# TTP Detail – T1218.013

## TTP Information

Name: Mavinject

Description: Adversaries may abuse mavinject.exe to proxy execution of malicious code. Mavinject.exe is the Microsoft Application Virtualization Injector, a Windows utility that can inject code into external processes as part of Microsoft Application Virtualization (App-V).(Citation: LOLBAS Mavinject)

Adversaries may abuse mavinject.exe to inject malicious DLLs into running processes (i.e. [Dynamic-link Library Injection](https://attack.mitre.org/techniques/T1055/001)), allowing for arbitrary code execution (ex. <code>C:\Windows\system32\mavinject.exe PID /INJECTRUNNING PATH\_DLL</code>).(Citation: ATT Lazarus TTP Evolution)(Citation: Reaqta Mavinject) Since mavinject.exe may be digitally signed by Microsoft, proxying execution via this method may evade detection by security products because the execution is masked under a legitimate process.

In addition to [Dynamic-link Library Injection](https://attack.mitre.org/techniques/T1055/001), Mavinject.exe can also be abused to perform import descriptor injection via its <code>/HMODULE</code> command-line parameter (ex. <code>mavinject.exe PID /HMODULE=BASE\_ADDRESS PATH\_DLL ORDINAL\_NUMBER</code>). This command would inject an import table entry consisting of the specified DLL into the module at the given base address.(Citation: Mavinject Functionality Deconstructed)

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: defense-evasion