# TTP Detail – T1012

## TTP Information

Name: Query Registry

Description: Adversaries may interact with the Windows Registry to gather information about the system, configuration, and installed software.

The Registry contains a significant amount of information about the operating system, configuration, software, and security.(Citation: Wikipedia Windows Registry) Information can easily be queried using the [Reg](https://attack.mitre.org/software/S0075) utility, though other means to access the Registry exist. Some of the information may help adversaries to further their operation within a network. Adversaries may use the information from [Query Registry](https://attack.mitre.org/techniques/T1012) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: discovery

## Malware

* ADVSTORESHELL
* Attor
* Azorult
* BACKSPACE
* BabyShark
* Bankshot
* Bazar
* BendyBear
* Bisonal
* BitPaymer
* BlackByte Ransomware
* Brave Prince
* Bumblebee
* CHOPSTICK
* Carbanak
* Carberp
* Carbon
* Cardinal RAT
* CharmPower
* Clambling
* Cobalt Strike
* ComRAT
* Crimson
* DUSTTRAP
* DarkWatchman
* Denis
* Derusbi
* DownPaper
* Dtrack
* Epic
* FELIXROOT
* FatDuke
* FinFisher
* FunnyDream
* Gelsemium
* Gold Dragon
* HOPLIGHT
* Hydraq
* Industroyer
* InvisiMole
* JPIN
* Kapeka
* LiteDuke
* LitePower
* Lucifer
* Mafalda
* Milan
* Mori
* OSInfo
* POWERSOURCE
* POWRUNER
* Pillowmint
* PlugX
* Proxysvc
* QUADAGENT
* QUIETCANARY
* RATANKBA
* REvil
* ROKRAT
* Raccoon Stealer
* Reaver
* Rising Sun
* SUNBURST
* SVCReady
* Saint Bot
* Samurai
* Shamoon
* Shark
* Sibot
* SodaMaster
* StoneDrill
* Stuxnet
* SynAck
* TEARDROP
* TRANSLATEXT
* Taidoor
* TinyTurla
* Uroburos
* Ursnif
* Valak
* Volgmer
* WINDSHIELD
* WastedLocker
* Waterbear
* Woody RAT
* Zebrocy
* Zeus Panda
* ZxShell
* ZxxZ
* gh0st RAT
* njRAT

## Tools

* PcShare
* PowerSploit
* Reg
* SILENTTRINITY

## APTs (Intrusion Sets)

* APT32
* APT39
* APT41
* BlackByte
* Chimera
* Daggerfly
* Dragonfly
* Fox Kitten
* Indrik Spider
* Kimsuky
* Lazarus Group
* Lotus Blossom
* OilRig
* Stealth Falcon
* Threat Group-3390
* Turla
* Volt Typhoon
* ZIRCONIUM