Archive Collected Data: Archive via Utility, Sub-technique T1560.001 - Enterprise

Archived: 2026-04-05 17:01:50 UTC

G1030 Agrius

Agrius used 7zip to archive extracted data in preparation for exfiltration.[5]

G1024 Akira

Akira uses utilities such as WinRAR to archive data prior to exfiltration.[6]

S0622 AppleSeed

AppleSeed can zip and encrypt data collected on a target system.[7]

G0006 APT1

APT1 has used RAR to compress files before moving them outside of the victim network.[8]

G0007 APT28

APT28 has used a variety of utilities, including WinRAR, to archive collected data with password protection.[9]

C0051 APT28 Nearest Neighbor Campaign

During APT28 Nearest Neighbor Campaign, APT28 used built-in PowerShell capabilities (`Compress-Archive` cmdlet) to compress collected data.[10]

G0022 APT3

APT3 has used tools to compress data before exfilling it.[11]

G0064 APT33

APT33 has used WinRAR to compress data prior to exfil.[12]

G0087 APT39

APT39 has used WinRAR and 7-Zip to compress an archive stolen data.[13]

G0096 APT41

APT41 created a RAR archive of targeted files for exfiltration.[14] Additionally, APT41 used the makecab.exe utility to both download tools, such as NATBypass, to the victim network and to archive a file for exfiltration.[15]

C0040 APT41 DUST

APT41 DUST used `rar` to compress data downloaded from internal Oracle databases prior to exfiltration.[16]

G1023 APT5

APT5 has used the JAR/ZIP file format for exfiltrated files.[17]

G0143 Aquatic Panda

Aquatic Panda has used several publicly available tools, including WinRAR and 7zip, to compress collected files and memory dumps prior to exfiltration.[18][19]

S1246 BeaverTail

BeaverTail has collected and archived sensitive data in a zip file.[20]

G0060 BRONZE BUTLER

BRONZE BUTLER has compressed data into password-protected RAR archives prior to exfiltration.[21][22]

C0026 C0026

During C0026, the threat actors used WinRAR to collect documents on targeted systems. The threat actors appeared to only exfiltrate files created after January 1, 2021.[23]

S0274 Calisto

Calisto uses the `zip -r` command to compress the data collected on the local system.[24][25]

S1043 ccf32

ccf32 has used `xcopy \\<target_host>\c$\users\public\path.7z c:\users\public\bin\<target_host>.7z /H /Y` to archive collected files.[26]

S0160 certutil

certutil may be used to Base64 encode collected data.[27][28]

G0114 Chimera

Chimera has used gzip for Linux OS and a modified RAR software to archive data on Windows hosts.[29][30]

G0052 CopyKittens

CopyKittens uses ZPP, a .NET console program, to compress files with ZIP.[31]

S0212 CORALDECK

CORALDECK has created password-protected RAR, WinImage, and zip archives to be exfiltrated.[32]

S0538 Crutch

Crutch has used the WinRAR utility to compress and encrypt stolen files.[33]

C0029 Cutting Edge

During Cutting Edge, threat actors saved collected data to a tar archive.[34]

S0187 Daserf

Daserf hides collected data in password-protected .rar archives.[35]

S0062 DustySky

DustySky can compress files via RAR while staging data to be exfiltrated.[36]

G1006 Earth Lusca

Earth Lusca has used WinRAR to compress stolen files into an archive prior to exfiltration.[37]

G1016 FIN13

FIN13 has compressed the dump output of compromised credentials with a 7zip binary.[38]

G0061 FIN8

FIN8 has used RAR to compress collected data before exfiltration.[39]

G0117 Fox Kitten

Fox Kitten has used 7-Zip to archive data.[40]

C0007 FunnyDream

During FunnyDream, the threat actors used 7zr.exe to add collected files to an archive.[26]

G0093 GALLIUM

GALLIUM used WinRAR to compress and encrypt stolen data prior to exfiltration.[41][42]

G0084 Gallmaker

Gallmaker has used WinZip, likely to archive data prior to exfiltration.[43]

G0125 HAFNIUM

HAFNIUM has used 7-Zip and WinRAR to compress stolen files for exfiltration.[44][45]

S1022 IceApple

IceApple can encrypt and compress files using Gzip prior to exfiltration.[46]

S0278 iKitten

iKitten will zip up the /Library/Keychains directory before exfiltrating it.[47]

G1032 INC Ransom

INC Ransom has used 7-Zip and WinRAR to archive collected data prior to exfiltration.[48][49][50][51]

S1245 InvisibleFerret

InvisibleFerret has used 7zip, RAR and zip files to archive collected data for exfiltration.[52][53]

S0260 InvisiMole

InvisiMole uses WinRAR to compress data that is intended to be exfiltrated.[54]

G0004 Ke3chang

Ke3chang is known to use 7Zip and RAR with passwords to encrypt data prior to exfiltration.[55][56]

G0094 Kimsuky

Kimsuky has used QuickZip to archive stolen files before exfiltration.[57]

G0030 Lotus Blossom

Lotus Blossom has used WinRAR for compressing data in RAR format.[58][59]

S1141 LunarWeb

LunarWeb can create a ZIP archive with specified files and directories.[60]

G0059 Magic Hound

Magic Hound has used gzip to archive dumped LSASS process memory and RAR to stage and compress local folders.[61][62][63]

G0045 menuPass

menuPass has compressed files before exfiltration using TAR and RAR.[64][65][66]

S0339 Micropsia

Micropsia creates a RAR archive based on collected files on the victim's machine.[67]

G0069 MuddyWater

MuddyWater has used the native Windows cabinet creation tool, makecab.exe, likely to compress stolen data to be uploaded.[68]

G0129 Mustang Panda

Mustang Panda has used RAR to create password-protected archives of collected documents prior to exfiltration.[69][70] Mustang Panda has used WinRAR "Rar.exe" to archive stolen files before exfiltration.[71] Mustang Panda has also used TONESHELL and post-exploitation tools such as RemCom and Impacket to execute WinRAR `rar.exe` to archive files for exfiltration.[72]

S0340 Octopus

Octopus has compressed data before exfiltrating it using a tool called Abbrevia.[73]

S0439 Okrum

Okrum was seen using a RAR archiver tool to compress/decompress data.[74]

S0264 OopsIE

OopsIE compresses collected files with GZipStream before sending them to its C2 server.[75]

C0012 Operation CuckooBees

During Operation CuckooBees, the threat actors used the Makecab utility to compress and a version of WinRAR to create password-protected archives of stolen data prior to exfiltration.[76]

C0022 Operation Dream Job

During Operation Dream Job, Lazarus Group archived victim's data into a RAR file.[77]

C0006 Operation Honeybee

During Operation Honeybee, the threat actors uses zip to pack collected files before exfiltration.[78]

C0014 Operation Wocao

During Operation Wocao, threat actors archived collected files with WinRAR, prior to exfiltration.[79]

G1040 Play

Play has used WinRAR to compress files prior to exfiltration.[80][81]

S0428 PoetRAT

PoetRAT has the ability to compress files with zip.[82]

S0378 PoshC2

PoshC2 contains a module for compressing data using ZIP.[83]

S0441 PowerShower

PowerShower has used 7Zip to compress .txt, .pdf, .xls or .doc files prior to exfiltration.[84]

S1228 PUBLOAD

PUBLOAD has used utilities such as `WinRAR` to archive data prior to exfiltration.[85]

S0196 PUNCHBUGGY

PUNCHBUGGY has Gzipped information and saved it to a random temp file before exfil.[86]

S0192 Pupy

Pupy can compress data with Zip before sending it over C2.[87]

S0458 Ramsay

Ramsay can compress and archive collected files using WinRAR.[88][89]

S1040 Rclone

Rclone can compress files using `gzip` prior to exfiltration.[90]

G1039 RedCurl

RedCurl has downloaded 7-Zip to decompress password protected archives.[91]

S1210 Sagerunex

Sagerunex has archived collected materials in RAR format.[58]

S1168 SampleCheck5000

SampleCheck5000 can gzip compress files uploaded to a shared mailbox used for C2 and exfiltration.[92]

G1041 Sea Turtle

Sea Turtle used the tar utility to create a local archive of email data on a victim system.[93]

C0024 SolarWinds Compromise

During the SolarWinds Compromise, APT29 used 7-Zip to compress stolen emails into password-protected archives prior to exfltration; APT29 also compressed text files into zipped archives.[94][95][96]

G0054 Sowbug

Sowbug extracted documents and bundled them into a RAR archive.[97]

G1022 ToddyCat

ToddyCat has leveraged xcopy, 7zip, and RAR to stage and compress collected documents prior to exfiltration.[98]

S1239 TONESHELL

TONESHELL used WinRAR rar.exe to archive files for exfiltration.[72][71] TONESHELL has also utilized a unique 13-character password consisting of upper lower case and digits to protect RAR archives.[71]

S0647 Turian

Turian can use WinRAR to create a password-protected archive for files of interest.[99]

G0010 Turla

Turla has encrypted files stolen from connected USB drives into a RAR file before exfiltration.[100]

G1048 UNC3886

UNC3886 has used Gzip and the Windows command `makecab` to compress files and stolen credentials from victim systems.[101][102]

G1017 Volt Typhoon

Volt Typhoon has archived the ntds.dit database as a multi-volume password-protected archive with 7-Zip.[103][104]

S0466 WindTail

WindTail has the ability to use the macOS built-in zip utility to archive files.[105]

G0102 Wizard Spider

Wizard Spider has archived data into ZIP files on compromised machines.[106]
