

# Post-Ex

△ADVERSARY IN THE MIDDLE: POST-EXPLOIT△TION



# Speaker bio



**Michael Allen**, OSCE, MLSE, CISSP 🙄, ...

- Pentesting and red teaming since 2014



Red Team Practice Lead at BHIS

- *Initial Access Specialist* on BHIS's ANTISOC™



I also teach: **Red Team Initial Access**

- **Live:** WWHF: Mile High (Denver, Feb '25), KernelCon (Omaha, Apr '25)
- **Antisyphon On-Demand:** Initial-Access.com



@Wh1t3Rh1n0 on GitHub, X, and LinkedIn



# Backstory...



# So far you have...

1. Executed Adversary-in-the-Middle phishing of a Single Sign-On portal.
2. Captured credentials and session tokens of users who signed in.
3. Successfully hijacked the user's session on the SSO portal. 👍





# Post-Exploitation



# AITM Post-Exploitation Triage

1. Prevent user alerts.
2. Add our own MFA token to the account.
  - Persistence if the session times out.
  - Ability to log into non-web resources. Example: VPN
3. Check for internal network access.
  - *Even if we can't add MFA!* 🧐
4. Access and persist in other web apps.
5. Device Code access to Microsoft services.
  - ⚠️ Use with caution! ⚠️



# 1. Prevent user alerts.

## Review a recent login from a new device

There was a recent login to your account.  
Please review the details:

@ **Account**

[REDACTED]

**Login method**  
Email

**IP & approximate location**  
[REDACTED] - Little River, US-SC, United States

**Device type**  
iOS

[EXTERNAL] **MFA Factor Enrolled**

Hi [REDACTED]

[REDACTED] enrolled in multi-factor authentication for your account [REDACTED]

### Details

Okta Verify

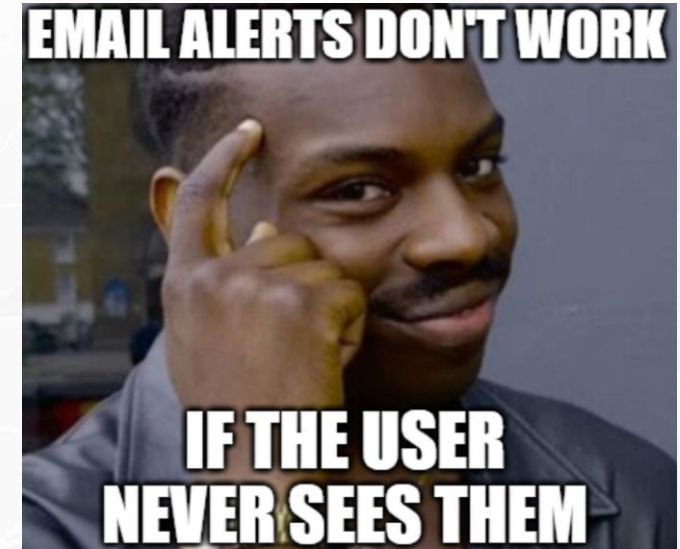
Tuesday, July 16, 2024

Florida, United States

### Don't recognize this activity?

The purpose of this email is to ensure that we update you when important actions are taken. The security of your account is important to us. If you don't recognize this activity, please contact your administrator immediately.

# Block email alerts with rules



**Rules**

✓ Filter Junk mail

✓ Add a condition

Subject or body includes

security alert × new sign × new signin ×  
new sign-in × new device × new log ×  
new log-in × new login ×  
new location × suspicious ×  
wasn't you × isn't you ×  
don't recognize × MFA × MFA factor ×  
token × multi-factor × multifactor ×

3 Add an action

Delete ×

Mark as read ×

[Add another action](#)

[Add an exception](#)

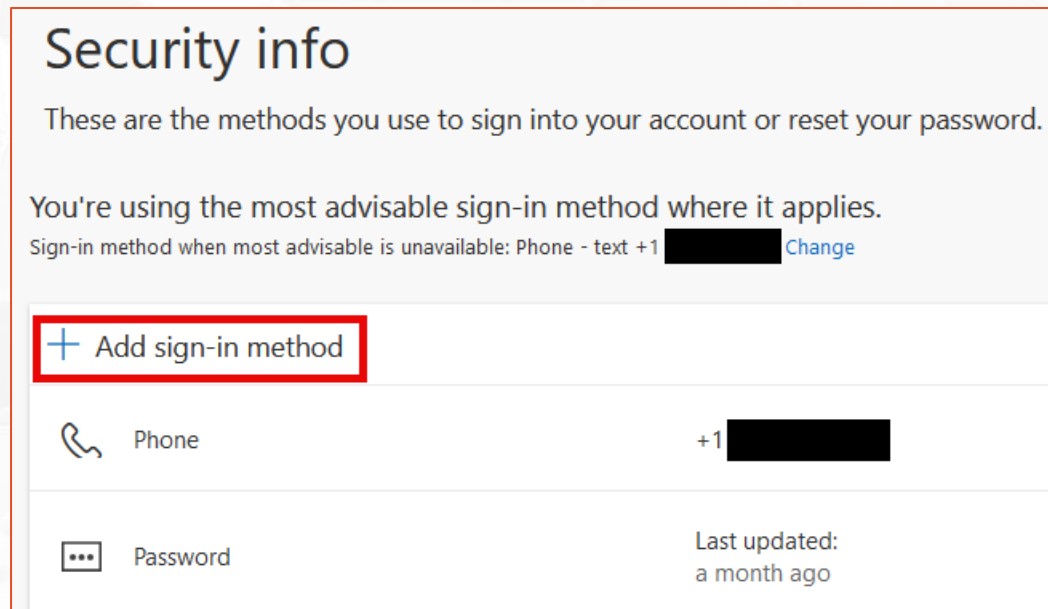
☒ Stop processing more rules ⓘ

☐ Run rule now



## 2. Add our own MFA token to the account.

- MFA is often ***not required*** to add a new MFA token.
  - Not required **by default**:
    - Microsoft 365
    - Okta



**Security info**

These are the methods you use to sign into your account or reset your password.

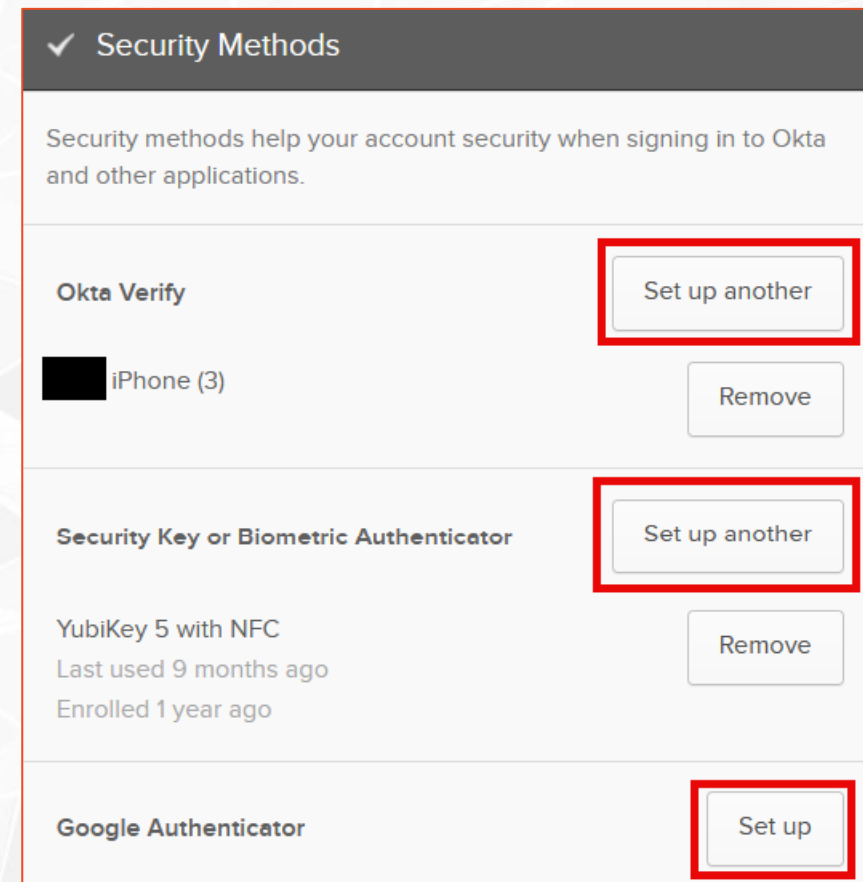
You're using the most advisable sign-in method where it applies.

Sign-in method when most advisable is unavailable: Phone - text +1 [redacted] [Change](#)

**+ Add sign-in method**

Phone +1 [redacted]

Password Last updated: a month ago



**✓ Security Methods**

Security methods help your account security when signing in to Okta and other applications.

**Okta Verify**

[redacted] iPhone (3)

**Set up another**

Remove

**Security Key or Biometric Authenticator**

**Set up another**

YubiKey 5 with NFC

Last used 9 months ago

Enrolled 1 year ago

Remove

**Google Authenticator**

**Set up**

# OPSEC when adding MFA Tokens (1/2)

1. Don't remove/reset any existing MFA tokens.
2. Use Google Authenticator/TOTP if available.
  - No push notifications generated on login.
  - No network traffic between your mobile device and the environment.
    - IP address, device model, etc. are not disclosed.
  - Easily shared between multiple testers. QR code / TOTP secret key.
3. All other token types:
  - Connect your phone to a **geolocated VPN**.
  - Avoid using push notifications if possible.
    - They typically push to all devices, including the user's real phone.
    - Minimize the number of sign-ins if not possible



# OPSEC when adding MFA Tokens (2/2)


4. Make sure the user's default MFA method remains the same after adding your MFA token.

## Security info


These are the methods you use to sign into your account or reset your password.

[Set default sign-in method](#)

+ Add sign-in method

 Authenticator app  
Time-based one-time password (TOTP)

Delete

 Microsoft Authenticator  
Push multi-factor authentication (MFA)

Delete

# What if you can't add an MFA token?

- Check SSO user profile, settings, and security info pages.
- Check internal documentation.
  - SharePoint, Email, ServiceNow, etc.
- Try default MFA enrollment URLs.
  - Okta, for example:  
[{COMPANY}.okta.com/signin/enroll](#)

## Still no luck?

- Ask the friendly AI chatbot! 

✓ Extra Verification	
Extra verification increases your account security when signing in to Okta and other applications you use	
Okta Verify	Enabled
SMS Authentication	Enabled



Can I add an additional multifactor token to my account?



Last read

ServiceBot 11:42 AM



Ok, I understand you are having issues with your Multi-Factor Authentication (MFA). I can help!

**Would you like me to reset your Okta MFA?**

Clicking 'Reset MFA' will reset all your configured factors e.g. SMS, call, push etc.

**Yes, reset MFA**

No

File ticket

ServiceBot 12:00 PM



*Got it, working on it...*

Reset complete!



[Click this link to set up your new Multi-Factor Authentication \(MFA\)](#)

If you are having login issues, you can try resetting your password by typing *reset my password*.



# Resetting all the MFA tokens

- Check the user's calendar,
- automatic reply settings,
- Inbox/Teams – Is the user active?

## Automatic replies

☒ Automatic replies on

Send automatic replies inside your organization

📧 AA A<sup>o</sup> **B** *I* U ✎ ✓ A ✓ ☰ ☷ ⌵ ⌶ ” ☰ ☷ ☷

I am OOO with limited access to email.

For questions concerning [REDACTED] please reach out to [REDACTED]

For escalations, please reach out to [REDACTED]



Remove  
existing  
MFA tokens




...when  
the user  
is out  
of the office

### 3. Check for internal network access

- If adding an MFA token was successful:
  - User ID + Password + MFA = **You can log in anywhere you want.**
  - Try logging into the VPN. (Search SharePoint, Email, ServiceNow, etc.)
- *Even if adding an MFA token was **not** successful:*
  - Check for web-based, remote/virtual desktop access.
    - **Windows 365** – <https://windows365.microsoft.com>
    - **Microsoft Virtual Desktop**
      - Direct access: <https://client.wvd.microsoft.com/webclient/index.html>
      - Published apps usually listed here: <https://myapps.microsoft.com>
    - **Citrix VDI, VMware Horizon, etc.** (choose Web/HTML client on login)
    - **Admin Portals:** <https://portal.azure.com>, <https://intune.microsoft.com>



# Web-based virtual desktops



## VMware Horizon

You can connect to your desktop and applications by using the VMware Horizon Client or through the browser.


The VMware Horizon Client offers better performance and features.

### Launch Native Client

☐ Check here to skip this screen and always use Native Client.

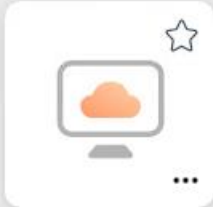
### VMware Horizon HTML Access

☐ Check here to skip this screen and always use HTML Access.




## Horizon


Q Search




BASIC




Warehouse-Floor




Google Chrome



Internet Explorer



Microsoft Edge



Oracle

# Windows 365 & Microsoft Virtual Desktop

https://windows365.microsoft.com

### Your Cloud PCs

**Win365 [REDACTED] - AAD with Az...**  
Last connected 2 hours ago

Windows 11

2 vCPU

8 GB RAM

128 GB Storage

**Open in browser** ▾

**Win365 [REDACTED] - AAD with Az...**  
Last connected 5 months ago

Windows 11

2 vCPU

8 GB RAM

256 GB Storage

**Open in browser** ▾


### In Session Settings

Select the devices or features your Cloud PC can use.


- ☐ Printer
- ☒ File transfer
- ☐ Microphone
- ☒ Clipboard
- ☐ Camera (Preview)
- ☐ Location (Preview)

☐ Don't show again **Connect**


Remote Apps




Access




Adobe Reader




Edge



Excel



Explorer



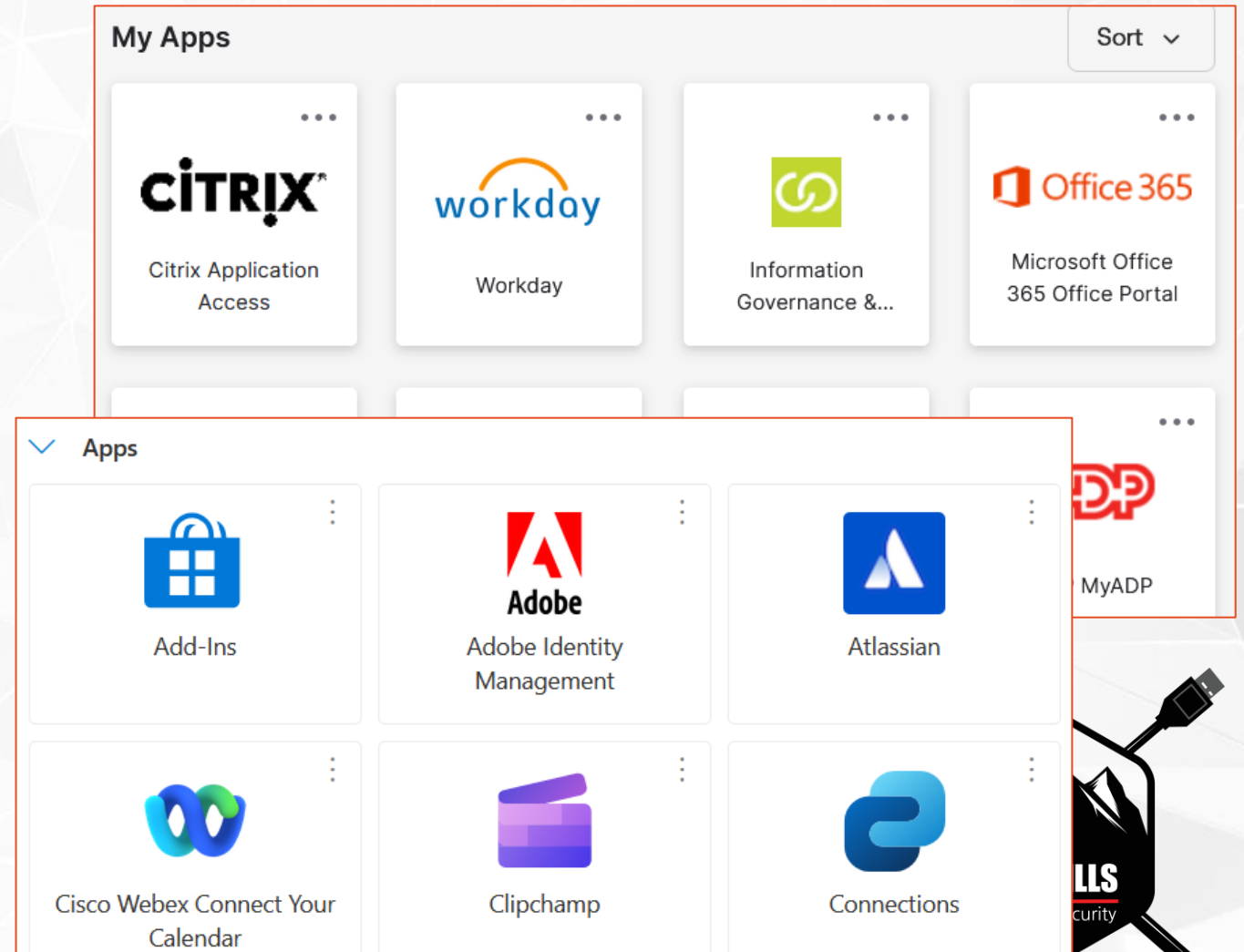
Notepad++



## 4. Access and persist in other web apps.

Find web apps in the SSO dashboard or “apps” page.

- **Okta apps page:**  
<https://COMPANY.okta.com/app/UserHome>
- **Microsoft “Apps” page:**
  - <https://microsoft365.com/apps>  
Then click “All apps”.
  - Scroll all the way to the bottom
  - Check this one ***even if Microsoft is not their SSO portal!***





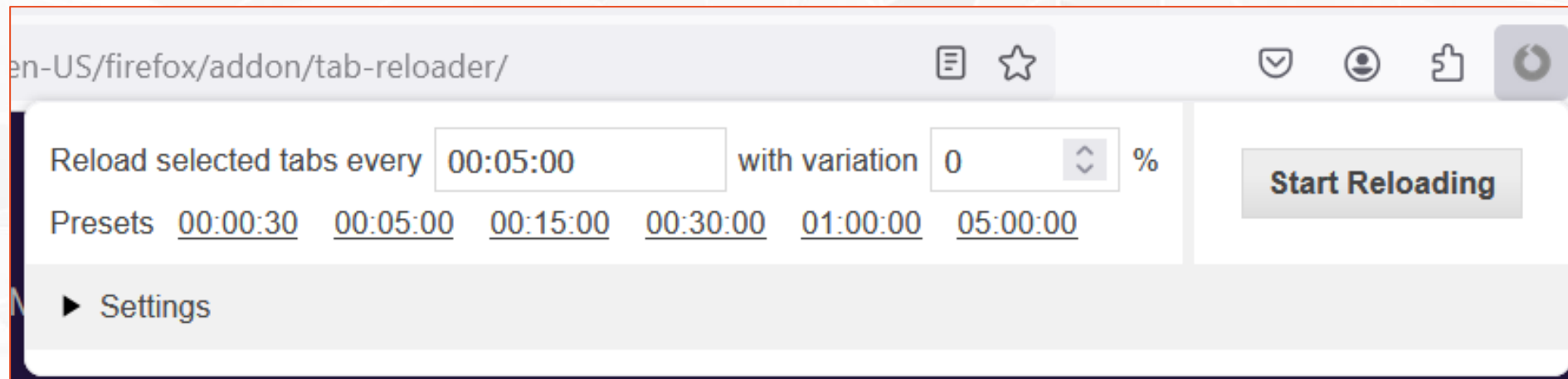
# How to persist in SSO-connected web apps?

1. From the SSO apps page/dashboard, open ***all*** available apps in new browser tabs/windows.
2. Use a browser extension to auto-refresh every tab.



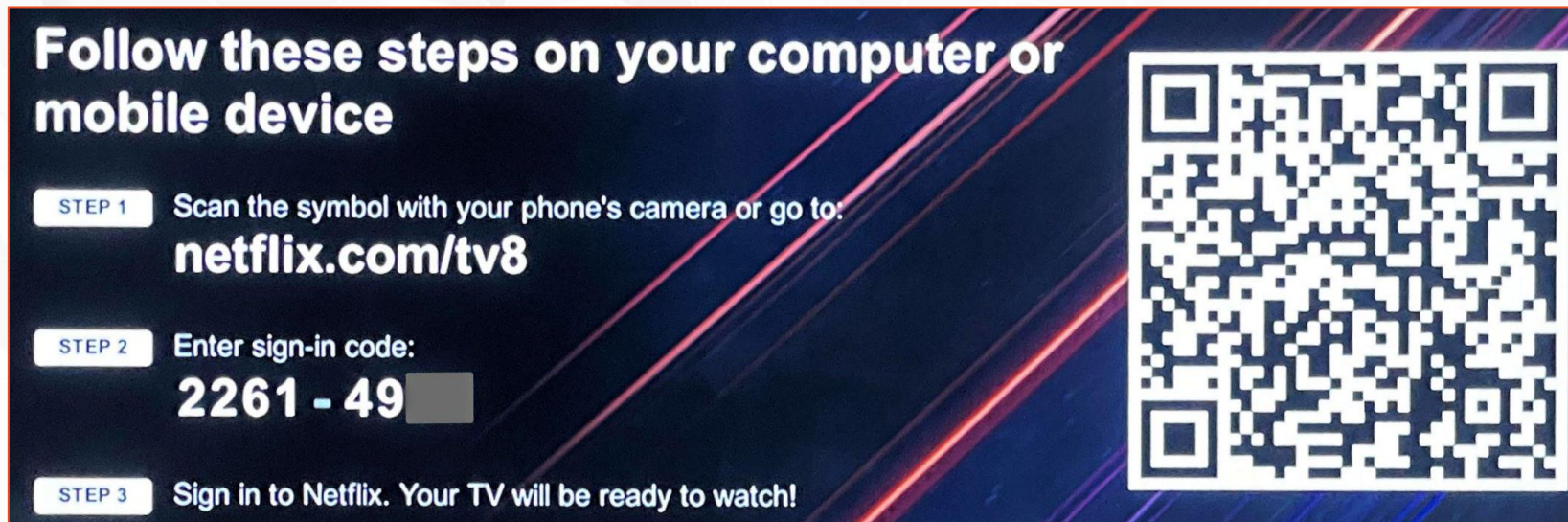
 Recommended

Tab Reloader (page auto refresh)  
by [James Fray](#)



## 5. Device Code access to Microsoft services.

- What is Device Code authentication? Example: Netflix




- Device Code auth does not require reauthentication (password/MFA) if the user is already logged in.



# Microsoft 365 Device Code Authentication

login.microsoftonline.com/common/oauth2/deviceauth


 Microsoft

## Enter code

Enter the code displayed on your app or device.

EPKUTNCX6|

[Next](#)


 Microsoft

[Redacted]

## Are you trying to sign in to Microsoft Edge?

Only continue if you downloaded the app from a store or website that you trust.

[Cancel](#) [Continue](#)

 Microsoft

## Microsoft Edge

You have signed in to the Microsoft Edge application on your device. You may now close this window.



# Abusing Device Code Authentication

## 1. [TokenTactics](#) ([Steve Borosh](#))

1. Initiate Device Code auth and get the initial token
2. Refresh to token types needed by other tools...

## 2. [ROADrecon](#) ([Dirk-jan Mollema](#))

## 3. [GraphRunner](#) ([Beau Bullock](#)) - See the [GraphRunner Wiki](#)

- Add a guest user
- Search SharePoint and OneDrive
  - “[Snaffler-like functionality](#)”
- Email, Teams, and lots more...

```
user@DESKTOP-64RR315> foreach($detect in $detector.Detectors){1
  $tokens -SearchTerm $detect.SearchQuery -DetectorName $detect.
0 -ReportOnly -OutFile $spout -GraphRun}
[*] Found 8 matches for detector: AWS Keys
[*] Found 7 matches for detector: Private Keys
[*] Found 115 matches for detector: Private Key Found In Non-S
[*] Found 60 matches for detector: Database Connection Strings
[*] Found 92 matches for detector: Image Deployment
[*] Found 931 matches for detector: Infrastructure As Code
```

## 4. [AzureHound](#) ([SpecterOps](#)) – like Bloodhound for Azure



# Device Code Auth: ⚠️ Use with Caution ⚠️

1. OPSEC: Generate tokens from a geolocated IP address.
2. Detections exist for some queries and tools.
  - Examples:
    - [A Defenders Guide to GraphRunner - Part I \(Invictus IR\)](#)
    - [A Defenders Guide to GraphRunner - Part II](#)
3. Detections exist for the Device Code authentication itself.
  - Possible honeypot scenario:
    - Account automatically disabled on authentication.
  - Tokens can alternatively be obtained from MS web apps (e.g., Teams) but often have greatly reduced scope.





# Conclusion



# Key takeaways for defenders (1/2)

**First, defend against Adversary-in-the-Middle in general:**

1. Consider switching to AITM-resistant MFA such as U2F/FIDO2.
2. Consider allowing logins **only** from the internal network or VPN.

**Next, defend against these post-exploitation actions, specifically:**

1. Disallow users from adding any new MFA tokens on their own. Require a request to the security team for adding new MFA tokens (not the helpdesk).
  - Alternatively: Require users to re-authenticate with an existing MFA token first whenever they attempt to add a new MFA token to their account.
2. Disallow Device Code authentication for all users by default. Add exceptions only when required.
  - This will also prevent a separate category of attack: Device Code phishing.



# Key takeaways for defenders (2/2)

## **Defend against these post-exploitation actions, specifically (continued):**

3. Configure the SSO portal *and all connected web applications* to expire sessions in the shortest period reasonable for the organization.
  - Recommended: 12 hours or less, regardless of user activity.
4. Consider restricting remote network access to software clients only and disallowing access from the web browser.



*\*These last two recommendations also harden the environment against other attacks, such as session tokens stolen with infostealer malware.*



# Thank you for listening!



Want to learn more?

-  **Red Team Initial Access**
  - Live and online at [Initial-Access.com](https://Initial-Access.com)
  - Learn all the attacks I mentioned in this talk and more!
-  **“Greetings From the Red Team”**

Follow me, Michael Allen (@Wh1t3Rh1n0) on:

- [X](#)
- [LinkedIn](#)
- [GitHub](#)

