# TTP Detail – T1055

## TTP Information

Name: Process Injection

Description: Adversaries may inject code into processes in order to evade process-based defenses as well as possibly elevate privileges. Process injection is a method of executing arbitrary code in the address space of a separate live process. Running code in the context of another process may allow access to the process's memory, system/network resources, and possibly elevated privileges. Execution via process injection may also evade detection from security products since the execution is masked under a legitimate process.

There are many different ways to inject code into a process, many of which abuse legitimate functionalities. These implementations exist for every major OS but are typically platform specific.

More sophisticated samples may perform multiple process injections to segment modules and further evade detection, utilizing named pipes or other inter-process communication (IPC) mechanisms as a communication channel.

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: defense-evasion

**•** mitre-attack: privilege-escalation

## Malware

* ABK
* ANDROMEDA
* Agent Tesla
* Attor
* AuditCred
* Avenger
* BADHATCH
* BBK
* Backdoor.Oldrea
* Bazar
* BlackByte 2.0 Ransomware
* Bumblebee
* COATHANGER
* Cardinal RAT
* Clambling
* Cobalt Strike
* CostaBricks
* DUSTTRAP
* Dyre
* Egregor
* Gazer
* GuLoader
* HOPLIGHT
* HyperBro
* InvisiMole
* JHUHUGIT
* JPIN
* Lizar
* Mis-Type
* Mispadu
* NETWIRE
* NavRAT
* Ninja
* Pandora
* QakBot
* REvil
* ROKRAT
* Ryuk
* SLOTHFULMEDIA
* ShadowPad
* Smoke Loader
* StoneDrill
* TSCookie
* TrickBot
* WarzoneRAT
* Waterbear
* Wiarp
* Wingbird
* Woody RAT
* gh0st RAT
* metaMain

## Tools

* Donut
* Empire
* HTRAN
* IronNetInjector
* PcShare
* PoshC2
* Remcos
* SILENTTRINITY
* Sliver

## APTs (Intrusion Sets)

* APT32
* APT37
* APT38
* APT41
* APT5
* BlackByte
* Cobalt Group
* Kimsuky
* PLATINUM
* Silence
* TA2541
* Turla
* Velvet Ant
* Wizard Spider