Automated Exfiltration, Technique T1020 - Enterprise

Archived: 2026-04-05 13:17:56 UTC

C0046 ArcaneDoor

ArcaneDoor included scripted exfiltration of collected data.[2]

S0438 Attor

Attor has a file uploader plugin that automatically exfiltrates the collected data and log files to the C2 server.[3]

S0050 CosmicDuke

CosmicDuke exfiltrates collected files automatically over FTP to remote servers.[4]

S0538 Crutch

Crutch has automatically exfiltrated stolen files to Dropbox.[5]

S0600 Doki

Doki has used a script that gathers information from a hardcoded list of IP addresses and uploads to an Ngrok URL.[6]

S0377 Ebury

If credentials are not collected for two weeks, Ebury encrypts the credentials using a public key and sends them via UDP to an IP address located in the DNS TXT record.[7][8]

S0363 Empire

Empire has the ability to automatically send collected data back to the threat actors' C2.[9]

C0001 Frankenstein

During Frankenstein, the threat actors collected information via Empire, which was automatically sent back to the adversary's C2.[9]

G0047 Gamaredon Group

Gamaredon Group has used modules that automatically upload gathered documents to the C2 server.[1]

S1211 Hannotog

Hannotog can upload encyrpted data for exfiltration.[10]

G0004 Ke3chang

Ke3chang has performed frequent and scheduled data exfiltration from compromised networks.[11]

S0395 LightNeuron

LightNeuron can be configured to automatically exfiltrate files under a specified directory.[12]

S0409 Machete

Machete's collected files are exfiltrated automatically to remote servers.[13]

S1017 OutSteel

OutSteel can automatically upload collected files to its C2 server.[14]

S0643 Peppy

Peppy has the ability to automatically exfiltrate files and keylogs.[15]

S1148 Raccoon Stealer

Raccoon Stealer will automatically collect and exfiltrate data identified in received configuration files from command and control nodes.[16][17][18]

G1039 RedCurl

RedCurl has used batch scripts to exfiltrate data.[19][20]

S0090 Rover

Rover automatically searches for files on local drives based on a predefined list of file extensions and sends them to the command and control server every 60 minutes. Rover also automatically sends keylogger files and screenshots to the C2 server on a regular timeframe.[21]

C0059 Salesforce Data Exfiltration

During Salesforce Data Exfiltration, threat actors used API queries to automatically exfiltrate large volumes of data.[22]

S0445 ShimRatReporter

ShimRatReporter sent collected system and network information compiled into a report to an adversary-controlled C2.[23]

G0121 Sidewinder

Sidewinder has configured tools to automatically send collected files to attacker controlled servers.[24]

S1166 Solar

Solar can automatically exfitrate files from compromised systems.[25]

S1183 StrelaStealer

StrelaStealer automatically sends gathered email credentials following collection to command and control servers via HTTP POST.[26][27]

S0491 StrongPity

StrongPity can automatically exfiltrate collected documents to the C2 server.[28][29]

S0467 TajMahal

TajMahal has the ability to manage an automated queue of egress files and commands sent to its C2.[30]

S0131 TINYTYPHON

When a document is found matching one of the extensions in the configuration, TINYTYPHON uploads it to the C2 server.[31]

G0081 Tropic Trooper

Tropic Trooper has used a copy function to automatically exfiltrate sensitive data from air-gapped systems using USB storage.[32]

S0136 USBStealer

USBStealer automatically exfiltrates collected files via removable media when an infected device connects to an air-gapped victim machine after initially being connected to an internet-enabled victim machine. [33]

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.[34]
