# TTP Detail – T1055.002

## TTP Information

Name: Portable Executable Injection

Description: Adversaries may inject portable executables (PE) into processes in order to evade process-based defenses as well as possibly elevate privileges. PE injection is a method of executing arbitrary code in the address space of a separate live process.

PE injection is commonly performed by copying code (perhaps without a file on disk) into the virtual address space of the target process before invoking it via a new thread. The write can be performed with native Windows API calls such as <code>VirtualAllocEx</code> and <code>WriteProcessMemory</code>, then invoked with <code>CreateRemoteThread</code> or additional code (ex: shellcode). The displacement of the injected code does introduce the additional requirement for functionality to remap memory references. (Citation: Elastic Process Injection July 2017)

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 PE injection may also evade detection from security products since the execution is masked under a legitimate process.

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: defense-evasion

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

## Malware

* Carbanak
* DUSTPAN
* Gootloader
* GreyEnergy
* InvisiMole
* Lizar
* Pikabot
* Zeus Panda

## Tools

* Brute Ratel C4

## APTs (Intrusion Sets)

* Gorgon Group
* Rocke