powerpwn

An offensive security toolset for Microsoft 365 Power Platform

About Them

Lana Salameh

- Team lead @ Zenity
- Passionate about Cyber security

@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

About Me

Inbar Raz

- VP of Research @ Zenity
- Hacker of Things
- Retro-computing collector and restorer
- Defcon, BSides, VB, SAS, CCC, CARO, and more

@inbarraz

Intro

- powerpwn is an offensive security toolset for Microsoft 365 Power Platform.
- Aimed at red teams and penetration testers for making sure their environment is secure.

- Comprised of multiple different modules.

github.com/mbrg/power-pwn

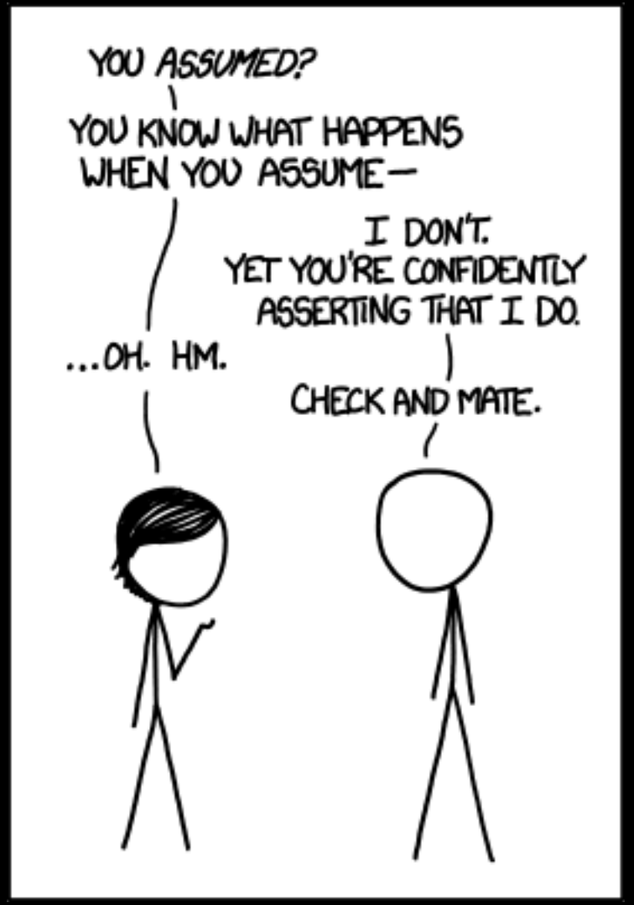
Let the fun begin

pip install powerpwn

More than meets the eye

Guest accounts have your corp data

- The assumption that guest users have limited access to the organization resources is completely wrong.



https://xkcd.com/1339/

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 attacks are focused on AAD enumeration (*AADInternals*).

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 attacks are focused on AAD enumeration (*AADInternals*).
- Guest users actually have access to resources, data, and **credentials**. You just don’t know it.

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 attacks are focused on AAD enumeration (*AADInternals*).

- Guest users actually have access to resources, data, and **credentials**. You just don't know it.

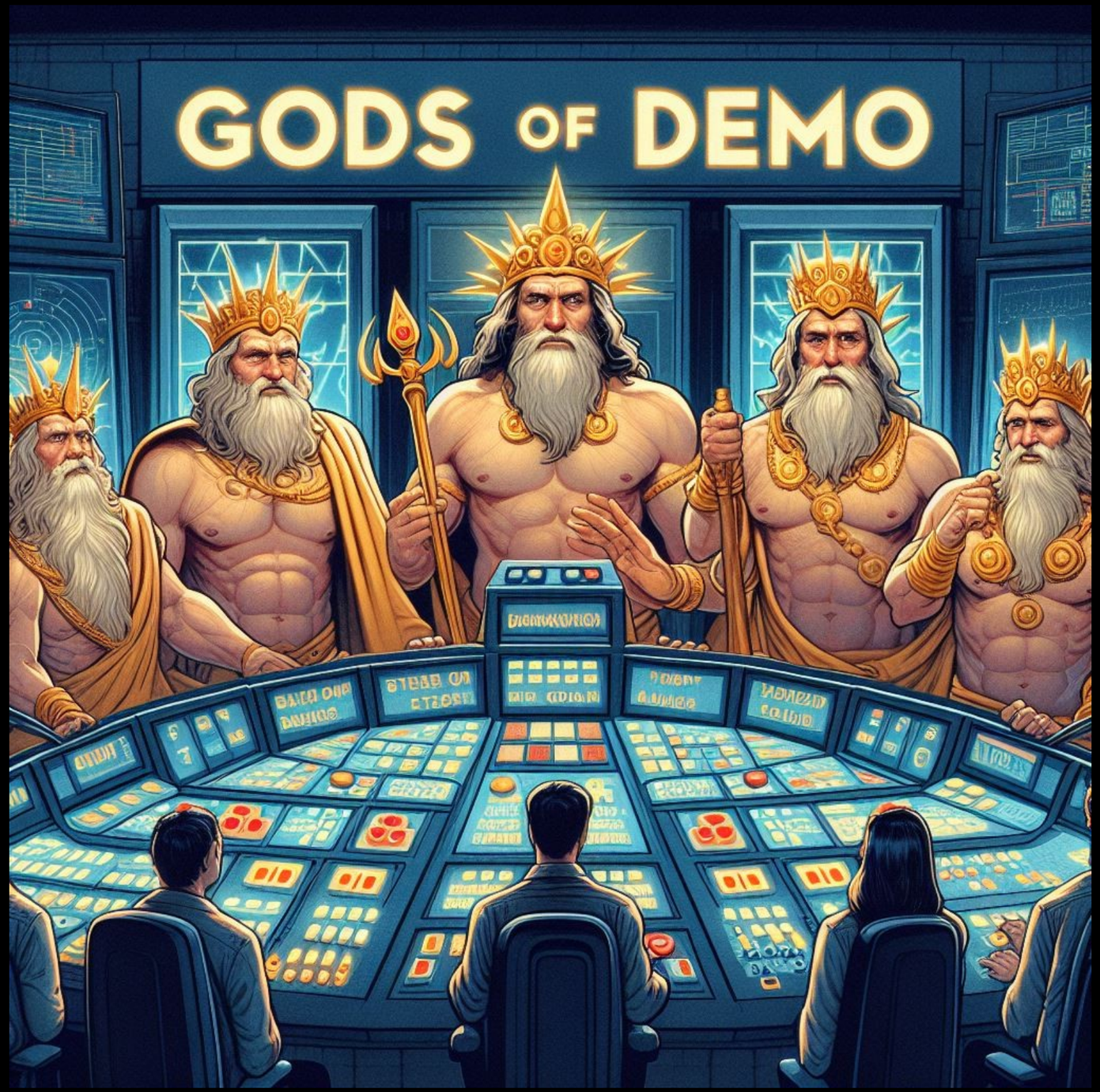
BlackHat USA 2023 talk: **All You Need Is Guest**
blackhat.com/us-23/briefings/schedule/index.html#all-you-need-is-guest-32647

Stanley Kubrick
@StanleyKubrick

You talk the talk...but can you walk the walk? #FullMetalJacket #StanleyKubrick

10:30 PM · Sep 5, 2018

Demo


GODS OF DEMO

Sign in to your account | New Incognito Tab

https://myapplications.microsoft.com/

Incognito

github | datadog | Zenity | AWS | Tools

You've gone Incognito

Now you can browse privately, and other people who use this device won't see your activity. However, downloads, bookmarks and reading list items will be saved. Learn more

Chrome won't save the following information:

- Your browsing history
- Cookies and site data
- Information entered in forms

Your activity might still be visible to:

- Websites you visit
- Your employer or school
- Your internet service provider

Block third-party cookies
When on, sites can't use cookies that track you across the web. Features on some sites may break.

So far, a Guest user has:

- Connected to a host tenant;
- Ran recon and enumerated on available resources;
- Harvested stored (and shared) credentials;
- Executed arbitrary commands on an SQL server.

So far, a Guest user has:

- Connectec
- Ran recon
- Harvested
- Executed a

Sign in to your account | New Incognito Tab

https://myapplications.microsoft.com/

Incognito

github | datadog | Zenity | AWS | Tools

You've gone Incognito

Now you can browse privately, and other people who use this device won't see your activity. However, downloads, bookmarks and reading list items will be saved. Learn more

Chrome won't save the following information:

- Your browsing history
- Cookies and site data
- Information entered in forms

Your activity might still be visible to:

- Websites you visit
- Your employer or school
- Your internet service provider

Block third-party cookies
When on, sites can't use cookies that track you across the web. Features on some sites may break.

So far, a Guest user has:

- Connected to a host tenant;
- Ran recon and enumerated on available resources;
- Harvested stored (and shared) credentials;
- Executed arbitrary commands on an SQL server.

So far, a Guest user has:

- Connected to a host tenant;
- Ran recon and enumerated on available resources;
- Harvested stored (and shared) credentials;
- Executed arbitrary commands on an SQL server;
- Executed arbitrary applications on the tenant.

JIT Access:

- A user request permission to perform actions;
- The approved user executes an app;
- The app triggers an automation to perform some of its tasks;
- The oblivious automation carries out its task.

But what happens if the app and automations are over-shared?

Sign in to your account | New Incognito Tab

https://myapplications.microsoft.com/

Incognito

github | datadog | Zenity | AWS | Tools

You've gone Incognito

Now you can browse privately, and other people who use this device won't see your activity. However, downloads, bookmarks and reading list items will be saved. Learn more

Chrome won't save the following information:

- Your browsing history
- Cookies and site data
- Information entered in forms

Your activity might still be visible to:

- Websites you visit
- Your employer or school
- Your internet service provider

Block third-party cookies
When on, sites can't use cookies that track you across the web. Features on some sites may break.


GREAT SUCCESS!
quickmeme.com

So far, a Guest user has:

- Connected to a host tenant;
- Ran recon and enumerated on available resources;
- Harvested stored (and shared) credentials;
- Executed arbitrary commands on an SQL server;
- Executed arbitrary applications on the tenant.

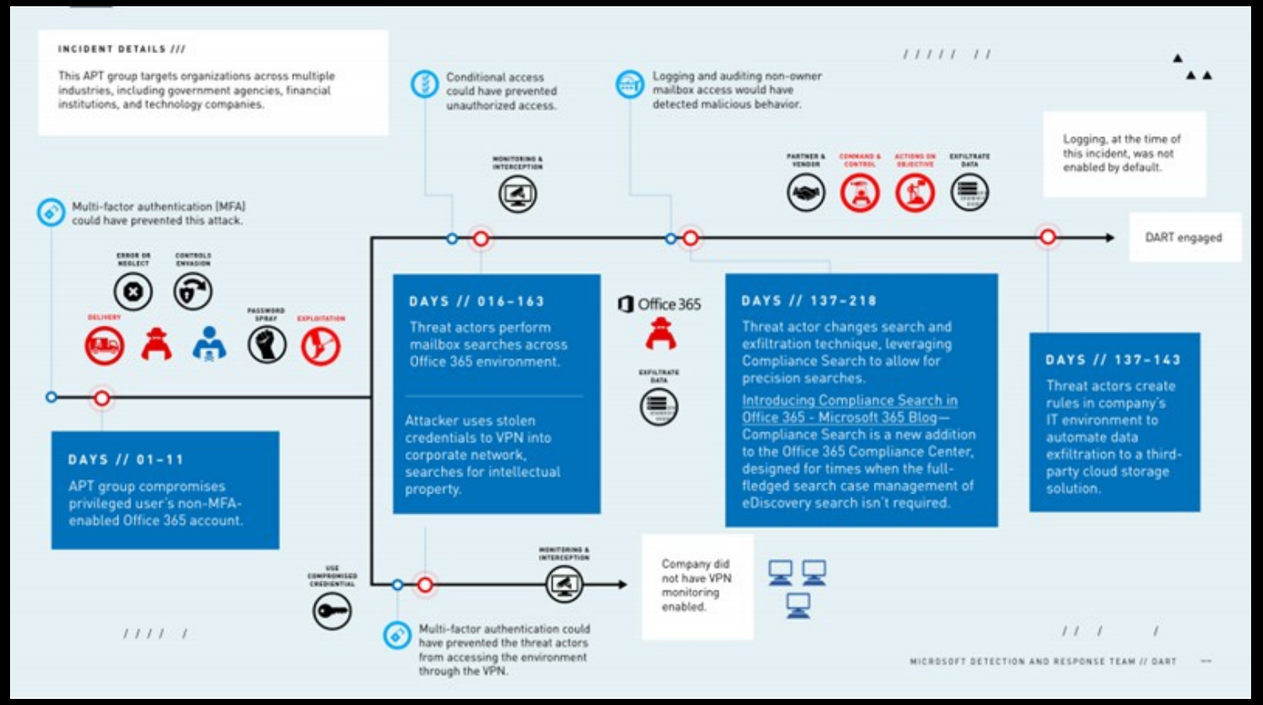
So far, a Guest user has:

- Connected to a host tenant;
- Ran recon and enumerated on available resources;
- Harvested stored (and shared) credentials;
- Executed arbitrary commands on an SQL server;
- Executed arbitrary applications on the tenant;
- Performed Privilege Escalation using an Automation.

Persistence

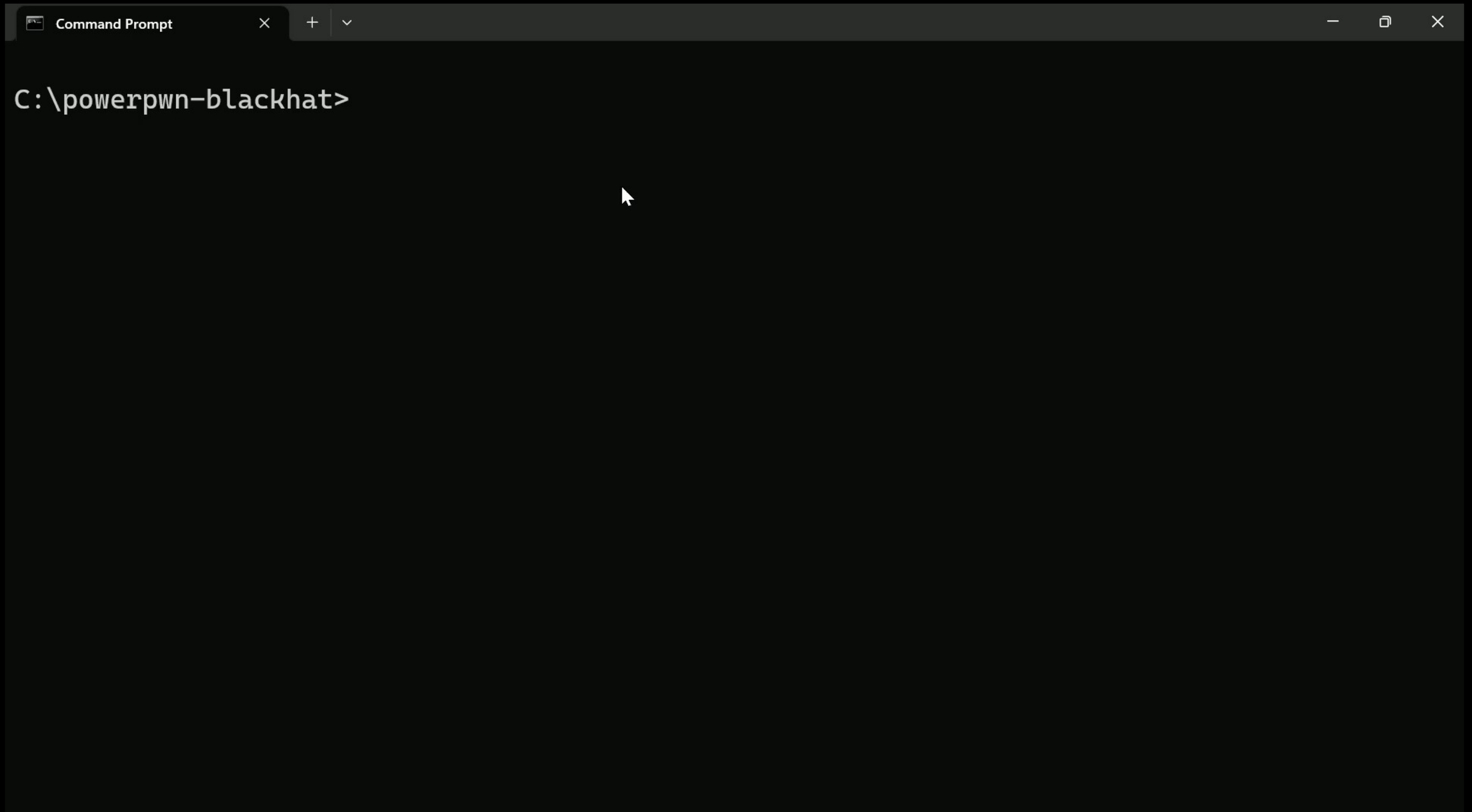
How to keep a ‘forever’ access

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



DEFCON30 talk: **Enterprise Domination via Low Code Abuse**
youtu.be/D3A62Rzozq4?t=1285

Demo

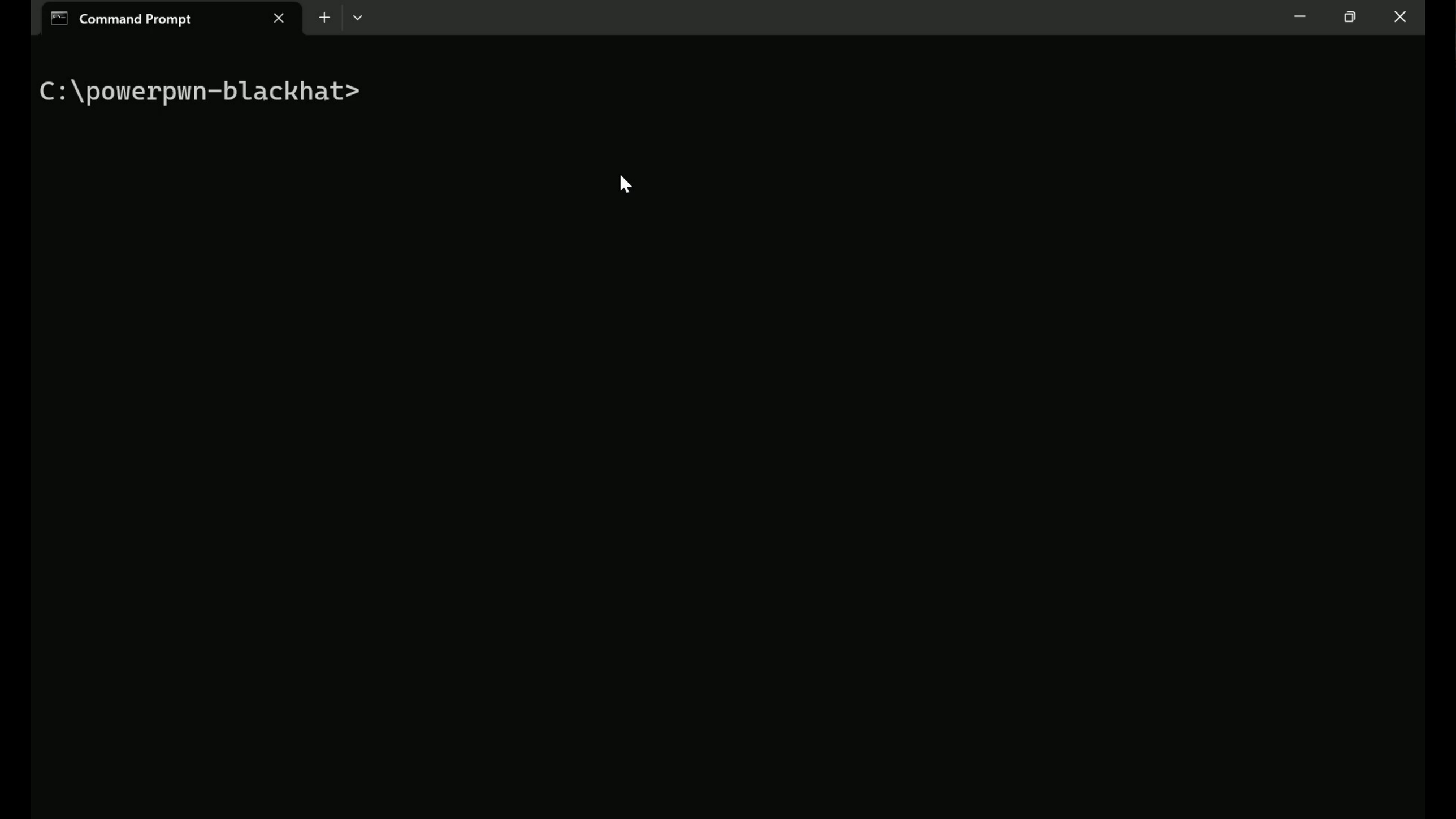

Command Prompt
C:\powerpwn-blackhat>

Where do we stand now?

- A person whose account was **disabled** regained access;
- This was done using a public webhook;
- The outsider could be anyone – it doesn't have to be Jamie

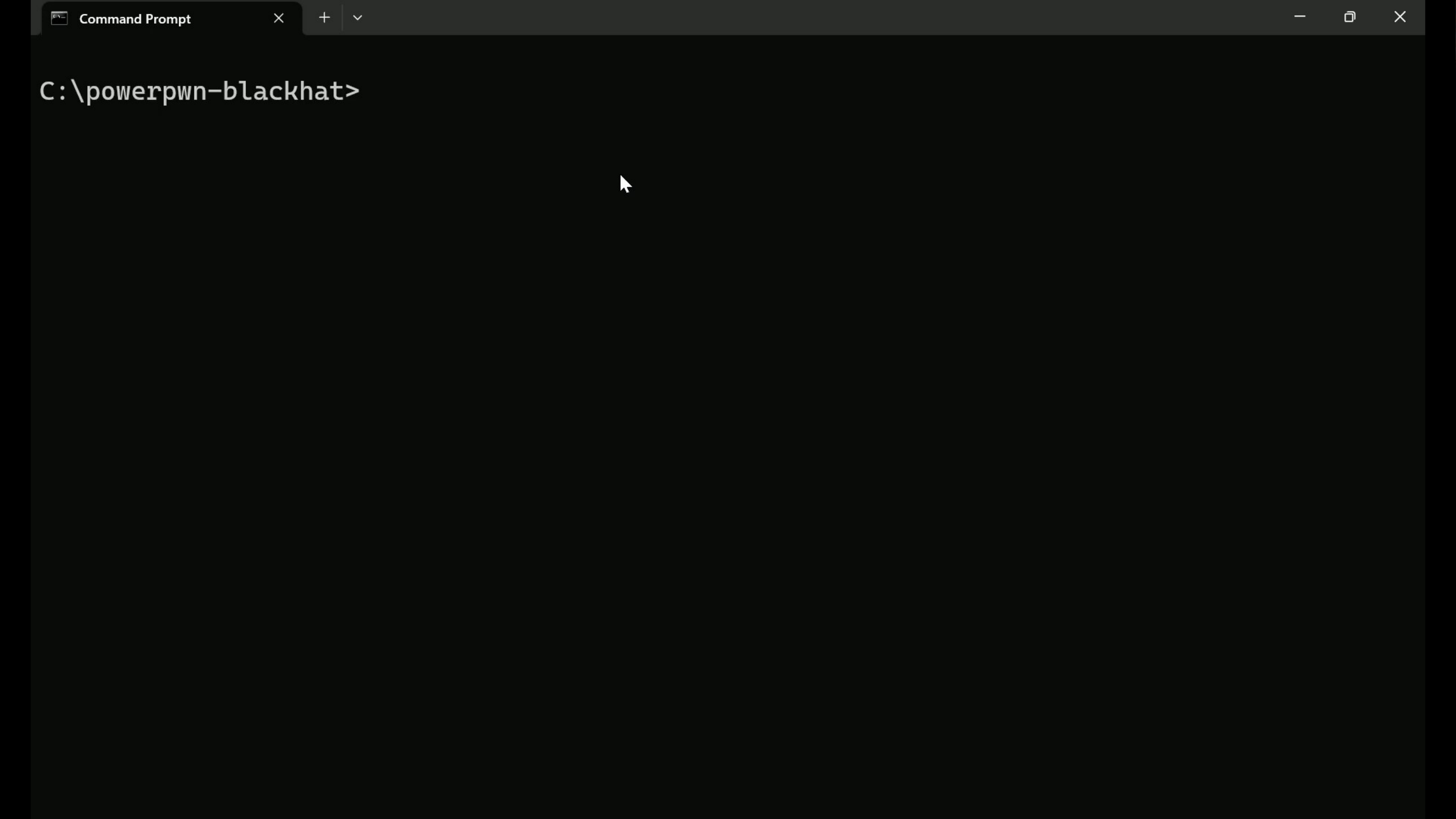
What's next?

- Create a new Automation;
- The Automation will get us access tokens to an Azure blob.


Command Prompt
C:\powerpwn-blackhat>

What about OPSEC?

- Executing Automations leaves behind logs;
- Deteting the Automation will delete its execution logs as well.


Command Prompt
C:\powerpwn-blackhat>

To add insult to injury:

- An active member installed a backdoor;
- At some later point, despite their account being **disabled**, the *no-longer-member* reconnected and gained access;
- A new Automation was created, for providing access to a tenant resource;
- Free access to the resource was gained from outside the tenant;
- The incriminating Automation was deleted along with its logs.


TAKE IT TO
THE NEXT LEVEL

Phishing

Collect the low-hanging fruits

A trusted Microsoft domain

Collect the low-hanging fruits

A trusted Microsoft domain

+

Built-in business SSO

Collect the low-hanging fruits

A trusted Microsoft domain

+

Built-in business SSO

+

Users are familiar with PowerApps

Collect the low-hanging fruits

A trusted Microsoft domain

+

Built-in business SSO

=

Phishing by a single URL click

+

Users are familiar with PowerApps

Collect the low-hanging fruits

A trusted Microsoft domain

+

Built-in business SSO

=

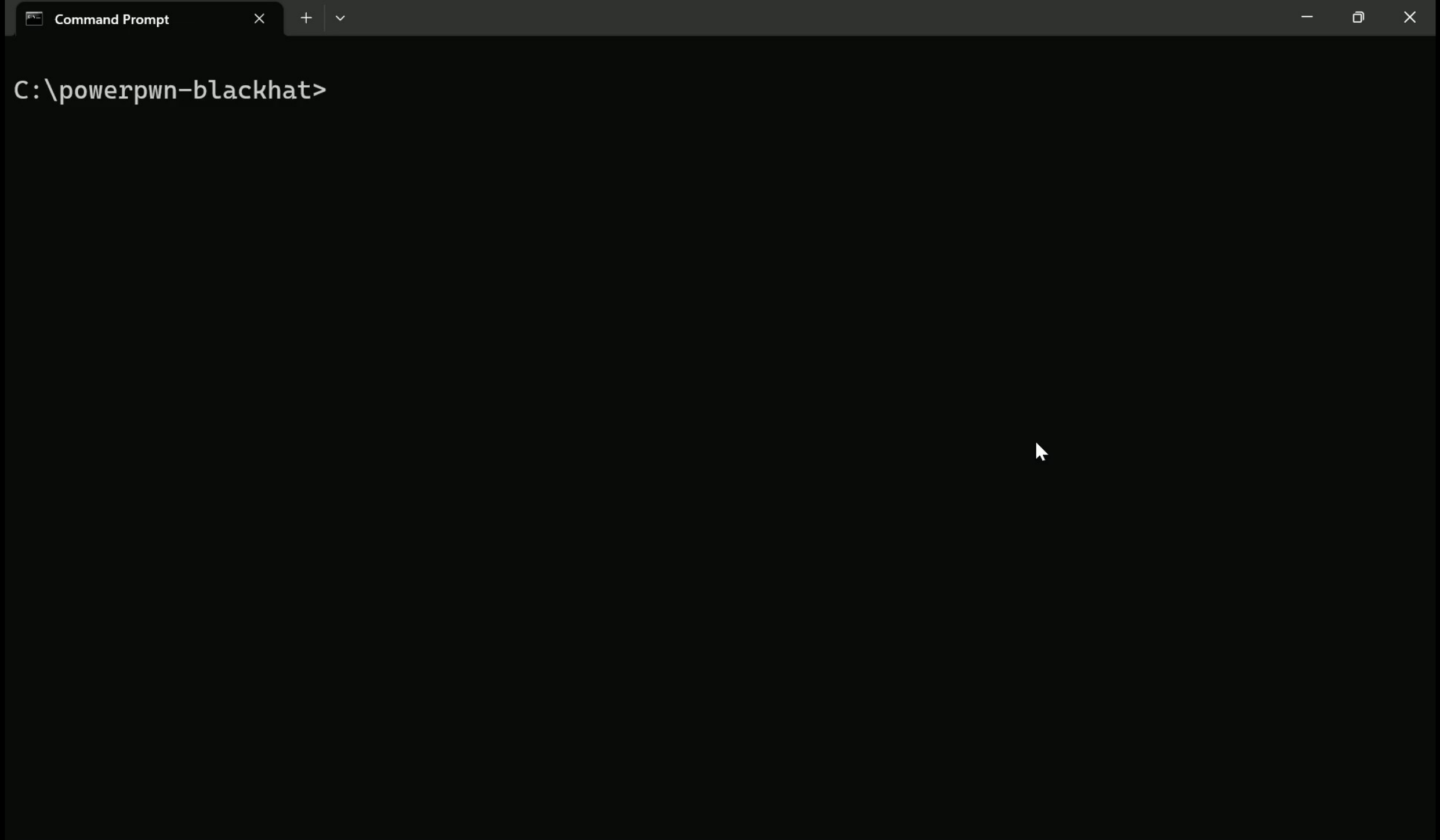
Phishing by a single URL click

+

Users are familiar with PowerApps

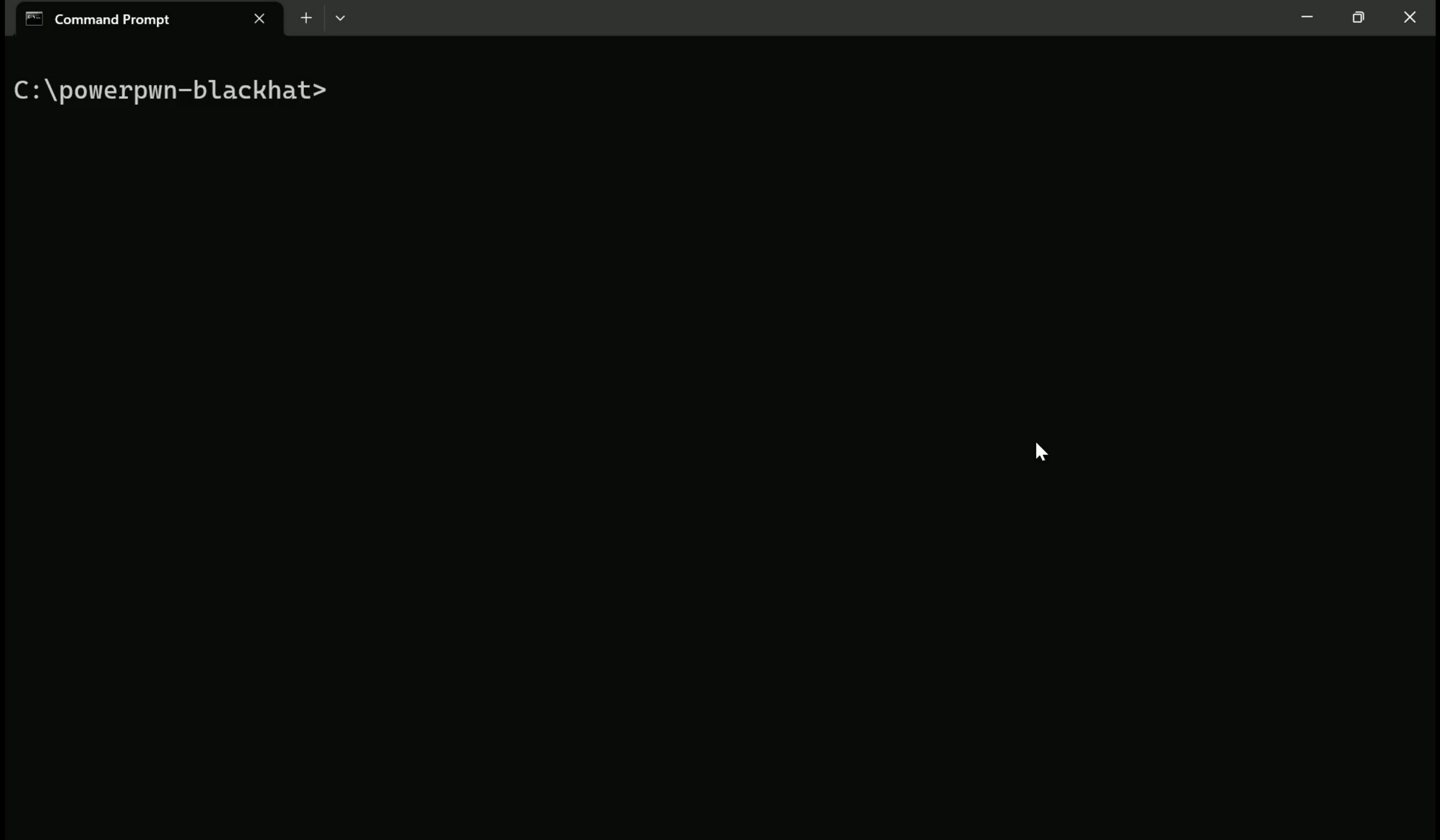
DEFCON30 talk: **Enterprise Domination via Low Code Abuse**: youtu.be/D3A62Rzozq4

Demo


Command Prompt
C:\powerpwn-blackhat>

What about OPSEC?

- We delete the sent items and the trash.


Command Prompt
C:\powerpwn-blackhat>

Recap

What did we see today?

What did we see today?

1. A guest user gaining access to corporate resources and **credentials**

What did we see today?

1. A guest user gaining access to corporate resources and **credentials**
2. Execution of arbitrary commands using obtained credentials

What did we see today?

1. A guest user gaining access to corporate resources and **credentials**
2. Execution of arbitrary commands using obtained credentials
3. Installation of a backdoor using an Automation and achieving persistence

What did we see today?

1. A guest user gaining access to corporate resources and **credentials**
2. Execution of arbitrary commands using obtained credentials
3. Installation of a backdoor using an Automation and achieving persistence
4. Carrying out a tenant-wide phishing attack

What did we see today?

1. A guest user gaining access to corporate resources and **credentials**
2. Execution of arbitrary commands using obtained credentials
3. Installation of a backdoor using an Automation and achieving persistence
4. Carrying out a tenant-wide phishing attack

What can *YOU* do?

What can *YOU* do?

1. Don’t over-share your resources (duh!)

What can *YOU* do?

1. Don’t over-share your resources (duh!)
2. Follow security best-practices – OWASP Top 10 for LCNC

What can *YOU* do?

1. Don’t over-share your resources (duh!)
2. Follow security best-practices – OWASP Top 10 for LCNC
3. Constantly monitor your environment and go threat-hunting

What can *YOU* do?

1. Don’t over-share your resources (duh!)
2. Follow security best-practices – OWASP Top 10 for LCNC
3. Constantly monitor your environment and go threat-hunting
4. GO HACK YOURSELF

powerpwn

An offensive security toolset for Microsoft 365 Power Platform

References:
bit.ly/mbrg-bhusa23