Local Storage Discovery, Technique T1680 - Enterprise

Archived: 2026-04-05 13:12:49 UTC

S0456 Aria-body

Aria-body has the ability to identify disk information on a compromised host.[8]

S1087 AsyncRAT

AsyncRAT can check the disk size through the values obtained with `DeviceInfo.` [9]

S0438 Attor

Attor monitors the free disk space on the system.[10]

S0473 Avenger

Avenger has the ability to identify the host volume ID.[11]

S0638 Babuk

Babuk can enumerate disk volumes, get disk information, and query service status.[12]

S0234 Bandook

Bandook can collect information about the drives available on the system.[13]

S0239 Bankshot

Bankshot gathers disk type and disk free space.[14][15]

S1070 Black Basta

Black Basta can enumerate volumes.[16][17]

S1068 BlackCat

BlackCat can enumerate local drives.[18]

S0564 BlackMould

BlackMould can enumerate local drives on a compromised host.[19]

S0520 BLINDINGCAN

BLINDINGCAN has collected disk information, including type and free space available.[20]

S0471 build_downer

build_downer has the ability to send system volume information to C2.[11]

C0017 C0017

During C0017, APT41 issued `ping -n 1 ((cmd /c dir c:\|findstr Number).split()[-1]+` commands to find the volume serial number of compromised systems.[21]

S0351 Cannon

Cannon can gather drive information from the victim's machine.[22][23]

G0114 Chimera

Chimera has used `fsutil fsinfo drives`, `systeminfo`, and `vssadmin list shadows` for system information including shadow volumes and drive information.[24]

S0667 Chrommme

Chrommme has the ability to list drives.[25]

G0142 Confucius

Confucius has used a file stealer that can examine system drives, including those other than the C drive.[26]

S0137 CORESHELL

CORESHELL collects the volume serial number from the victim and sends the information to its C2 server.[27]

S0488 CrackMapExec

CrackMapExec can enumerate the system drives and associated system name.[28]

S0115 Crimson

Crimson contains a command to collect disk drive information.[29][30][31]

S0625 Cuba

Cuba can enumerate local drives, disk type, and disk free space.[32]

S1111 DarkGate

DarkGate uses the Delphi methods `Sysutils::DiskSize` and `GlobalMemoryStatusEx` to collect disk size and physical memory as part of the malware's anti-analysis checks for running in a virtualized environment.[33]

S0616 DEATHRANSOM

DEATHRANSOM can enumerate logical drives on a target system.[34]

S0472 down_new

down_new has the ability to identify the system volume information of a compromised host.[11]

S0091 Epic

Epic collects disk space information.[35]

S0181 FALLCHILL

FALLCHILL can collect information about installed disks from the victim.[36]

S0267 FELIXROOT

FELIXROOT collects the victim’s volume serial number.[37][38]

S1044 FunnyDream

FunnyDream can enumerate all logical drives on a targeted machine.[39]

S0617 HELLOKITTY

HELLOKITTY can enumerate logical drives on a target system.[34]

S0697 HermeticWiper

HermeticWiper can enumerate physical drives on a targeted host.[40][41][42][43]

S1027 Heyoka Backdoor

Heyoka Backdoor can enumerate drives on a compromised host.[44]

G0126 Higaisa

Higaisa collected the system volume serial number.[45][46]

S0376 HOPLIGHT

HOPLIGHT has been observed collecting victim machine volume information.[47]

S1139 INC Ransomware

INC Ransomware can discover and mount hidden drives to encrypt them.[48]

S0259 InnaputRAT

InnaputRAT gathers volume drive information.[49]

S0260 InvisiMole

InvisiMole can gather information on the mapped drives and system volume serial number.[50][51]

S0044 JHUHUGIT

JHUHUGIT obtains a build identifier as well as victim hard drive information from Windows registry key `HKLM\SYSTEM\CurrentControlSet\Services\Disk\Enum`. Another JHUHUGIT variant gathers the victim storage volume serial number and the storage device name.[52][53]

S0265 Kazuar

Kazuar gathers information on local drives.[54]

S0271 KEYMARBLE

KEYMARBLE has the capability to collect information on disk devices.[55]

S0526 KGH_SPY

KGH_SPY can collect drive information from a compromised host.[56]

S0607 KillDisk

KillDisk retrieves the hard disk name by calling the `CreateFileA to \.\PHYSICALDRIVE0` API.[57]

G0094 Kimsuky

Kimsuky has enumerated drives.[58][59]

S0356 KONNI

KONNI can gather information on connected drives and disk space from the victim's machine.[60][61][62]

S1075 KOPILUWAK

KOPILUWAK can discover logical drive information on compromised hosts.[63]

G0032 Lazarus Group

A Destover-like variant used by Lazarus Group collects disk space information and sends it to its C2 server.[64][65][66][67][68][69]

S0680 LitePower

LitePower has the ability to list local drives.[70]

S1199 LockBit 2.0

LockBit 2.0 can enumerate local drive configuration.[71][72]

S1202 LockBit 3.0

LockBit 3.0 can enumerate local drive configuration.[73]

S1016 MacMa

MacMa can collect information about a compromised computer's disk sizes.[74]

S1048 macOS.OSAMiner

macOS.OSAMiner has checked to ensure there is enough disk space using the Unix utility `df`.[75]

S1060 Mafalda

Mafalda can enumerate all drives on a compromised host.[76][77]

S1244 Medusa Ransomware

Medusa Ransomware has enumerated logical drives on infected hosts.[78]

S1026 Mongall

Mongall can identify drives on compromised hosts.[44]

S0630 Nebulae

Nebulae can discover logical drive information including the drive type, free space, and volume information.[79]

S1147 Nightdoor

Nightdoor can collect information about disk drives, their total and free space, and file system type.[80]

S1100 Ninja

Ninja can obtain information on physical drives from targeted hosts.[81][82]

S0353 NOKKI

NOKKI can gather information on drives on the victim’s machine.[83]

S0340 Octopus

Octopus can collect system drive and disk size information.[84]

C0014 Operation Wocao

During Operation Wocao, threat actors discovered the local disks attached to the system and their hardware information including manufacturer and model.[85]

S0208 Pasam

Pasam creates a backdoor through which remote attackers can retrieve information like free disk space.[86]

G0040 Patchwork

Patchwork enumerated all available drives on the victim's machine.[87][88]

S0587 Penquin

Penquin can report the disk space of a compromised host to C2.[89]

S0013 PlugX

PlugX has collected a list of all mapped drives on the infected host.[90]

S0238 Proxysvc

Proxysvc collects volume information for all drives on the system.[68]

S1228 PUBLOAD

PUBLOAD has leveraged `wmic logicaldisk get` to map local network drives.[3]

S1242 Qilin

Qilin has used `GetLogicalDrives()` and `EnumResourceW()` to locate mounted drives and shares.[91]

S0458 Ramsay

Ramsay can detect system information--including disk names, total space, and remaining space--to create a hardware profile GUID which acts as a system identifier for operators.[92][93]

S0172 Reaver

Reaver collects volume serial number from the victim.[94]

S0496 REvil

REvil can identify system drive information on a compromised host.[95][96][97][98][98][99][100][101]

S0448 Rising Sun

Rising Sun can detect drive information, including drive type, total number of bytes on disk, total number of free bytes on disk, and name of a specified volume.[102]

S1150 ROADSWEEP

ROADSWEEP can enumerate logical drives on targeted devices.[103][104]

S1073 Royal

Royal can use `GetLogicalDrives` to enumerate logical drives.[105][106]

S0253 RunningRAT

RunningRAT gathers logical drives information and volume information.[107]

S0446 Ryuk

Ryuk has called `GetLogicalDrives` to emumerate all mounted drives, and `GetDriveTypeW` to determine the drive type.[108]

S1168 SampleCheck5000

SampleCheck5000 can create unique victim identifiers by using the compromised system's volume ID.[109]

S1085 Sardonic

Sardonic has the ability to collect the C:\ drive serial number from a compromised machine.[110]

S0596 ShadowPad

ShadowPad has discovered system information including volume serial numbers.[111]

S1089 SharpDisco

SharpDisco can use a plugin to enumerate system drives.[112]

S0692 SILENTTRINITY

SILENTTRINITY can collect information related to a compromised host, including a list of drives.[113]

S0533 SLOTHFULMEDIA

SLOTHFULMEDIA has collected disk information from a victim machine.[114]

C0024 SolarWinds Compromise

During the SolarWinds Compromise, APT29 used `fsutil` to check available free space before executing actions that might create large files on disk.[115]

S0516 SoreFang

SoreFang can collect disk space information on victim machines by executing Systeminfo.[116]

S0491 StrongPity

StrongPity can identify the hard disk volume serial number on a compromised host.[117]

S1049 SUGARUSH

MoonWind can obtain the number of drives on the victim machine.[118]

S0663 SysUpdate

SysUpdate can collect a system's drive information.[119][120]

S0586 TAINTEDSCRIBE

TAINTEDSCRIBE can use `DriveList` to retrieve drive information.[121]

G0139 TeamTNT

TeamTNT has searched for disk partition and logical volume information.[122][123]

G1022 ToddyCat

ToddyCat has collected information on bootable drives including model, vendor, and serial numbers.[82]

S1239 TONESHELL

TONESHELL has retrieved the disk serial number of the device using WMI query `SELECT volumeserialnumber FROM win32_logicaldisk where Name ='C:` to identify the victim machine.[124]

S0678 Torisma

Torisma can use `GetlogicalDrives` to get a bitmask of all drives available on a compromised system. It can also use `GetDriveType` to determine if a new drive is a CD-ROM drive.[125]

G0081 Tropic Trooper

Tropic Trooper has detected a target system’s system volume information.[126][127]

S0263 TYPEFRAME

TYPEFRAME can gather the disk volume information.[128]

G1017 Volt Typhoon

Volt Typhoon has discovered file system types, drive names, size, and free space on compromised systems.[129][130][131][132]

S0689 WhisperGate

WhisperGate has the ability to enumerate fixed logical drives on a targeted system.[133]

S1065 Woody RAT

Woody RAT can retrieve information about storage drives from an infected machine.[134]

S0248 yty

yty gathers the the serial number of the main disk volume.[135]

S0251 Zebrocy

Zebrocy collects the serial number for the storage volume C:..[136][22][137][23][138][139][140]

S1151 ZeroCleare

ZeroCleare can use the `IOCTL_DISK_GET_DRIVE_GEOMETRY_EX`, `IOCTL_DISK_GET_DRIVE_GEOMETRY`, and `IOCTL_DISK_GET_LENGTH_INFO` system calls to compute disk size.[103]

S0672 Zox

Zox can enumerate attached drives.[141]
