Masquerading: Masquerade Task or Service, Sub-technique T1036.004 - Enterprise

Archived: 2026-04-05 14:35:50 UTC

C0034 2022 Ukraine Electric Power Attack

During the 2022 Ukraine Electric Power Attack, Sandworm Team leveraged Systemd service units to masquerade GOGETTER malware as legitimate or seemingly legitimate services.[5]

G0099 APT-C-36

APT-C-36 has disguised its scheduled tasks as those used by Google.[6]

G0050 APT32

APT32 has used hidden or non-printing characters to help masquerade service names, such as appending a Unicode no-break space character to a legitimate service name. APT32 has also impersonated the legitimate Flash installer file name "install_flashplayer.exe".[7]

G0096 APT41

APT41 has created services to appear as benign system tools.[8]

C0040 APT41 DUST

APT41 DUST disguised DUSTPAN as a legitimate Windows binary such as `w3wp.exe` or `conn.exe`.[9]

G0143 Aquatic Panda

Aquatic Panda created new, malicious services using names such as `Windows User Service` to attempt to blend in with legitimate items on victim systems.[10]

S0438 Attor

Attor's dispatcher disguises itself as a legitimate task (i.e., the task name and description appear legitimate).[11]

G0135 BackdoorDiplomacy

BackdoorDiplomacy has disguised their backdoor droppers with naming conventions designed to blend into normal operations.[12]

S0534 Bazar

Bazar can create a task named to appear benign.[13]

G1002 BITTER

BITTER has disguised malware as a Windows Security update service.[14]

S1070 Black Basta

Black Basta has established persistence by creating a new service named `FAX` after deleting the legitimate service by the same name.[15][16][17]

S1226 BOOKWORM

BOOKWORM has created services that attempt to resemble legitimate services to include a service named `Microsoft Windows DeviceSync Service`.[18]

S0471 build_downer

build_downer has added itself to the Registry Run key as "NVIDIA" to appear legitimate.[19]

C0017 C0017

During C0017, APT41 used `SCHTASKS /Change` to modify legitimate scheduled tasks to run malicious code.[20]

G0008 Carbanak

Carbanak has copied legitimate service names to use for malicious services.[21]

S0261 Catchamas

Catchamas adds a new service named NetAdapter in an apparent attempt to masquerade as a legitimate service.[22]

S0126 ComRAT

ComRAT has used a task name associated with Windows SQM Consolidator.[23]

S0538 Crutch

Crutch has established persistence with a scheduled task impersonating the Outlook item finder.[24]

S0527 CSPY Downloader

CSPY Downloader has attempted to appear as a legitimate Windows service with a fake description claiming it is used to support packed applications.[25]

S1033 DCSrv

DCSrv has masqueraded its service as a legitimate svchost.exe process.[26]

S1052 DEADEYE

DEADEYE has used `schtasks /change` to modify scheduled tasks including `\Microsoft\Windows\PLA\Server Manager Performance Monitor`, `\Microsoft\Windows\Ras\ManagerMobility`, `\Microsoft\Windows\WDI\SrvSetupResults`, and `\Microsoft\Windows\WDI\USOShared`.[20]

S1134 DEADWOOD

DEADWOOD will attempt to masquerade its service execution using benign-looking names such as `ScDeviceEnums`.[27]

S0554 Egregor

Egregor has masqueraded the svchost.exe process to exfiltrate data.[28]

S0367 Emotet

Emotet has installed itself as a new service with the service name `Windows Defender System Service` and display name `WinDefService`.[29]

S0343 Exaramel for Windows

The Exaramel for Windows dropper creates and starts a Windows service named wsmprovav with the description "Windows Check AV" in an apparent attempt to masquerade as a legitimate service.[30]

G1016 FIN13

FIN13 has used scheduled tasks names such as `acrotyr` and `AppServicesr` to mimic the same names in a compromised network's `C:\Windows` directory.[31]

G0037 FIN6

FIN6 has renamed the "psexec" service name to "mstdc" to masquerade as a legitimate Windows service.[32]

G0046 FIN7

FIN7 has created a scheduled task named "AdobeFlashSync" to establish persistence.[33]

G0117 Fox Kitten

Fox Kitten has named the task for a reverse proxy lpupdate to appear legitimate.[34]

C0001 Frankenstein

During Frankenstein, the threat actors named a malicious scheduled task "WinUpdate" for persistence.[35]

S1044 FunnyDream

FunnyDream has used a service named `WSearch` for execution.[36]

S0410 Fysbis

Fysbis has masqueraded as the rsyncd and dbus-inotifier services.[4]

S0588 GoldMax

GoldMax has impersonated systems management software to avoid detection.[37]

S0690 Green Lambert

Green Lambert has created a new executable named `Software Update Check` to appear legitimate.[38][39]

S1027 Heyoka Backdoor

Heyoka Backdoor has been named `srvdll.dll` to appear as a legitimate service.[40]

G0126 Higaisa

Higaisa named a shellcode loader binary `svchast.exe` to spoof the legitimate `svchost.exe`.[41][42]

S0601 Hildegard

Hildegard has disguised itself as a known Linux process.[43]

S0259 InnaputRAT

InnaputRAT variants have attempted to appear legitimate by adding a new service named OfficeUpdateService.[44]

S0260 InvisiMole

InvisiMole has attempted to disguise itself by registering under a seemingly legitimate service name.[45]

S0581 IronNetInjector

IronNetInjector has been disguised as a legitimate service using the name PythonUpdateSrvc.[46]

S0607 KillDisk

KillDisk registers as a service under the Plug-And-Play Support name.[47]

G0094 Kimsuky

Kimsuky has disguised services to appear as benign software or related to operating system functions.[48][49]

S0356 KONNI

KONNI has pretended to be the xmlProv Network Provisioning service.[50]

C0035 KV Botnet Activity

KV Botnet Activity installation steps include first identifying, then stopping, any process containing `[kworker\/0:1]`, then renaming its initial installation stage to this process name.[51]

S0236 Kwampirs

Kwampirs establishes persistence by adding a new service with the display name "WMI Performance Adapter Extension" in an attempt to masquerade as a legitimate WMI service.[52]

G0032 Lazarus Group

Lazarus Group has used a scheduled task named `SRCheck` to mask the execution of a malicious .dll.[53]

S0409 Machete

Machete renamed task names to masquerade as legitimate Google Chrome, Java, Dropbox, Adobe Reader and Python tasks.[54]

G0059 Magic Hound

Magic Hound has named a malicious script CacheTask.bat to mimic a legitimate task.[55]

S0449 Maze

Maze operators have created scheduled tasks masquerading as "Windows Update Security", "Windows Update Security Patches", and "Google Chrome Security Update" designed to launch the ransomware.[56]

S0688 Meteor

Meteor has been disguised as the Windows Power Efficiency Diagnostics report tool.[57]

G0019 Naikon

Naikon renamed a malicious service `taskmgr` to appear to be a legitimate version of Task Manager.[58]

S0630 Nebulae

Nebulae has created a service named "Windows Update Agent1" to appear legitimate.[58]

S0118 Nidiran

Nidiran can create a new service named msamger (Microsoft Security Accounts Manager), which mimics the legitimate Microsoft database by the same name.[59][60]

S1090 NightClub

NightClub has created a service named `WmdmPmSp` to spoof a Windows Media service.[61]

S0439 Okrum

Okrum can establish persistence by adding a new service NtmsSvc with the display name Removable Storage to masquerade as a legitimate Removable Storage Manager.[62]

S0352 OSX_OCEANLOTUS.D

OSX_OCEANLOTUS.D uses file naming conventions with associated executable locations to blend in with the macOS TimeMachine and OpenSSL services. Such as, naming a LaunchAgent plist file `com.apple.openssl.plist` which executes OSX_OCEANLOTUS.D from the user's `~/Library/OpenSSL/` folder upon user login.[63]

S1031 PingPull

PingPull can mimic the names and descriptions of legitimate services such as `iphlpsvc`, `IP Helper`, and `Onedrive` to evade detection.[64]

S0013 PlugX

In one instance, menuPass added PlugX as a service with a display name of "Corel Writing Tools Utility."[65]

S0223 POWERSTATS

POWERSTATS has created a scheduled task named "MicrosoftEdge" to establish persistence.[66]

G0056 PROMETHIUM

PROMETHIUM has named services to appear legitimate.[67][68]

S0629 RainyDay

RainyDay has named services and scheduled tasks to appear benign including "ChromeCheck" and "googleupdate."[58]

S1130 Raspberry Robin

Raspberry Robin will execute its payload prior to initializing command and control traffic by impersonating one of several legitimate program names such as dllhost.exe, regsvr32.exe, or rundll32.exe.[69]

S0169 RawPOS

New services created by RawPOS are made to appear like legitimate Windows services, with names such as "Windows Management Help Service", "Microsoft Support", and "Windows Advanced Task Manager".[70][71][72]

S0495 RDAT

RDAT has used Windows Video Service as a name for malicious services.[73]

C0047 RedDelta Modified PlugX Infection Chain Operations

Mustang Panda masqueraded Registry run keys as legitimate-looking service names such as `OneNote Update` during RedDelta Modified PlugX Infection Chain Operations.[74]

S0148 RTM

RTM has named the scheduled task it creates "Windows Update".[75]

S0345 Seasalt

Seasalt has masqueraded as a service called "SaSaut" with a display name of "System Authorization Service" in an apparent attempt to masquerade as a legitimate service.[76]

S0140 Shamoon

Shamoon creates a new service named "ntssrv" that attempts to appear legitimate; the service's display name is "Microsoft Network Realtime Inspection Service" and its description is "Helps guard against time change attempts targeting known and newly discovered vulnerabilities in network time protocols." Newer versions create the "MaintenaceSrv" service, which misspells the word "maintenance."[3][77]

S0444 ShimRat

ShimRat can impersonate Windows services and antivirus products to avoid detection on compromised systems.[78]

S0533 SLOTHFULMEDIA

SLOTHFULMEDIA has named a service it establishes on victim machines as "TaskFrame" to hide its malicious purpose.[79]

C0024 SolarWinds Compromise

During the SolarWinds Compromise, APT29 named tasks `\Microsoft\Windows\SoftwareProtectionPlatform\EventCacheManager` in order to appear legitimate.[80]

S1140 Spica

Spica has created a scheduled task named `CalendarChecker` for persistence on compromised hosts.[81]

G1053 Storm-0501

Storm-0501 has utilized Rclone masqueraded as svhost.exe and scvhost.exe.[82]

S0491 StrongPity

StrongPity has named services to appear legitimate.[67][68]

S1042 SUGARDUMP

SUGARDUMP's scheduled task has been named `MicrosoftInternetExplorerCrashRepoeterTaskMachineUA` or `MicrosoftEdgeCrashRepoeterTaskMachineUA`, depending on the Windows OS version.[83]

S1064 SVCReady

SVCReady has named a task `RecoveryExTask` as part of its persistence activity.[84]

S0663 SysUpdate

SysUpdate has named their unit configuration file similarly to other unit files residing in the same directory, `/usr/lib/systemd/system/`, to appear benign.[85]

S1011 Tarrask

Tarrask creates a scheduled task called "WinUpdate" to re-establish any dropped C2 connections.[86]

S0668 TinyTurla

TinyTurla has mimicked an existing Windows service by being installed as `Windows Time Service`.[87]

S1239 TONESHELL

TONESHELL has masqueraded as the legitimate Windows utility service DISMsrv (Dism Images Servicing Utility Service).[88]

S0178 Truvasys

To establish persistence, Truvasys adds a Registry Run key with a value "TaskMgr" in an attempt to masquerade as the legitimate Windows Task Manager.[89]

S0647 Turian

Turian can disguise as a legitimate service to blend into normal operations.[12]

G1048 UNC3886

UNC3886 has named a file ‘fgfm’ in an attempt to disguise it as the legitimate service ‘fgfmd’ which facilitates communication between FortiManager and the FortiGate firewall.[90]

S0022 Uroburos

Uroburos has registered a service named `WerFaultSvc`, likely to spoof the legitimate Windows error reporting service.[91]

S1217 VIRTUALPITA

VIRTUALPITA has utilized VMware service names and ports to masquerade as legitimate services.[92]

S0180 Volgmer

Some Volgmer variants add new services with display names generated by a list of hard-coded strings such as Application, Background, Security, and Windows, presumably as a way to masquerade as a legitimate service.[93] [94]

G1035 Winter Vivern

Winter Vivern has distributed malicious scripts and executables mimicking virus scanners.[95]

G0102 Wizard Spider

Wizard Spider has used scheduled tasks to install TrickBot, using task names to appear legitimate such as WinDotNet, GoogleTask, or Sysnetsf.[96] It has also used common document file names for other malware binaries.[97]

G0128 ZIRCONIUM

ZIRCONIUM has created a run key named `Dropbox Update Setup` to mask a persistence mechanism for a malicious binary.[98]

S1013 ZxxZ

ZxxZ has been disguised as a Windows security update service.[14]
