GitHub - orlyjamie/mimikittenz: A post-exploitation powershell tool for extracting juicy info from memory.

By orlyjamie

Archived: 2026-04-05 16:17:34 UTC

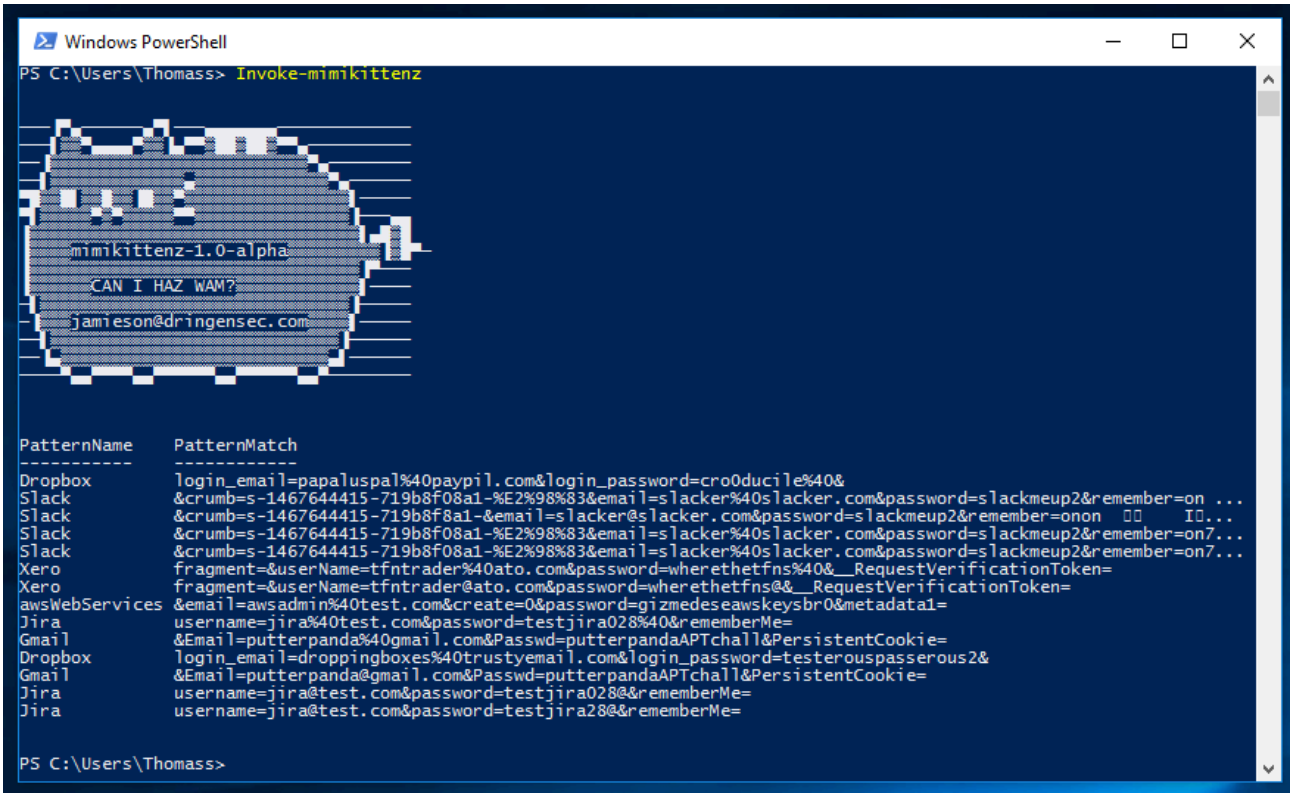
`mimikittenz` is a post-exploitation powershell tool that utilizes the Windows function `ReadProcessMemory()` in order to extract plain-text passwords from various target processes.

`mimikittenz` can also easily extract other kinds of juicy info from target processes using regex patterns including but not limited to:

- TRACK2 (CreditCard) data from merchant/POS processes
- PII data
- Encryption Keys & All the other goodstuff

note: This tool is targeting running process memory address space, once a process is killed it's memory 'should' be cleaned up and inaccessible however there are some edge cases in which this does not happen.

Screenshot(s)



Description

The aim of `mimikittenz` is to provide user-level (non-admin privileged) sensitive data extraction in order to maximise post exploitation efforts and increase value of information gathered per target.

Currently `mimikittenz` is able to extract the following credentials from memory:

#####Webmail#####

- Gmail
- Office365
- Outlook Web

#####Accounting#####

- Xero
- MYOB

#####Remote Access#####

- Juniper SSL-VPN
- Citrix NetScaler
- Remote Desktop Web Access 2012

#####Development#####

- Jira
- Github
- Bugzilla
- Zendesk
- Cpanel

#####IHateReverseEngineers#####

- Malwr
- VirusTotal
- AnubisLabs

#####Misc#####

- Dropbox
- Microsoft Onedrive
- AWS Web Services
- Slack
- Twitter
- Facebook

License

https://creativecommons.org/licenses/by/4.0/

Customization

- Custom regex - The syntax for adding custom regex is as follows:

```
[mimikittenz.MemProcInspector]::AddRegex("<NameOfTarget>","<regex_here>")
```

- Custom target process - Just append your target process name into the array:

```
[mimikittenz.MemProcInspector]::InspectManyProcs("iexplore","chrome","firefox")
```

Contributions

I'd love to see the list of regex's and target processe's grow in order to build a comprehensive post-exploitaiton hit list.
