# TTP Detail – T1216

## TTP Information

Name: System Script Proxy Execution

Description: Adversaries may use trusted scripts, often signed with certificates, to proxy the execution of malicious files. Several Microsoft signed scripts that have been downloaded from Microsoft or are default on Windows installations can be used to proxy execution of other files.(Citation: LOLBAS Project) This behavior may be abused by adversaries to execute malicious files that could bypass application control and signature validation on systems.(Citation: GitHub Ultimate AppLocker Bypass List)

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: defense-evasion