# TTP Detail – T1218

## TTP Information

Name: System Binary Proxy Execution

Description: Adversaries may bypass process and/or signature-based defenses by proxying execution of malicious content with signed, or otherwise trusted, binaries. Binaries used in this technique are often Microsoft-signed files, indicating that they have been either downloaded from Microsoft or are already native in the operating system.(Citation: LOLBAS Project) Binaries signed with trusted digital certificates can typically execute on Windows systems protected by digital signature validation. Several Microsoft signed binaries that are default on Windows installations can be used to proxy execution of other files or commands.

Similarly, on Linux systems adversaries may abuse trusted binaries such as <code>split</code> to proxy execution of malicious commands.(Citation: split man page)(Citation: GTFO split)

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: defense-evasion

## APTs (Intrusion Sets)

* Lazarus Group
* Volt Typhoon