System Script Proxy Execution: SyncAppvPublishingServer, Sub-technique T1216.002 - Enterprise

Archived: 2026-04-05 12:46:50 UTC

Adversaries may abuse SyncAppvPublishingServer.vbs to proxy execution of malicious PowerShell commands. SyncAppvPublishingServer.vbs is a Visual Basic script associated with how Windows virtualizes applications (Microsoft Application Virtualization, or App-V).[1] 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.[2][3]

The SyncAppvPublishingServer.vbs script is legitimate, may be signed by Microsoft, and is commonly executed from `\System32` through the command line via `wscript.exe`.[4][5]

Adversaries may abuse SyncAppvPublishingServer.vbs to bypass PowerShell execution restrictions and evade defensive counter measures by "living off the land."[6][4] Proxying execution may function as a trusted/signed alternative to directly invoking `powershell.exe`.[7]

For example, PowerShell commands may be invoked using:[5]

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

Source: https://attack.mitre.org/techniques/T1216/002