# TTP Detail – T1543.003

## TTP Information

Name: Windows Service

Description: Adversaries may create or modify Windows services to repeatedly execute malicious payloads as part of persistence. When Windows boots up, it starts programs or applications called services that perform background system functions.(Citation: TechNet Services) Windows service configuration information, including the file path to the service's executable or recovery programs/commands, is stored in the Windows Registry.  
  
Adversaries may install a new service or modify an existing service to execute at startup in order to persist on a system. Service configurations can be set or modified using system utilities (such as sc.exe), by directly modifying the Registry, or by interacting directly with the Windows API.   
  
Adversaries may also use services to install and execute malicious drivers. For example, after dropping a driver file (ex: `.sys`) to disk, the payload can be loaded and registered via [Native API](https://attack.mitre.org/techniques/T1106) functions such as `CreateServiceW()` (or manually via functions such as `ZwLoadDriver()` and `ZwSetValueKey()`), by creating the required service Registry values (i.e. [Modify Registry](https://attack.mitre.org/techniques/T1112)), or by using command-line utilities such as `PnPUtil.exe`.(Citation: Symantec W.32 Stuxnet Dossier)(Citation: Crowdstrike DriveSlayer February 2022)(Citation: Unit42 AcidBox June 2020) Adversaries may leverage these drivers as [Rootkit](https://attack.mitre.org/techniques/T1014)s to hide the presence of malicious activity on a system. Adversaries may also load a signed yet vulnerable driver onto a compromised machine (known as "Bring Your Own Vulnerable Driver" (BYOVD)) as part of [Exploitation for Privilege Escalation](https://attack.mitre.org/techniques/T1068).(Citation: ESET InvisiMole June 2020)(Citation: Unit42 AcidBox June 2020)  
  
Services may be created with administrator privileges but are executed under SYSTEM privileges, so an adversary may also use a service to escalate privileges. Adversaries may also directly start services through [Service Execution](https://attack.mitre.org/techniques/T1569/002).  
  
To make detection analysis more challenging, malicious services may also incorporate [Masquerade Task or Service](https://attack.mitre.org/techniques/T1036/004) (ex: using a service and/or payload name related to a legitimate OS or benign software component). Adversaries may also create ‘hidden’ services (i.e., [Hide Artifacts](https://attack.mitre.org/techniques/T1564)), for example by using the `sc sdset` command to set service permissions via the Service Descriptor Definition Language (SDDL). This may hide a Windows service from the view of standard service enumeration methods such as `Get-Service`, `sc query`, and `services.exe`.(Citation: SANS 1)(Citation: SANS 2)

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: persistence

**•** mitre-attack: privilege-escalation

## Malware

* Anchor
* AppleJeus
* Attor
* AuditCred
* BBSRAT
* Bankshot
* Bisonal
* BitPaymer
* Black Basta
* BlackEnergy
* Briba
* Carbon
* Catchamas
* Clambling
* Cobalt Strike
* Conficker
* CosmicDuke
* CozyCar
* Cuba
* DCSrv
* DUSTPAN
* Dtrack
* Duqu
* Dyre
* Elise
* Emissary
* Emotet
* Exaramel for Windows
* FALLCHILL
* FinFisher
* FunnyDream
* Gelsemium
* GoldenSpy
* GreyEnergy
* Hannotog
* HermeticWiper
* Hydraq
* Industroyer
* InnaputRAT
* InvisiMole
* JHUHUGIT
* KONNI
* Kazuar
* KeyBoy
* Kwampirs
* LockBit 3.0
* LoudMiner
* MoonWind
* Naid
* Nebulae
* Nerex
* Nidiran
* NightClub
* Ninja
* Okrum
* Pandora
* PingPull
* PipeMon
* PlugX
* PoisonIvy
* QakBot
* RDAT
* Ragnar Locker
* RainyDay
* RawPOS
* Reaver
* SLOTHFULMEDIA
* STARWHALE
* SUGARUSH
* Sakula
* Samurai
* Seasalt
* Shamoon
* ShimRat
* StreamEx
* StrongPity
* Stuxnet
* SysUpdate
* TDTESS
* TEARDROP
* TYPEFRAME
* ThreatNeedle
* TinyZBot
* TrickBot
* Uroburos
* Ursnif
* Volgmer
* WannaCry
* WastedLocker
* Wiarp
* Wingbird
* Winnti for Windows
* ZLib
* ZeroT
* ZxShell
* gh0st RAT
* hcdLoader
* zwShell

## Tools

* Empire
* PowerSploit
* PsExec
* SILENTTRINITY

## APTs (Intrusion Sets)

* APT19
* APT3
* APT32
* APT38
* APT41
* Agrius
* Aquatic Panda
* BlackByte
* Blue Mockingbird
* Carbanak
* Cinnamon Tempest
* Cobalt Group
* DarkVishnya
* Earth Lusca
* FIN7
* Ke3chang
* Kimsuky
* Lazarus Group
* Lotus Blossom
* OilRig
* PROMETHIUM
* TeamTNT
* Threat Group-3390
* Tropic Trooper
* Wizard Spider