# TTP Detail – T1036.004

## TTP Information

Name: Masquerade Task or Service

Description: Adversaries may attempt to manipulate the name of a task or service to make it appear legitimate or benign. Tasks/services executed by the Task Scheduler or systemd will typically be given a name and/or description.(Citation: TechNet Schtasks)(Citation: Systemd Service Units) Windows services will have a service name as well as a display name. Many benign tasks and services exist that have commonly associated names. Adversaries may give tasks or services names that are similar or identical to those of legitimate ones.

Tasks or services contain other fields, such as a description, that adversaries may attempt to make appear legitimate.(Citation: Palo Alto Shamoon Nov 2016)(Citation: Fysbis Dr Web Analysis)

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: defense-evasion

## Malware

* Attor
* Bazar
* Black Basta
* Catchamas
* ComRAT
* Crutch
* DCSrv
* DEADEYE
* DEADWOOD
* Egregor
* Emotet
* Exaramel for Windows
* FunnyDream
* Fysbis
* GoldMax
* Green Lambert
* Heyoka Backdoor
* Hildegard
* InnaputRAT
* InvisiMole
* KONNI
* KillDisk
* Kwampirs
* Machete
* Maze
* Meteor
* Nebulae
* Nidiran
* NightClub
* OSX\_OCEANLOTUS.D
* Okrum
* POWERSTATS
* PingPull
* PlugX
* RDAT
* RTM
* RainyDay
* Raspberry Robin
* RawPOS
* SLOTHFULMEDIA
* SUGARDUMP
* SVCReady
* Seasalt
* Shamoon
* ShimRat
* Spica
* StrongPity
* SysUpdate
* Tarrask
* TinyTurla
* Truvasys
* Turian
* Uroburos
* Volgmer
* ZxxZ
* build\_downer

## Tools

* CSPY Downloader
* IronNetInjector

## APTs (Intrusion Sets)

* APT-C-36
* APT32
* APT41
* Aquatic Panda
* BITTER
* BackdoorDiplomacy
* Carbanak
* FIN13
* FIN6
* FIN7
* Fox Kitten
* Higaisa
* Kimsuky
* Lazarus Group
* Magic Hound
* Naikon
* PROMETHIUM
* Winter Vivern
* Wizard Spider
* ZIRCONIUM