# TTP Detail – T1127

## TTP Information

Name: Trusted Developer Utilities Proxy Execution

Description: Adversaries may take advantage of trusted developer utilities to proxy execution of malicious payloads. There are many utilities used for software development related tasks that can be used to execute code in various forms to assist in development, debugging, and reverse engineering.(Citation: engima0x3 DNX Bypass)(Citation: engima0x3 RCSI Bypass)(Citation: Exploit Monday WinDbg)(Citation: LOLBAS Tracker) These utilities may often be signed with legitimate certificates that allow them to execute on a system and proxy execution of malicious code through a trusted process that effectively bypasses application control solutions.

Smart App Control is a feature of Windows that blocks applications it considers potentially malicious from running by verifying unsigned applications against a known safe list from a Microsoft cloud service before executing them.(Citation: Microsoft Smart App Control) However, adversaries may leverage "reputation hijacking" to abuse an operating system’s trust of safe, signed applications that support the execution of arbitrary code. By leveraging [Trusted Developer Utilities Proxy Execution](https://attack.mitre.org/techniques/T1127) to run their malicious code, adversaries may bypass Smart App Control protections.(Citation: Elastic Security Labs)

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: defense-evasion