# TTP Detail – T1547.001

## TTP Information

Name: Registry Run Keys / Startup Folder

Description: Adversaries may achieve persistence by adding a program to a startup folder or referencing it with a Registry run key. Adding an entry to the "run keys" in the Registry or startup folder will cause the program referenced to be executed when a user logs in.(Citation: Microsoft Run Key) These programs will be executed under the context of the user and will have the account's associated permissions level.

The following run keys are created by default on Windows systems:

\* <code>HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Run</code>
\* <code>HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce</code>
\* <code>HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run</code>
\* <code>HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce</code>

Run keys may exist under multiple hives.(Citation: Microsoft Wow6432Node 2018)(Citation: Malwarebytes Wow6432Node 2016) The <code>HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnceEx</code> is also available but is not created by default on Windows Vista and newer. Registry run key entries can reference programs directly or list them as a dependency.(Citation: Microsoft Run Key) For example, it is possible to load a DLL at logon using a "Depend" key with RunOnceEx: <code>reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx\0001\Depend /v 1 /d "C:\temp\evil[.]dll"</code> (Citation: Oddvar Moe RunOnceEx Mar 2018)

Placing a program within a startup folder will also cause that program to execute when a user logs in. There is a startup folder location for individual user accounts as well as a system-wide startup folder that will be checked regardless of which user account logs in. The startup folder path for the current user is <code>C:\Users\\[Username]\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup</code>. The startup folder path for all users is <code>C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp</code>.

The following Registry keys can be used to set startup folder items for persistence:

\* <code>HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders</code>
\* <code>HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders</code>
\* <code>HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders</code>
\* <code>HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders</code>

The following Registry keys can control automatic startup of services during boot:

\* <code>HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce</code>
\* <code>HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce</code>
\* <code>HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices</code>
\* <code>HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\RunServices</code>

Using policy settings to specify startup programs creates corresponding values in either of two Registry keys:

\* <code>HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run</code>
\* <code>HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run</code>

Programs listed in the load value of the registry key <code>HKEY\_CURRENT\_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows</code> run automatically for the currently logged-on user.

By default, the multistring <code>BootExecute</code> value of the registry key <code>HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Control\Session Manager</code> is set to <code>autocheck autochk \*</code>. This value causes Windows, at startup, to check the file-system integrity of the hard disks if the system has been shut down abnormally. Adversaries can add other programs or processes to this registry value which will automatically launch at boot.

Adversaries can use these configuration locations to execute malware, such as remote access tools, to maintain persistence through system reboots. Adversaries may also use [Masquerading](https://attack.mitre.org/techniques/T1036) to make the Registry entries look as if they are associated with legitimate programs.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: persistence

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

## Malware

* ADVSTORESHELL
* ANDROMEDA
* Agent Tesla
* Amadey
* AppleSeed
* Aria-body
* Astaroth
* AuTo Stealer
* Avaddon
* AvosLocker
* BACKSPACE
* BADNEWS
* BBSRAT
* BabyShark
* Backdoor.Oldrea
* BadPatch
* Bazar
* Bisonal
* BitPaymer
* BlackEnergy
* BoomBox
* Briba
* CORESHELL
* Carbanak
* Carberp
* Cardinal RAT
* ChChes
* Chaes
* Chinoxy
* Clambling
* Cobian RAT
* Comnie
* Conficker
* CozyCar
* Crimson
* CrossRAT
* DarkComet
* DarkGate
* DarkTortilla
* DnsSystem
* DownPaper
* DustySky
* EVILNUM
* Elise
* Emissary
* Emotet
* EvilBunny
* EvilGrab
* FELIXROOT
* FLASHFLOOD
* FatDuke
* FinFisher
* Final1stspy
* Flagpro
* FlawedAmmyy
* FunnyDream
* GRIFFON
* Gazer
* Gelsemium
* Gold Dragon
* Gootloader
* Grandoreiro
* GrimAgent
* GuLoader
* HTTPBrowser
* Hancitor
* Helminth
* Heyoka Backdoor
* Hi-Zor
* IcedID
* InnaputRAT
* InvisiMole
* Ixeshe
* JCry
* JHUHUGIT
* KOCTOPUS
* KONNI
* Kasidet
* Kazuar
* Latrodectus
* LiteDuke
* LoJax
* LockBit 2.0
* LookBack
* Lucifer
* Lumma Stealer
* Machete
* MagicRAT
* MarkiRAT
* Matryoshka
* Maze
* Metamorfo
* Mispadu
* Mivast
* MoleNet
* Mongall
* Mosquito
* NETEAGLE
* NETWIRE
* NOKKI
* NanHaiShu
* NanoCore
* NavRAT
* Nebulae
* ObliqueRAT
* Octopus
* Okrum
* PLAINTEE
* POWERSOURCE
* POWERTON
* PUNCHBUGGY
* Pikabot
* Pisloader
* PlugX
* PoetRAT
* PoisonIvy
* PowerDuke
* PowerShower
* Prikormka
* Pteranodon
* QakBot
* RCSession
* ROADSWEEP
* RTM
* Ramsay
* RansomHub
* Raspberry Robin
* Reaver
* RedLeaves
* Remexi
* Rifdoor
* RogueRobin
* Rover
* RunningRAT
* Ryuk
* S-Type
* SDBbot
* SHIPSHAPE
* SMOKEDHAM
* SNUGRIDE
* SPACESHIP
* STARWHALE
* Saint Bot
* Sakula
* SeaDuke
* Seasalt
* ServHelper
* SharpStage
* ShimRat
* Small Sieve
* Smoke Loader
* Snip3
* SslMM
* StrongPity
* Sykipot
* SysUpdate
* TAINTEDSCRIBE
* TINYTYPHON
* TURNEDUP
* Taidoor
* ThreatNeedle
* TinyZBot
* TrickBot
* Trojan.Karagany
* Truvasys
* Turian
* USBStealer
* Ursnif
* VBShower
* Vasport
* WarzoneRAT
* Winnti for Windows
* XLoader
* Xbash
* Zebrocy
* Zeus Panda
* build\_downer
* gh0st RAT
* njRAT

## Tools

* Empire
* Koadic
* MCMD
* PowerSploit
* Pupy
* QuasarRAT
* Remcos
* SILENTTRINITY

## APTs (Intrusion Sets)

* APT18
* APT19
* APT28
* APT29
* APT3
* APT32
* APT33
* APT37
* APT39
* APT41
* BRONZE BUTLER
* BlackByte
* Cobalt Group
* Confucius
* Dark Caracal
* Darkhotel
* Dragonfly
* FIN10
* FIN13
* FIN6
* FIN7
* Gamaredon Group
* Gorgon Group
* Higaisa
* Inception
* Ke3chang
* Kimsuky
* Lazarus Group
* LazyScripter
* Leviathan
* LuminousMoth
* Magic Hound
* Molerats
* Moonstone Sleet
* MuddyWater
* Mustang Panda
* Naikon
* PROMETHIUM
* Patchwork
* Putter Panda
* RTM
* RedCurl
* Rocke
* Sidewinder
* Silence
* Storm-1811
* TA2541
* TeamTNT
* Threat Group-3390
* Tropic Trooper
* Turla
* Windshift
* Wizard Spider
* ZIRCONIUM