# TTP Detail – T1216.002

## TTP Information

Name: SyncAppvPublishingServer

Description: Adversaries may abuse SyncAppvPublishingServer.vbs to proxy execution of malicious [PowerShell](https://attack.mitre.org/techniques/T1059/001) commands. SyncAppvPublishingServer.vbs is a Visual Basic script associated with how Windows virtualizes applications (Microsoft Application Virtualization, or App-V).(Citation: 1 - appv) For example, Windows may render Win32 applications to users as virtual applications, allowing users to launch and interact with them as if they were installed locally.(Citation: 2 - appv)(Citation: 3 - appv)

The SyncAppvPublishingServer.vbs script is legitimate, may be signed by Microsoft, and is commonly executed from `\System32` through the command line via `wscript.exe`.(Citation: 4 - appv)(Citation: 5 - appv)

Adversaries may abuse SyncAppvPublishingServer.vbs to bypass [PowerShell](https://attack.mitre.org/techniques/T1059/001) execution restrictions and evade defensive counter measures by "living off the land."(Citation: 6 - appv)(Citation: 4 - appv) Proxying execution may function as a trusted/signed alternative to directly invoking `powershell.exe`.(Citation: 7 - appv)

For example, [PowerShell](https://attack.mitre.org/techniques/T1059/001) commands may be invoked using:(Citation: 5 - appv)

`SyncAppvPublishingServer.vbs "n; {PowerShell}"`

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: defense-evasion