# File and Directory Discovery, Technique T1083 - Enterprise

Archived: 2026-04-05 18:00:02 UTC

S0066 3PARA RAT

3PARA RAT has a command to retrieve metadata for files on disk as well as a command to list the current working directory.[3]

S0065 4H RAT

4H RAT has the capability to obtain file and directory listings.[3]

S1167 AcidPour

AcidPour can identify specific files and directories within the Linux operating system corresponding with storage devices for follow-on wiping activity, similar to AcidRain.[4]

S1125 AcidRain

AcidRain identifies specific files and directories in the Linux operating system associated with storage devices.[5]

S1028 Action RAT

Action RAT has the ability to collect drive and file information on an infected machine.[6]

G0018 admin@338

admin@338 actors used the following commands after exploiting a machine with LOWBALL malware to obtain information about files and directories: `dir c:\ >> %temp%\download` `dir "c:\Documents and Settings" >> %temp%\download` `dir "c:\Program Files\" >> %temp%\download` `dir d:\ >> %temp%\download` [7]

S0045 ADVSTORESHELL

ADVSTORESHELL can list files and directories.[8][9]

S1129 Akira

Akira examines files prior to encryption to determine if they meet requirements for encryption and can be encrypted by the ransomware. These checks are performed through native Windows functions such as `GetFileAttributesW`.[10][11]

S1194 Akira_v2

Akira_v2 can target specific files and folders for encryption.[12][11][13]

S1025 Amadey

Amadey has searched for folders associated with antivirus software.[14]

G1007 Aoqin Dragon

Aoqin Dragon has run scripts to identify file formats including Microsoft Word.[15]

S0622 AppleSeed

AppleSeed has the ability to search for .txt, .ppt, .hwp, .pdf, and .doc files in specified directories.[16]

G0026 APT18

APT18 can list files information for specific directories.[17]

G0007 APT28

APT28 has used Forfiles to locate PDF, Excel, and Word documents during collection. The group also searched a compromised DCCC computer for specific terms.[18][19]

G0022 APT3

APT3 has a tool that looks for files and directories on the local file system.[20][21]

G0050 APT32

APT32's backdoor possesses the capability to list files and directories on a machine. [22]

G0082 APT38

APT38 have enumerated files and directories, or searched in specific locations within a compromised host.[23]

G0087 APT39

APT39 has used tools with the ability to search for files on a compromised host.[24]

G0096 APT41

APT41 has executed `file /bin/pwd` on exploited victims, perhaps to return architecture related information.[25]

G1023 APT5

APT5 has used the BLOODMINE utility to discover files with .css, .jpg, .png, .gif, .ico, .js, and .jsp extensions in Pulse Secure Connect logs.[26]

S0456 Aria-body

Aria-body has the ability to gather metadata from a file and to search for file and directory names.[27]

S0438 Attor

Attor has a plugin that enumerates files with specific extensions on all hard disk drives and stores file information in encrypted log files.[28]

S0347 AuditCred

AuditCred can search through folders and files on the system.[29]

S0129 AutoIt backdoor

AutoIt backdoor is capable of identifying documents on the victim with the following extensions: .doc; .pdf, .csv, .ppt, .docx, .pst, .xls, .xlsx, .pptx, and .jpeg.[30]

S0640 Avaddon

Avaddon has searched for specific files prior to encryption.[31]

S0473 Avenger

Avenger has the ability to browse files in directories such as Program Files and the Desktop.[32]

S1053 AvosLocker

AvosLocker has searched for files and directories on a compromised network.[33][34]

S0344 Azorult

Azorult can recursively search for files in folders and collects files from the desktop with certain extensions.[35]

S0638 Babuk

Babuk has the ability to enumerate files on a targeted system.[36][37]

S0414 BabyShark

BabyShark has used `dir` to search for "programfiles" and "appdata".[38]

S0475 BackConfig

BackConfig has the ability to identify folders and files related to previous infections.[39]

S0093 Backdoor.Oldrea

Backdoor.Oldrea collects information about available drives, default browser, desktop file list, My Documents, Internet history, program files, and root of available drives. It also searches for ICS-related software files.[40]

S0031 BACKSPACE

BACKSPACE allows adversaries to search for files.[41]

S0642 BADFLICK

BADFLICK has searched for files on the infected host.[42]

S0128 BADNEWS

BADNEWS identifies files with certain extensions from USB devices, then copies them to a predefined directory.[43]

S0337 BadPatch

BadPatch searches for files with specific file extensions.[44]

S0234 Bandook

Bandook has a command to list files on a system.[45]

S0239 Bankshot

Bankshot searches for files on the victim's machine.[46]

S0534 Bazar

Bazar can enumerate the victim's desktop.[47][48]

S0127 BBSRAT

BBSRAT can list file and directory information.[49]

S1246 BeaverTail

BeaverTail has searched for .ldb and .log files stored in browser extension directories for collection and exfiltration.[50][51][52]

S0268 Bisonal

Bisonal can retrieve a file listing from the system.[53][54]

S1070 Black Basta

Black Basta can enumerate specific files for encryption.[55][56][57][58][59][60][61][62]

S1068 BlackCat

BlackCat can enumerate files for encryption.[63]

S0069 BLACKCOFFEE

BLACKCOFFEE has the capability to enumerate files.[64]

S0089 BlackEnergy

BlackEnergy gathers a list of installed apps from the uninstall program Registry. It also gathers registered mail, browser, and instant messaging clients from the Registry. BlackEnergy has searched for given file types.[65][66]

S0564 BlackMould

BlackMould has the ability to find files on the targeted system.[67]

S0520 BLINDINGCAN

BLINDINGCAN can search, read, write, move, and execute files.[68][69]

S0657 BLUELIGHT

BLUELIGHT can enumerate files and collect associated metadata.[70]

S1184 BOLDMOVE

BOLDMOVE can list information of all files in the system recursively from the root directory or from a specified directory.[71]

S0635 BoomBox

BoomBox can search for specific files and directories on a machine.[72]

S0651 BoxCaon

BoxCaon has searched for files on the system, such as documents located in the desktop folder.[73]

S0252 Brave Prince

Brave Prince gathers file and directory information from the victim's machine.[74]

G0060 BRONZE BUTLER

BRONZE BUTLER has collected a list of files from the victim and uploaded it to its C2 server, and then created a new list of specific files to steal.[75]

C0015 C0015

During C0015, the threat actors conducted a file listing discovery against multiple hosts to ensure locker encryption was successful.[76]

S0693 CaddyWiper

CaddyWiper can enumerate all files and directories on a compromised host.[77]

S0351 Cannon

Cannon can obtain victim drive information as well as a list of folders in C:\Program Files.[78]

S0348 Cardinal RAT

Cardinal RAT checks its current working directory upon execution and also contains watchdog functionality that ensures its executable is located in the correct path (else it will rewrite the payload).[79]

S0572 Caterpillar WebShell

Caterpillar WebShell can search for files in directories.[80]

S1043 ccf32

ccf32 can parse collected files to identify specific file extensions.[81]

S0674 CharmPower

CharmPower can enumerate drives and list the contents of the C: drive on a victim's computer.[82]

S0144 ChChes

ChChes collects the victim's %TEMP% directory path and version of Internet Explorer.[83]

S1096 Cheerscrypt

Cheerscrypt can search for log and VMware-related files with .log, .vmdk, .vmem, .vswp, and .vmsn extensions.[84]

G0114 Chimera

Chimera has utilized multiple commands to identify data of interest in file and directory listings.[85]

S1149 CHIMNEYSWEEP

CHIMNEYSWEEP has the ability to enumerate directories for files that match a set list.[86]

S0020 China Chopper

China Chopper's server component can list directory contents.[87][88]

S0023 CHOPSTICK

An older version of CHOPSTICK has a module that monitors all mounted volumes for files with the extensions .doc, .docx, .pgp, .gpg, .m2f, or .m2o.[8]

S0660 Clambling

Clambling can browse directories on a compromised host.[89][90]

S0611 Clop

Clop has searched folders and subfolders for files to encrypt.[91]

S0106 cmd

cmd can be used to find files and directories with native functionality such as `dir` commands.[92]

S1105 COATHANGER

COATHANGER will survey the contents of system files during installation.[93]

S0154 Cobalt Strike

Cobalt Strike can explore files on a compromised system.[94]

G0142 Confucius

Confucius has used a file stealer that checks the Document, Downloads, Desktop, and Picture folders for documents and images with specific extensions.[95]

G1052 Contagious Interview

Contagious Interview has conducted key word searches within files and directories on a compromised hosts to identify files for exfiltration.[52][96]

S0575 Conti

Conti can discover files on a local system.[97]

S0492 CookieMiner

CookieMiner has looked for files in the user's home directory with "wallet" in their name using `find`.[98]

S0212 CORALDECK

CORALDECK searches for specified files.[99]

S0050 CosmicDuke

CosmicDuke searches attached and mounted drives for file extensions and keywords that match a predefined list.[100]

S0488 CrackMapExec

CrackMapExec can discover specified filetypes and log files on a targeted system.[101]

S1023 CreepyDrive

CreepyDrive can specify the local file path to upload files from.[102]

S0115 Crimson

Crimson contains commands to list files and directories, as well as search for files matching certain extensions from a defined list.[103][104][105]

S0235 CrossRAT

CrossRAT can list all files on a system.[106]

S0498 Cryptoistic

Cryptoistic can scan a directory to identify files for deletion.[107]

S0625 Cuba

Cuba can enumerate files by using a variety of functions.[108]

S1153 Cuckoo Stealer

Cuckoo Stealer can search for files associated with specific applications.[109][110]

S0687 Cyclops Blink

Cyclops Blink can use the Linux API `statvfs` to enumerate the current working directory.[111][112]

S0497 Dacls

Dacls can scan directories on a compromised host.[113]

G0070 Dark Caracal

Dark Caracal collected file listings of all default Windows directories.[106]

S1111 DarkGate

Some versions of DarkGate search for the hard-coded folder `C:\Program Files\e Carte Bleue`.[114]

G0012 Darkhotel

Darkhotel has used malware that searched for files with specific patterns.[115]

S0673 DarkWatchman

DarkWatchman has the ability to enumerate file and folder names.[116]

S0255 DDKONG

DDKONG lists files on the victim’s machine.[117]

S0616 DEATHRANSOM

DEATHRANSOM can use loop operations to enumerate directories on a compromised host.[118]

S0354 Denis

Denis has several commands to search directories for files.[119][120]

S0021 Derusbi

Derusbi is capable of obtaining directory, file, and drive listings.[121][87]

S0659 Diavol

Diavol has a command to traverse the files and directories in a given path.[122]

S0600 Doki

Doki has resolved the path of a process PID to use as a script argument.[123]

S0472 down_new

down_new has the ability to list the directories on a compromised host.[32]

G0035 Dragonfly

Dragonfly has used a batch script to gather folder and file names from victim hosts.[124][125][126]

S0547 DropBook

DropBook can collect the names of all files and folders in the Program Files directories.[127][128]

S0567 Dtrack

Dtrack can list files on available disk volumes.[129][130]

S1159 DUSTTRAP

DUSTTRAP can enumerate files and directories.[131]

S0062 DustySky

DustySky scans the victim for files that contain certain keywords and document types including PDF, DOC, DOCX, XLS, and XLSX, from a list that is obtained from the C2 as a text file. It can also identify logical drives for the infected machine.[132][133]

S0081 Elise

A variant of Elise executes `dir C:\progra~1` when initially run.[134][135]

S0064 ELMER

ELMER is capable of performing directory listings.[136]

S1247 Embargo

Embargo has searched for folders, subfolders and other networked or mounted drives for follow on encryption actions.[137] Embargo has also iterated device volumes using `FindFirstVolumeW()` and `FindNextVolumeW()` functions and then calls the `GetVolumePathNamesForVolumeNameW()` function to retrieve a list of drive letters and mounted folder paths for each specified volume.[137]

S0363 Empire

Empire includes various modules for finding files of interest on hosts and network shares.[138]

S0091 Epic

Epic recursively searches for all .doc files on the system and collects a directory listing of the Desktop, %TEMP%, and %WINDOWS%\Temp directories.[139][140]

S1179 Exbyte

Exbyte enumerates all document files on an infected machine, then creates a summary of these items including filename and directory location prior to exfiltration to cloud hosting services.[141]

S0181 FALLCHILL

FALLCHILL can search files on a victim.[142]

S0512 FatDuke

FatDuke can enumerate directories on target machines.[143]

G1016 FIN13

FIN13 has used the Windows `dir` command to enumerate files and directories in a victim's network.[144]

S0182 FinFisher

FinFisher enumerates directories and scans for certain files.[145][146]

S0618 FIVEHANDS

FIVEHANDS has the ability to enumerate files on a compromised host in order to encrypt files with specific extensions.[147][148]

S0036 FLASHFLOOD

FLASHFLOOD searches for interesting files (either a default or customized set of file extensions) on the local system and removable media.[41]

S0661 FoggyWeb

FoggyWeb's loader can check for the FoggyWeb backdoor .pri file on a compromised AD FS server.[149]

S0193 Forfiles

Forfiles can be used to locate certain types of files/directories in a system.(ex: locate all files with a specific extension, name, and/or age)[18]

G0117 Fox Kitten

Fox Kitten has used WizTree to obtain network files and directory listings.[150]

S0277 FruitFly

FruitFly looks for specific files and file types.[151]

S1044 FunnyDream

FunnyDream can identify files with .doc, .docx, .ppt, .pptx, .xls, .xlsx, and .pdf extensions and specific timestamps for collection.[81]

S0628 FYAnti

FYAnti can search the `C:\Windows\Microsoft.NET\` directory for files of a specified size.[152]

S0410 Fysbis

Fysbis has the ability to search for files.[153]

G0047 Gamaredon Group

Gamaredon Group macros can scan for Microsoft Word and Excel files to inject with additional malicious macros. Gamaredon Group has also used its backdoors to automatically list interesting files (such as Office documents) found on a system.[154][155][156] Gamaredon Group has also identified directory trees, folders and files on the compromised host.[157]

S0666 Gelsemium

Gelsemium can retrieve data from specific Windows directories, as well as open random files as part of Virtualization/Sandbox Evasion.[158]

S0049 GeminiDuke

GeminiDuke collects information from the victim, including installed drivers, programs previously executed by users, programs and services configured to automatically run at startup, files and folders present in any user's home folder, files and folders present in any user's My Documents, programs installed to the Program Files folder, and recently accessed files, folders, and programs.[159]

S0249 Gold Dragon

Gold Dragon lists the directories for Desktop, program files, and the user’s recently accessed files.[74]

S0493 GoldenSpy

GoldenSpy has included a program "ExeProtector", which monitors for the existence of GoldenSpy on the infected system and redownloads if necessary.[160]

S1198 Gomir

Gomir collects information about directory and file structures, including total number of subdirectories, total number of files, and total size of files on infected systems.[161]

S0237 GravityRAT

GravityRAT collects the volumes mapped on the system, and also steals files with the following extensions: .docx, .doc, .pptx, .ppt, .xlsx, .xls, .rtf, and .pdf.[162]

S0632 GrimAgent

GrimAgent has the ability to enumerate files and directories on a compromised host.[163]

G0125 HAFNIUM

HAFNIUM has searched file contents on a compromised host.[88]

S1229 Havoc

The Havoc interface can display a file explorer view of the compromised host.[164]

S0697 HermeticWiper

HermeticWiper can enumerate common folders such as My Documents, Desktop, and AppData.[165][166]

S1027 Heyoka Backdoor

Heyoka Backdoor has the ability to search the compromised host for files.[15]

S0376 HOPLIGHT

HOPLIGHT has been observed enumerating system drives and partitions.[167]

S0431 HotCroissant

HotCroissant has the ability to retrieve a list of files in a given directory as well as drives and drive types.[168]

S0070 HTTPBrowser

HTTPBrowser is capable of listing files, folders, and drives on a victim.[169][170]

S0203 Hydraq

Hydraq creates a backdoor through which remote attackers can check for the existence of files, including its own components, as well as retrieve a list of logical drives.[171][172]

S1022 IceApple

The IceApple Directory Lister module can list information about files and directories including creation time, last write time, name, and size.[173]

S0434 Imminent Monitor

Imminent Monitor has a dynamic debugging feature to check whether it is located in the %TEMP% directory, otherwise it copies itself there.[174]

S1139 INC Ransomware

INC Ransomware can receive command line arguments to encrypt specific files and directories.[175][176]

G0100 Inception

Inception used a file listing plugin to collect information about file and directories both on local and remote drives.[177]

S0604 Industroyer

Industroyer's data wiper component enumerates specific files on all the Windows drives.[178]

S0259 InnaputRAT

InnaputRAT enumerates directories and obtains file attributes on a system.[179]

S1245 InvisibleFerret

InvisibleFerret has identified specific directories and files for exfiltration using the `ssh_upload` command which contains subcommands of `.sdira`, `sdir`, `sfile`, `sfinda`, `sfindr`, `sfind`.[52][180] InvisibleFerret also has the capability to scan and upload files of interest from multiple OS systems through the use of scripts that check file names, file extensions, and avoids certain path names.[181][96] InvisibleFerret has utilized the `findstr` on Windows or the macOS `find` commands to search for files of interest.[182]

S0260 InvisiMole

InvisiMole can list information about files in a directory and recently opened or used documents. InvisiMole can also search for specific files by supplied file mask.[183]

S0015 Ixeshe

Ixeshe can list file and directory information.[184]

S0201 JPIN

JPIN can enumerate drives and their types. It can also change file permissions using cacls.exe.[185]

S0283 jRAT

jRAT can browse file systems.[186][187]

S0088 Kasidet

Kasidet has the ability to search for a given filename on a victim.[188]

S0265 Kazuar

Kazuar finds a specified directory, lists the files and metadata about those files.[189]

G0004 Ke3chang

Ke3chang uses command-line interaction to search files and directories.[190][191]

S0387 KeyBoy

KeyBoy has a command to launch a file browser or explorer on the system.[192]

S0271 KEYMARBLE

KEYMARBLE has a command to search for files on the victim's machine.[193]

S0526 KGH_SPY

KGH_SPY can enumerate files and directories on a compromised host.[194]

S0607 KillDisk

KillDisk has used the `FindNextFile` command as part of its file deletion process.[195]

G0094 Kimsuky

Kimsuky has the ability to enumerate all files and directories on an infected system.[196][197][198]

S0599 Kinsing

Kinsing has used the find command to search for specific files.[199]

S0437 Kivars

Kivars has the ability to list drives on the infected host.[200]

S0250 Koadic

Koadic can obtain a list of directories.[201]

S0356 KONNI

A version of KONNI searches for filenames created with a previous version of the malware, suggesting different versions targeted the same victims and the versions may work together.[202]

C0035 KV Botnet Activity

KV Botnet Activity gathers a list of filenames from the following locations during execution of the final botnet stage: `\/usr\/sbin\/` , `\/usr\/bin\/` , `\/sbin\/` , `\/pfrm2.0\/bin\/` , `\/usr\/local\/bin\/` .[203]

S0236 Kwampirs

Kwampirs collects a list of files and directories in C:\ with the command `dir /s /a c:\ >> "C:\windows\TEMP[RANDOM].tmp"` .[204]

S1160 Latrodectus

Latrodectus can collect desktop filenames.[205][206][207]

G0032 Lazarus Group

Lazarus Group malware can use a common function to identify target files by their extension, and some also enumerate files and directories, including a Destover-like variant that lists files and gathers information for all drives.[208][209][210][211]

G0077 Leafminer

Leafminer used a tool called MailSniper to search for files on the desktop and another utility called Sobolsoft to extract attachments from EML files.[212]

S1185 LightSpy

LightSpy uses the `NSFileManager` to move, create and delete files. LightSpy can also use the assembly `bt` instruction to determine a file's executable permissions.[213]

S0211 Linfo

Linfo creates a backdoor through which remote attackers can list contents of drives and search for files.[214]

S1121 LITTLELAMB.WOOLTEA

LITTLELAMB.WOOLTEA can monitor for system upgrade events by checking for the presence of `/tmp/data/root/dev`.[215]

S1199 LockBit 2.0

LockBit 2.0 can exclude files associated with core system functions from encryption.[216]

S1202 LockBit 3.0

LockBit 3.0 can exclude files associated with core system functions from encryption.[217]

S1101 LoFiSe

LoFiSe can monitor the file system to identify files less than 6.4 MB in size with file extensions including .doc, .docx, .xls, .xlsx, .ppt, .pptx, .pdf, .rtf, .tif, .odt, .ods, .odp, .eml, and .msg.[218]

S0447 Lokibot

Lokibot can search for specific files on an infected host.[219]

S0582 LookBack

LookBack can retrieve file listings from the victim machine.[220]

G0030 Lotus Blossom

Lotus Blossom has used commands such as `dir` to examine the local filesystem of victim machines.[221]

G1014 LuminousMoth

LuminousMoth has used malware that scans for files in the Documents, Desktop, and Download folders and in other drives.[222][223]

S1142 LunarMail

LunarMail can search its staging directory for output files it has produced.[224]

S1141 LunarWeb

LunarWeb has the ability to retrieve directory listings.[224]

S0409 Machete

Machete produces file listings in order to search for files to be exfiltrated.[225][226][227]

S1016 MacMa

MacMa can search for a specific file on the compromised computer and can enumerate files in Desktop, Downloads, and Documents folders.[228]

S1060 Mafalda

Mafalda can search for files and directories.[229]

G0059 Magic Hound

Magic Hound malware can list a victim's logical drives and the type, as well the total/free space of the fixed devices. Other malware can list a directory's contents.[230]

S1169 Mango

Mango can enumerate the contents of current working or other specified directories.[231]

S1156 Manjusaka

Manjusaka can gather information about specific files on the victim system.[232]

S0652 MarkiRAT

MarkiRAT can look for files carrying specific extensions such as: .rtf, .doc, .docx, .xls, .xlsx, .ppt, .pptx, .pps, .ppsx, .txt, .gpg, .pkr, .kdbx, .key, and .jpb.[233]

G1051 Medusa Group

Medusa Group has searched for files within the victim environment for encryption and exfiltration.[234][235][236] Medusa Group has also identified files associated with remote management services.[234][235]

S1244 Medusa Ransomware

Medusa Ransomware has searched for files within the victim environment for encryption and exfiltration.[234][235][236] Medusa Ransomware has also identified files associated with remote management services.[234][235]

S0576 MegaCortex

MegaCortex can parse the available drives and directories to determine which files to encrypt.[237]

S1191 Megazord

Megazord can ignore specified directories for encryption.[13]

G0045 menuPass

menuPass has searched compromised systems for folders of interest including those related to HR, audit and expense, and meeting memos.[238]

S0443 MESSAGETAP

MESSAGETAP checks for the existence of two configuration files (keyword_parm.txt and parm.txt) and attempts to read the files every 30 seconds.[239]

S1059 metaMain

metaMain can recursively enumerate files in an operator-provided directory.[229][240]

S0455 Metamorfo

Metamorfo has searched the Program Files directories for specific folders and has searched for strings related to its mutexes.[241][242][243]

S0339 Micropsia

Micropsia can perform a recursive directory listing for all volume drives available on the victim's machine and can also fetch specific files by their paths.[244]

S0051 MiniDuke

MiniDuke can enumerate local drives.[143]

S0083 Misdat

Misdat is capable of running commands to obtain a list of files and directories, as well as enumerating logical drives.[245]

S1122 Mispadu

Mispadu searches for various filesystem paths to determine what banking applications are installed on the victim’s machine.[246]

S0079 MobileOrder

MobileOrder has a command to upload to its C2 server information about files on the victim mobile device, including SD card size, installed app list, SMS content, contacts, and calling history.[247]

S0149 MoonWind

MoonWind has a command to return a directory listing for a specified directory.[248]

G0069 MuddyWater

MuddyWater has used malware that checked if the ProgramData folder had folders or files with the keywords "Kasper," "Panda," or "ESET."[249]

S1135 MultiLayer Wiper

MultiLayer Wiper generates a list of all files and paths on the fixed drives of an infected system, enumerating all files on the system except specific folders defined in a hardcoded list.[250]

G0129 Mustang Panda

Mustang Panda has searched the entire target system for DOC, DOCX, PPT, PPTX, XLS, XLSX, and PDF files.[251][252]

S0272 NDiskMonitor

NDiskMonitor can obtain a list of all files and directories as well as logical drives.[43]

S0630 Nebulae

Nebulae can list files and directories on a compromised host.[253]

S0034 NETEAGLE

NETEAGLE allows adversaries to enumerate and modify the infected host's file system. It supports searching for directories, creating directories, listing directory contents, reading and writing to files, retrieving file attributes, and retrieving volume information.[41]

S0198 NETWIRE

NETWIRE has the ability to search for files on the compromised host.[254]

C0002 Night Dragon

During Night Dragon, threat actors used zwShell to establish full remote control of the connected machine and browse the victim file system.[255]

S1090 NightClub

NightClub can use a file monitor to identify .lnk, .doc, .docx, .xls, .xslx, and .pdf files.[256]

S1100 Ninja

Ninja has the ability to enumerate directory content.[257][218]

S0385 njRAT

njRAT can browse file systems using a file manager module.[258]

S0368 NotPetya

NotPetya searches for files ending with dozens of different file extensions prior to encryption.[259]

S0644 ObliqueRAT

ObliqueRAT has the ability to recursively enumerate files on an infected endpoint.[260]

S0346 OceanSalt

OceanSalt can extract drive information from the endpoint and search files on the system.[261]

S0340 Octopus

Octopus can collect information on the Windows directory and searches for compressed RAR files on the host. [262][263][264]

S1170 ODAgent

ODAgent can identify the current working directory.[265]

S0439 Okrum

Okrum has used DriveLetterView to enumerate drive information.[266]

C0012 Operation CuckooBees

During Operation CuckooBees, the threat actors used `dir c:\\` to search for files.[267]

C0022 Operation Dream Job

During Operation Dream Job, Lazarus Group conducted word searches within documents on a compromised host in search of security and financial matters.[268]

C0006 Operation Honeybee

During Operation Honeybee, the threat actors used a malicious DLL to search for files with specific keywords. [269]

C0014 Operation Wocao

During Operation Wocao, threat actors gathered a recursive directory listing to find files and directories of interest.[270]

S0229 Orz

Orz can gather victim drive information.[271]

S0402 OSX/Shlayer

OSX/Shlayer has used the command `appDir="$(dirname $(dirname "$currentDir"))"` and `$(dirname "$(pwd -P)")` to construct installation paths.[272][273]

S1017 OutSteel

OutSteel can search for specific file extensions, including zipped files.[274]

S0072 OwaAuth

OwaAuth has a command to list its directory and logical drives.[169]

S0598 P.A.S. Webshell

P.A.S. Webshell has the ability to list files and file characteristics including extension, size, ownership, and permissions.[275]

S1109 PACEMAKER

PACEMAKER can parse `/proc/"process_name"/cmdline` to look for the string `dswsd` within the command line.[276]

S0208 Pasam

Pasam creates a backdoor through which remote attackers can retrieve lists of files.[277]

G0040 Patchwork

A Patchwork payload has searched all fixed drives on the victim for files matching a specified list of extensions.[278][43]

S1102 Pcexter

Pcexter has the ability to search for files in specified directories.[218]

S0587 Penquin

Penquin can use the command code `do_vslist` to send file names, size, and status to C2.[279]

S0643 Peppy

Peppy can identify specific files for exfiltration.[103]

S0048 PinchDuke

PinchDuke searches for files created within a certain timeframe and whose file extension matches a predefined list.[159]

S1031 PingPull

PingPull can enumerate storage volumes and folder contents of a compromised host.[280]

S0124 Pisloader

Pisloader has commands to list drives on the victim machine and to list file information for a given directory.[281]

G1040 Play

Play has used the Grixba information stealer to list security files and processes.[282]

S1162 Playcrypt

Playcrypt can avoid encrypting files with a .PLAY, .exe, .msi, .dll, .lnk, or .sys file extension.[282]

S0435 PLEAD

PLEAD has the ability to list drives and files on the compromised host.[200][283]

S0013 PlugX

PlugX has a module to enumerate drives and find files recursively.[284][285][286][287] PlugX has also checked the path from which it is running for specific parameters prior to execution. [284][288][289]

S0428 PoetRAT

PoetRAT has the ability to list files upon receiving the `ls` command from C2.[290]

S0216 POORAIM

POORAIM can conduct file browsing.[99]

S0378 PoshC2

PoshC2 can enumerate files on the local file system and includes a module for enumerating recently accessed files.[291]

S0139 PowerDuke

PowerDuke has commands to get the current directory name as well as the size of a file. It also has commands to obtain information about logical drives, drive type, and free space.[292]

S0184 POWRUNER

POWRUNER may enumerate user directories on a victim.[293]

S1058 Prestige

Prestige can traverse the file system to discover files to encrypt by identifying specific extensions defined in a hardcoded list.[294]

S0113 Prikormka

A module in Prikormka collects information about the paths, size, and creation time of files with specific file extensions, but not the actual content of the file.[295]

S0238 Proxysvc

Proxysvc lists files in directories.[209]

S0078 Psylo

Psylo has commands to enumerate all storage devices and to find all files that start with a particular string.[247]

S0147 Pteranodon

Pteranodon identifies files matching certain file extension and copies them to subdirectories it created.[296]

S0192 Pupy

Pupy can walk through directories and recursively search for strings in files.[297]

S0650 QakBot

QakBot can identify whether it has been run previously on a host by checking for a specified folder.[298]

S1242 Qilin

Qilin can exclude specific directories and files from encryption.[299]

S0686 QuietSieve

QuietSieve can search files on the target host by extension, including doc, docx, xls, rtf, odt, txt, jpg, pdf, rar, zip, and 7z.[300]

S1148 Raccoon Stealer

Raccoon Stealer identifies target files and directories for collection based on a configuration file.[301][302]

S0629 RainyDay

RainyDay can use a file exfiltration tool to collect recently changed files with specific extensions.[253]

S0458 Ramsay

Ramsay can collect directory and file lists.[303][304]

S1212 RansomHub

RansomHub has the ability to only encrypt specific files.[305]

S0055 RARSTONE

RARSTONE obtains installer properties from Uninstall Registry Key entries to obtain information about installed applications and how to uninstall certain applications.[306]

S1130 Raspberry Robin

Raspberry Robin will check to see if the initial executing script is located on the user's Desktop as an anti-analysis check.[307]

S1040 Rclone

Rclone can list files and directories with the `ls`, `lsd`, and `lsl` commands.[308]

G1039 RedCurl

RedCurl has searched for and collected files on local and network drives.[309][310][311]

S0153 RedLeaves

RedLeaves can enumerate and search for files and directories.[312][83]

S0332 Remcos

Remcos can search for files on the infected machine.[313]

S0375 Remexi

Remexi searches for files on the system. [314]

S0592 RemoteUtilities

RemoteUtilities can enumerate files and directories on a target machine.[315]

S0125 Remsec

Remsec is capable of listing contents of folders on the victim. Remsec also searches for custom network encryption software on victims.[316][317][318]

S0496 REvil

REvil has the ability to identify specific files and directories that are not to be encrypted.[319][320][321][322][323][324]

S0448 Rising Sun

Rising Sun can enumerate information about files from the infected system, including file size, attributes, creation time, last access time, and write time. Rising Sun can enumerate the compilation timestamp of Windows executable files.[325]

S1150 ROADSWEEP

ROADSWEEP can enumerate files on infected devices and avoid encrypting files with .exe, .dll, .sys, .lnk, or . lck extensions.[86][326][327]

S0240 ROKRAT

ROKRAT has the ability to gather a list of files and directories on the infected system.[328][329][330]

S0090 Rover

Rover automatically searches for files on local drives based on a predefined list of file extensions.[331]

S1073 Royal

Royal can identify specific files and directories to exclude from the encryption process.[332][333][334]

S0148 RTM

RTM can check for specific files and directories associated with virtualization and malware analysis.[335]

S0446 Ryuk

Ryuk has enumerated files and folders on all mounted drives.[336]

S1018 Saint Bot

Saint Bot can search a compromised host for specific files.[274]

C0059 Salesforce Data Exfiltration

During Salesforce Data Exfiltration, threat actors queried customers' Salesforce environments to identify sensitive information for exfiltration.[337]

S1099 Samurai

Samurai can use a specific module for file enumeration.[257]

G0034 Sandworm Team

Sandworm Team has enumerated files on a compromised host.[259][338]

G1015 Scattered Spider

Scattered Spider Spider enumerates a target organization for files and directories of interest, including source code, user provisioning, MFA device registration, network diagrams, and shared credentials in documents or spreadsheets.[339][340][341][342][343]

S0461 SDBbot

SDBbot has the ability to get directory listings or drive information on a compromised host.[344]

S0345 Seasalt

Seasalt has the capability to identify the drive type on a victim.[261]

C0058 SharePoint ToolShell Exploitation

During SharePoint ToolShell Exploitation, threat actors leveraged commands to locate accessible file shares, backup paths, or SharePoint content.[345]

S1089 SharpDisco

SharpDisco can identify recently opened files by using an LNK format parser to extract the original file path from LNK files found in either `%USERPROFILE%\Recent` (Windows XP) or `%APPDATA%\Microsoft\Windows\Recent` (newer Windows versions) .[256]

S0444 ShimRat

ShimRat can list directories.[346]

S0063 SHOTPUT

SHOTPUT has a command to obtain a directory listing.[347]

S0610 SideTwist

SideTwist has the ability to search for specific files.[348]

G0121 Sidewinder

Sidewinder has used malware to collect information on files and directories.[349]

S0692 SILENTTRINITY

SILENTTRINITY has several modules, such as `ls.py` , `pwd.py` , and `recentFiles.py` , to enumerate directories and files.[350]

S0623 Siloscape

Siloscape searches for the Kubernetes config file and other related files using a regular expression.[351]

S0468 Skidmap

Skidmap has checked for the existence of specific files including `/usr/sbin/setenforce` and `/etc/selinux/config` . It also has the ability to monitor the cryptocurrency miner file and process. [352]

S0633 Sliver

Sliver can enumerate files on a target system.[353]

S0533 SLOTHFULMEDIA

SLOTHFULMEDIA can enumerate files and directories.[354]

S0226 Smoke Loader

Smoke Loader recursively searches through directories for files.[355]

C0024 SolarWinds Compromise

During the SolarWinds Compromise, APT29 obtained information about the configured Exchange virtual directory using `Get-WebServicesVirtualDirectory`.[356]

S0615 SombRAT

SombRAT can execute `enum` to enumerate files in storage on a compromised system.[357]

S0516 SoreFang

SoreFang has the ability to list directories.[358]

S0157 SOUNDBITE

SOUNDBITE is capable of enumerating and manipulating files and directories.[359]

G0054 Sowbug

Sowbug identified and extracted all Word documents on a server by using a command containing * .doc and *.docx. The actors also searched for documents based on a specific date range and attempted to identify all installed software on a victim.[360]

S0035 SPACESHIP

SPACESHIP identifies files and directories for collection by searching for specific file extensions or file modification time.[41]

S1140 Spica

Spica can list filesystem contents on targeted systems.[361]

S1234 SplatCloak

SplatCloak has used Windows API to identify files associated with Windows Defender and Kaspersky.[362]

S1200 StealBit

StealBit can be configured to exfiltrate specific file types.[216][363]

S0142 StreamEx

StreamEx has the ability to enumerate drive types.[364]

S1034 StrifeWater

StrifeWater can enumerate files on a compromised host.[365]

S0491 StrongPity

StrongPity can parse the hard drive on a compromised host to identify specific file extensions.[366]

S0603 Stuxnet

Stuxnet uses a driver to scan for specific filesystem driver objects.[367]

S1042 SUGARDUMP

SUGARDUMP can search for and collect data from specific Chrome, Opera, Microsoft Edge, and Firefox files, including any folders that have the string `Profile` in its name.[368]

S0559 SUNBURST

SUNBURST had commands to enumerate files and directories.[369][370]

S0562 SUNSPOT

SUNSPOT enumerated the Orion software Visual Studio solution directory path.[371]

S0242 SynAck

SynAck checks its directory location in an attempt to avoid launching in a sandbox.[372][373]

S0663 SysUpdate

SysUpdate can search files on a compromised host.[374][375]

S0011 Taidoor

Taidoor can search for specific files.[376]

S0586 TAINTEDSCRIBE

TAINTEDSCRIBE can use `DirectoryList` to enumerate files in a specified directory.[377]

S0467 TajMahal

TajMahal has the ability to index files from drives, user profiles, and removable drives.[378]

G0139 TeamTNT

TeamTNT has used a script that checks `/proc/*/environ` for environment variables related to AWS.[379]

S0665 ThreatNeedle

ThreatNeedle can obtain file and directory information.[380]

S0131 TINYTYPHON

TINYTYPHON searches through the drive containing the OS, then all drive letters C through to Z, for documents matching certain extensions.[30]

G1022 ToddyCat

ToddyCat has run scripts to enumerate recently modified documents having either a .pdf, .doc, .docx, .xls or .xlsx extension.[218]

S0266 TrickBot

TrickBot searches the system for all of the following file extensions: .avi, .mov, .mkv, .mpeg, .mpeg4, .mp4, .mp3, .wav, .ogg, .jpeg, .jpg, .png, .bmp, .gif, .tiff, .ico, .xlsx, and .zip. It can also obtain browsing history, cookies, and plug-in information.[381][382]

S0094 Trojan.Karagany

Trojan.Karagany can enumerate files and directories on a compromised host.[383]

S1196 Troll Stealer

Troll Stealer can enumerate and collect items from local drives and folders.[384]

G0081 Tropic Trooper

Tropic Trooper has monitored files' modified time.[385]

S0436 TSCookie

TSCookie has the ability to discover drive information on the infected host.[386]

S0647 Turian

Turian can search for specific files and list directories.[387]

G0010 Turla

Turla surveys a system upon check-in to discover files in specific locations on the hard disk %TEMP% directory, the current user's desktop, the Program Files directory, and Recent.[139][388] Turla RPC backdoors have also searched for files matching the `lPH*.dll` pattern.[389]

S0263 TYPEFRAME

TYPEFRAME can search directories for files on the victim’s machine.[390]

G1048 UNC3886

UNC3886 has used `vmtoolsd.exe` to enumerate files on guest machines.[391][392]

S0275 UPPERCUT

UPPERCUT has the capability to gather the victim's current directory.[393]

S0022 Uroburos

Uroburos can search for specific files on a compromised system.[394]

S0452 USBferry

USBferry can detect the victim's file or folder list.[385]

S0136 USBStealer

USBStealer searches victim drives for files matching certain extensions (".skr",".pkr" or ".key") or names.[395][396]

G1047 Velvet Ant

Velvet Ant has enumerated local files and folders on victim devices.[397]

S0180 Volgmer

Volgmer can list directories on a victim.[398]

G1017 Volt Typhoon

Volt Typhoon has enumerated directories containing vulnerability testing and cyber related content and facilities data such as construction drawings.[399]

S0366 WannaCry

WannaCry searches for variety of user files by file extension before encrypting them using RSA and AES, including Office, PDF, image, audio, video, source code, archive/compression format, and key and certificate files.[400][401]

S0670 WarzoneRAT

WarzoneRAT can enumerate directories on a compromise host.[402]

S0612 WastedLocker

WastedLocker can enumerate files and directories just prior to encryption.[403]

S0689 WhisperGate

WhisperGate can locate files based on hardcoded file extensions.[404][405][406][407]

G0124 Windigo

Windigo has used a script to check for the presence of files created by OpenSSH backdoors.[408]

S0466 WindTail

WindTail has the ability to enumerate the users home directory and the path to its own application bundle.[409] [410]

S0219 WINERACK

WINERACK can enumerate files and directories.[99]

S0059 WinMM

WinMM sets a WH_CBT Windows hook to search for and capture files on the victim.[411]

S0141 Winnti for Windows

Winnti for Windows can check for the presence of specific files prior to moving to the next phase of execution. [412]

G0044 Winnti Group

Winnti Group has used a program named ff.exe to search for specific documents on compromised hosts.[413]

G1035 Winter Vivern

Winter Vivern delivered malicious JavaScript payloads capable of listing folders and emails in exploited email servers.[414]

S1065 Woody RAT

Woody RAT can list all files and their associated attributes, including filename, type, owner, creation time, last access time, last write time, size, and permissions.[415]

S0161 XAgentOSX

XAgentOSX contains the readFiles function to return a detailed listing (sometimes recursive) of a specified directory.[416] XAgentOSX contains the showBackupIosFolder function to check for IOS device backups by running `ls -la ~/Library/Application\ Support/MobileSync/Backup/`.[416]

S0658 XCSSET

XCSSET has used `mdfind` to enumerate a list of apps known to grant screen sharing permissions and leverages a module to run the command `ls -la ~/Desktop`.[417][418]

S0248 yty

yty gathers information on victim's drives and has a plugin for document listing.[419]

S0251 Zebrocy

Zebrocy searches for files that are 60mb and less and contain the following extensions: .doc, .docx, .xls, .xlsx, .ppt, .pptx, .exe, .zip, and .rar. Zebrocy also runs the `echo %APPDATA%` command to list the contents of the directory.[420][421][422] Zebrocy can obtain the current execution path as well as perform drive enumeration.[423] [424]

S0330 Zeus Panda

Zeus Panda searches for specific directories on the victim's machine.[425]

S1114 ZIPLINE

ZIPLINE can find and append specific files on Ivanti Connect Secure VPNs based upon received commands.[426]

S0086 ZLib

ZLib has the ability to enumerate files and drives.[245]

S0672 Zox

Zox can enumerate files on a compromised host.[427]

S0350 zwShell

zwShell can browse the file system.[255]

S0412 ZxShell

ZxShell has a command to open a file manager and explorer on the system.[428]

---