Product Solutions Resources Open Source Enterprise Pricing Sign in Sign up

This repository has been archived by the owner on Dec 11, 2018. It is now read-only.

api0cradle / LOLBAS Public archive

Notifications Fork 342 Star 1.6k

Code Issues Pull requests Actions Projects Security Insights

Files

d148d27

Go to file

- Logo
- OSBinaries
- OSLibraries
- OSScripts
  - Payload
  - CL_mutexverifiers.md
  - Cl_invocation.md
  - Manage-bde.md
  - Pubprn.md
  - Slmgr.md
  - Syncappvpublishingserver.md
  - Winrm.md
  - pester.md
- OtherBinaries
- OtherMSBinaries
- OtherScripts
- Backlog.txt
- Contribute.md
- LOLBins.md
- LOLLibs.md
- LOLScripts.md
- README.md

LOLBAS / OSScripts / pester.md

api0cradle Added moved message 3ea62e5 · 6 years ago History

Preview Code Blame 110 lines (76 loc) · 3.35 KB Raw

UPDATE BOOKMARKS - PROJECT MOVED TO A DEDICATED PROJECT SITE. THIS SITE WILL NOT BE UPDATED ANYMORE, BUT WILL BE KEPT FOR HISTORICAL REASONS.

New site: https://github.com/LOLBAS-Project/LOLBAS Web portal: https://lolbas-project.github.io/

pester.bat

- Functions: Execute

```
# Execute notepad
Pester.bat /help "$null; notepad"
# Execute calc
Pester.bat /help "$null; calc"
# Execute Get-Process cmdlet
Pester.bat /help "$null; ps"

# Other options for 2nd parameter
pester.bat help "$null; notepad"
pester.bat /help "$null; notepad"
pester.bat ? "$null; notepad"
pester.bat -? "$null; notepad"
pester.bat /? "$null; notepad"

# 3rd parameter can be anything
pester.bat /help "'doesnotexist'; notepad"
pester.bat /help "Get-Help; notepad"
pester.bat /help "gcm;notepad"

# 4th parameter is the payload
```

Acknowledgements:

- Emin Atac - @p0w3rsh3ll

Code sample: None

Resources: None

Full path:

```
# Shipped inbox
"c:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\bin\Pester.bat"

# There can be other versions present as well
Dir "c:\Program Files\WindowsPowerShell\Modules\Pester\*\bin\Pester.bat"
```

Notes: This file is digitally signed by a Microsoft certificate

```
 Get-FileHash "C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\b


Algorithm       Hash
---------       ----
SHA256          EB83A9D837CFE2F409CA3839B017E307A7A65782CB6A0AE0C50731C2


Get-AuthenticodeSignature "C:\Program Files\WindowsPowerShell\Modules\Pe


SignerCertificate      : [Subject]
                           CN=Microsoft Windows, O=Microsoft Corporation

                         [Issuer]
                           CN=Microsoft Windows Production PCA 2011, O=M
                         C=US

                         [Serial Number]
                           33000001733031072665B8B9B3000000000173

                         [Not Before]
                           11/08/2017 22:23:35

                         [Not After]
                           11/08/2018 22:23:35

                         [Thumbprint]
                           14590DC5C3AAF238FCFD7785B4B93F4071402C34

TimeStamperCertificate : [Subject]
                           CN=Microsoft Time-Stamp Service, OU=nCipher D
                         Corporation, L=Redmond, S=Washington, C=US

                         [Issuer]
                           CN=Microsoft Time-Stamp PCA 2010, O=Microsoft

                         [Serial Number]
                           33000000AC8A21BC7AD29B72F40000000000AC

                         [Not Before]
                           07/09/2016 19:56:54

                         [Not After]
                           07/09/2018 19:56:54

                         [Thumbprint]
                           3970258B14C879DD5F0C5DE98B9CB39499F71CB7

Status                 : Valid
StatusMessage          : Signature verified.
Path                   : C:\Program Files\WindowsPowerShell\Modules\Pest
SignatureType          : Catalog
IsOSBinary             : True
```