Masquerading: Match Legitimate Resource Name or Location, Sub-technique T1036.005 - Enterprise

Archived: 2026-04-02 12:31:58 UTC

C0025 2016 Ukraine Electric Power Attack

During the 2016 Ukraine Electric Power Attack, DLLs and EXEs with filenames associated with common electric power sector protocols were used to masquerade files.[2]

G0018 admin@338

admin@338 actors used the following command to rename one of their tools to a benign file name: `ren "%temp%\upload" audiodg.exe` [3]

G1024 Akira

Akira has used legitimate names and locations for files to evade defenses.[4]

S1074 ANDROMEDA

ANDROMEDA has been installed to `C:\Temp\TrustedInstaller.exe` to mimic a legitimate Windows installer service.[5]

S0622 AppleSeed

AppleSeed has the ability to rename its payload to ESTCommon.dll to masquerade as a DLL belonging to ESTsecurity.[6]

G0006 APT1

The file name AcroRD32.exe, a legitimate process name for Adobe's Acrobat Reader, was used by APT1 as a name for malware.[7][8]

G0007 APT28

APT28 has changed extensions on files containing exfiltrated data to make them appear benign, and renamed a web shell instance to appear as a legitimate OWA page.[9]

G0016 APT29

APT29 has renamed malicious DLLs with legitimate names to appear benign; they have also created an Azure AD certificate with a Common Name that matched the display name of the compromised service principal.[10][11]

G0050 APT32

APT32 has renamed a NetCat binary to kb-10233.exe to masquerade as a Windows update. APT32 has also renamed a Cobalt Strike beacon payload to install_flashplayers.exe. [12][13]

G0087 APT39

APT39 has used malware disguised as Mozilla Firefox and a tool named mfevtpse.exe to proxy C2 communications, closely mimicking a legitimate McAfee file mfevtps.exe.[14][15]

G0096 APT41

APT41 attempted to masquerade their files as popular anti-virus software.[16][17]

G1044 APT42

APT42 has masqueraded the VINETHORN payload as a VPN application.[18]

G1023 APT5

APT5 has named exfiltration archives to mimic Windows Updates at times using filenames with a `KB<digits>.zip` pattern.[19]

G0143 Aquatic Panda

Aquatic Panda renamed or moved malicious binaries to legitimate locations to evade defenses and blend into victim environments.[20]

S0475 BackConfig

BackConfig has hidden malicious payloads in `%USERPROFILE%\Adobe\Driver\dwg\` and mimicked the legitimate DHCP service binary.[21]

G0135 BackdoorDiplomacy

BackdoorDiplomacy has dropped implants in folders named for legitimate software.[22]

S0606 Bad Rabbit

Bad Rabbit has masqueraded as a Flash Player installer through the executable file `install_flash_player.exe`. [23][24]

S0128 BADNEWS

BADNEWS attempts to hide its payloads using legitimate filenames.[25]

S0534 Bazar

The Bazar loader has named malicious shortcuts "adobe" and mimicked communications software.[26][27][28]

S0268 Bisonal

Bisonal has renamed malicious code to `msacm32.dll` to hide within a legitimate library; earlier versions were disguised as `winhelp`.[29]

S1070 Black Basta

The Black Basta dropper has mimicked an application for creating USB bootable drivers.[30]

S0520 BLINDINGCAN

BLINDINGCAN has attempted to hide its payload by using legitimate file names such as "iconcache.db".[31]

G0108 Blue Mockingbird

Blue Mockingbird has masqueraded their XMRIG payload name by naming it wercplsupporte.dll after the legitimate wercplsupport.dll file.[32]

G0060 BRONZE BUTLER

BRONZE BUTLER has given malware the same name as an existing file on the file share server to cause users to unwittingly launch and install the malware on additional systems.[33]

S1063 Brute Ratel C4

Brute Ratel C4 has used a payload file named OneDrive.update to appear benign.[34]

S1039 Bumblebee

Bumblebee has named component DLLs "RapportGP.dll" to match those used by the security company Trusteer.[35]

S0482 Bundlore

Bundlore has disguised a malicious .app file as a Flash Player update.[36]

C0017 C0017

During C0017, APT41 used file names beginning with USERS, SYSUSER, and SYSLOG for DEADEYE, and changed KEYPLUG file extensions from .vmp to .upx likely to avoid hunting detections.[37]

C0018 C0018

For C0018, the threat actors renamed a Sliver payload to `vmware_kb.exe`.[38]

C0032 C0032

During the C0032 campaign, TEMP.Veles renamed files to look like legitimate files, such as Windows update files or Schneider Electric application files.[39]

S0274 Calisto

Calisto's installation file is an unsigned DMG image under the guise of Intego’s security solution for mac.[40]

S1237 CANONSTAGER

CANONSTAGER has leveraged naming conventions of its malicious DLL to match legitimate services to include cnmpaui.dll which matches the legitimate executable cnmpaui.exe that is aligned with a Canon Ink Jet Printer Assistant Tool.[41]

G0008 Carbanak

Carbanak has named malware "svchost.exe," which is the name of the Windows shared service host program.[42]

S0484 Carberp

Carberp has masqueraded as Windows system file names, as well as "chkntfs.exe" and "syscron.exe".[43][44]

S0631 Chaes

Chaes has used an unsigned, crafted DLL module named `hha.dll` that was designed to look like a legitimate 32-bit Windows DLL.[45]

S0144 ChChes

ChChes copies itself to an .exe file with a filename that is likely intended to imitate Norton Antivirus but has several letters reversed (e.g. notron.exe).[46]

G0114 Chimera

Chimera has renamed malware to GoogleUpdate.exe and WinRAR to jucheck.exe, RecordedTV.ms, teredo.tmp, update.exe, and msadcs1.exe.[47]

S1041 Chinoxy

Chinoxy has used the name `eoffice.exe` in attempt to appear as a legitimate file.[48]

S1236 CLAIMLOADER

CLAIMLOADER has imitated legitimate software directories through the creation and storage of the EXE and DLL in `C:\ProgramData\` and the use of legitimate looking names of software.[49]

S0625 Cuba

Cuba has been disguised as legitimate 360 Total Security Antivirus and OpenVPN programs.[50]

S1153 Cuckoo Stealer

Cuckoo Stealer has copied and renamed itself to DumpMediaSpotifyMusicConverter.[51][52]

S0687 Cyclops Blink

Cyclops Blink can rename its running process to `[kworker:0/1]` to masquerade as a Linux kernel thread. Cyclops Blink has also named RC scripts used for persistence after WatchGuard artifacts.[53]

S1014 DanBot

DanBot files have been named `UltraVNC.exe` and `WINVNC.exe` to appear as legitimate VNC tools.[54]

S0334 DarkComet

DarkComet has dropped itself onto victim machines with file names such as WinDefender.Exe and winupdate.exe in an apparent attempt to masquerade as a legitimate file.[55]

G0012 Darkhotel

Darkhotel has used malware that is disguised as a Secure Shell (SSH) tool.[56]

S0187 Daserf

Daserf uses file and folder names related to legitimate programs in order to blend in, such as HP, Intel, Adobe, and perflogs.[57]

S0600 Doki

Doki has disguised a file as a Linux kernel module.[58]

S0694 DRATzarus

DRATzarus has been named `Flash.exe`, and its dropper has been named `IExplorer`.[59]

S0567 Dtrack

One of Dtrack can hide in replicas of legitimate programs like OllyDbg, 7-Zip, and FileZilla.[60]

S1158 DUSTPAN

DUSTPAN is often disguised as a legitimate Windows binary such as `w3wp.exe` or `conn.exe`.[61]

G1006 Earth Lusca

Earth Lusca used the command `move [file path] c:\windows\system32\spool\prtprocs\x64\spool.dll` to move and register a malicious DLL name as a Windows print processor, which eventually was loaded by the Print Spooler service.[62]

S0605 EKANS

EKANS has been disguised as `update.exe` to appear as a valid executable.[63]

S0081 Elise

If installing itself as a service fails, Elise instead writes itself as a file named svchost.exe saved in %APPDATA%\Microsoft\Network.[64]

G1003 Ember Bear

Ember Bear has renamed tools to match legitimate utilities, such as renaming GOST tunneling instances to `java` in victim environments.[65]

S0171 Felismus

Felismus has masqueraded as legitimate Adobe Content Management System files.[66]

G0137 Ferocious Kitten

Ferocious Kitten has named malicious files `update.exe` and loaded them into the compromise host's "Public" folder.[67]

G1016 FIN13

FIN13 has masqueraded WAR files to look like legitimate packages such as, wsexample.war, wsexamples.com, examples.war, and exampl3s.war.[68]

G0046 FIN7

FIN7 has attempted to run Darkside ransomware with the filename sleep.exe.[69] Additionally, FIN7 has mimicked WsTaskLoad.exe, which is associated with the Wondershare software suite, by using a malicious executable under the same name.[70]

S0182 FinFisher

FinFisher renames one of its .dll files to uxtheme.dll in an apparent attempt to masquerade as a legitimate file.[71] [72]

S0661 FoggyWeb

FoggyWeb can be disguised as a Visual Studio file such as `Windows.Data.TimeZones.zh-PH.pri` to evade detection. Also, FoggyWeb's loader can mimic a genuine `dll` file that carries out the same import functions as the legitimate Windows `version.dll` file.[73]

G0117 Fox Kitten

Fox Kitten has named binaries and configuration files svhost and dllhost respectively to appear legitimate.[74]

S0410 Fysbis

Fysbis has masqueraded as trusted software rsyncd and dbus-inotifier.[75]

G0047 Gamaredon Group

Gamaredon Group has used legitimate process names to hide malware including `svchosst`.[76] Additionally, Gamaredon Group disguised malicious ZIP archives as Office documents that are related to the invasion.[77]

S0666 Gelsemium

Gelsemium has named malicious binaries `serv.exe`, `winprint.dll`, and `chrome_elf.dll` and has set its persistence in the Registry with the key value `Chrome Update` to appear legitimate.[78]

S1197 GoBear

GoBear is installed through droppers masquerading as legitimate, signed software installers.[79]

S0493 GoldenSpy

GoldenSpy's setup file installs initial executables under the folder `%WinDir%\System32\PluginManager`.[80]

S0588 GoldMax

GoldMax has used filenames that matched the system name, and appeared as a scheduled task impersonating systems management software within the corresponding ProgramData subfolder.[81][82]

S0477 Goopy

Goopy has impersonated the legitimate goopdate.dll, which was dropped on the target system with a legitimate GoogleUpdate.exe.[12]

S0531 Grandoreiro

Grandoreiro has named malicious browser extensions and update files to appear legitimate.[83][84]

S0690 Green Lambert

Green Lambert has been disguised as a Growl help file.[85][86]

S0697 HermeticWiper

HermeticWiper has used the name `postgressql.exe` to mask a malicious payload.[87]

S0698 HermeticWizard

HermeticWizard has been named `exec_32.dll` to mimic a legitimate MS Outlook .dll.[87]

S1249 HexEval Loader

HexEval Loader has masqueraded and typosquatted as legitimate code repository packages and projects.[88][89]

C0038 HomeLand Justice

During HomeLand Justice, threat actors renamed ROADSWEEP to GoXML.exe and ZeroCleare to cl.exe.[90][91]

S0070 HTTPBrowser

HTTPBrowser's installer contains a malicious file named navlu.dll to decrypt and run the RAT. navlu.dll is also the name of a legitimate Symantec DLL.[92]

S1022 IceApple

IceApple .NET assemblies have used `App_Web_` in their file names to appear legitimate.[93]

S0483 IcedID

IcedID has modified legitimate .dll files to include malicious code.[94]

G1032 INC Ransom

INC Ransom has named a PsExec executable winupd to mimic a legitimate Windows update file.[95][96]

G0119 Indrik Spider

Indrik Spider used fake updates for FlashPlayer plugin and Google Chrome as initial infection vectors.[97]

S0259 InnaputRAT

InnaputRAT variants have attempted to appear legitimate by using the file names SafeApp.exe and NeutralApp.exe.[98]

S0260 InvisiMole

InvisiMole has disguised its droppers as legitimate software or documents, matching their original names and locations, and saved its files as mpr.dll in the Windows folder.[99][100]

S0015 Ixeshe

Ixeshe has used registry values and file names associated with Adobe software, such as AcroRd32.exe.[101]

S1203 J-magic

J-magic can rename itself as "[nfsiod 0]" to masquerade as the local Network File System (NFS) asynchronous I/O server.[102]

C0050 J-magic Campaign

During the J-magic Campaign, threat actors used the name "JunoscriptService" to masquerade malware as the Junos automation scripting service.[102]

G0004 Ke3chang

Ke3chang has dropped their malware into legitimate installed software paths including: `C:\ProgramFiles\Realtek\Audio\HDA\AERTSr.exe`, `C:\Program Files (x86)\Foxit Software\Foxit`

`Reader\FoxitRdr64.exe`, `C:\Program Files (x86)\Adobe\Flash Player\AddIns\airappinstaller\airappinstall.exe`, and `C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd64.exe`.[103]

S0526 KGH_SPY

KGH_SPY has masqueraded as a legitimate Windows tool.[104]

G0094 Kimsuky

Kimsuky has renamed malware to legitimate names such as `ESTCommon.dll` or `patch.dll`.[105] Kimsuky has also disguised payloads using legitimate file names including a PowerShell payload named chrome.ps1. [106]

S0669 KOCTOPUS

KOCTOPUS has been disguised as legitimate software programs associated with the travel and airline industries. [107]

S0356 KONNI

KONNI has created a shortcut called "Anti virus service.lnk" in an apparent attempt to masquerade as a legitimate file.[108]

S1160 Latrodectus

Latrodectus has been packed to appear as a component to Bitdefender’s kernel-mode driver, TRUFOS.SYS.[109]

G0032 Lazarus Group

Lazarus Group has renamed malicious code to disguise it as Microsoft's narrator and other legitimate files.[110] [111]

S0395 LightNeuron

LightNeuron has used filenames associated with Exchange and Outlook for binary and configuration files, such as `winmail.dat`.[112]

S0582 LookBack

LookBack has a C2 proxy tool that masquerades as `GUP.exe`, which is software used by Notepad++.[113]

G1014 LuminousMoth

LuminousMoth has disguised their exfiltration malware as `ZoomVideoApp.exe`.[114]

S0409 Machete

Machete renamed payloads to masquerade as legitimate Google Chrome, Java, Dropbox, Adobe Reader and Python executables.[115][116]

G0095 Machete

Machete's Machete MSI installer has masqueraded as a legitimate Adobe Acrobat Reader installer.[117]

G0059 Magic Hound

Magic Hound has used `dllhost.exe` to mask Fast Reverse Proxy (FRP) and `MicrosoftOutLookUpdater.exe` for Plink.[118][119][120]

S1182 MagicRAT

MagicRAT stores configuration data in files and file paths mimicking legitimate operating system resources.[121]

S0652 MarkiRAT

MarkiRAT can masquerade as `update.exe` and `svehost.exe`; it has also mimicked legitimate Telegram and Chrome files.[67]

S0500 MCMD

MCMD has been named Readme.txt to appear legitimate.[122]

S0459 MechaFlounder

MechaFlounder has been downloaded as a file named lsass.exe, which matches the legitimate Windows file.[123]

G0045 menuPass

menuPass has been seen changing malicious files to appear legitimate.[124]

S0455 Metamorfo

Metamorfo has disguised an MSI file as the Adobe Acrobat Reader Installer and has masqueraded payloads as OneDrive, WhatsApp, or Spotify, for example.[125][126]

S0084 Mis-Type

Mis-Type saves itself as a file named `msdtc.exe`, which is also the name of the legitimate Microsoft Distributed Transaction Coordinator service binary.[127][128]

S0083 Misdat

Misdat saves itself as a file named `msdtc.exe`, which is also the name of the legitimate Microsoft Distributed Transaction Coordinator service binary.[127][128]

G0069 MuddyWater

MuddyWater has disguised malicious executables and used filenames and Registry key names associated with Windows Defender.[129][130][131]

G0129 Mustang Panda

Mustang Panda has used names like `adobeupdate.dat` and `PotPlayerDB.dat` to disguise PlugX, and a file named `OneDrive.exe` to load a Cobalt Strike payload.[132] Mustang Panda has also masqueraded legitimate browser plugin updates to include AdobePlugins.exe.[41]

G1020 Mustard Tempest

Mustard Tempest has used the filename `AutoUpdater.js` to mimic legitimate update files and has also used the Cyrillic homoglyph characters C `(0xd0a1)` and a `(0xd0b0)`, to produce the filename `Chrome.Update.zip`.[133][134]

G0019 Naikon

Naikon has disguised malicious programs as Google Chrome, Adobe, and VMware executables.[135]

S0630 Nebulae

Nebulae uses functions named `StartUserModeBrowserInjection` and `StopUserModeBrowserInjection` indicating that it's trying to imitate chrome_frame_helper.dll.[135]

S0198 NETWIRE

NETWIRE has masqueraded as legitimate software including TeamViewer and macOS Finder.[136]

S1090 NightClub

NightClub has chosen file names to appear legitimate including EsetUpdate-0117583943.exe for its dropper.[137]

S1100 Ninja

Ninja has used legitimate looking filenames for its loader including update.dll and x64.dll.[138]

S0353 NOKKI

NOKKI is written to %LOCALAPPDATA%\MicroSoft Updatea\svServiceUpdate.exe prior being executed in a new process in an apparent attempt to masquerade as a legitimate folder and file.[139]

S0340 Octopus

Octopus has been disguised as legitimate programs, such as Java and Telegram Messenger.[140][141]

G0049 OilRig

OilRig has named a downloaded copy of the Plink tunneling utility as \ProgramData\Adobe.exe.[142]

S0138 OLDBAIT

OLDBAIT installs itself in `%ALLUSERPROFILE%\Application Data\Microsoft\MediaPlayer\updatewindws.exe`; the directory name is missing a space and the file name is missing the letter "o."[143]

C0012 Operation CuckooBees

During Operation CuckooBees, the threat actors renamed a malicious executable to `rundll32.exe` to allow it to blend in with other Windows system files.[144]

C0006 Operation Honeybee

During Operation Honeybee, the threat actors used a legitimate Windows executable and secure directory for their payloads to bypass UAC.[145]

C0013 Operation Sharpshooter

During Operation Sharpshooter, threat actors installed Rising Sun in the Startup folder and disguised it as `mssync.exe`.[146]

C0014 Operation Wocao

During Operation Wocao, the threat actors renamed some tools and executables to appear as legitimate programs.[147]

S0402 OSX/Shlayer

OSX/Shlayer can masquerade as a Flash Player update.[148][149]

S1017 OutSteel

OutSteel attempts to download and execute Saint Bot to a statically-defined location attempting to mimic svchost: `%TEMP%\svjhost.exe`.[150]

S0072 OwaAuth

OwaAuth uses the filename owaauth.dll, which is a legitimate file that normally resides in `%ProgramFiles%\Microsoft\Exchange Server\ClientAccess\Owa\Auth\`; the malicious file by the same name is saved in `%ProgramFiles%\Microsoft\Exchange Server\ClientAccess\Owa\bin\`.[151]

G0040 Patchwork

Patchwork installed its payload in the startup programs folder as "Baidu Software Update." The group also adds its second stage payload to the startup programs as "Net Monitor."[152] They have also dropped QuasarRAT binaries as files named microsoft_network.exe and crome.exe.[153]

S1050 PcShare

PcShare has been named `wuauclt.exe` to appear as the legitimate Windows Update AutoUpdate Client.[48]

S0587 Penquin

Penquin has mimicked the Cron binary to hide itself on compromised systems.[154]

S0501 PipeMon

PipeMon modules are stored on disk with seemingly benign names including use of a file extension associated with a popular word processor.[155]

S0013 PlugX

PlugX has been disguised as legitimate Adobe and PotPlayer files.[156] PlugX has also imitated legitimate software directories and file names through the creation and storage of a legitimate EXE and the malicious DLLs.[157][158][159][160]

G0033 Poseidon Group

Poseidon Group tools attempt to spoof anti-virus processes as a means of self-defense.[161]

S1046 PowGoop

PowGoop has used a DLL named Goopdate.dll to impersonate a legitimate Google update file.[162]

G0056 PROMETHIUM

PROMETHIUM has disguised malicious installer files by bundling them with legitimate software installers.[163][164]

S1228 PUBLOAD

PUBLOAD has renamed malicious files to mimic legitimate file names such as adobe_wf.exe.[165]

S0196 PUNCHBUGGY

PUNCHBUGGY mimics filenames from %SYSTEM%\System32 to hide DLLs in %WINDIR% and/or %TEMP%.[166][167]

S1032 PyDCrypt

PyDCrypt has dropped DCSrv under the `svchost.exe` name to disk.[168]

S0583 Pysa

Pysa has executed a malicious executable by naming it svchost.exe.[169]

S0269 QUADAGENT

QUADAGENT used the PowerShell filenames `Office365DCOMCheck.ps1` and `SystemDiskClean.ps1`.[170]

S1084 QUIETEXIT

QUIETEXIT has attempted to change its name to `cron` upon startup. During incident response, QUIETEXIT samples have been identified that were renamed to blend in with other legitimate files.[171]

S0565 Raindrop

Raindrop was installed under names that resembled legitimate Windows file and directory names.[172][173]

S0629 RainyDay

RainyDay has used names to mimic legitimate software including "vmtoolsd.exe" to spoof Vmtools.[135]

S0458 Ramsay

Ramsay has masqueraded as a 7zip installer.[174][175]

S0495 RDAT

RDAT has masqueraded as VMware.exe.[176]

G1039 RedCurl

RedCurl mimicked legitimate file names and scheduled tasks, e.g. `MicrosoftCurrentupdatesCheck` and `MdMMaintenenceTask` to mask malicious files and scheduled tasks.[177][178]

C0056 RedPenguin

During RedPenguin, UNC3886 created multiple strains of malware using names to mimic legitimate binaries such as appid, to, irad, lmpad, jdosd, and oemd.[179]

S0125 Remsec

The Remsec loader implements itself with the name Security Support Provider, a legitimate Windows function. Various Remsec .exe files mimic legitimate file names used by Microsoft, Symantec, Kaspersky, Hewlett-Packard, and VMWare. Remsec also disguised malicious modules using similar filenames as custom network encryption software on victims.[180][181]

S0496 REvil

REvil can mimic the names of known executables.[182]

G0106 Rocke

Rocke has used shell scripts which download mining executables and saves them with the filename "java".[183]

S1078 RotaJakiro

RotaJakiro has used the filename `systemd-daemon` in an attempt to appear legitimate.[184]

S0446 Ryuk

Ryuk has constructed legitimate appearing installation folder paths by calling `GetWindowsDirectoryW` and then inserting a null byte at the fourth character of the path. For Windows Vista or higher, the path would appear as `C:\Users\Public`.[185]

S0085 S-Type

S-Type may save itself as a file named `msdtc.exe`, which is also the name of the legitimate Microsoft Distributed Transaction Coordinator service binary.[127][128]

S1018 Saint Bot

Saint Bot has been disguised as a legitimate executable, including as Windows SDK.[186]

S1099 Samurai

Samurai has created the directory `%COMMONPROGRAMFILES%\Microsoft Shared\wmi\` to contain DLLs for loading successive stages.[187]

G0034 Sandworm Team

Sandworm Team has avoided detection by naming a malicious binary explorer.exe.[188][189]

S1019 Shark

Shark binaries have been named `audioddg.pdb` and `Winlangdb.pdb` in order to appear legitimate.[54]

S0445 ShimRatReporter

ShimRatReporter spoofed itself as `AlphaZawgyl_font.exe`, a specialized Unicode font.[190]

S0589 Sibot

Sibot has downloaded a DLL to the `C:\windows\system32\drivers\` folder and renamed it with a `.sys` extension.[81]

G1008 SideCopy

SideCopy has used a legitimate DLL file name, `Duser.dll` to disguise a malicious remote access tool.[191]

G0121 Sidewinder

Sidewinder has named malicious files `rekeywiz.exe` to match the name of a legitimate Windows executable.[192]

G0091 Silence

Silence has named its backdoor "WINWORD.exe".[193]

S0468 Skidmap

Skidmap has created a fake `rm` binary to replace the legitimate Linux binary.[194]

S0533 SLOTHFULMEDIA

SLOTHFULMEDIA has mimicked the names of known executables, such as mediaplayer.exe.[195]

S1035 Small Sieve

Small Sieve can use variations of Microsoft and Outlook spellings, such as "Microsift", in its file names to avoid detection.[196]

S1124 SocGholish

SocGholish has been named `AutoUpdater.js` to mimic legitimate update files.[134]

C0024 SolarWinds Compromise

During the SolarWinds Compromise, APT29 renamed software and DLLs with legitimate names to appear benign.[197][198]

G0054 Sowbug

Sowbug named its tools to masquerade as Windows or Adobe Reader software, such as by using the file name adobecms.exe and the directory `CSIDL_APPDATA\microsoft\security`.[199]

S0058 SslMM

To establish persistence, SslMM identifies the Start Menu Startup directory and drops a link to its own executable disguised as an "Office Start," "Yahoo Talk," "MSN Gaming Z0ne," or "MSN Talk" shortcut.[200]

S0188 Starloader

Starloader has masqueraded as legitimate software update packages such as Adobe Acrobat Reader and Intel.[199]

S1238 STATICPLUGIN

STATICPLUGIN has leveraged naming conventions that match legitimate services to include AdobePlugins.exe.[41]

G1046 Storm-1811

Storm-1811 has disguised Cobalt Strike installers as a malicious DLL masquerading as part of a legitimate 7zip installation package.[201]

S1183 StrelaStealer

StrelaStealer payloads have tailored filenames to include names identical to the name of the targeted organization or company.[202]

S1034 StrifeWater

StrifeWater has been named `calc.exe` to appear as a legitimate calculator program.[203]

S0491 StrongPity

StrongPity has been bundled with legitimate software installation files for disguise.[163]

S1042 SUGARDUMP

SUGARDUMP has been named `CrashReporter.exe` to appear as a legitimate Mozilla executable.[204]

S0559 SUNBURST

SUNBURST created VBScripts that were named after existing services or folders to blend into legitimate activities.[173]

S0562 SUNSPOT

SUNSPOT was identified on disk with a filename of `taskhostsvc.exe` and it created an encrypted log file at `C:\Windows\Temp\vmware-vmdmp.log`.[205]

S0578 SUPERNOVA

SUPERNOVA has masqueraded as a legitimate SolarWinds DLL.[206][207]

G1018 TA2541

TA2541 has used file names to mimic legitimate Windows files or system functionality.[208]

S0586 TAINTEDSCRIBE

The TAINTEDSCRIBE main executable has disguised itself as Microsoft's Narrator.[110]

S1011 Tarrask

Tarrask has masqueraded as executable files such as `winupdate.exe`, `date.exe`, or `win.exe`.[209]

G0139 TeamTNT

TeamTNT has replaced .dockerd and .dockerenv with their own scripts and cryptocurrency mining software.[210]

S0560 TEARDROP

TEARDROP files had names that resembled legitimate Window file and directory names.[211][173]

S0595 ThiefQuest

ThiefQuest prepends a copy of itself to the beginning of an executable file while maintaining the name of the executable.[212][213]

S0665 ThreatNeedle

ThreatNeedle chooses its payload creation path from a randomly selected service name from netsvc.[214]

S0668 TinyTurla

TinyTurla has been deployed as `w64time.dll` to appear legitimate.[215]

G1022 ToddyCat

ToddyCat has used the name `debug.exe` for malware components.[187]

S1239 TONESHELL

TONESHELL has renamed malicious files to mimic legitimate file names and file extensions.[165] TONESHELL has also masqueraded as legitimate file names to include LogMeIn.dll.[216]

S1201 TRANSLATEXT

TRANSLATEXT has been named `GoogleTranslate.crx` to masquerade as a legitimate Chrome extension.[217]

G0134 Transparent Tribe

Transparent Tribe can mimic legitimate Windows directories by using the same icons and names.[218]

C0030 Triton Safety Instrumented System Attack

In the Triton Safety Instrumented System Attack, TEMP.Veles renamed files to look like legitimate files, such as Windows update files or Schneider Electric application files.

S1196 Troll Stealer

Troll Stealer is typically installed via a dropper file that masquerades as a legitimate security program installation file.[219][79]

G0081 Tropic Trooper

Tropic Trooper has hidden payloads in Flash directories and fake installer files.[220]

G0010 Turla

Turla has named components of LunarWeb to mimic Zabbix agent logs.[221]

S0386 Ursnif

Ursnif has used strings from legitimate system files and existing folders for its file, folder, and Registry entry names.[222]

S0136 USBStealer

USBStealer mimics a legitimate Russian program called USB Disk Security.[223]

G1047 Velvet Ant

Velvet Ant used a malicious DLL, `iviewers.dll`, that mimics the legitimate "OLE/COM Object Viewer" within Windows.[224]

S1217 VIRTUALPITA

VIRTUALPITA samples have been found in `/usr/libexec/setconf/ksmd` and `/usr/bin/ksmd`, named to spoof the legitimate Kernel Same-Page Merging Daemon binary. [225]

G1017 Volt Typhoon

Volt Typhoon has used legitimate looking filenames for compressed copies of the ntds.dit database and used names including cisco_up.exe, cl64.exe, vm3dservice.exe, watchdogd.exe, Win.exe, WmiPreSV.exe, and WmiPrvSE.exe for the Earthworm and Fast Reverse Proxy tools.[226][227][228]

G0107 Whitefly

Whitefly has named the malicious DLL the same name as DLLs belonging to legitimate software from various security vendors.[229]

S0141 Winnti for Windows

A Winnti for Windows implant file was named ASPNET_FILTER.DLL, mimicking the legitimate ASP.NET ISAPI filter DLL with the same name.[230]

G0090 WIRTE

WIRTE has named a first stage dropper `Kaspersky Update Agent` in order to appear legitimate.[231]

S1248 XORIndex Loader

XORIndex Loader has leveraged legitimate package names to mimic frequently utilized tools to entice victims to download and execute malicious payloads.[232]

S0086 ZLib

ZLib mimics the resource version information of legitimate Realtek Semiconductor, Nvidia, or Synaptics modules.[127]

Source: https://attack.mitre.org/techniques/T1036/005