# TTP Detail – T1620

## TTP Information

Name: Reflective Code Loading

Description: Adversaries may reflectively load code into a process in order to conceal the execution of malicious payloads. Reflective loading involves allocating then executing payloads directly within the memory of the process, vice creating a thread or process backed by a file path on disk (e.g., [Shared Modules](https://attack.mitre.org/techniques/T1129)).

Reflectively loaded payloads may be compiled binaries, anonymous files (only present in RAM), or just snubs of fileless executable code (ex: position-independent shellcode).(Citation: Introducing Donut)(Citation: S1 Custom Shellcode Tool)(Citation: Stuart ELF Memory)(Citation: 00sec Droppers)(Citation: Mandiant BYOL) For example, the `Assembly.Load()` method executed by [PowerShell](https://attack.mitre.org/techniques/T1059/001) may be abused to load raw code into the running process.(Citation: Microsoft AssemblyLoad)

Reflective code injection is very similar to [Process Injection](https://attack.mitre.org/techniques/T1055) except that the “injection” loads code into the processes’ own memory instead of that of a separate process. Reflective loading may evade process-based detections since the execution of the arbitrary code may be masked within a legitimate or otherwise benign process. Reflectively loading payloads directly into memory may also avoid creating files or other artifacts on disk, while also enabling malware to keep these payloads encrypted (or otherwise obfuscated) until execution.(Citation: Stuart ELF Memory)(Citation: 00sec Droppers)(Citation: Intezer ACBackdoor)(Citation: S1 Old Rat New Tricks)

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: defense-evasion

## Malware

* BADHATCH
* Cobalt Strike
* Cuba
* Emotet
* FoggyWeb
* Gelsemium
* IceApple
* Lokibot
* Lumma Stealer
* LunarLoader
* Pikabot
* Sardonic
* ThiefQuest
* Uroburos
* WhisperGate
* metaMain

## Tools

* Brute Ratel C4
* Donut
* PowerSploit
* SILENTTRINITY

## APTs (Intrusion Sets)

* Kimsuky
* Lazarus Group