Exfiltration Over C2 Channel, Technique T1041 - Enterprise

Archived: 2026-04-05 12:38:03 UTC

S0045 ADVSTORESHELL

ADVSTORESHELL exfiltrates data over the same channel used for C2.[1]

G1030 Agrius

Agrius exfiltrated staged data using tools such as Putty and WinSCP, communicating with command and control servers.[2]

S1025 Amadey

Amadey has sent victim data to its C2 servers.[3]

S0584 AppleJeus

AppleJeus has exfiltrated collected host information to a C2 server.[4]

S0622 AppleSeed

AppleSeed can exfiltrate files via the C2 channel.[5]

G0022 APT3

APT3 has a tool that exfiltrates data over the C2 channel.[6]

G0050 APT32

APT32's backdoor has exfiltrated data using the already opened channel with its C&C server.[7]

G0087 APT39

APT39 has exfiltrated stolen victim data through C2 communications.[8]

C0046 ArcaneDoor

ArcaneDoor included use of existing command and control channels for data exfiltration.[9][10]

S0373 Astaroth

Astaroth exfiltrates collected information from its r1.log file to the external C2 server. [11]

S0438 Attor

Attor has exfiltrated data over the C2 channel.[12]

S1029 AuTo Stealer

AuTo Stealer can exfiltrate data over actor-controlled C2 servers via HTTP or TCP.[13]

S0031 BACKSPACE

Adversaries can direct BACKSPACE to upload files to the C2 Server.[14]

S1081 BADHATCH

BADHATCH can exfiltrate data over the C2 channel.[15][16]

S0234 Bandook

Bandook can upload files from a victim's machine over the C2 channel.[17]

S0239 Bankshot

Bankshot exfiltrates data over its C2 channel.[18]

S1246 BeaverTail

BeaverTail has exfiltrated data collected from victim devices to C2 servers.[19][20][21]

S0268 Bisonal

Bisonal has added the exfiltrated data to the URL over the C2 channel.[22]

G1043 BlackByte

BlackByte transmitted collected victim host information via HTTP POST to command and control infrastructure.[23]

S0520 BLINDINGCAN

BLINDINGCAN has sent user and system information to a C2 server via HTTP POST requests.[24][25]

S0657 BLUELIGHT

BLUELIGHT has exfiltrated data over its C2 channel.[26]

S0651 BoxCaon

BoxCaon uploads files and data from a compromised host over the existing C2 channel.[27]

S1039 Bumblebee

Bumblebee can send collected data in JSON format to C2.[28]

C0017 C0017

During C0017, APT41 used its Cloudflare services C2 channels for data exfiltration.[29]

S0077 CallMe

CallMe exfiltrates data to its C2 server over the same protocol as C2 communications.[30]

S0351 Cannon

Cannon exfiltrates collected data over email via SMTP/S and POP3/S C2 channels.[31]

S0484 Carberp

Carberp has exfiltrated data via HTTP to already established C2 servers.[32][33]

S0572 Caterpillar WebShell

Caterpillar WebShell can upload files over the C2 channel.[34]

S0674 CharmPower

CharmPower can exfiltrate gathered data to a hardcoded C2 URL via HTTP POST.[35]

G0114 Chimera

Chimera has used Cobalt Strike C2 beacons for data exfiltration.[36]

S1149 CHIMNEYSWEEP

CHIMNEYSWEEP can upload collected files to the command-and-control server.[37]

S0667 Chrommme

Chrommme can exfiltrate collected data via C2.[38]

G0142 Confucius

Confucius has exfiltrated stolen files to its C2 server.[39]

G1052 Contagious Interview

Contagious Interview has exfiltrated data from a compromised host to actor-controlled C2 servers.[40][41][42][43][19][44][45][46][20][21]

S1024 CreepySnail

CreepySnail can connect to C2 for data exfiltration.[47]

S0115 Crimson

Crimson can exfiltrate stolen information over its C2.[48]

S0538 Crutch

Crutch can exfiltrate data over the primary C2 channel (Dropbox HTTP API).[49]

S1153 Cuckoo Stealer

Cuckoo Stealer can send information about the targeted system to C2 including captured passwords, OS build, hostname, and username.[50]

G1012 CURIUM

CURIUM has used IMAP and SMTPS for exfiltration via tools such as IMAPLoader.[51]

S0687 Cyclops Blink

Cyclops Blink has the ability to upload exfiltrated files to a C2 server.[52]

S1111 DarkGate

DarkGate uses existing command and control channels to retrieve captured cryptocurrency wallet credentials.[53]

S1021 DnsSystem

DnsSystem can exfiltrate collected data to its C2 server.[54]

S0600 Doki

Doki has used Ngrok to establish C2 and exfiltrate data.[55]

S0502 Drovorub

Drovorub can exfiltrate files over C2 infrastructure.[56]

S1159 DUSTTRAP

DUSTTRAP can exfiltrate collected data over C2 channels.[57]

S0062 DustySky

DustySky has exfiltrated data to the C2 server.[58]

S0024 Dyre

Dyre has the ability to send information staged on a compromised host externally to C2.[59]

S0377 Ebury

Ebury exfiltrates a list of outbound and inbound SSH sessions using OpenSSH's `known_host` files and `wtmp` records. Ebury can exfiltrate SSH credentials through custom DNS queries or use the command `Xcat` to send the process's ssh session's credentials to the C2 server.[60][61]

S0367 Emotet

Emotet has exfiltrated data over its C2 channel.[62][63]

S0363 Empire

Empire can send data gathered from a target through the command and control channel.[64][65]

S0568 EVILNUM

EVILNUM can upload files over the C2 channel from the infected host.[66]

S0696 Flagpro

Flagpro has exfiltrated data to the C2 server.[67]

S0381 FlawedAmmyy

FlawedAmmyy has sent data collected from a compromised host to its C2 servers.[68]

S0661 FoggyWeb

FoggyWeb can remotely exfiltrate sensitive information from a compromised AD FS server.[69]

C0001 Frankenstein

During Frankenstein, the threat actors collected information via Empire, which sent the data back to the adversary's C2.[65]

S1044 FunnyDream

FunnyDream can execute commands, including gathering user information, and send the results to C2.[70]

G0093 GALLIUM

GALLIUM used Web shells and HTRAN for C2 and to exfiltrate data.[71]

G0047 Gamaredon Group

A Gamaredon Group file stealer can transfer collected files to a hardcoded C2 server.[72][73][74]

S0493 GoldenSpy

GoldenSpy has exfiltrated host environment information to an external C2 domain via port 9006.[75]

S0588 GoldMax

GoldMax can exfiltrate files over the existing C2 channel.[76][77]

S0477 Goopy

Goopy has the ability to exfiltrate data over the Microsoft Outlook C2 channel.[78]

S0531 Grandoreiro

Grandoreiro can send data it retrieves to the C2 server.[79]

S0632 GrimAgent

GrimAgent has sent data related to a compromise host over its C2 channel.[80]

S0391 HAWKBALL

HAWKBALL has sent system information and files over the C2 channel.[81]

S1249 HexEval Loader

HexEval Loader has exfiltrated victim data using HTTPS POST requests to its C2 servers.[43][44]

G0126 Higaisa

Higaisa exfiltrated data over its C2 channel.[82]

C0038 HomeLand Justice

During HomeLand Justice, threat actors used HTTP to transfer data from compromised Exchange servers.[83]

S0376 HOPLIGHT

HOPLIGHT has used its C2 channel to exfiltrate data.[84]

S0431 HotCroissant

HotCroissant has the ability to download files from the infected host to the command and control (C2) server.[85]

S1022 IceApple

IceApple's Multi File Exfiltrator module can exfiltrate multiple files from a compromised host as an HTTP response over C2.[86]

S0434 Imminent Monitor

Imminent Monitor has uploaded a file containing debugger logs, network information and system information to the C2.[87]

S0604 Industroyer

Industroyer sends information about hardware profiles and previously-received commands back to the C2 server in a POST-request.[88]

S1245 InvisibleFerret

InvisibleFerret has used HTTP communications to the "/Uploads" URI for file exfiltration.[89]

S1132 IPsec Helper

IPsec Helper exfiltrates specific files through its command and control framework.[90]

G0004 Ke3chang

Ke3chang transferred compressed and encrypted RAR files containing exfiltration through the established backdoor command and control channel during operations.[91]

S0487 Kessel

Kessel has exfiltrated information gathered from the infected system to the C2 server.[92]

S1020 Kevin

Kevin can send data from the victim host through a DNS C2 channel.[93]

S0526 KGH_SPY

KGH_SPY can exfiltrate collected information from the host to the C2 server.[94]

G0094 Kimsuky

Kimsuky has exfiltrated data over its C2 channel.[95][96]

S0356 KONNI

KONNI has sent data and files to its C2 server.[97][98][99]

S1075 KOPILUWAK

KOPILUWAK has exfiltrated collected data to its C2 via POST requests.[100]

S1160 Latrodectus

Latrodectus can exfiltrate encrypted system information to the C2 server.[101][102]

G0032 Lazarus Group

Lazarus Group has exfiltrated data and files over a C2 channel through its various tools and malware.[103][104][105]

G0065 Leviathan

Leviathan has exfiltrated data over its C2 channel.[106]

C0049 Leviathan Australian Intrusions

Leviathan exfiltrated collected data over existing command and control channels during Leviathan Australian Intrusions.[107]

S0395 LightNeuron

LightNeuron exfiltrates data over its email C2 channel.[108]

S1185 LightSpy

To exfiltrate data, LightSpy configures each module to send an obfuscated JSON blob to hardcoded URL endpoints or paths aligned to the module name.[109]

S1186 Line Dancer

Line Dancer exfiltrates collected data via command and control channels.[9]

S1188 Line Runner

Line Runner utilizes HTTP to retrieve and exfiltrate information staged using Line Dancer.[9]

S0680 LitePower

LitePower can send collected data, including screenshots, over its C2 channel.[110]

S0447 Lokibot

Lokibot has the ability to initiate contact with command and control (C2) to exfiltrate stolen data.[111]

G1014 LuminousMoth

LuminousMoth has used malware that exfiltrates stolen data to its C2 server.[112]

S1213 Lumma Stealer

Lumma Stealer has exfiltrated collected data over existing HTTP and HTTPS C2 channels.[113][114]

S1142 LunarMail

LunarMail can use email image attachments with embedded data for receiving C2 commands and data exfiltration.[115]

S0409 Machete

Machete's collected data is exfiltrated over the same channel used for C2.[116]

S1016 MacMa

MacMa exfiltrates data from a supplied path over its C2 channel.[117]

S1060 Mafalda

Mafalda can send network system data and files to its C2 server.[118]

S1182 MagicRAT

MagicRAT exfiltrates data via HTTP over existing command and control channels.[119]

S1169 Mango

Mango can use its HTTP C2 channel for exfiltration.[120]

S1156 Manjusaka

Manjusaka data exfiltration takes place over HTTP channels.[121]

S0652 MarkiRAT

MarkiRAT can exfiltrate locally stored data via its C2.[122]

S0459 MechaFlounder

MechaFlounder has the ability to send the compromised user's account name and hostname within a URL to C2.[123]

S1059 metaMain

metaMain can upload collected files and data to its C2 server.[124]

S0455 Metamorfo

Metamorfo can send the data it collects to the C2 server.[125]

S0084 Mis-Type

Mis-Type has transmitted collected files and data to its C2 server.[126]

S0083 Misdat

Misdat has uploaded files and data to its C2 servers.[126]

S1122 Mispadu

Mispadu can sends the collected financial data to the C2 server.[127][128]

S0079 MobileOrder

MobileOrder exfiltrates data to its C2 server over the same protocol as C2 communications.[30]

S1026 Mongall

Mongall can upload files and information from a compromised host to its C2 server.[129]

G0069 MuddyWater

MuddyWater has used C2 infrastructure to receive exfiltrated data.[130]

G0129 Mustang Panda

Mustang Panda has exfiltrated stolen data and files to its C2 server.[131][132][133]

S0034 NETEAGLE

NETEAGLE is capable of reading files over the C2 channel.[14]

S1090 NightClub

NightClub can use SMTP and DNS for file exfiltration and C2.[134]

S0385 njRAT

njRAT has used HTTP to receive stolen information from the infected machine.[135]

S0340 Octopus

Octopus has uploaded stolen files and data from a victim's machine over its C2 channel.[136]

S1170 ODAgent

ODAgent can use an attacker-controlled OneDrive account to receive C2 commands and to exfiltrate files.[137]

S1172 OilBooster

OilBooster can use an actor-controlled OneDrive account for C2 communication and exfiltration.[137]

S0439 Okrum

Data exfiltration is done by Okrum using the already opened channel with the C2 server.[138]

S0264 OopsIE

OopsIE can upload files from the victim's machine to its C2 server.[139]

C0022 Operation Dream Job

During Operation Dream Job, Lazarus Group exfiltrated data from a compromised host to actor-controlled C2 servers.[140]

C0006 Operation Honeybee

During Operation Honeybee, the threat actors uploaded stolen files to their C2 servers.[141]

C0014 Operation Wocao

During Operation Wocao, threat actors used the XServer backdoor to exfiltrate data.[142]

S1017 OutSteel

OutSteel can upload files from a compromised host over its C2 channel.[143]

S1050 PcShare

PcShare can upload files and information from a compromised host to its C2 servers.[70]

S0587 Penquin

Penquin can execute the command code `do_upload` to send files to C2.[144]

S1145 Pikabot

During the initial Pikabot command and control check-in, Pikabot will transmit collected system information encrypted using RC4.[145]

S1031 PingPull

PingPull has the ability to exfiltrate stolen victim data through its C2 channel.[146]

S0013 PlugX

PlugX has exfiltrated stolen data and files to its C2 server.[147][133]

S0428 PoetRAT

PoetRAT has exfiltrated data over the C2 channel.[148]

S1173 PowerExchange

PowerExchange can exfiltrate files via its email C2 channel.[149]

S0441 PowerShower

PowerShower has used a PowerShell document stealer module to pack and exfiltrate .txt, .pdf, .xls or .doc files smaller than 5MB that were modified during the past two days.[150]

S0238 Proxysvc

Proxysvc performs data exfiltration over the control server channel using a custom protocol.[151]

S0078 Psylo

Psylo exfiltrates data to its C2 server over the same protocol as C2 communications.[30]

S0147 Pteranodon

Pteranodon exfiltrates screenshot files to its C2 server.[72]

S0192 Pupy

Pupy can send screenshots files, keylogger data, files, and recorded audio back to the C2 server.[152]

S0650 QakBot

QakBot can send stolen information to C2 nodes including passwords, accounts, and emails.[153]

S1148 Raccoon Stealer

Raccoon Stealer uses existing HTTP-based command and control channels for exfiltration.[154][155][156]

S0495 RDAT

RDAT can exfiltrate data gathered from the infected system via the established Exchange Web Services API C2 channel.[157]

S1240 RedLine Stealer

RedLine Stealer has sent victim data to its C2 server or RedLine panel server.[158]

C0056 RedPenguin

During RedPenguin, UNC3886 uploaded specified files from compromised devices to a remote server. [159]

S0375 Remexi

Remexi performs exfiltration over BITSAdmin, which is also used for the C2 channel.[160]

S0496 REvil

REvil can exfiltrate host and malware information to C2 servers.[161]

S0448 Rising Sun

Rising Sun can send data gathered from the infected machine via HTTP POST request to the C2.[162]

S0240 ROKRAT

ROKRAT can send collected files back over same C2 channel.[163]

S1078 RotaJakiro

RotaJakiro sends device and other collected data back to the C2 using the established C2 channels over TCP. [164]

S0085 S-Type

S-Type has uploaded data and files from a compromised host to its C2 servers.[126]

S1210 Sagerunex

Sagerunex encrypts collected system data then exfiltrates via existing command and control channels.[165]

G0034 Sandworm Team

Sandworm Team has sent system information to its C2 server using HTTP.[166]

G1015 Scattered Spider

Scattered Spider has exfiltrated data from compromised VMware vCenter servers through an established C2 channel using the Teleport remote access tool.[167]

S0461 SDBbot

SDBbot has sent collected data from a compromised host to its C2 servers.[68]

C0058 SharePoint ToolShell Exploitation

During SharePoint ToolShell Exploitation, threat actors exfiltrated stolen credentials and internal data over HTTPS to C2 infrastructure.[168]

S1019 Shark

Shark has the ability to upload files from the compromised host over a DNS or HTTP C2 channel.[169]

S1089 SharpDisco

SharpDisco can load a plugin to exfiltrate stolen files to SMB shares also used in C2.[134]

S0445 ShimRatReporter

ShimRatReporter sent generated reports to the C2 via HTTP POST requests.[170]

S1178 ShrinkLocker

ShrinkLocker will exfiltrate victim system information along with the encryption key via an HTTP POST.[171] [172]

S0610 SideTwist

SideTwist has exfiltrated data over its C2 channel.[173]

S0692 SILENTTRINITY

SILENTTRINITY can transfer files from an infected host to the C2 server.[174]

S0633 Sliver

Sliver can exfiltrate files from the victim using the `download` command.[175]

S0533 SLOTHFULMEDIA

SLOTHFULMEDIA has sent system information to a C2 server via HTTP and HTTPS POST requests.[176]

S0649 SMOKEDHAM

SMOKEDHAM has exfiltrated data to its C2 server.[177]

S1166 Solar

Solar can send staged files to C2 for exfiltration.[120]

S0615 SombRAT

SombRAT has uploaded collected data and files from a compromised host to its C2 server.[178]

S0543 Spark

Spark has exfiltrated data over the C2 channel.[179]

S1030 Squirrelwaffle

Squirrelwaffle has exfiltrated victim data using HTTP POST requests to its C2 servers.[180]

S1037 STARWHALE

STARWHALE can exfiltrate collected data to its C2 servers.[181]

G0038 Stealth Falcon

After data is collected by Stealth Falcon malware, it is exfiltrated over the existing C2 channel.[182]

S1183 StrelaStealer

StrelaStealer exfiltrates collected email credentials via HTTP POST to command and control servers.[183][184][185][186]

S1034 StrifeWater

StrifeWater can send data and files from a compromised host to its C2 server.[187]

S0491 StrongPity

StrongPity can exfiltrate collected documents through C2 channels.[188][189]

S0603 Stuxnet

Stuxnet sends compromised victim information via HTTP.[190]

S1042 SUGARDUMP

SUGARDUMP has sent stolen credentials and other data to its C2 server.[191]

S1064 SVCReady

SVCReady can send collected data in JSON format to its C2 server.[192]

S0663 SysUpdate

SysUpdate has exfiltrated data over its C2 channel.[193]

S0467 TajMahal

TajMahal has the ability to send collected files over its C2.[194]

S0595 ThiefQuest

ThiefQuest exfiltrates targeted file extensions in the `/Users/` folder to the command and control server via unencrypted HTTP. Network packets contain a string with two pieces of information: a file path and the contents of the file in a base64 encoded string.[195][196]

S0671 Tomiris

Tomiris can upload files matching a hardcoded set of extensions, such as .doc, .docx, .pdf, and .rar, to its C2 server.[197]

S0678 Torisma

Torisma can send victim data to an actor-controlled C2 server.[198]

S1201 TRANSLATEXT

TRANSLATEXT has exfiltrated collected credentials to the C2 server.[199]

S0266 TrickBot

TrickBot can send information about the compromised host and upload data to a hardcoded C2 server.[200][201]

S1196 Troll Stealer

Troll Stealer exfiltrates collected information to its command and control infrastructure.[202]

S0386 Ursnif

Ursnif has used HTTP POSTs to exfil gathered information.[203][204][205]

S0476 Valak

Valak has the ability to exfiltrate data over the C2 channel.[206][207][208]

S0670 WarzoneRAT

WarzoneRAT can send collected victim data to its C2 server.[209]

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.[210]

G0102 Wizard Spider

Wizard Spider has exfiltrated domain credentials and network enumeration information over command and control (C2) channels.[211][212]

S1065 Woody RAT

Woody RAT can exfiltrate files from an infected machine to its C2 server.[213]

S0658 XCSSET

XCSSET retrieves files that match the pattern defined in the INAME_QUERY variable within the user's home directory, such as `*test.txt`, and are below a specific size limit. It then archives the files and exfiltrates the data over its C2 channel.[214][215]

S1248 XORIndex Loader

XORIndex Loader has exfiltrated victim data using HTTPS POST requests to its C2 servers.[19]

S0251 Zebrocy

Zebrocy has exfiltrated data to the designated C2 server using HTTP POST requests.[216][217]

G0128 ZIRCONIUM

ZIRCONIUM has exfiltrated files via the Dropbox API C2.[218]

S0086 ZLib

ZLib has sent data and files from a compromised host to its C2 servers.[126]
