System Information Discovery, Technique T1082 - Enterprise

Archived: 2026-04-05 18:42:08 UTC

S0065 4H RAT

4H RAT sends an OS version identifier in its beacons.[9]

S1167 AcidPour

AcidPour can identify various system locations and mapped devices on Linux systems as a precursor to wiping activity.[10]

S1028 Action RAT

Action RAT has the ability to collect the hostname, OS version, and OS architecture of an infected host.[11]

G0018 admin@338

admin@338 actors used the following commands after exploiting a machine with LOWBALL malware to obtain information about the OS: `ver >> %temp%\download` `systeminfo >> %temp%\download` [12]

S0045 ADVSTORESHELL

ADVSTORESHELL can run Systeminfo to gather information about the victim.[13][14]

S0331 Agent Tesla

Agent Tesla can collect the system's computer name and also has the capability to collect information on the processor, memory, OS, and video card from the system.[15][16][17]

S1129 Akira

Akira uses the `GetSystemInfo` Windows function to determine the number of processors on a victim machine.[18]

S1025 Amadey

Amadey has collected the computer name and OS version from a compromised machine.[19][20]

S0504 Anchor

Anchor can determine the hostname and linux version on a compromised host.[21]

S0584 AppleJeus

AppleJeus has collected the victim host information after infection.[22]

S0622 AppleSeed

AppleSeed can identify the OS version of a targeted system.[23]

G0026 APT18

APT18 can collect system information from the victim's machine.[24]

G0073 APT19

APT19 collected system architecture information. APT19 used an HTTP malware variant and a Port 22 malware variant to gather the hostname and CPU information from the victim's machine.[25][26]

G0022 APT3

APT3 has a tool that can obtain information about the local system.[27][28]

G0050 APT32

APT32 has collected the OS version and computer name from victims. One of the group's backdoors can also query the Windows Registry to gather system information, and another macOS backdoor performs a fingerprint of the machine on its first connection to the C&C server. APT32 executed shellcode to identify the name of the infected host.[29][30][31][32]

G0067 APT37

APT37 collects the computer name, the BIOS model, and execution path.[33]

G0082 APT38

APT38 has attempted to get detailed information about a compromised host, including the operating system, version, patches, hotfixes, and service packs.[34]

G0096 APT41

APT41 uses multiple built-in commands such as `systeminfo` and `net config Workstation` to enumerate victim system basic configuration information.[35]

G1044 APT42

APT42 has used malware, such as GHAMBAR and POWERPOST, to collect system information.[36]

G0143 Aquatic Panda

Aquatic Panda has used native OS commands to understand privilege levels and system details.[37]

C0046 ArcaneDoor

ArcaneDoor included collection of victim device configuration information.[38]

S0456 Aria-body

Aria-body has the ability to identify the hostname, computer name, Windows version, processor speed, and machine GUID on a compromised host.[39]

S0373 Astaroth

Astaroth collects the machine name and keyboard language from the system. [40][41]

S1029 AuTo Stealer

AuTo Stealer has the ability to collect the hostname and OS information from an infected host.[11]

S0473 Avenger

Avenger has the ability to identify the OS architecture on a compromised host.[42]

S0344 Azorult

Azorult can collect the machine information, system architecture, the OS version, computer name, Windows product name, the number of CPU cores, video card information, and the system language.[43][44]

S0414 BabyShark

BabyShark has executed the `ver` command.[45]

S0475 BackConfig

BackConfig has the ability to gather the victim's computer name.[46]

S0093 Backdoor.Oldrea

Backdoor.Oldrea collects information about the OS and computer name.[47][48]

S0031 BACKSPACE

During its initial execution, BACKSPACE extracts operating system information from the infected host.[49]

S0245 BADCALL

BADCALL collects the computer name and host name on the compromised system.[50]

S0642 BADFLICK

BADFLICK has captured victim computer name, memory space, and CPU details.[51]

S1081 BADHATCH

BADHATCH can obtain current system information from a compromised machine such as the `SHELL PID`, `PSVERSION`, `HOSTNAME`, `LOGONSERVER`, `LASTBOOTUP`, OS type/version, bitness, and hostname.[52][53]

S0337 BadPatch

BadPatch collects the OS system, OS version, MAC address, and the computer name from the victim's machine. [54]

S0239 Bankshot

Bankshot gathers system information, network addresses, and the operation system version.[55][56]

S0534 Bazar

Bazar can fingerprint architecture, computer name, and OS version on the compromised host. Bazar can also check if the Russian language is installed on the infected machine and terminate if it is found.[57][58]

S1246 BeaverTail

BeaverTail has been known to collect basic system information.[59][60] BeaverTail has also collected data to include hostname and current timestamp prior to uploading data to the API endpoint `/uploads` on the C2 server. [61]

S0017 BISCUIT

BISCUIT has a command to collect the processor type, operation system, computer name, and whether the system is a laptop or PC.[62]

S0268 Bisonal

Bisonal has used commands and API calls to gather system information.[63][64][65]

S1070 Black Basta

Black Basta can collect system boot configuration and CPU information.[66][67]

G1043 BlackByte

BlackByte used various system commands and tools to pull system information during operations.[68][69][70]

S1180 BlackByte Ransomware

BlackByte Ransomware gathers victim system information to generate a unique victim identifier.[71]

S1068 BlackCat

BlackCat can obtain the computer name and UUID.[72]

S0089 BlackEnergy

BlackEnergy has used Systeminfo to gather the OS version, as well as information on the system configuration, BIOS, the motherboard, and the processor.[73][74]

S0520 BLINDINGCAN

BLINDINGCAN has collected from a victim machine the system name, processor information, and OS version.[75]

G0108 Blue Mockingbird

Blue Mockingbird has collected hardware details for the victim's system, including CPU and memory information.[76]

S0657 BLUELIGHT

BLUELIGHT has collected the computer name and OS version from victim machines.[77]

S1184 BOLDMOVE

BOLDMOVE performs system survey actions following initial execution.[78]

S0486 Bonadan

Bonadan has discovered the OS version, CPU model, and RAM size of the system it has been installed on.[79]

S0635 BoomBox

BoomBox can enumerate the hostname, domain, and IP of a compromised host.[80]

S0252 Brave Prince

Brave Prince collects hard drive content and system configuration information.[81]

S0043 BUBBLEWRAP

BUBBLEWRAP collects system information, including the operating system version and hostname.[12]

S1039 Bumblebee

Bumblebee can enumerate the OS version and domain on a targeted system.[82][83][84]

S0482 Bundlore

Bundlore will enumerate the macOS version to determine which follow-on behaviors to execute using `/usr/bin/sw_vers -productVersion`.[85][8]

S0693 CaddyWiper

CaddyWiper can use `DsRoleGetPrimaryDomainInformation` to determine the role of the infected machine. CaddyWiper can also halt execution if the compromised host is identified as a domain controller.[86][87]

S0454 Cadelspy

Cadelspy has the ability to discover information about the compromised host.[88]

S0351 Cannon

Cannon can gather system information from the victim's machine such as the OS version, and machine name.[89] [90]

S0484 Carberp

Carberp has collected the operating system version from the infected system.[91]

S0348 Cardinal RAT

Cardinal RAT can collect the hostname, Microsoft Windows version, and processor architecture from a victim machine.[92]

S0462 CARROTBAT

CARROTBAT has the ability to determine the operating system of the compromised host and whether Windows is being run with x86 or x64 architecture.[93][94]

S0572 Caterpillar WebShell

Caterpillar WebShell has a module to gather information from the compromised asset, including the computer version, computer name, IIS version, and more.[95]

S0631 Chaes

Chaes has collected system information, including the machine name and OS version.[96]

S0674 CharmPower

CharmPower can enumerate the OS version and computer name on a targeted system.[97]

S0144 ChChes

ChChes collects the victim hostname, window resolution, and Microsoft Windows version.[98][99]

S0667 Chrommme

Chrommme has the ability to obtain the computer name of a compromised host.[100]

S0660 Clambling

Clambling can discover the hostname, computer name, and Windows version of a targeted machine.[101][102]

S0106 cmd

cmd can be used to find information about the operating system.[103]

S0244 Comnie

Comnie collects the hostname of the victim machine.[104]

G1052 Contagious Interview

Contagious Interview has configured malicious webpages to identify the victim's operating system by reviewing the details of the victims User-Agent of their browser.[105]

S0137 CORESHELL

CORESHELL collects hostname and OS version data from the victim and sends the information to its C2 server.[106]

S1155 Covenant

Covenant implants can gather basic information on infected systems.[107]

S0046 CozyCar

A system info module in CozyCar gathers information on the victim host's configuration.[108]

S0115 Crimson

Crimson contains a command to collect the victim PC name and operating system.[109][110][111]

S1153 Cuckoo Stealer

Cuckoo Stealer can gather information about the OS version and hardware on compromised hosts.[112][113]

G1012 CURIUM

CURIUM deploys information gathering tools focused on capturing IP configuration, running application, system information, and network connectivity information.[114]

C0029 Cutting Edge

During Cutting Edge, threat actors used the ENUM4LINUX Perl script for discovery on Windows and Samba hosts.[115]

S0687 Cyclops Blink

Cyclops Blink has the ability to query device information.[116]

G1034 Daggerfly

Daggerfly utilizes victim machine operating system information to create custom User Agent strings for subsequent command and control communication.[117]

S0334 DarkComet

DarkComet can collect the computer name, RAM used, and operating system version from the victim's machine.[118][119]

S1111 DarkGate

DarkGate will gather various system information such as domain, display adapter description, operating system type and version, processor type, and RAM amount.[120][121]

G0012 Darkhotel

Darkhotel has collected the hostname, OS version, service pack version, and the processor architecture from the victim's machine.[122][123]

S1066 DarkTortilla

DarkTortilla can obtain system information by querying the `Win32_ComputerSystem`, `Win32_BIOS`, `Win32_MotherboardDevice`, `Win32_PnPEntity`, and `Win32_DiskDrive` WMI objects.[124]

S0673 DarkWatchman

DarkWatchman can collect the OS version, system architecture, and computer name.[125]

S1052 DEADEYE

DEADEYE can enumerate a victim computer's volume serial number and host name.[126]

S0354 Denis

Denis collects OS information and the computer name from the victim's machine.[127][128]

S0021 Derusbi

Derusbi gathers the name of the local host, version of GNU Compiler Collection (GCC), and the system information about the CPU, machine, and operating system.[129]

S0659 Diavol

Diavol can collect the computer name and OS version from the system.[130]

S0186 DownPaper

DownPaper collects the victim host name and serial number, and then sends the information to the C2 server.[131]

S0384 Dridex

Dridex has collected the computer name and OS architecture information from the system.[132]

S0547 DropBook

DropBook has checked for the presence of Arabic language in the infected machine's settings.[133]

S0105 dsquery

dsquery has the ability to enumerate various information, such as the operating system and host name, for systems within a domain.[126]

S0567 Dtrack

Dtrack can collect the victim's computer name, hostname and adapter information to create a unique identifier. [134][135]

S1159 DUSTTRAP

DUSTTRAP reads the value of the infected system's `HKLM\SYSTEM\Microsoft\Cryptography\MachineGUID` value. [136]

S0062 DustySky

DustySky extracts basic information about the operating system.[137]

S0024 Dyre

Dyre has the ability to identify the computer name, OS version, and hardware configuration on a compromised host.[138]

S0554 Egregor

Egregor can perform a language check of the infected system and can query the CPU information (cupid).[139] [140]

S0081 Elise

Elise executes `systeminfo` after initial communication is made to the remote server.[141]

S0082 Emissary

Emissary has the capability to execute ver and systeminfo commands.[142]

S0363 Empire

Empire can enumerate host system information like OS, architecture, domain name, applied patches, and more. [143][144]

S0634 EnvyScout

EnvyScout can determine whether the ISO payload was received by a Windows or iOS device.[80]

S0091 Epic

Epic collects the OS version, hardware information, computer name, available system memory status, and system and user language settings.[145]

S0568 EVILNUM

EVILNUM can obtain the computer name from the victim's system.[146]

S0569 Explosive

Explosive has collected the computer name from the infected host.[147]

S0181 FALLCHILL

FALLCHILL can collect operating system (OS) version information, processor information, and system name from the victim.[148]

S0512 FatDuke

FatDuke can collect the user name, Windows version, computer name, and available space on discs from a compromised host.[149]

S0171 Felismus

Felismus collects the system information, including hostname and OS version, and sends it to the C2 server.[150]

S0267 FELIXROOT

FELIXROOT collects the victim’s computer name, processor architecture, OS version, and system type.[151][152]

S0679 Ferocious

Ferocious can use `GET.WORKSPACE` in Microsoft Excel to determine the OS version of the compromised host.[153]

G1016 FIN13

FIN13 has collected local host information by utilizing Windows commands `systeminfo`, `fsutil`, and `fsinfo`. FIN13 has also utilized a compromised Symantex Altiris console and LanDesk account to retrieve host information.[154][155]

G0046 FIN7

FIN7 has used csvde.exe, which is a built-in Windows command line tool, to export system information. Additionally, WsTaskLoad has gathered system information, such as operating system and hostname.[156]

G0061 FIN8

FIN8 has used PowerShell Scripts to check the architecture of a compromised machine before the selection of a 32-bit or 64-bit version of a malicious .NET loader.[157]

S0355 Final1stspy

Final1stspy obtains victim Microsoft Windows version information and CPU architecture.[158]

S0182 FinFisher

FinFisher checks if the victim OS is 32 or 64-bit.[159][160]

S0381 FlawedAmmyy

FlawedAmmyy can collect the victim's operating system and computer name during the initial infection.[161]

C0001 Frankenstein

During Frankenstein, the threat actors used Empire to obtain the compromised machine's name.[144]

C0007 FunnyDream

During FunnyDream, the threat actors used Systeminfo to collect information on targeted hosts.[162]

S0410 Fysbis

Fysbis has used the command `ls /etc | egrep -e"fedora*|debian*|gentoo*|mandriva*|mandrake*|meego*|redhat*|lsb-*|sun-*|SUSE*|release"` to determine which Linux OS version is running.[163]

G0047 Gamaredon Group

A Gamaredon Group file stealer can gather the victim's computer name and drive serial numbers to send to a C2 server.[164][165][166][167][168]

S0666 Gelsemium

Gelsemium can determine the operating system and whether a targeted machine has a 32 or 64 bit architecture.[100]

S0460 Get2

Get2 has the ability to identify the computer name and Windows version of an infected host.[169]

S0032 gh0st RAT

gh0st RAT has gathered system architecture, processor, OS configuration, and installed hardware information.[170]

S0249 Gold Dragon

Gold Dragon collects endpoint information using the `systeminfo` command.[81]

S0493 GoldenSpy

GoldenSpy has gathered operating system information.[171]

S1198 Gomir

Gomir collects information on infected systems such as hostname, username, CPU, and RAM information.[172]

S1138 Gootloader

Gootloader can inspect the User-Agent string in GET request header information to determine the operating system of targeted systems.[173]

S0531 Grandoreiro

Grandoreiro can collect the computer name and OS version from a compromised host.[174]

S0237 GravityRAT

GravityRAT collects the MAC address, computer name, and CPU information.[175]

S0690 Green Lambert

Green Lambert can use `uname` to identify the operating system name, version, and processor type.[176][177]

S0417 GRIFFON

GRIFFON has used a reconnaissance module that can be used to retrieve information about a victim's computer, including the resolution of the workstation .[178]

S0632 GrimAgent

GrimAgent can collect the OS, and build version on a compromised host.[179]

S0151 HALFBAKED

HALFBAKED can obtain information about the OS, processor, and BIOS.[180]

S0214 HAPPYWORK

can collect system information, including computer name, system manufacturer, IsDebuggerPresent state, and execution path.[181]

S1229 Havoc

Havoc can gather system information including hostname, domain, and OS details.[182]

S0391 HAWKBALL

HAWKBALL can collect the OS version, architecture information, and computer name.[183]

S0697 HermeticWiper

HermeticWiper can determine the OS version and bitness on a targeted host.[184][185][186][187]

G1001 HEXANE

HEXANE has collected the hostname of a compromised machine.[188]

S1249 HexEval Loader

HexEval Loader has identified the OS and MAC address of victim device through host fingerprinting scripting.[189]

G0126 Higaisa

Higaisa collected the system GUID and computer name.[190][191]

S0601 Hildegard

Hildegard has collected the host's OS, CPU, and memory information.[192]

S0376 HOPLIGHT

HOPLIGHT has been observed collecting victim machine information like OS version.[193]

S0431 HotCroissant

HotCroissant has the ability to determine if the current user is an administrator, Windows product name, processor name, screen resolution, and physical RAM of the infected host.[194]

S0203 Hydraq

Hydraq creates a backdoor through which remote attackers can retrieve information such as computer name, OS version, processor speed, memory size, and CPU speed.[195]

S1022 IceApple

The IceApple Server Variable Dumper module iterates over all server variables present for the current request and returns them to the adversary.[196]

S0483 IcedID

IcedID has the ability to identify the computer name and OS version on a compromised host.[197][198]

S1152 IMAPLoader

IMAPLoader uses WMI queries to gather information about the victim machine.[199]

G0100 Inception

Inception has used a reconnaissance module to gather information about the operating system and hardware on the infected host.[200]

S0604 Industroyer

Industroyer collects the victim machine’s Windows GUID.[201]

S0259 InnaputRAT

InnaputRAT gathers system information.[202]

S1245 InvisibleFerret

InvisibleFerret has collected OS type, hostname and system version through the "pay" module.[59][61]
InvisibleFerret has also queried the victim device using Python scripts to obtain the User and Hostname.[203][60]

S0260 InvisiMole

InvisiMole can gather information on the OS version, computer name, DEP policy, and memory size.[204][205]

S0015 Ixeshe

Ixeshe collects the computer name of the victim's system during the initial infection.[206]

S0201 JPIN

JPIN can obtain system information such as OS version and disk space.[207]

S0283 jRAT

jRAT collects information about the OS (version, build type, install date) as well as system up-time upon receiving a connection from a backdoor.[208]

C0044 Juicy Mix

During Juicy Mix, OilRig used a script to send the name of the compromised host via HTTP `POST` to register it with C2.[209]

S1190 Kapeka

Kapeka utilizes WinAPI calls and registry queries to gather system information.[210]

S0215 KARAE

KARAE can collect system information.[181]

S0088 Kasidet

Kasidet has the ability to obtain a victim's system name and operating system version.[211]

S0265 Kazuar

Kazuar gathers information on the system.[212]

G0004 Ke3chang

Ke3chang performs operating system information discovery using `systeminfo` and has used implants to identify the system language and computer name.[213][214][215]

S0585 Kerrdown

Kerrdown has the ability to determine if the compromised host is running a 32 or 64 bit OS architecture.[216]

S0487 Kessel

Kessel has collected the system architecture, OS version, and MAC address information.[79]

S1020 Kevin

Kevin can enumerate the OS version and hostname of a targeted machine.[188]

S0387 KeyBoy

KeyBoy can gather extended system information, such as information about the operating system and memory.[217][218]

S0271 KEYMARBLE

KEYMARBLE has the capability to collect the computer name, language settings, the OS version, CPU information, and time elapsed since system start.[219]

G0094 Kimsuky

Kimsuky has enumerated OS type, OS version, and other information using a script or the "systeminfo" command.[220][221] Kimsuky has also obtained system information such as OS type, OS version, and system type through querying various Windows Management Instrumentation (WMI) classes including `Win32_OperatingSystem`.[222]

S0250 Koadic

Koadic can obtain the OS version and build, computer name, and processor architecture from a compromised host.[223]

S0641 Kobalos

Kobalos can record the hostname and kernel version of the target machine.[224]

S0669 KOCTOPUS

KOCTOPUS has checked the OS version using `wmic.exe` and the `find` command.[223]

S0156 KOMPROGO

KOMPROGO is capable of retrieving information about the infected system.[225]

S0356 KONNI

KONNI can gather the OS version, architecture information, hostname, and RAM size information from the victim's machine and has used `cmd /c systeminfo` command to get a snapshot of the current system state of the target machine.[226][227][228]

C0035 KV Botnet Activity

KV Botnet Activity includes use of native system tools, such as `uname`, to obtain information about victim device architecture, as well as gathering other system information such as the victim's hosts file and CPU utilization.[229]

S0236 Kwampirs

Kwampirs collects OS version information such as registered owner details, manufacturer details, processor type, available storage, installed patches, hostname, version info, system date, and other system information by using the commands `systeminfo`, `net config workstation`, `hostname`, `ver`, `set`, and `date /t`.[230]

S1160 Latrodectus

Latrodectus can gather operating system information.[231][232][232][233]

G0032 Lazarus Group

Several Lazarus Group malware families collect information on the type and version of the victim OS, as well as the victim computer name and CPU information.[234][235][236][237][238][239]

C0049 Leviathan Australian Intrusions

Leviathan performed host enumeration and data gathering operations on victim machines during Leviathan Australian Intrusions.[240]

S0395 LightNeuron

LightNeuron gathers the victim computer name using the Win32 API call `GetComputerName`.[241]

S1185 LightSpy

LightSpy's second stage implant uses the `DeviceInformation` class to collect system information, including CPU usage, battery statistics, memory allocations, screen size, etc.[242]

S1186 Line Dancer

Line Dancer can gather system configuration information by running the native `show configuration` command.[243]

S0211 Linfo

Linfo creates a backdoor through which remote attackers can retrieve system information.[244]

S0513 LiteDuke

LiteDuke can enumerate the CPUID and BIOS version on a compromised system.[149]

S0680 LitePower

LitePower has the ability to enumerate the OS architecture.[153]

S1121 LITTLELAMB.WOOLTEA

LITTLELAMB.WOOLTEA can check the type of Ivanti VPN device it is running on by executing `first_run()` to identify the first four bytes of the motherboard serial number.[245]

S0681 Lizar

Lizar can collect the computer name from the machine.[246][247]

S1199 LockBit 2.0

LockBit 2.0 can enumerate system information including hostname and domain information.[248][249]

S1202 LockBit 3.0

LockBit 3.0 can enumerate system hostname and domain.[250]

S0447 Lokibot

Lokibot has the ability to discover the computer name and Windows product name/version.[251]

S0451 LoudMiner

LoudMiner has monitored CPU usage.[252]

S0532 Lucifer

Lucifer can collect the computer name, system architecture, default language, and processor frequency of a compromised host.[253]

S1213 Lumma Stealer

Lumma Stealer has gathered various system information from victim machines.[254][255][256]

S1142 LunarMail

LunarMail can capture environmental variables on compromised hosts.[257]

S1141 LunarWeb

LunarWeb can use WMI queries and shell commands such as systeminfo.exe to collect the operating system, BIOS version, and domain name of the targeted system.[257]

S0409 Machete

Machete collects the hostname of the target computer.[258]

S1016 MacMa

MacMa can collect information about a compromised computer, including: Hardware UUID, Mac serial number, and macOS version.[259]

S1048 macOS.OSAMiner

macOS.OSAMiner can gather the device serial number.[260]

S1060 Mafalda

Mafalda can collect the computer name of a compromised host.[261][262]

G0059 Magic Hound

Magic Hound malware has used a PowerShell command to check the victim system architecture to determine if it is an x64 machine. Other malware has obtained the OS version, UUID, and computer/host name to send to the C2 server.[263][264][265]

S1182 MagicRAT

MagicRAT collects basic system information from victim machines.[266]

G1026 Malteiro

Malteiro collects the machine information, system architecture, the OS version, computer name, and Windows product name.[267]

S1169 Mango

Mango can collect the machine name of a compromised system which is later used as part of a unique victim identifier.[209]

S1156 Manjusaka

Manjusaka performs basic system profiling actions to fingerprint and register the victim system with the C2 controller.[268]

S0652 MarkiRAT

MarkiRAT can obtain the computer name from a compromised host.[269]

S0449 Maze

Maze has checked the language of the infected system using the "GetUSerDefaultUILanguage" function.[270]

G1051 Medusa Group

Medusa Group has leveraged `cmd.exe` to identify system info `cmd.exe /c systeminfo`.[271]

S1244 Medusa Ransomware

Medusa Ransomware has collected data from the SMBIOS firmware table using `GetSystemFirmwareTable`.[272]

S1059 metaMain

metaMain can collect the computer name from a compromised host.[262]

S0455 Metamorfo

Metamorfo has collected the hostname and operating system version from the compromised host.[273][274][275]

S0688 Meteor

Meteor has the ability to discover the hostname of a compromised host.[276]

S0339 Micropsia

Micropsia gathers the hostname and OS version from the victim’s machine.[277][278]

S1015 Milan

Milan can enumerate the targeted machine's name and GUID.[279][280]

S0051 MiniDuke

MiniDuke can gather the hostname on a compromised machine.[149]

S0280 MirageFox

MirageFox can collect CPU and architecture information from the victim’s machine.[281]

S0084 Mis-Type

The initial beacon packet for Mis-Type contains the operating system version and file system of the victim.[282]

S0083 Misdat

The initial beacon packet for Misdat contains the operating system version of the victim.[282]

S1122 Mispadu

Mispadu collects the OS version, computer name, and language ID.[283]

S0079 MobileOrder

MobileOrder has a command to upload to its C2 server victim mobile device information, including IMEI, IMSI, SIM card serial number, phone number, Android version, and other information.[284]

S0553 MoleNet

MoleNet can collect information about the about the system.[133]

S1026 Mongall

Mongall can retrieve the hostname via `gethostbyname`.[285]

G1036 Moonstone Sleet

Moonstone Sleet has gathered information on victim systems.[286]

S0149 MoonWind

MoonWind can obtain the victim hostname, Windows version, RAM amount, and screen resolution.[287]

S0284 More_eggs

More_eggs has the capability to gather the OS version and computer name.[288][289]

G1009 Moses Staff

Moses Staff collected information about the infected host, including the machine names and OS architecture.[290]

G0069 MuddyWater

MuddyWater has used malware that can collect the victim's OS version and machine name.[291][292][293][294][295]

S0233 MURKYTOP

MURKYTOP has the capability to retrieve information about the OS.[296]

G0129 Mustang Panda

Mustang Panda has gathered system information using `systeminfo`.[297]

G1020 Mustard Tempest

Mustard Tempest has used implants to perform system reconnaissance on targeted systems.[298]

S0205 Naid

Naid collects a unique identifier (UID) from a compromised host.[299]

S0228 NanHaiShu

NanHaiShu can gather the victim computer name and serial number.[300]

S0247 NavRAT

NavRAT uses `systeminfo` on a victim's machine.[301]

S0272 NDiskMonitor

NDiskMonitor obtains the victim computer name and encrypts the information to send over its C2 channel.[302]

S0691 Neoichor

Neoichor can collect the OS version and computer name from a compromised host.[215]

S0457 Netwalker

Netwalker can determine the system architecture it is running on to choose which version of the DLL to use.[303]

S0198 NETWIRE

NETWIRE can discover and collect victim system information.[304]

S1147 Nightdoor

Nightdoor gathers information on the victim system such as CPU and Computer name as well as device drivers. [117]

S1100 Ninja

Ninja can obtain the computer name and information on the OS from targeted hosts.[305][306]

S0385 njRAT

njRAT enumerates the victim operating system and computer name during the initial infection.[307]

S1107 NKAbuse

NKAbuse conducts multiple system checks and includes these in subsequent "heartbeat" messages to the malware's command and control server.[308]

S0353 NOKKI

NOKKI can gather information on the operating system on the victim’s machine.[309]

S0644 ObliqueRAT

ObliqueRAT has the ability to check for blocklisted computer names on infected endpoints.[310]

S0346 OceanSalt

OceanSalt can collect the computer name from the system.[311]

S0340 Octopus

Octopus can collect the computer name, OS version, and OS architecture information.[312]

S1172 OilBooster

OilBooster can identify the compromised system's hostname which is used to create a unique identifier.[313]

G0049 OilRig

OilRig has run `hostname` and `systeminfo` on a victim.[314][315][316][317][318]

S0439 Okrum

Okrum can collect computer name, locale information, and information about the OS and architecture.[319]

S0264 OopsIE

OopsIE checks for information on the CPU fan, temperature, mouse, hard disk, and motherboard as part of its anti-VM checks.[320]

C0012 Operation CuckooBees

During Operation CuckooBees, the threat actors used the `systeminfo` command to gather details about a compromised system.[321]

C0006 Operation Honeybee

During Operation Honeybee, the threat actors collected the computer name, OS, and other system information using `cmd /c systeminfo > %temp%\ temp.ini` .[322]

C0014 Operation Wocao

During Operation Wocao, threat actors discovered the OS versions of systems connected to a targeted network.[323]

S0229 Orz

Orz can gather the victim OS version and whether it is 64 or 32 bit.[300]

S0165 OSInfo

OSInfo discovers information about the infected machine.[27]

S0402 OSX/Shlayer

OSX/Shlayer has collected the IOPlatformUUID, session UID, and the OS version using the command `sw_vers -productVersion`.[324][325]

S0352 OSX_OCEANLOTUS.D

OSX_OCEANLOTUS.D collects processor information, memory information, computer name, hardware UUID, serial number, and operating system version. OSX_OCEANLOTUS.D has used the `ioreg` command to gather some of this information.[326][327][8]

S0208 Pasam

Pasam creates a backdoor through which remote attackers can retrieve information like hostname.[328]

G0040 Patchwork

Patchwork collected the victim computer name, OS version, and architecture type and sent the information to its C2 server.[329][302]

S0556 Pay2Key

Pay2Key has the ability to gather the hostname of the victim machine.[330]

S0587 Penquin

Penquin can report the file system type of a compromised host to C2.[331]

S1145 Pikabot

Pikabot performs a variety of system checks and gathers system information, including commands such as `whoami`.[332][333]

S0048 PinchDuke

PinchDuke gathers system configuration information.[334]

S1031 PingPull

PingPull can retrieve the hostname of a compromised host.[335]

S0501 PipeMon

PipeMon can collect and send OS version and computer name as a part of its C2 beacon.[336]

S0124 Pisloader

Pisloader has a command to collect victim system information, including the system name and OS version.[337]

S0254 PLAINTEE

PLAINTEE collects general system enumeration data about the infected machine and checks the OS version.[338]

G1040 Play

Play has leveraged tools to enumerate system information.[339]

S0013 PlugX

PlugX has collected system information including OS version, processor information, RAM size, location, host name, IP, and screen size of the infected host.[340]

S0428 PoetRAT

PoetRAT has the ability to gather information about the compromised host.[341]

S0453 Pony

Pony has collected the Service Pack, language, and region information to send to the C2.[342]

S0216 POORAIM

POORAIM can identify system information, including battery status.[181]

S0378 PoshC2

PoshC2 contains modules, such as `Get-ComputerInfo`, for enumerating common system information.[343]

S0139 PowerDuke

PowerDuke has commands to get information about the victim's name, build, version, serial number, and memory usage.[344]

S0441 PowerShower

PowerShower has collected system information on the infected host.[345]

S0223 POWERSTATS

POWERSTATS can retrieve OS name/architecture and computer/domain name information from compromised hosts.[346][347]

S0184 POWRUNER

POWRUNER may collect information about the system by running `hostname` and `systeminfo` on a victim.[348]

S0113 Prikormka

A module in Prikormka collects information from the victim about Windows OS version, computer name, battery info, and physical memory.[349]

S0238 Proxysvc

Proxysvc collects the OS version, country name, MAC address, computer name, and physical memory statistics.[238]

S1228 PUBLOAD

PUBLOAD has collected and sent system information including volume serial number, computer name, and system uptime to designated C2.[350][351] PUBLOAD has also used several commands executed in sequence via `cmd` in a short interval to gather system information about the infected host including `systeminfo`.[352] PUBLOAD has decrypted shellcode that collects the computer name.[353]

S0196 PUNCHBUGGY

PUNCHBUGGY can gather system information such as computer names.[354]

S0192 Pupy

Pupy can grab a system's information including the OS version, architecture, etc.[355]

S0650 QakBot

QakBot can collect system information including the OS version and domain on a compromised host.[356][357][358][298]

S0262 QuasarRAT

QuasarRAT can gather system information from the victim's machine including the OS type.[359]

S1148 Raccoon Stealer

Raccoon Stealer gathers information on infected systems such as operating system, processor information, RAM, and display information.[360][361]

S1212 RansomHub

RansomHub can retrieve information about virtual machines.[362]

S1130 Raspberry Robin

Raspberry Robin performs several system checks as part of anti-analysis mechanisms, including querying the operating system build number, processor vendor and type, video controller, and CPU temperature.[363]

S0241 RATANKBA

RATANKBA gathers information about the OS architecture, OS name, and OS version/Service pack.[364][365]

S0662 RCSession

RCSession can gather system information from a compromised host.[366]

S0172 Reaver

Reaver collects system information from the victim, including CPU speed, computer name, ANSI code page, OEM code page identifier for the OS, Microsoft Windows version, and memory information.[367]

G1039 RedCurl

RedCurl has collected information about the target system, such as system information and list of network connections.[368][369]

C0047 RedDelta Modified PlugX Infection Chain Operations

Mustang Panda captured victim operating system type via User Agent analysis during RedDelta Modified PlugX Infection Chain Operations.[370]

S0153 RedLeaves

RedLeaves can gather extended system information including the hostname, OS version number, platform, memory information, time elapsed since system startup, and CPU information.[99][371]

S1240 RedLine Stealer

RedLine Stealer can collect information about the local system.[372][373][374][375]

S0125 Remsec

Remsec can obtain the OS version information, computer name, processor architecture, machine role, and OS edition.[376]

S0379 Revenge RAT

Revenge RAT collects the CPU information, OS information, and system language.[377]

S0496 REvil

REvil can identify the username, machine name, system language, keyboard layout, and OS version on a compromised host.[378][379][380][381][381][382][383][384]

S0433 Rifdoor

Rifdoor has the ability to identify the Windows version on the compromised host.[385]

S1222 RIFLESPINE

RIFLESPINE can collect system information after installation on infected systems.[386]

S0448 Rising Sun

Rising Sun can detect the computer name and operating system.[387]

G0106 Rocke

Rocke has used uname -m to collect the name and information about the infected system's kernel.[388]

S0270 RogueRobin

RogueRobin gathers BIOS versions and manufacturers, the number of CPU cores, the total physical memory, and the computer name.[389]

S0240 ROKRAT

ROKRAT can gather the hostname and the OS version to ensure it doesn’t run on a Windows XP or Windows Server 2003 systems.[390][391][392][393][394][395]

S1078 RotaJakiro

RotaJakiro executes a set of commands to collect device information, including `uname`. Another example is the `cat /etc/*release | uniq` command used to collect the current OS distribution.[396]

S1073 Royal

Royal can use `GetNativeSystemInfo` to enumerate system processors.[397][398]

S0148 RTM

RTM can obtain the computer name, OS version, and default language identifier.[399]

S0253 RunningRAT

RunningRAT gathers the OS version and processor information.[81]

S0085 S-Type

The initial beacon packet for S-Type contains the operating system version and file system of the victim.[282]

S1210 Sagerunex

Sagerunex gathers information from the infected system such as hostname.[400]

S1018 Saint Bot

Saint Bot can identify the OS version, CPU, and other details from a victim's machine.[401]

S1168 SampleCheck5000

SampleCheck5000 can create unique victim identifiers by using the compromised system’s computer name.[313]

G0034 Sandworm Team

Sandworm Team used a backdoor to enumerate information about the infected system's operating system.[402][403]

S1085 Sardonic

Sardonic has the ability to collect the computer name, and CPU manufacturer name from a compromised machine. Sardonic also has the ability to execute the `ver` and `systeminfo` commands.[404]

G1015 Scattered Spider

Scattered Spider has executed scripts to identify the underlying operating system to ensure it uses the correct installation package for malicious payloads.[405]

S0461 SDBbot

SDBbot has the ability to identify the OS version, OS bit information and computer name.[169][19]

S0382 ServHelper

ServHelper will attempt to enumerate Windows version and system architecture.[406]

S0596 ShadowPad

ShadowPad has discovered system information including memory status, CPU frequency, and OS versions.[407]

S0140 Shamoon

Shamoon obtains the victim's operating system version and keyboard layout and sends the information to the C2 server.[408][409]

C0058 SharePoint ToolShell Exploitation

During SharePoint ToolShell Exploitation, threat actors fingerprinted targeted SharePoint servers to identify OS version and running processes.[410]

S1019 Shark

Shark can collect the GUID of a targeted machine.[279][280]

S0546 SharpStage

SharpStage has checked the system settings to see if Arabic is the configured language.[411]

S0450 SHARPSTATS

SHARPSTATS has the ability to identify the IP address, machine name, and OS of the compromised host.[347]

S0445 ShimRatReporter

ShimRatReporter gathered the operating system name and specific Windows version of an infected machine.[412]

S1178 ShrinkLocker

ShrinkLocker uses WMI queries to gather various information about the victim machine and operating system.[413][414]

S0217 SHUTTERSPEED

SHUTTERSPEED can collect system information.[181]

G1008 SideCopy

SideCopy has identified the OS version of a compromised host.[11]

S0610 SideTwist

SideTwist can collect the computer name of a targeted system.[317]

G0121 Sidewinder

Sidewinder has used tools to collect the computer name, OS version, installed hotfixes, as well as information regarding the memory and processor on a compromised host.[415][416]

S0692 SILENTTRINITY

SILENTTRINITY can collect information related to a compromised host, including OS version.[417]

S0468 Skidmap

Skidmap has the ability to check whether the infected system’s OS is Debian or RHEL/CentOS to determine which cryptocurrency miner it should use.[418]

S0533 SLOTHFULMEDIA

SLOTHFULMEDIA has collected system name, OS version, adapter information, and memory usage from a victim machine.[419]

S0218 SLOWDRIFT

SLOWDRIFT collects and sends system information to its C2.[181]

S0649 SMOKEDHAM

SMOKEDHAM has used the `systeminfo` command on a compromised host.[420]

S1086 Snip3

Snip3 has the ability to query `Win32_ComputerSystem` for system information. [421]

S1124 SocGholish

SocGholish has the ability to enumerate system information including the victim computer name.[422][423][424]

S0627 SodaMaster

SodaMaster can enumerate the host name and OS version on a target system.[425]

S1166 Solar

Solar can send basic information about the infected host to C2.[209]

S0615 SombRAT

SombRAT can execute `getinfo` to enumerate the computer name and OS version of a compromised system.[426]

S0516 SoreFang

SoreFang can collect the hostname, operating system configuration, and product ID on victim machines by executing Systeminfo.[427]

S0157 SOUNDBITE

SOUNDBITE is capable of gathering system information.[225]

G0054 Sowbug

Sowbug obtained OS version and hardware configuration from a victim.[428]

S0543 Spark

Spark can collect the hostname, keyboard layout, and language from the system.[429]

S0374 SpeakUp

SpeakUp uses the `cat /proc/cpuinfo | grep -c "cpu family" 2>&1` command to gather system information. [430]

S0646 SpicyOmelette

SpicyOmelette can identify the system name of a compromised host.[431]

S1234 SplatCloak

SplatCloak has collected the Windows build number using the windows kernel API `RtlGetVersion` to determine if the response is 19000 or higher (Windows 10 version 2004 or later).[432]

S1030 Squirrelwaffle

Squirrelwaffle has gathered victim computer information and configurations.[433]

S0058 SslMM

SslMM sends information to its hard-coded C2, including OS version, service pack information, processor speed, system name, and OS install date.[434]

S1037 STARWHALE

STARWHALE can gather the computer name of an infected host.[435][436]

S1200 StealBit

StealBit can enumerate the computer name and domain membership of the compromised system.[437]

G0038 Stealth Falcon

Stealth Falcon malware gathers system information via WMI, including the system directory, build number, serial number, version, manufacturer, model, and total physical memory.[438]

S0380 StoneDrill

StoneDrill has the capability to discover the system OS, Windows version, architecture and environment.[439]

G1053 Storm-0501

Storm-0501 has leveraged native Windows tools and commands such as `systeminfo` and open-source tools including OSQuery and ossec-win32 to query details about the endpoint.[440]

S0142 StreamEx

StreamEx has the ability to enumerate system information.[441]

S1183 StrelaStealer

StrelaStealer variants collect victim system information for exfiltration.[442]

S1034 StrifeWater

StrifeWater can collect the OS version, architecture, and machine name to create a unique token for the infected host.[443]

S0603 Stuxnet

Stuxnet collects system information including computer and domain names, OS version, and S7P paths.[444]

S0559 SUNBURST

SUNBURST collected hostname and OS version.[445][446]

S1064 SVCReady

SVCReady has the ability to collect information such as computer name, computer manufacturer, BIOS, operating system, and firmware, including through the use of `systeminfo.exe`.[447]

S0242 SynAck

SynAck gathers computer names, OS version info, and also checks installed keyboard layouts to estimate if it has been launched from a certain list of countries.[448]

S0060 Sys10

Sys10 collects the computer name, OS versioning information, and OS install date and sends the information to the C2.[434]

S0464 SYSCON

SYSCON has the ability to use Systeminfo to identify system information.[94]

S0096 Systeminfo

Systeminfo can be used to gather information about the operating system.[449]

S0663 SysUpdate

SysUpdate can collect a system's architecture, operating system version, and hostname.[450][451]

S0098 T9000

T9000 gathers and beacons the operating system build number and CPU Architecture (32-bit/64-bit) during installation.[452]

G1018 TA2541

TA2541 has collected system information prior to downloading malware on the targeted host.[453]

S0467 TajMahal

TajMahal has the ability to identify hardware information, the computer name, and OS information on an infected host.[454]

G0139 TeamTNT

TeamTNT has searched for system version, architecture, and hostname information.[455][456]

S0665 ThreatNeedle

ThreatNeedle can collect system profile information from a compromised host.[457]

S1239 TONESHELL

TONESHELL has the ability to retrieve the name of the infected machine.[351][458][459]

S0266 TrickBot

TrickBot gathers the OS version, machine name, CPU type, amount of RAM available, and UEFI/BIOS firmware information from the victim’s machine.[460][461][462][463]

S0094 Trojan.Karagany

Trojan.Karagany can capture information regarding the victim's OS, security, and hardware configuration.[464]

S1196 Troll Stealer

Troll Stealer can collect local system information.[465][172]

G0081 Tropic Trooper

Tropic Trooper has detected a target system’s OS version.[466][467]

S0647 Turian

Turian can retrieve system information including OS version, memory usage, local hostname, and system adapter information.[468]

G0010 Turla

Turla surveys a system upon check-in to discover operating system configuration details using the `systeminfo` and `set` commands.[469][470]

S0199 TURNEDUP

TURNEDUP is capable of gathering system information.[471]

S0130 Unknown Logger

Unknown Logger can obtain information about the victim computer name, physical memory, country, and date.[472]

S0275 UPPERCUT

UPPERCUT has the capability to gather the system's hostname and OS version.[473]

S0022 Uroburos

Uroburos has the ability to gather basic system information and run the POSIX API `gethostbyname`.[474]

S0386 Ursnif

Ursnif has used Systeminfo to gather system information.[475]

S0476 Valak

Valak can determine the Windows version and computer name on a compromised host.[476][477]

S0257 VERMIN

VERMIN collects the OS name, machine name, and architecture information.[478]

S0180 Volgmer

Volgmer can gather system information, the computer name, OS version, drive and serial information from the victim's machine.[479][480][481]

S0670 WarzoneRAT

WarzoneRAT can collect compromised host information, including OS version, PC name, RAM size, and CPU details.[482]

S0514 WellMess

WellMess can identify the computer name of a compromised host.[483][484]

G0124 Windigo

Windigo has used a script to detect which Linux distribution and version is currently installed on the system.[79]

S0155 WINDSHIELD

WINDSHIELD can gather the victim computer name.[225]

G0112 Windshift

Windshift has used malware to identify the computer name of a compromised host.[485]

S0219 WINERACK

WINERACK can gather information about the host.[181]

S0176 Wingbird

Wingbird checks the victim OS version after executing to determine where to drop files based on whether the victim is 32-bit or 64-bit.[486]

S0059 WinMM

WinMM collects the system name, OS version including service pack, and system install date and sends the information to the C2 server.[434]

S0141 Winnti for Windows

Winnti for Windows can determine if the OS on a compromised host is newer than Windows XP.[487]

G1035 Winter Vivern

Winter Vivern script execution includes basic victim information gathering steps which are then transmitted to command and control servers.[488]

G0102 Wizard Spider

Wizard Spider has used Systeminfo and similar commands to acquire detailed configuration information of a victim's machine. Wizard Spider has also utilized the PowerShell cmdlet `Get-ADComputer` to collect DNS hostnames, last logon dates, and operating system information from Active Directory.[489][490]

S1065 Woody RAT

Woody RAT can retrieve the following information from an infected machine: OS, architecture, computer name, OS build version, and environment variables.[491]

S0161 XAgentOSX

XAgentOSX contains the getInstalledAPP function to run `ls -la /Applications` to gather what applications are installed.[492]

S0658 XCSSET

XCSSET identifies the macOS version and uses `ioreg` to determine serial number.[493]

S1207 XLoader

XLoader can collect system information and supported language information from the victim machine.[494]

S1248 XORIndex Loader

XORIndex Loader has the ability to collect the hostname, OS Username, Geolocation, and OS version of an infected host.[495]

S0388 YAHOYAH

YAHOYAH checks for the system's Windows OS version and hostname.[466]

S0248 yty

yty gathers the computer name, CPU information, Microsoft Windows version, and runs the command `systeminfo`.[496]

S0251 Zebrocy

Zebrocy collects the OS version and computer name. Zebrocy also runs the `systeminfo` command to gather system information. [497][89][498][90][499][500][501]

S0230 ZeroT

ZeroT gathers the victim's computer name, Windows version, and system language, and then sends it to its C2 server.[502]

S0330 Zeus Panda

Zeus Panda collects the OS version, system architecture, computer name, product ID, install date, and information on the keyboard mapping to determine the language used on the system.[503][504]

G0128 ZIRCONIUM

ZIRCONIUM has used a tool to capture the processor architecture of a compromised host in order to register it with C2.[505]

S0086 ZLib

ZLib has the ability to enumerate system information.[282]

S0350 zwShell

zwShell can obtain the victim PC name and OS version.[506]

S0412 ZxShell

ZxShell can collect the local hostname, operating system details, CPU speed, and total physical memory.[507]

S1013 ZxxZ

ZxxZ has collected the host name and operating system product name from a compromised machine.[508]

Source: https://attack.mitre.org/techniques/T1082