Automated Collection, Technique T1119 - Enterprise

Archived: 2026-04-05 15:31:33 UTC

G1030 Agrius

Agrius used a custom tool, `sql.net4.exe`, to query SQL databases and then identify and extract personally identifiable information.[2]

S0622 AppleSeed

AppleSeed has automatically collected data from USB drives, keystrokes, and screen images before exfiltration.[3]

G0006 APT1

APT1 used a batch script to perform a series of discovery techniques and saves it to a text file.[4]

G0007 APT28

APT28 used a publicly available tool to gather and compress multiple documents on the DCCC and DNC networks.[5]

C0040 APT41 DUST

APT41 DUST used tools such as SQLULDR2 and PINEGROVE to gather local system and database information.[6]

C0046 ArcaneDoor

ArcaneDoor included collection of packet capture and system configuration information.[7]

S0438 Attor

Attor has automatically collected data about the compromised system.[8]

S0128 BADNEWS

BADNEWS monitors USB devices and copies files with certain extensions to a predefined directory.[9]

S0239 Bankshot

Bankshot recursively generates a list of files within a directory and sends them back to the control server.[10]

S1043 ccf32

ccf32 can be used to automatically collect files from a compromised host.[11]

G0114 Chimera

Chimera has used custom DLLs for continuous retrieval of data from memory.[12]

S0244 Comnie

Comnie executes a batch script to store discovery information in %TEMP%\info.dat and then uploads the temporarily file to the remote C2 server.[13]

G0142 Confucius

Confucius has used a file stealer to steal documents and images with the following extensions: txt, pdf, png, jpg, doc, xls, xlm, odp, ods, odt, rtf, ppt, xlsx, xlsm, docx, pptx, and jpeg.[14]

S0538 Crutch

Crutch can automatically monitor removable drives in a loop and copy interesting files.[15]

S1111 DarkGate

DarkGate searches for stored credentials associated with cryptocurrency wallets and notifies the command and control server when identified.[16]

G1003 Ember Bear

Ember Bear engages in mass collection from compromised systems during intrusions.[17]

S0363 Empire

Empire can automatically gather the username, domain name, machine name, and other information from a compromised system.[18]

G0053 FIN5

FIN5 scans processes on all victim systems in the environment and uses automated scripts to pull back the results.[19]

G0037 FIN6

FIN6 has used a script to iterate through a list of compromised PoS systems, copy and remove data to a log file, and to bind to events from the submit payment button.[20][21]

C0001 Frankenstein

During Frankenstein, the threat actors used Empire to automatically gather the username, domain name, machine name, and other system information.[18]

S1044 FunnyDream

FunnyDream can monitor files for changes and automatically collect them.[11]

G0047 Gamaredon Group

Gamaredon Group has deployed scripts on compromised systems that automatically scan for interesting documents.[22]

S0597 GoldFinder

GoldFinder logged and stored information related to the route or hops a packet took from a compromised machine to a hardcoded C2 server, including the target C2 URL, HTTP response/status code, HTTP response headers and values, and data received from the C2 node.[23]

G0125 HAFNIUM

HAFNIUM has used MSGraph to exfiltrate data from email, OneDrive, and SharePoint.[24]

S0170 Helminth

A Helminth VBScript receives a batch script to execute a set of commands in a command prompt.[25]

S0260 InvisiMole

InvisiMole can sort and collect specific documents as well as generate a list of all files on a newly inserted drive and store them in an encrypted file.[26][27]

G0004 Ke3chang

Ke3chang has performed frequent and scheduled data collection from victim networks.[28]

S0395 LightNeuron

LightNeuron can be configured to automatically collect files under a specified directory.[29]

S1101 LoFiSe

LoFiSe can collect all the files from the working directory every three hours and place them into a password-protected archive for further exfiltration.[30]

S1213 Lumma Stealer

Lumma Stealer has automated collection of various information including cryptocurrency wallet details.[31]

G0045 menuPass

menuPass has used the Csvde tool to collect Active Directory files and data.[32]

S0443 MESSAGETAP

MESSAGETAP checks two files, keyword_parm.txt and parm.txt, for instructions on how to target and save data parsed and extracted from SMS message data from the network traffic. If an SMS message contained either a phone number, IMSI number, or keyword that matched the predefined list, it is saved to a CSV file for later theft by the threat actor.[33]

S0455 Metamorfo

Metamorfo has automatically collected mouse clicks, continuous screenshots on the machine, and set timers to collect the contents of the clipboard and website browsing.[34]

S0339 Micropsia

Micropsia executes an RAR tool to recursively archive files based on a predefined list of file extensions (*.xls*, .xlsx, *.csv*, .odt, *.doc*, .docx, *.ppt*, .pptx, *.pdf*, .mdb, *.accdb*, .accde, *.txt).[35]

G0129 Mustang Panda

Mustang Panda used custom batch scripts to collect files automatically from a targeted system.[36]

S0699 Mythic

Mythic supports scripting of file downloads from agents.[37]

S0198 NETWIRE

NETWIRE can automatically archive collected data.[38]

S1131 NPPSPY

NPPSPY collection is automatically recorded to a specified file on the victim machine.[39]

G0049 OilRig

OilRig has used automated collection.[40]

C0014 Operation Wocao

During Operation Wocao, threat actors used a script to collect information about the infected system.[41]

S1017 OutSteel

OutSteel can automatically scan for and collect files with specific extensions.[42]

S1109 PACEMAKER

PACEMAKER can enter a loop to read `/proc/` entries every 2 seconds in order to read a target application's memory.[43]

S1091 Pacu

Pacu can automatically collect data, such as CloudFormation templates, EC2 user data, AWS Inspector reports, and IAM credential reports.[44]

G0040 Patchwork

Patchwork developed a file stealer to search C:\ and collect files with certain extensions. Patchwork also executed a script to enumerate all drives, store them as a list, and upload generated files to the C2 server.[9]

S0428 PoetRAT

PoetRAT used file system monitoring to track modification and enable automatic exfiltration.[45]

S0378 PoshC2

PoshC2 contains a module for recursively parsing through files and directories to gather valid credit card numbers.[46]

S0238 Proxysvc

Proxysvc automatically collects data about the victim and sends it to the control server.[47]

S1148 Raccoon Stealer

Raccoon Stealer collects files and directories from victim systems based on configuration data downloaded from command and control servers.[48][49][50]

S0458 Ramsay

Ramsay can conduct an initial scan for Microsoft Word documents on the local system, removable media, and connected network drives, before tagging and collecting them. It can continue tagging documents to collect with follow up scans.[51]

G1039 RedCurl

RedCurl has used batch scripts to collect data.[52][53]

S0684 ROADTools

ROADTools automatically gathers data from Azure AD environments using the Azure Graph API.[54]

S1078 RotaJakiro

Depending on the Linux distribution, RotaJakiro executes a set of commands to collect device information and sends the collected information to the C2 server.[55]

S0090 Rover

Rover automatically collects files from the local system and removable drives based on a predefined list of file extensions on a regular timeframe.[56]

S0148 RTM

RTM monitors browsing activity and automatically captures screenshots if a victim browses to a URL matching one of a list of strings.[57][58]

C0058 SharePoint ToolShell Exploitation

During SharePoint ToolShell Exploitation, threat actors used a command shell to automatically iterate through web.config files to expose and collect machineKey settings.[59][60]

S0445 ShimRatReporter

ShimRatReporter gathered information automatically, without instruction from a C2, related to the user and host machine that is compiled into a report and sent to the operators.[61]

G0121 Sidewinder

Sidewinder has used tools to automatically collect system and network configuration information.[62]

S1183 StrelaStealer

StrelaStealer attempts to identify and collect mail login data from Thunderbird and Outlook following execution.[63][64][65][66]

S0491 StrongPity

StrongPity has a file searcher component that can automatically collect and archive files based on a predefined list of file extensions.[67]

S0098 T9000

T9000 searches removable storage devices for files with a pre-defined list of file extensions (e.g. * .doc, *.ppt*, .xls, *.docx*, .pptx, *.xlsx). Any matching files are encrypted and written to a local user directory.[68]

S0467 TajMahal

TajMahal has the ability to index and compress files into a send queue for exfiltration.[69]

G0027 Threat Group-3390

Threat Group-3390 ran a command to compile an archive of file types of interest from the victim user's directories.[70]

G0081 Tropic Trooper

Tropic Trooper has collected information automatically using the adversary's USBferry attack.[71]

S0136 USBStealer

For all non-removable drives on a victim, USBStealer executes automated collection of certain files for later exfiltration.[72]

S0476 Valak

Valak can download a module to search for and build a report of harvested credential data.[73]

S0257 VERMIN

VERMIN saves each collected file with the automatically generated format {0:dd-MM-yyyy}.txt .[74]

S0466 WindTail

WindTail can identify and add files that possess specific file extensions to an array for archiving.[75]

G1035 Winter Vivern

Winter Vivern delivered a PowerShell script capable of recursively scanning victim machines looking for various file types before exfiltrating identified files via HTTP.[76]

S0251 Zebrocy

Zebrocy scans the system and automatically collects files with the following extensions: .doc, .docx, ,.xls, .xlsx, .pdf, .pptx, .rar, .zip, .jpg, .jpeg, .bmp, .tiff, .kum, .tlg, .sbx, .cr, .hse, .hsf, and .lhz.[77][78]
