# TTP Detail – T1218.007

## TTP Information

Name: Msiexec

Description: Adversaries may abuse msiexec.exe to proxy execution of malicious payloads. Msiexec.exe is the command-line utility for the Windows Installer and is thus commonly associated with executing installation packages (.msi).(Citation: Microsoft msiexec) The Msiexec.exe binary may also be digitally signed by Microsoft.

Adversaries may abuse msiexec.exe to launch local or network accessible MSI files. Msiexec.exe can also execute DLLs.(Citation: LOLBAS Msiexec)(Citation: TrendMicro Msiexec Feb 2018) Since it may be signed and native on Windows systems, msiexec.exe can be used to bypass application control solutions that do not account for its potential abuse. Msiexec.exe execution may also be elevated to SYSTEM privileges if the <code>AlwaysInstallElevated</code> policy is enabled.(Citation: Microsoft AlwaysInstallElevated 2018)

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: defense-evasion

## Malware

* AppleJeus
* Chaes
* Clop
* DEADEYE
* Duqu
* FlawedAmmyy
* Grandoreiro
* IcedID
* Javali
* Latrodectus
* LoudMiner
* Maze
* Melcoz
* Metamorfo
* Mispadu
* QakBot
* RCSession
* Ragnar Locker
* Raspberry Robin

## Tools

* RemoteUtilities

## APTs (Intrusion Sets)

* APT38
* Machete
* Molerats
* Rancor
* TA505
* ZIRCONIUM