# TTP Detail – T1112

## TTP Information

Name: Modify Registry

Description: Adversaries may interact with the Windows Registry as part of a variety of other techniques to aid in defense evasion, persistence, and execution.

Access to specific areas of the Registry depends on account permissions, with some keys requiring administrator-level access. The built-in Windows command-line utility [Reg](https://attack.mitre.org/software/S0075) may be used for local or remote Registry modification.(Citation: Microsoft Reg) Other tools, such as remote access tools, may also contain functionality to interact with the Registry through the Windows API.

The Registry may be modified in order to hide configuration information or malicious payloads via [Obfuscated Files or Information](https://attack.mitre.org/techniques/T1027).(Citation: Unit42 BabyShark Feb 2019)(Citation: Avaddon Ransomware 2021)(Citation: Microsoft BlackCat Jun 2022)(Citation: CISA Russian Gov Critical Infra 2018) The Registry may also be modified to [Impair Defenses](https://attack.mitre.org/techniques/T1562), such as by enabling macros for all Microsoft Office products, allowing privilege escalation without alerting the user, increasing the maximum number of allowed outbound requests, and/or modifying systems to store plaintext credentials in memory.(Citation: CISA LockBit 2023)(Citation: Unit42 BabyShark Feb 2019)

The Registry of a remote system may be modified to aid in execution of files as part of lateral movement. It requires the remote Registry service to be running on the target system.(Citation: Microsoft Remote) Often [Valid Accounts](https://attack.mitre.org/techniques/T1078) are required, along with access to the remote system's [SMB/Windows Admin Shares](https://attack.mitre.org/techniques/T1021/002) for RPC communication.

Finally, Registry modifications may also include actions to hide keys, such as prepending key names with a null character, which will cause an error and/or be ignored when read via [Reg](https://attack.mitre.org/software/S0075) or other utilities using the Win32 API.(Citation: Microsoft Reghide NOV 2006) Adversaries may abuse these pseudo-hidden keys to conceal payloads/commands used to maintain persistence.(Citation: TrendMicro POWELIKS AUG 2014)(Citation: SpectorOps Hiding Reg Jul 2017)

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: defense-evasion

**•** mitre-attack: persistence

## Malware

* ADVSTORESHELL
* Agent Tesla
* Amadey
* Attor
* Avaddon
* BACKSPACE
* BADCALL
* Bankshot
* Bisonal
* BitPaymer
* Black Basta
* BlackByte 2.0 Ransomware
* BlackByte Ransomware
* BlackCat
* CHIMNEYSWEEP
* CHOPSTICK
* Cardinal RAT
* Catchamas
* Caterpillar WebShell
* Chaes
* CharmPower
* Clambling
* Clop
* Cobalt Strike
* ComRAT
* Conficker
* Crimson
* DCSrv
* DarkComet
* DarkTortilla
* DarkWatchman
* EVILNUM
* Exaramel for Windows
* Explosive
* FELIXROOT
* Ferocious
* Gelsemium
* Grandoreiro
* GreyEnergy
* HOPLIGHT
* HermeticWiper
* Hydraq
* HyperStack
* IPsec Helper
* InvisiMole
* KEYMARBLE
* KOCTOPUS
* KONNI
* Kapeka
* LoJax
* LockBit 2.0
* LockBit 3.0
* Lokibot
* Mafalda
* MegaCortex
* Metamorfo
* Mori
* Mosquito
* NETWIRE
* Naid
* NanoCore
* Neoichor
* Nerex
* Netwalker
* NightClub
* Orz
* PHOREAL
* PLAINTEE
* Pandora
* Pillowmint
* PipeMon
* PlugX
* PoetRAT
* PoisonIvy
* PolyglotDuke
* PowerShower
* Prestige
* Pysa
* QUADAGENT
* QakBot
* RCSession
* REvil
* ROKRAT
* RTM
* RegDuke
* Regin
* Rover
* SLOTHFULMEDIA
* SMOKEDHAM
* SOUNDBITE
* SUNBURST
* Samurai
* ShadowPad
* Shamoon
* ShimRat
* ShrinkLocker
* Sibot
* StreamEx
* Stuxnet
* SynAck
* SysUpdate
* TEARDROP
* TRANSLATEXT
* TYPEFRAME
* Taidoor
* TajMahal
* Tarrask
* ThreatNeedle
* TinyTurla
* TrickBot
* Uroburos
* Ursnif
* Valak
* Volgmer
* WarzoneRAT
* WastedLocker
* Waterbear
* Zeus Panda
* ZxShell
* gh0st RAT
* metaMain
* njRAT
* zwShell

## Tools

* AADInternals
* CSPY Downloader
* CrackMapExec
* NPPSPY
* PcShare
* QuasarRAT
* Reg
* Remcos
* SILENTTRINITY

## APTs (Intrusion Sets)

* APT19
* APT32
* APT38
* APT41
* APT42
* Aquatic Panda
* BlackByte
* Blue Mockingbird
* Dragonfly
* Earth Lusca
* Ember Bear
* FIN8
* Gamaredon Group
* Gorgon Group
* Indrik Spider
* Kimsuky
* Lotus Blossom
* LuminousMoth
* Magic Hound
* OilRig
* Patchwork
* Saint Bear
* Silence
* TA505
* Threat Group-3390
* Turla
* Volt Typhoon
* Wizard Spider