# TTP Detail – T1036.001

## TTP Information

Name: Invalid Code Signature

Description: Adversaries may attempt to mimic features of valid code signatures to increase the chance of deceiving a user, analyst, or tool. Code signing provides a level of authenticity on a binary from the developer and a guarantee that the binary has not been tampered with. Adversaries can copy the metadata and signature information from a signed program, then use it as a template for an unsigned program. Files with invalid code signatures will fail digital signature validation checks, but they may appear more legitimate to users and security tools may improperly handle these files.(Citation: Threatexpress MetaTwin 2017)

Unlike [Code Signing](https://attack.mitre.org/techniques/T1553/002), this activity will not result in a valid signature.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: defense-evasion

## Malware

* BADNEWS
* Gelsemium
* NETWIRE
* Regin
* WindTail

## Tools

* PcShare

## APTs (Intrusion Sets)

* APT37
* Windshift