# TTP Detail – T1036.003

## TTP Information

Name: Rename Legitimate Utilities

Description: Adversaries may rename legitimate / system utilities to try to evade security mechanisms concerning the usage of those utilities. Security monitoring and control mechanisms may be in place for legitimate utilities adversaries are capable of abusing, including both built-in binaries and tools such as PSExec, AutoHotKey, and IronPython.(Citation: LOLBAS Main Site)(Citation: Huntress Python Malware 2025)(Citation: The DFIR Report AutoHotKey 2023)(Citation: Splunk Detect Renamed PSExec) It may be possible to bypass those security mechanisms by renaming the utility prior to utilization (ex: rename <code>rundll32.exe</code>).(Citation: Elastic Masquerade Ball) An alternative case occurs when a legitimate utility is copied or moved to a different directory and renamed to avoid detections based on these utilities executing from non-standard paths.(Citation: F-Secure CozyDuke)

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: defense-evasion

## Malware

* CozyCar
* DarkGate
* Kevin
* StrelaStealer

## APTs (Intrusion Sets)

* APT32
* APT38
* Daggerfly
* GALLIUM
* Lazarus Group
* menuPass