
black hat®
ARSENAL 2023
AUGUST 9-10
MANDALAY BAY/LAS VEGAS

~~PowerGuest~~ powerpwn

An offensive security toolset for Microsoft 365 Power Platform

Intro

- powerpwn is an offensive security toolset for Microsoft 365 Power Platform.
- Targeting red teams and penetration testers to make sure your environment is secured.

- All materials and talks can be found in our repo.

github.com/mbrg/power-pwn

@lana__salameh
@mbrg0

black hat ARSENAL 2023

About Us

Lana Salameh

- Team lead @ Zenity
- Passionate about Cyber security
- My first BlackHat

@lana__salameh

linkedin.com/in/salameh-lana

Michael Bargury

- CTO and Co-founder @ Zenity
- OWASP LCNC Top 10 project lead
- Dark Reading columnist
- Defcon, BSides, RSAC, OWASP

@mbrg0

github.com/mbrg

DR darkreading.com/author/michael-bargury

Let the fun begin with

pip install powerpwn

Beyond recon

Guest accounts have your corp data

- The assumption that guest users have limited access to the organization resources is completely wrong.
- State of the art is focused on AAD enumeration (*AADInternals*).
- Guest users actually have access to credentials, resources and data.

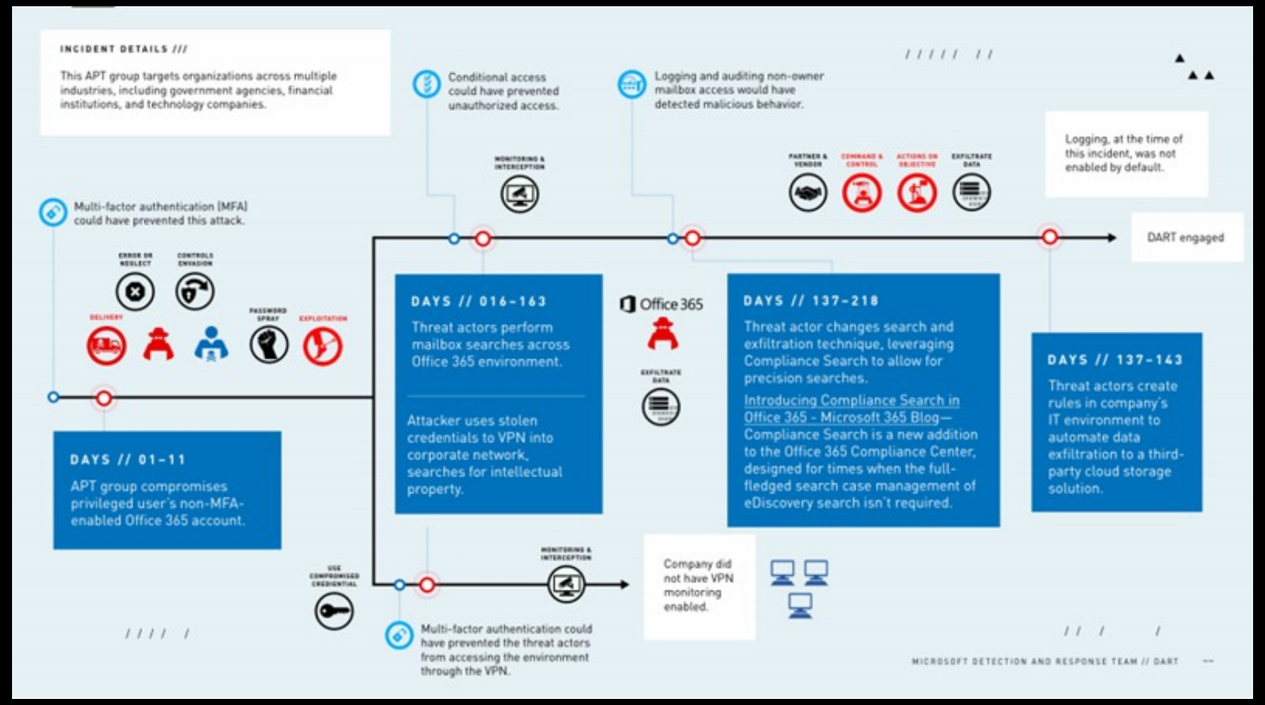
Check out our BlackHat 2023 talk titled **All You Need Is Guest**. black hat.com/us-23/briefings/schedule/index.html#all-you-need-is-guest-32647

Demo

Persistency

How to keep a ‘forever’ access

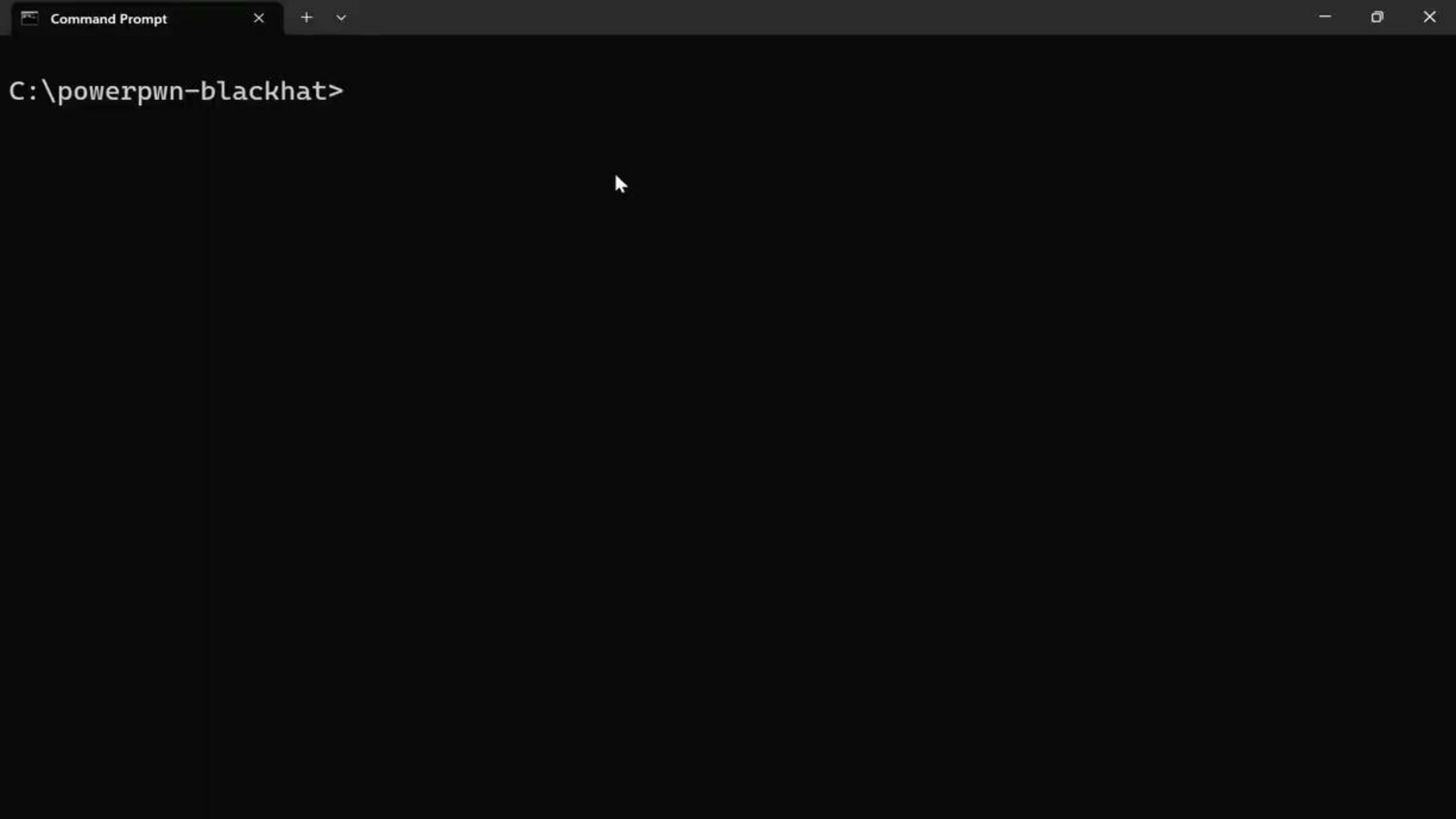
We want to remain persistent within Microsoft 365 even if the user gets deleted or their access is revoked.



Enterprise Domination via Low Code Abuse, DEFCON30

youtu.be/D3A62Rzozq4?t=1285

Demo


Command Prompt
C:\powerpwn-blackhat>

Phishing

Collect the hanging fruits

A trusted Microsoft domain

+

Built-in business SSO

+

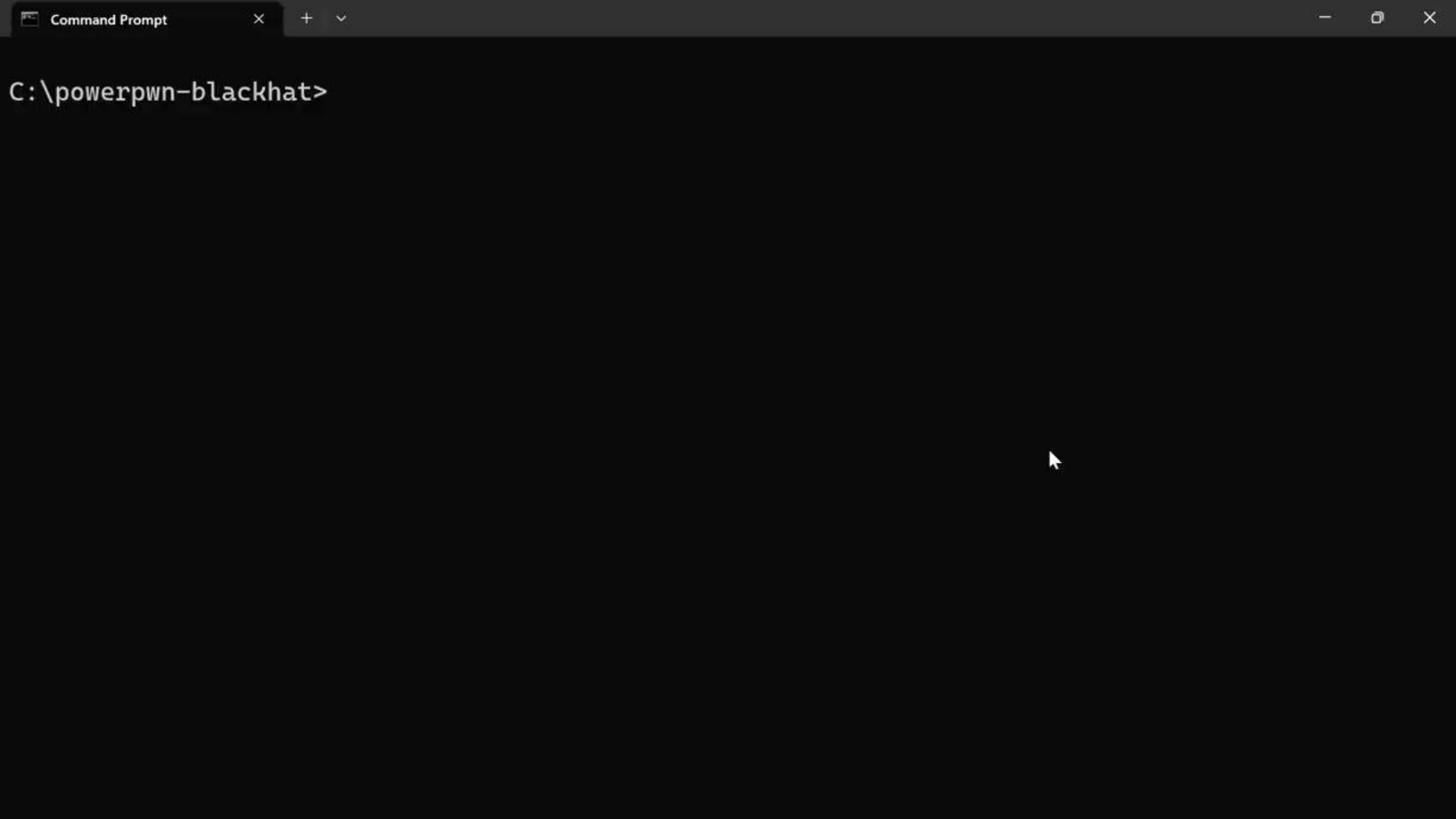
Users are familiar with PowerApps

=

Phishing by a single URL click

Enterprise Domination via
Low Code Abuse, DEFCON30
youtu.be/D3A62Rzozq4

Demo


Command Prompt
C:\powerpwn-blackhat>

Hack your environment

Power Pwn

Black Hat Arsenal USA 2023 DEFCON 30

Stars 173 Follow michael.bargury owasp.org

Power Pwn is an offensive security toolset for Microsoft Power Platform.

Install with `pip install powerpwn`.

Check out our Wiki for docs, guides and related talks!

```
--------------------------------------------------------------------


 _ __    ___   __      __ ___  _ __  _ __   __      __ _ __
| '_ \  / _ \  \ \ /\ / // _ \| '__|| '_ \  \ \ /\ / /| '_ \
| |_) || (_) |  \ V  V / |  __/| |   | |_) |  \ V  V / | | | |
| .__/  \___/    \_/\_/   \___||_|   | .__/    \_/\_/  |_| |_|
|_|                                   |_|

--------------------------------------------------------------------
```

bit.ly/mbrg-bhusa23

~~PowerGuest~~ powerpwn

An offensive security toolset for Microsoft 365 Power Platform

black hat ARSENAL 2023

Power Pwn

Black Hat Arsenal USA 2023 DEFCON 30

Stars 173 Follow michael.bargury owasp.org

Power Pwn is an offensive security toolset for Microsoft Power Platform.

Install with `pip install powerpwn`.

Check out our Wiki for docs, guides and related talks!

```
----------------------------------------------------------------------


 _ __    ___   __      __  ___  _ __   _ __   __      __ _ __
| '_ \  / _ \ \ \ /\ / / / _ \| '__| | '_ \ \ \ /\ / /| '_ \
| |_) || (_) | \ V  V / |  __/| |    | |_) | \ V  V / | | | |
| .__/  \___/   \_/\_/   \___||_|    | .__/   \_/\_/  |_| |_|
|_|                                   |_|

-----
                        command
    dump                Recon for available data connections and dump their content.
    gui                 Show collected resources and data via GUI.
    backdoor            Install a backdoor on the target tenant
    nocodemalware       Repurpose trusted execs, service accounts and cloud services to power a malware
    phishing            Deploy a trustworthy phishing app.
```

Find us at BlackHat Arsenal!

PowerGuest: AAD Guest Exploitation Beyond Enumeration

+ on GitHub!
github.com/mbrg/power-pwn

D3FCON

@mbrg0