# TTP Detail – T1218.004

## TTP Information

Name: InstallUtil

Description: Adversaries may use InstallUtil to proxy execution of code through a trusted Windows utility. InstallUtil is a command-line utility that allows for installation and uninstallation of resources by executing specific installer components specified in .NET binaries. (Citation: MSDN InstallUtil) The InstallUtil binary may also be digitally signed by Microsoft and located in the .NET directories on a Windows system: <code>C:\Windows\Microsoft.NET\Framework\v<version>\InstallUtil.exe</code> and <code>C:\Windows\Microsoft.NET\Framework64\v<version>\InstallUtil.exe</code>.

InstallUtil may also be used to bypass application control through use of attributes within the binary that execute the class decorated with the attribute <code>[System.ComponentModel.RunInstaller(true)]</code>. (Citation: LOLBAS Installutil)

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: defense-evasion

## Malware

* Chaes
* Saint Bot
* WhisperGate

## Tools

* Covenant

## APTs (Intrusion Sets)

* Mustang Panda
* menuPass