# TTP Detail – T1553.002

## TTP Information

Name: Code Signing

Description: Adversaries may create, acquire, or steal code signing materials to sign their malware or tools. Code signing provides a level of authenticity on a binary from the developer and a guarantee that the binary has not been tampered with. (Citation: Wikipedia Code Signing) The certificates used during an operation may be created, acquired, or stolen by the adversary. (Citation: Securelist Digital Certificates) (Citation: Symantec Digital Certificates) Unlike [Invalid Code Signature](https://attack.mitre.org/techniques/T1036/001), this activity will result in a valid signature.

Code signing to verify software on first run can be used on modern Windows and macOS systems. It is not used on Linux due to the decentralized nature of the platform. (Citation: Wikipedia Code Signing)(Citation: EclecticLightChecksonEXECodeSigning)

Code signing certificates may be used to bypass security policies that require signed code to execute on a system.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: defense-evasion

## Malware

* Anchor
* AppleJeus
* BLINDINGCAN
* BOOSTWRITE
* BackConfig
* Bandook
* Bazar
* Black Basta
* CHIMNEYSWEEP
* ChChes
* Clop
* Cobalt Strike
* Daserf
* Ebury
* Ecipekac
* Epic
* Gazer
* GoBear
* GreyEnergy
* Helminth
* HermeticWiper
* HermeticWizard
* Janicab
* LockerGoga
* Lumma Stealer
* MacMa
* Metamorfo
* More\_eggs
* Nerex
* PipeMon
* QakBot
* ROADSWEEP
* RTM
* SUNBURST
* SpicyOmelette
* StrelaStealer
* StrongPity
* Stuxnet
* SysUpdate
* TrickBot
* Troll Stealer
* ZeroCleare

## Tools

* CSPY Downloader
* QuasarRAT

## APTs (Intrusion Sets)

* APT41
* CopyKittens
* Daggerfly
* Darkhotel
* FIN6
* FIN7
* GALLIUM
* Kimsuky
* Lazarus Group
* Leviathan
* LuminousMoth
* Molerats
* Moses Staff
* OilRig
* PROMETHIUM
* Patchwork
* Saint Bear
* Scattered Spider
* Silence
* Suckfly
* TA505
* Winnti Group
* Wizard Spider
* menuPass