Data from Removable Media, Technique T1025 - Enterprise

Archived: 2026-04-05 13:03:42 UTC

S0622 AppleSeed

AppleSeed can find and collect data from removable media devices.[1][2]

G0007 APT28

An APT28 backdoor may collect the entire contents of an inserted USB device.[3]

S0456 Aria-body

Aria-body has the ability to collect data from USB devices.[4]

S0128 BADNEWS

BADNEWS copies files with certain extensions from USB devices to a predefined directory.[5]

S0050 CosmicDuke

CosmicDuke steals user files from removable media with file extensions and keywords that match a predefined list.[6]

S0115 Crimson

Crimson contains a module to collect data from removable drives.[7][8]

S0538 Crutch

Crutch can monitor removable drives and exfiltrate files matching a given extension list.[9]

S0569 Explosive

Explosive can scan all .exe files located in the USB drive.[10]

S0036 FLASHFLOOD

FLASHFLOOD searches for interesting files (either a default or customized set of file extensions) on removable media and copies them to a staging area. The default file types copied would include data copied to the drive by SPACESHIP.[11]

S1044 FunnyDream

The FunnyDream FilePakMonitor component has the ability to collect files from removable devices.[12]

G0047 Gamaredon Group

A Gamaredon Group file stealer has the capability to steal data from newly connected logical volumes on a system, including USB drives.[13][14][15]

S0237 GravityRAT

GravityRAT steals files based on an extension list if a USB drive is connected to the system.[16]

S0260 InvisiMole

InvisiMole can collect jpeg files from connected MTP devices.[17]

S0409 Machete

Machete can find, encrypt, and upload files from fixed and removable drives.[18][19]

S1146 MgBot

MgBot includes modules capable of gathering information from USB thumb drives and CD-ROMs on the victim machine given a list of provided criteria.[20]

S0644 ObliqueRAT

ObliqueRAT has the ability to extract data from removable devices connected to the endpoint.[21]

G0049 OilRig

OilRig has used Wireshark's usbcapcmd utility to capture USB traffic.[22]

S0113 Prikormka

Prikormka contains a module that collects documents with certain extensions from removable media or fixed drives connected via USB.[23]

S0458 Ramsay

Ramsay can collect data from removable media and stage it for exfiltration.[24]

S0125 Remsec

Remsec has a package that collects documents from any inserted USB sticks.[25]

S0090 Rover

Rover searches for files on attached removable drives based on a predefined list of file extensions every five seconds.[26]

S0467 TajMahal

TajMahal has the ability to steal written CD images and files of interest from previously connected removable drives when they become available again.[27]

G0010 Turla

Turla RPC backdoors can collect files from USB thumb drives.[28][29]

S0136 USBStealer

Once a removable media device is inserted back into the first victim, USBStealer collects data from it that was exfiltrated from a second victim.[30][31]

Source: https://attack.mitre.org/techniques/T1025