Masquerading, Technique T1036 - Enterprise

Archived: 2026-04-02 12:32:07 UTC

G1030 Agrius

Agrius used the Plink tool for tunneling and connections to remote machines, renaming it `systems.exe` in some instances.[2]

G1007 Aoqin Dragon

Aoqin Dragon has used fake icons including antivirus and external drives to disguise malicious payloads.[3]

S0622 AppleSeed

AppleSeed can disguise JavaScript files as PDFs.[4]

G0007 APT28

APT28 has renamed the WinRAR utility to avoid detection.[5]

G0050 APT32

APT32 has disguised a Cobalt Strike beacon as a Flash Installer.[6]

C0046 ArcaneDoor

ArcaneDoor involved the use of digital certificates on adversary-controlled network infrastructure that mimicked the formatting used by legitimate Cisco ASA appliances.[7]

S1246 BeaverTail

BeaverTail has masqueraded as MiroTalk installation packages: "MiroTalk.dmg" for macOS and "MiroTalk.msi" for Windows, and has included login GUIs with MiroTalk themes.[8]

S0268 Bisonal

Bisonal dropped a decoy payload with a .jpg extension that contained a malicious Visual Basic script.[9]

S0635 BoomBox

BoomBox has the ability to mask malicious data strings as PDF files.[10]

G0060 BRONZE BUTLER

BRONZE BUTLER has masked executables with document file icons including Word and Adobe PDF.[11]

C0015 C0015

During C0015, the threat actors named a binary file `compareForfor.jpg` to disguise it as a JPG file.[12]

C0018 C0018

During C0018, AvosLocker was disguised using the victim company name as the filename.[13]

G1052 Contagious Interview

Contagious Interview has delivered BeaverTail malware masquerading as legitimate software or applications.[14][15][16][17][8] Contagious Interview has also delivered malicious payloads masquerading as legitimate software drivers.[18]

S0497 Dacls

The Dacls Mach-O binary has been disguised as a .nib file.[19]

S1111 DarkGate

DarkGate can masquerade as pirated media content for initial delivery to victims.[20]

S1066 DarkTortilla

DarkTortilla's payload has been renamed `PowerShellInfo.exe`.[21]

S0673 DarkWatchman

DarkWatchman has used an icon mimicking a text file to mask a malicious executable.[22]

G1003 Ember Bear

Ember Bear has renamed the legitimate Sysinternals tool procdump to alternative names such as `dump64.exe` to evade detection.[23]

S0634 EnvyScout

EnvyScout has used folder icons for malicious files to lure victims into opening them.[10]

G1016 FIN13

FIN13 has masqueraded staged data by using the Windows certutil utility to generate fake Base64 encoded certificates with the input file.[24][25]

S0696 Flagpro

Flagpro can download malicious files with a .tmp extension and append them with .exe prior to execution.[26]

S0661 FoggyWeb

FoggyWeb can masquerade the output of C2 commands as a fake, but legitimately formatted WebP file.[27]

C0035 KV Botnet Activity

KV Botnet Activity involves changing process filename to `pr_set_mm_exe_file` and process name to `pr_set_name` during later infection stages.[28]

G0140 LazyScripter

LazyScripter has used several different security software icons to disguise executables.[29]

G0045 menuPass

menuPass has used esentutl to change file extensions to their true type that were masquerading as .txt files.[30]

S1015 Milan

Milan has used an executable named `companycatalogue` to appear benign.[31]

S0637 NativeZone

NativeZone has, upon execution, displayed a message box that appears to be related to a Ukrainian electronic document management system.[32]

G0133 Nomadic Octopus

Nomadic Octopus attempted to make Octopus appear as a Telegram Messenger with a Russian interface.[33]

S0368 NotPetya

NotPetya drops PsExec with the filename dllhost.dat.[34]

G0049 OilRig

OilRig has used .doc file extensions to mask malicious executables.[35]

C0016 Operation Dust Storm

For Operation Dust Storm, the threat actors disguised some executables as JPG files.[36]

C0006 Operation Honeybee

During Operation Honeybee, the threat actors modified the MaoCheng dropper so its icon appeared as a Word document.[37]

G0068 PLATINUM

PLATINUM has renamed rar.exe to avoid detection.[38]

S0453 Pony

Pony has used the Adobe Reader icon for the downloaded file to look more trustworthy.[39]

S1046 PowGoop

PowGoop has disguised a PowerShell script as a .dat file (goopdate.dat).[40]

S0565 Raindrop

Raindrop was built to include a modified version of 7-Zip source code (including associated export names) and Far Manager source code.[41][42]

S0458 Ramsay

Ramsay has masqueraded as a JPG image file.[43]

S0662 RCSession

RCSession has used a file named English.rtf to appear benign on victim hosts.[44][45]

S1240 RedLine Stealer

RedLine Stealer malware has masqueraded as legitimate software such as "PDF Converter Software" which has been distributed through poisoned search engine results often resembling legitimate software lures with the combination of typo squatted domains.[46]

S0148 RTM

RTM has been delivered as archived Windows executable files masquerading as PDF documents.[47]

S0446 Ryuk

Ryuk can create .dll files that actually contain a Rich Text File format document.[48]

S1018 Saint Bot

Saint Bot has renamed malicious binaries as `wallpaper.mp4` and `slideshow.mp4` to avoid detection.[49][50]

C0059 Salesforce Data Exfiltration

During Salesforce Data Exfiltration, threat actors used voice calls to socially engineer victims into authorizing a modified version of the Salesforce Data Loader app.[51]

G0034 Sandworm Team

Sandworm Team masqueraded malicious installers as Windows update packages to evade defense and entice users to execute binaries.[52]

S0615 SombRAT

SombRAT can use a legitimate process name to hide itself.[53]

G1046 Storm-1811

Storm-1811 has prompted users to download and execute batch scripts that masquerade as legitimate update files during initial access and social engineering operations.[54]

S1183 StrelaStealer

StrelaStealer PE executable payloads have used uncommon but legitimate extensions such as `.com` instead of `.exe`.[55]

G0127 TA551

TA551 has masked malware DLLs as dat and jpg files.[56]

G0139 TeamTNT

TeamTNT has disguised their scripts with docker-related file names.[57]

S0682 TrailBlazer

TrailBlazer has used filenames that match the name of the compromised system in attempt to avoid detection.[58]

S0266 TrickBot

The TrickBot downloader has used an icon to appear as a Microsoft Word document.[59]

S1164 UPSTYLE

UPSTYLE has masqueraded filenames using examples such as `update.py`.[60]

S0689 WhisperGate

WhisperGate has been disguised as a JPG extension to avoid detection as a malicious PE file.[61]

G0112 Windshift

Windshift has used icons mimicking MS Office files to mask malicious executables.[62] Windshift has also attempted to hide executables by changing the file extension to ".scr" to mimic Windows screensavers.[63]

S0466 WindTail

WindTail has used icons mimicking MS Office files to mask payloads.[62]

G1035 Winter Vivern

Winter Vivern created specially-crafted documents mimicking legitimate government or similar documents during phishing campaigns.[64]

S0658 XCSSET

XCSSET installs malicious application bundles that mimic native macOS apps, such as Safari, by using the legitimate app's icon and customizing the `Info.plist` to match expected metadata.[65][66]

G0128 ZIRCONIUM

ZIRCONIUM has spoofed legitimate applications in phishing lures and changed file extensions to conceal installation of malware.[67][68]
