Data Staged: Local Data Staging, Sub-technique T1074.001 - Enterprise

Archived: 2026-04-05 16:21:17 UTC

S0045 ADVSTORESHELL

ADVSTORESHELL stores output from command execution in a .dat file in the %TEMP% directory.[2]

G1030 Agrius

Agrius has used the folder, `C:\windows\temp\s\` , to stage data for exfiltration.[3]

S0622 AppleSeed

AppleSeed can stage files in a central location prior to exfiltration.[4]

G0007 APT28

APT28 has stored captured credential information in a file named pi.log.[5]

C0051 APT28 Nearest Neighbor Campaign

During APT28 Nearest Neighbor Campaign, APT28 staged captured credential information in the `C:\ProgramData` directory.[6]

G0022 APT3

APT3 has been known to stage files for exfiltration in a single location.[7]

G0087 APT39

APT39 has utilized tools to aggregate data prior to exfiltration.[8]

C0040 APT41 DUST

APT41 DUST involved exporting data from Oracle databases to local CSV files prior to exfiltration.[9]

G1023 APT5

APT5 has staged data on compromised systems prior to exfiltration often in `C:\Users\Public` .[10]

S0373 Astaroth

Astaroth collects data in a plaintext file named r1.log before exfiltration. [11]

S0438 Attor

Attor has staged collected data in a central upload directory prior to exfiltration.[12]

S1029 AuTo Stealer

AuTo Stealer can store collected data from an infected host to a file named `Hostname_UserName.txt` prior to exfiltration.[13]

G0135 BackdoorDiplomacy

BackdoorDiplomacy has copied files of interest to the main drive's recycle bin.[14]

S0128 BADNEWS

BADNEWS copies documents under 15MB found on the victim system to is the user's `%temp%\SMB\` folder. It also copies files from USB devices to a predefined directory.[15][16]

S0337 BadPatch

BadPatch stores collected data in log files before exfiltration.[17]

S1246 BeaverTail

BeaverTail has staged collected data to the system’s temporary directory.[18]

S0651 BoxCaon

BoxCaon has created a working folder for collected files that it sends to the C2 server.[19]

C0015 C0015

During C0015, PowerView's file share enumeration results were stored in the file `c:\ProgramData\found_shares.txt`.[20]

C0017 C0017

During C0017, APT41 copied the local `SAM` and `SYSTEM` Registry hives to a staging directory.[21]

C0032 C0032

During the C0032 campaign, TEMP.Veles used staging folders that are infrequently used by legitimate users or processes to store data for exfiltration and tool deployment.[22]

S0274 Calisto

Calisto uses a hidden directory named .calisto to store data from the victim’s machine before exfiltration.[23][24]

S0335 Carbon

Carbon creates a base directory that contains the files and folders that are collected.[25]

S0261 Catchamas

Catchamas stores the gathered data from the machine in .db files and .bmp files under four separate locations.[26]

S1043 ccf32

ccf32 can temporarily store files in a hidden directory on the local host.[27]

G0114 Chimera

Chimera has staged stolen data locally on compromised hosts.[28]

S1149 CHIMNEYSWEEP

CHIMNEYSWEEP can store captured screenshots to disk including to a covert store named `APPX.%x%x%x%x%x.tmp` where `%x` is a random value.[29]

S0667 Chrommme

Chrommme can store captured system information locally prior to exfiltration.[30]

S1235 CorKLOG

CorKLOG has stored the captured data in an encrypted file using a 48-character RC4 key.[31]

S0538 Crutch

Crutch has staged stolen files in the `C:\AMD\Temp` directory.[32]

S1153 Cuckoo Stealer

Cuckoo Stealer has staged collected application data from Safari, Notes, and Keychain to `/var/folder`.[33]

S0673 DarkWatchman

DarkWatchman can stage local data in the Windows Registry.[1]

G0035 Dragonfly

Dragonfly has created a directory named "out" in the user's %AppData% folder and copied files to it.[34]

S0567 Dtrack

Dtrack can save collected data to disk, different file formats, and network shares.[35][36]

S0038 Duqu

Modules can be pushed to and executed by Duqu that copy data to a staging area, compress it, and XOR encrypt it.[37]

S0062 DustySky

DustySky created folders in temp directories to host collected files before exfiltration.[38]

S0024 Dyre

Dyre has the ability to create files in a TEMP folder to act as a database to store information.[39]

S0593 ECCENTRICBANDWAGON

ECCENTRICBANDWAGON has stored keystrokes and screenshots within the `%temp%\GoogleChrome`, `%temp%\Downloads`, and `%temp%\TrendMicroUpdate` directories.[40]

S0081 Elise

Elise creates a file in `AppData\Local\Microsoft\Windows\Explorer` and stores all harvested data in that file.[41]

S0343 Exaramel for Windows

Exaramel for Windows specifies a path to store files scheduled for exfiltration.[42]

G1016 FIN13

FIN13 has utilized the following temporary folders on compromised Windows and Linux systems for their operations prior to exfiltration: `C:\Windows\Temp` and `/tmp`.[43][44]

G0053 FIN5

FIN5 scripts save memory dump data into a specific directory on hosts in the victim environment.[45]

S0036 FLASHFLOOD

FLASHFLOOD stages data it copies from the local system or removable drives in the "%WINDIR%\$NtUninstallKB885884$\" directory.[46]

S0503 FrameworkPOS

FrameworkPOS can identifiy payment card track data on the victim and copy it to a local file in a subdirectory of C:\Windows.[47]

S1044 FunnyDream

FunnyDream can stage collected information including screen captures and logged keystrokes locally.[27]

G0093 GALLIUM

GALLIUM compressed and staged files in multi-part archives in the Recycle Bin prior to exfiltration.[48]

S0249 Gold Dragon

Gold Dragon stores information gathered from the endpoint in a file named 1.hwp.[49]

S0170 Helminth

Helminth creates folders to store output from batch scripts prior to sending the information to its C2 server.[50]

G0119 Indrik Spider

Indrik Spider has stored collected data in a .tmp file.[51]

S1245 InvisibleFerret

InvisibleFerret has staged data in consolidated folders prior to exfiltration.[52]

S0260 InvisiMole

InvisiMole determines a working directory where it stores all the gathered data about the compromised machine.[53][54]

C0044 Juicy Mix

During Juicy Mix, OilRig used browser data and credential stealer tools to stage stolen files named Cupdate, Eupdate, and IUpdate in the %TEMP% directory.[55]

S0265 Kazuar

Kazuar stages command output and collected data in files before exfiltration.[56]

S0526 KGH_SPY

KGH_SPY can save collected system information to a file named "info" before exfiltration.[57]

G0094 Kimsuky

Kimsuky has staged collected data files under `C:\Program Files\Common Files\System\Ole DB\`.[58][59]

S1075 KOPILUWAK

KOPILUWAK has piped the results from executed C2 commands to `%TEMP%\result2.dat` on the local machine.[60]

G0032 Lazarus Group

Lazarus Group malware IndiaIndia saves information gathered about the victim to a file that is saved in the %TEMP% directory, then compressed, encrypted, and uploaded to a C2 server.[61][62]

G0065 Leviathan

Leviathan has used C:\Windows\Debug and C:\Perflogs as staging directories.[63][64]

C0049 Leviathan Australian Intrusions

Leviathan stored captured credential material on local log files on victim systems during Leviathan Australian Intrusions.[65]

S0395 LightNeuron

LightNeuron can store email data in files and directories specified in its configuration, such as `C:\Windows\ServiceProfiles\NetworkService\appdata\Local\Temp\`.[66]

S1101 LoFiSe

LoFiSe can save files to be evaluated for further exfiltration in the `C:\Programdata\Microsoft\` and `C:\windows\temp\` folders.
[67]

G0030 Lotus Blossom

Lotus Blossom has locally staged compressed and archived data for follow-on exfiltration.[68]

S1213 Lumma Stealer

Lumma Stealer has configured a custom user data directory such as a folder within `%USERPROFILE%\AppData\Roaming` for staging data.[69]

S1142 LunarMail

LunarMail can create a directory in `%TEMP%\` to stage data prior to exfilration.[70]

S0409 Machete

Machete stores files and logs in a folder on the local drive.[71][72]

S1016 MacMa

MacMa has stored collected files locally before exfiltration.[73]

S1060 Mafalda

Mafalda can place retrieved files into a destination directory.[74]

S0652 MarkiRAT

MarkiRAT can store collected data locally in a created .nfo file.[75]

G0045 menuPass

menuPass stages data prior to exfiltration in multi-part archives, often saved in the Recycle Bin.[76]

S0443 MESSAGETAP

MESSAGETAP stored targeted SMS messages that matched its target list in CSV files on the compromised system.[77]

S1059 metaMain

metaMain has stored the collected system files in a working directory.[74][78]

S1015 Milan

Milan has saved files prior to upload from a compromised host to folders beginning with the characters `a9850d2f`.[79]

S0084 Mis-Type

Mis-Type has temporarily stored collected information to the files `"%AppData%\{Unique Identifier}\HOSTRURKLSR"` and `"%AppData%\{Unique Identifier}\NEWERSSEMP"`.[80]

S0149 MoonWind

MoonWind saves information from its keylogging routine as a .zip file in the present working directory.[81]

G0069 MuddyWater

MuddyWater has stored a decoy PDF file within a victim's `%temp%` folder.[82]

G0129 Mustang Panda

Mustang Panda has stored collected credential files in `c:\windows\temp` prior to exfiltration. Mustang Panda has also stored documents for exfiltration in a hidden folder on USB drives.[83][84]

S0247 NavRAT

NavRAT writes multiple outputs to a TMP file using the >> method.[85]

S0198 NETWIRE

NETWIRE has the ability to write collected data to a file created in the `./LOGS` directory.[86]

S1090 NightClub

NightClub has copied captured files and keystrokes to the `%TEMP%` directory of compromised hosts.[87]

S0353 NOKKI

NOKKI can collect data from the victim and stage it in `LOCALAPPDATA%\MicroSoft Updatea\uplog.tmp`.[88]

S0644 ObliqueRAT

ObliqueRAT can copy specific files, webcam captures, and screenshots to local directories.[89]

S0340 Octopus

Octopus has stored collected information in the Application Data directory on a compromised host.[90][91]

S1172 OilBooster

OilBooster can stage files in the `tempFiles` directory for exfiltration.[92]

S0264 OopsIE

OopsIE stages the output from command execution and collected files in specific folders before exfiltration.[93]

C0006 Operation Honeybee

During Operation Honeybee, stolen data was copied into a text file using the format `From <COMPUTER-NAME> (<Month>-<Day> <Hour>-<Minute>-<Second>).txt` prior to compression, encoding, and exfiltration.[94]

C0048 Operation MidnightEclipse

During Operation MidnightEclipse, threat actors copied files to the web application folder on compromised devices for exfiltration.[95]

C0014 Operation Wocao

During Operation Wocao, threat actors staged archived files in a temporary directory prior to exfiltration.[96]

S1109 PACEMAKER

PACEMAKER has written extracted data to `tmp/dsserver-check.statementcounters`.[97]

S1233 PAKLOG

PAKLOG has stored the captured data in a file located `C:\\Users\\Public\\Libraries\\record.txt`.[31]

G0040 Patchwork

Patchwork copied all targeted files to a directory called index that was eventually uploaded to the C&C server.[16]

S0013 PlugX

PlugX has collected and staged the victim’s computer files for exfiltration.[98]

S0012 PoisonIvy

PoisonIvy stages collected data in a text file.[99]

S1012 PowerLess

PowerLess can stage stolen browser data in `C:\\Windows\\Temp\\cup.tmp` and keylogger data in `C:\\Windows\\Temp\\Report.06E17A5A-7325-4325-8E5D-E172EBA7FC5BK`.[100]

S0113 Prikormka

Prikormka creates a directory, `%USERPROFILE%\AppData\Local\SKC\`, which is used to store collected log files.[101]

S0147 Pteranodon

Pteranodon creates various subdirectories under `%Temp%\reports\%` and copies files to those subdirectories. It also creates a folder at `C:\Users\\AppData\Roaming\Microsoft\store` to store screenshot JPEG files.[102]

S0196 PUNCHBUGGY

PUNCHBUGGY has saved information to a random temp file before exfil.[103]

S0197 PUNCHTRACK

PUNCHTRACK aggregates collected data in a tmp file.[104]

S0650 QakBot

QakBot has stored stolen emails and other data into new folders prior to exfiltration.[105]

S0629 RainyDay

RainyDay can use a file exfiltration tool to copy files to `C:\ProgramData\Adobe\temp` prior to exfiltration.[106]

S0458 Ramsay

Ramsay can stage data prior to exfiltration in `%APPDATA%\Microsoft\UserSetting` and `%APPDATA%\Microsoft\UserSetting\MediaCache`.[107][108]

S0169 RawPOS

Data captured by RawPOS is placed in a temporary file under a directory named "memdump".[109]

S1222 RIFLESPINE

RIFLESPINE can stage the output from executed C2 commands to a temporary file.[110]

S0090 Rover

Rover copies files from removable drives to `C:\system`.[111]

S1210 Sagerunex

Sagerunex gathers host information and stages it locally as a RAR file prior to exfiltration.[68] Sagerunex stores logged data in an encrypted file located at `%TEMP%/TS_FB56.tmp` during execution.[112]

S1168 SampleCheck5000

SampleCheck5000 can log the output from C2 commands in an encrypted and compressed format on disk prior to exfiltration.[92]

C0058 SharePoint ToolShell Exploitation

During SharePoint ToolShell Exploitation, threat actors staged stolen data from web.config files to debug_dev.js.[113][114]

G0121 Sidewinder

Sidewinder has collected stolen files in a temporary folder in preparation for exfiltration.[115]

S1110 SLIGHTPULSE

SLIGHTPULSE has piped the output from executed commands to `/tmp/1`.[97]

S1104 SLOWPULSE

SLOWPULSE can write logged ACE credentials to `/home/perl/PAUS.pm` in append mode, using the format string `%s:%s\n`.[97]

S1124 SocGholish

SocGholish can send output from `whoami` to a local temp file using the naming convention `rad<5-hex-chars>.tmp`.[116]

S0615 SombRAT

SombRAT can store harvested data in a custom database under the %TEMP% directory.[117]

S0035 SPACESHIP

SPACESHIP identifies files with certain extensions and copies them to a directory in the user's profile.[46]

S1037 STARWHALE

STARWHALE has stored collected data in a file called `stari.txt`.[118]

G1046 Storm-1811

Storm-1811 has locally staged captured credentials for subsequent manual exfiltration.[119]

S1042 SUGARDUMP

SUGARDUMP has stored collected data under `%<malware_execution_folder>%\\CrashLog.txt`.[120]

G0139 TeamTNT

TeamTNT has aggregated collected credentials in text files before exfiltrating.[121]

G0027 Threat Group-3390

Threat Group-3390 has locally staged encrypted archives for later exfiltration efforts.[122]

S0094 Trojan.Karagany

Trojan.Karagany can create directories to store plugin output and stage data for exfiltration.[123][124]

S1196 Troll Stealer

Troll Stealer encrypts gathered information on victim devices prior to exfiltrating it through command and control infrastructure.[125]

S0647 Turian

Turian can store copied files in a specific directory prior to exfiltration.[14]

G1048 UNC3886

UNC3886 has staged captured credentials in `var/log/ldapd<unique_keyword>.2.gz`.[110]

S0386 Ursnif

Ursnif has used tmp files to stage gathered information.[126]

S0136 USBStealer

USBStealer collects files matching certain criteria from the victim and stores them in a local directory for later exfiltration.[127][128]

S1154 VersaMem

VersaMem staged captured credentials locally at `/tmp/.temp.data`.[129]

G1017 Volt Typhoon

Volt Typhoon has saved stolen files including the `ntds.dit` database and the `SYSTEM` and `SECURITY` Registry hives locally to the `C:\Windows\Temp\` directory.[130][131]

G0102 Wizard Spider

Wizard Spider has staged ZIP files in local directories such as, `C:\PerfLogs\1\` and `C:\User\1\` prior to exfiltration.[132]

S0251 Zebrocy

Zebrocy stores all collected information in a single file before exfiltration.[133]
