# TTP Detail – T1055.004

## TTP Information

Name: Asynchronous Procedure Call

Description: Adversaries may inject malicious code into processes via the asynchronous procedure call (APC) queue in order to evade process-based defenses as well as possibly elevate privileges. APC injection is a method of executing arbitrary code in the address space of a separate live process.

APC injection is commonly performed by attaching malicious code to the APC Queue (Citation: Microsoft APC) of a process's thread. Queued APC functions are executed when the thread enters an alterable state.(Citation: Microsoft APC) A handle to an existing victim process is first created with native Windows API calls such as <code>OpenThread</code>. At this point <code>QueueUserAPC</code> can be used to invoke a function (such as <code>LoadLibrayA</code> pointing to a malicious DLL).

A variation of APC injection, dubbed "Early Bird injection", involves creating a suspended process in which malicious code can be written and executed before the process' entry point (and potentially subsequent anti-malware hooks) via an APC. (Citation: CyberBit Early Bird Apr 2018) AtomBombing (Citation: ENSIL AtomBombing Oct 2016) is another variation that utilizes APCs to invoke malicious code previously written to the global atom table.(Citation: Microsoft Atom Table)

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 APC 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

* Attor
* BADHATCH
* Bumblebee
* Carberp
* IcedID
* InvisiMole
* Pillowmint
* Saint Bot
* Sardonic
* TURNEDUP
* XLoader

## APTs (Intrusion Sets)

* FIN8