# TTP Detail – T1127.003

## TTP Information

Name: JamPlus

Description: Adversaries may use `JamPlus` to proxy the execution of a malicious script. `JamPlus` is a build utility tool for code and data build systems. It works with several popular compilers and can be used for generating workspaces in code editors such as Visual Studio.(Citation: JamPlus manual)

Adversaries may abuse the `JamPlus` build utility to execute malicious scripts via a `.jam` file, which describes the build process and required dependencies. Because the malicious script is executed from a reputable developer tool, it may subvert application control security systems such as Smart App Control.(Citation: Cyble)(Citation: Elastic Security Labs)

## Threat-Mapped Scoring

Score: 1.4

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: defense-evasion