# TTP Detail – T1036

## TTP Information

Name: Masquerading

Description: Adversaries may attempt to manipulate features of their artifacts to make them appear legitimate or benign to users and/or security tools. Masquerading occurs when the name or location of an object, legitimate or malicious, is manipulated or abused for the sake of evading defenses and observation. This may include manipulating file metadata, tricking users into misidentifying the file type, and giving legitimate task or service names.

Renaming abusable system utilities to evade security monitoring is also a form of [Masquerading](https://attack.mitre.org/techniques/T1036).(Citation: LOLBAS Main Site)

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: defense-evasion

## Malware

* AppleSeed
* Bisonal
* BoomBox
* Dacls
* DarkGate
* DarkTortilla
* DarkWatchman
* EnvyScout
* FatDuke
* Flagpro
* FoggyWeb
* Milan
* NativeZone
* NotPetya
* Pony
* PowGoop
* RCSession
* RTM
* Raindrop
* Ramsay
* Ryuk
* Saint Bot
* SombRAT
* StrelaStealer
* TrailBlazer
* TrickBot
* UPSTYLE
* WhisperGate
* WindTail
* XCSSET

## APTs (Intrusion Sets)

* APT28
* APT32
* Agrius
* Aoqin Dragon
* BRONZE BUTLER
* Ember Bear
* FIN13
* LazyScripter
* Nomadic Octopus
* OilRig
* PLATINUM
* Sandworm Team
* Storm-1811
* TA551
* TeamTNT
* Windshift
* Winter Vivern
* ZIRCONIUM
* menuPass