# TTP Detail – T1036.005

## TTP Information

Name: Match Legitimate Resource Name or Location

Description: Adversaries may match or approximate the name or location of legitimate files, Registry keys, or other resources when naming/placing them. This is done for the sake of evading defenses and observation.

This may be done by placing an executable in a commonly trusted directory (ex: under System32) or giving it the name of a legitimate, trusted program (ex: `svchost.exe`). Alternatively, a Windows Registry key may be given a close approximation to a key used by a legitimate program. In containerized environments, a threat actor may create a resource in a trusted namespace or one that matches the naming convention of a container pod or cluster.(Citation: Aquasec Kubernetes Backdoor 2023)

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: defense-evasion

## Malware

* ANDROMEDA
* AppleSeed
* BADNEWS
* BLINDINGCAN
* BackConfig
* Bad Rabbit
* Bazar
* Bisonal
* Black Basta
* Bumblebee
* Bundlore
* Calisto
* Carberp
* ChChes
* Chaes
* Chinoxy
* Cuba
* Cuckoo Stealer
* Cyclops Blink
* DRATzarus
* DUSTPAN
* DanBot
* DarkComet
* Daserf
* Doki
* Dtrack
* EKANS
* Elise
* Felismus
* FinFisher
* FoggyWeb
* Fysbis
* Gelsemium
* GoBear
* GoldMax
* GoldenSpy
* Goopy
* Grandoreiro
* Green Lambert
* HTTPBrowser
* HermeticWiper
* HermeticWizard
* IceApple
* IcedID
* InnaputRAT
* InvisiMole
* Ixeshe
* J-magic
* KGH\_SPY
* KOCTOPUS
* KONNI
* Latrodectus
* LightNeuron
* LookBack
* Machete
* MagicRAT
* MarkiRAT
* MechaFlounder
* Metamorfo
* Mis-Type
* Misdat
* NETWIRE
* NOKKI
* Nebulae
* NightClub
* Ninja
* OLDBAIT
* OSX/Shlayer
* Octopus
* OutSteel
* OwaAuth
* PUNCHBUGGY
* Penquin
* PipeMon
* PlugX
* PowGoop
* PyDCrypt
* Pysa
* QUADAGENT
* QUIETEXIT
* RDAT
* REvil
* Raindrop
* RainyDay
* Ramsay
* Remsec
* RotaJakiro
* Ryuk
* S-Type
* SLOTHFULMEDIA
* SUGARDUMP
* SUNBURST
* SUNSPOT
* SUPERNOVA
* Saint Bot
* Samurai
* Shark
* Sibot
* Skidmap
* Small Sieve
* SocGholish
* SslMM
* Starloader
* StrelaStealer
* StrifeWater
* StrongPity
* TAINTEDSCRIBE
* TEARDROP
* TRANSLATEXT
* Tarrask
* ThiefQuest
* ThreatNeedle
* TinyTurla
* Troll Stealer
* USBStealer
* Ursnif
* Winnti for Windows
* ZLib

## Tools

* Brute Ratel C4
* MCMD
* PcShare
* ShimRatReporter

## APTs (Intrusion Sets)

* APT1
* APT28
* APT29
* APT32
* APT39
* APT41
* APT42
* APT5
* Akira
* Aquatic Panda
* BRONZE BUTLER
* BackdoorDiplomacy
* Blue Mockingbird
* Carbanak
* Chimera
* Darkhotel
* Earth Lusca
* Ember Bear
* FIN13
* FIN7
* Ferocious Kitten
* Fox Kitten
* Gamaredon Group
* INC Ransom
* Indrik Spider
* Ke3chang
* Kimsuky
* Lazarus Group
* LuminousMoth
* Machete
* Magic Hound
* MuddyWater
* Mustang Panda
* Mustard Tempest
* Naikon
* OilRig
* PROMETHIUM
* Patchwork
* Poseidon Group
* RedCurl
* Rocke
* Sandworm Team
* SideCopy
* Sidewinder
* Silence
* Sowbug
* Storm-1811
* TA2541
* TeamTNT
* ToddyCat
* Transparent Tribe
* Tropic Trooper
* Turla
* Velvet Ant
* Volt Typhoon
* WIRTE
* Whitefly
* admin@338
* menuPass