowerDuke has a command to get the victim's domain and NetBIOS name.[215]

S0441 PowerShower

PowerShower has the ability to identify the current Windows domain of the infected host.[216]

S0223 POWERSTATS

POWERSTATS can retrieve IP, network adapter configuration information, and domain from compromised hosts.[217][218]

S0184 POWRUNER

POWRUNER may collect network configuration data by running `ipconfig /all` on a victim.[219]

S0113 Prikormka

A module in Prikormka collects information from the victim about its IP addresses and MAC addresses.[220]

S0238 Proxysvc

Proxysvc collects the network adapter information and domain/username information based on current remote sessions.[221]

S1228 PUBLOAD

PUBLOAD has obtained information about local networks through the `ipconfig /all` command.[222]

S0192 Pupy

Pupy has built in commands to identify a host's IP address and find out other network configuration settings by viewing connected sessions.[223]

S0583 Pysa

Pysa can perform network reconnaissance using the Advanced IP Scanner tool.[224]

S0650 QakBot

QakBot can use `net config workstation`, `arp -a`, `nslookup`, and `ipconfig /all` to gather network configuration information.[225][226][227][228][229]

S1242 Qilin

Qilin can accept a command line argument identifying specific IPs.[230]

S0269 QUADAGENT

QUADAGENT gathers the current domain the victim system belongs to.[231]

S0262 QuasarRAT

QuasarRAT has the ability to enumerate the Wide Area Network (WAN) IP through requests to ip-api[.]com, freegeoip[.]net, or api[.]ipify[.]org observed with user-agent string `Mozilla/5.0 (Windows NT 6.3; rv:48.0) Gecko/20100101 Firefox/48.0`.[232]

S1076 QUIETCANARY

QUIETCANARY can identify the default proxy setting on a compromised host.[145]

S0458 Ramsay

Ramsay can use ipconfig and Arp to collect network configuration information, including routing information and ARP tables.[233]

S0241 RATANKBA

RATANKBA gathers the victim's IP address via the `ipconfig -all` command.[234][235]

S0172 Reaver

Reaver collects the victim's IP address.[236]

S0153 RedLeaves

RedLeaves can obtain information about network parameters.[170]

S1240 RedLine Stealer

RedLine Stealer can enumeate information about victims' systems including IP addresses.[237]

C0056 RedPenguin

During RedPenguin, UNC3886 leveraged JunoOS CLI queries to obtain the interface index which contains system and network details.[238][239]

S0125 Remsec

Remsec can obtain information about network configuration, including the routing table, ARP cache, and DNS cache.[240]

S0379 Revenge RAT

Revenge RAT collects the IP address and MAC address from the system.[241]

S0433 Rifdoor

Rifdoor has the ability to identify the IP address of the compromised host.[242]

S0448 Rising Sun

Rising Sun can detect network adapter and IP address information.[243]

S0270 RogueRobin

RogueRobin gathers the IP address and domain from the victim's machine.[244]

S0103 route

route can be used to discover routing configuration information.

S1073 Royal

Royal can enumerate IP addresses using `GetIpAddrTable`.[245]

S0446 Ryuk

Ryuk has called `GetIpNetTable` in attempt to identify all mounted drives and hosts that have Address Resolution Protocol (ARP) entries.[246][247]

S0085 S-Type

S-Type has used `ipconfig /all` on a compromised host.[172]

S1210 Sagerunex

Sagerunex will gather system information such as MAC and IP addresses.[156]

S1018 Saint Bot

Saint Bot can collect the IP address of a victim machine.[248]

S1085 Sardonic

Sardonic has the ability to execute the `ipconfig` command.[249]

G1015 Scattered Spider

Scattered Spider has used network reconnaissance commands for discovery including `ping` and `nltest`.[250]

S0461 SDBbot

SDBbot has the ability to determine the domain name and whether a proxy is configured on a compromised host.[251]

S0596 ShadowPad

ShadowPad has collected the domain name of the victim system.[252]

C0045 ShadowRay

During ShadowRay, threat actors invoked DNS queries from targeted machines to identify their IP addresses.[253]

S0140 Shamoon

Shamoon obtains the target's IP address and local network segment.[254][255]

S0450 SHARPSTATS

SHARPSTATS has the ability to identify the domain of the compromised host.[218]

S0445 ShimRatReporter

ShimRatReporter gathered the local proxy, domain, IP, routing tables, mac address, gateway, DNS servers, and DHCP status information from an infected host.[256]

S1178 ShrinkLocker

ShrinkLocker captures the IP address of the victim system and sends this to the attacker following encryption.[257]

S0589 Sibot

Sibot checked if the compromised system is configured to use proxies.[102]

G1008 SideCopy

SideCopy has identified the IP address of a compromised host.[4]

S0610 SideTwist

SideTwist has the ability to collect the domain name on a compromised host.[258]

G0121 Sidewinder

Sidewinder has used malware to collect information on network interfaces, including the MAC address.[259]

S0633 Sliver

Sliver has the ability to gather network configuration information.[260]

S1035 Small Sieve

Small Sieve can obtain the IP address of a victim host.[261]

S1124 SocGholish

SocGholish has the ability to enumerate the domain name of a victim, as well as if the host is a member of an Active Directory domain.[262][263][264]

S0516 SoreFang

SoreFang can collect the TCP/IP, DNS, DHCP, and network adapter configuration on a compromised host via `ipconfig.exe /all`.[265]

S0374 SpeakUp

SpeakUp uses the `ifconfig -a` command. [266]

S0646 SpicyOmelette

SpicyOmelette can identify the IP of a compromised system.[267]

S1030 Squirrelwaffle

Squirrelwaffle has collected the victim's external IP address.[268]

S1037 STARWHALE

STARWHALE has the ability to collect the IP address of an infected host.[269]

G0038 Stealth Falcon

Stealth Falcon malware gathers the Address Resolution Protocol (ARP) table from the victim.[270]

S0491 StrongPity

StrongPity can identify the IP address of a compromised host.[271]

S0603 Stuxnet

Stuxnet collects the IP address of a compromised system.[272]

S0559 SUNBURST

SUNBURST collected all network interface MAC addresses that are up and not loopback devices, as well as IP address, DHCP configuration, and domain information.[273]

S0018 Sykipot

Sykipot may use `ipconfig /all` to gather system network configuration details.[274]

S0060 Sys10

Sys10 collects the local IP address of the victim and sends it to the C2.[182]

S0663 SysUpdate

SysUpdate can collected the IP address and domain name of a compromised host.[275]

S0098 T9000

T9000 gathers and beacons the MAC and IP addresses during installation.[276]

S0011 Taidoor

Taidoor has collected the MAC address of a compromised host; it can also use `GetAdaptersInfo` to identify network adapters.[277][278]

S0467 TajMahal

TajMahal has the ability to identify the MAC address on an infected host.[279]

G0139 TeamTNT

TeamTNT has enumerated the host machine's IP address.[280]

G0027 Threat Group-3390

Threat Group-3390 actors use NBTscan to discover vulnerable systems.[281]

S0678 Torisma

Torisma can collect the local MAC address using `GetAdaptersInfo` as well as the system's IP address.[282]

S0266 TrickBot

TrickBot obtains the IP address, location, and other relevant network information from the victim's machine.[283][284][63]

S0094 Trojan.Karagany

Trojan.Karagany can gather information on the network configuration of a compromised host.[285]

S1196 Troll Stealer

Troll Stealer collects the MAC address of victim devices.[286]

G0081 Tropic Trooper

Tropic Trooper has used scripts to collect the host's network topology.[287]

S0436 TSCookie

TSCookie has the ability to identify the IP of the infected host.[288]

S0647 Turian

Turian can retrieve the internal IP address of a compromised host.[289]

G0010 Turla

Turla surveys a system upon check-in to discover network configuration details using the `arp -a`, `nbtstat -n`, `net config`, `ipconfig /all`, and `route` commands, as well as NBTscan.[90][290][291] Turla RPC backdoors have also retrieved registered RPC interface information from process memory.[292]

S0130 Unknown Logger

Unknown Logger can obtain information about the victim's IP address.[293]

S0275 UPPERCUT

UPPERCUT has the capability to gather the victim's proxy information.[294]

S0452 USBferry

USBferry can detect the infected machine's network topology using `ipconfig` and `arp`.[287]

S0476 Valak

Valak has the ability to identify the domain and the MAC and IP addresses of an infected machine.[295]

S0257 VERMIN

VERMIN gathers the local IP address.[296]

S0180 Volgmer

Volgmer can gather the IP address from the victim's machine.[297]

G1017 Volt Typhoon

Volt Typhoon has executed multiple commands to enumerate network topology and settings including `ipconfig`, `netsh interface firewall show all`, and `netsh interface portproxy show all`.[298]

S0366 WannaCry

WannaCry will attempt to determine the local network segment it is a part of.[299]

S0515 WellMail

WellMail can identify the IP address of the victim system.[300]

S0514 WellMess

WellMess can identify the IP address and user domain on the target machine.[301][302]

G0102 Wizard Spider

Wizard Spider has used ipconfig to identify the network configuration of a victim machine. Wizard Spider has also used the PowerShell cmdlet `Get-ADComputer` to collect IP address data from Active Directory.[303][304]

S1065 Woody RAT

Woody RAT can retrieve network interface and proxy information.[305]

S0341 Xbash

Xbash can collect IP addresses and local intranet information from a victim’s machine.[306]

S0653 xCaon

xCaon has used the GetAdaptersInfo() API call to get the victim's MAC address.[47]

S1248 XORIndex Loader

XORIndex Loader has leveraged webservices to identify the public IP of the victim host.[307]

S0248 yty

yty runs `ipconfig /all` and collects the domain name.[308]

S0251 Zebrocy

Zebrocy runs the `ipconfig /all` command.[309]

S0230 ZeroT

ZeroT gathers the victim's IP address and domain information, and then sends it to its C2 server.[310]

G0128 ZIRCONIUM

ZIRCONIUM has used a tool to enumerate proxy settings in the target environment.[311]

S0350 zwShell

zwShell can obtain the victim IP address.[312]
