# TTP Detail – T1127.001

## TTP Information

Name: MSBuild

Description: Adversaries may use MSBuild to proxy execution of code through a trusted Windows utility. MSBuild.exe (Microsoft Build Engine) is a software build platform used by Visual Studio. It handles XML formatted project files that define requirements for loading and building various platforms and configurations.(Citation: MSDN MSBuild)

Adversaries can abuse MSBuild to proxy execution of malicious code. The inline task capability of MSBuild that was introduced in .NET version 4 allows for C# or Visual Basic code to be inserted into an XML project file.(Citation: MSDN MSBuild)(Citation: Microsoft MSBuild Inline Tasks 2017) MSBuild will compile and execute the inline task. MSBuild.exe is a signed Microsoft binary, so when it is used this way it can execute arbitrary code and bypass application control defenses that are configured to allow MSBuild.exe execution.(Citation: LOLBAS Msbuild)

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: defense-evasion

## Malware

* PlugX

## Tools

* Empire