Viktor Hedberg

Keep the front door shut - How cybercriminals are abusing Entra ID to gain a foothold.

NIC

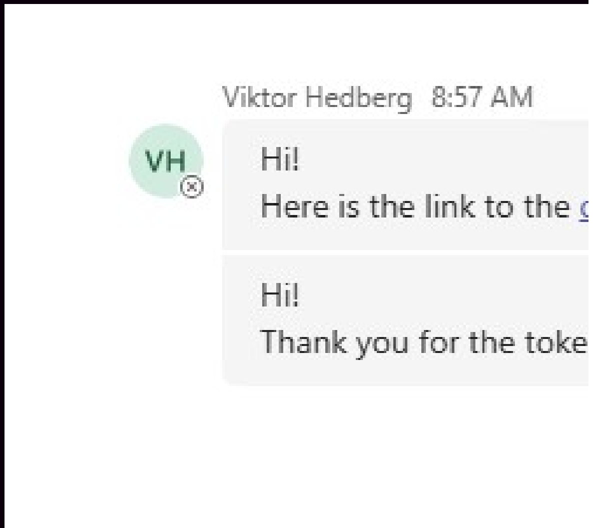
EMPOWER

/whoami

- Senior Technical Architect @ Truesec
- Works in the CSIRT
- Security Research (MS Cloud and On-Premises)

BEC – Business Email Compromise

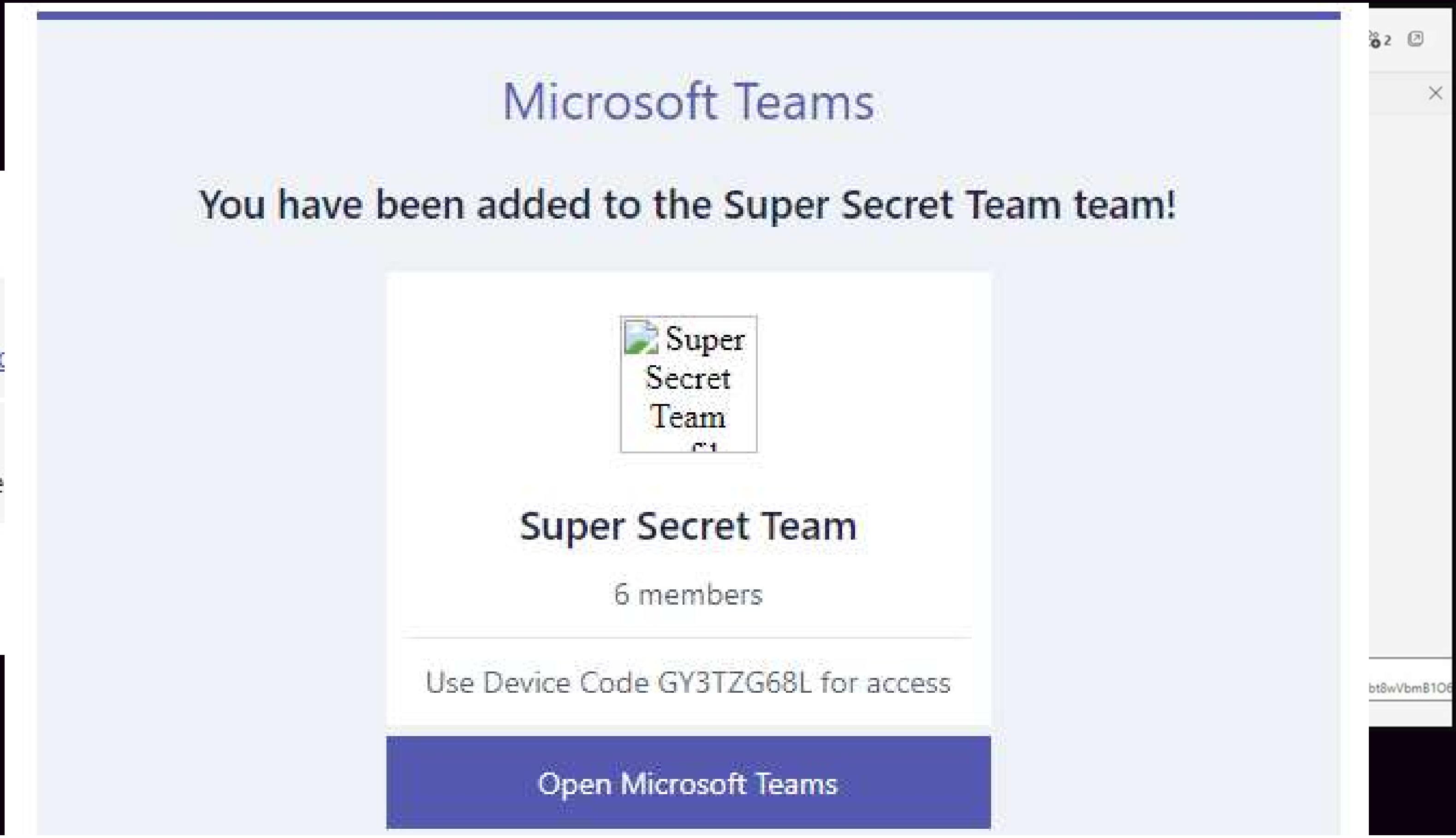
- Phishing



Viktor Hedberg 8:57 AM

Hi!
Here is the link to the g

Hi!
Thank you for the toke



Microsoft Teams

You have been added to the Super Secret Team team!

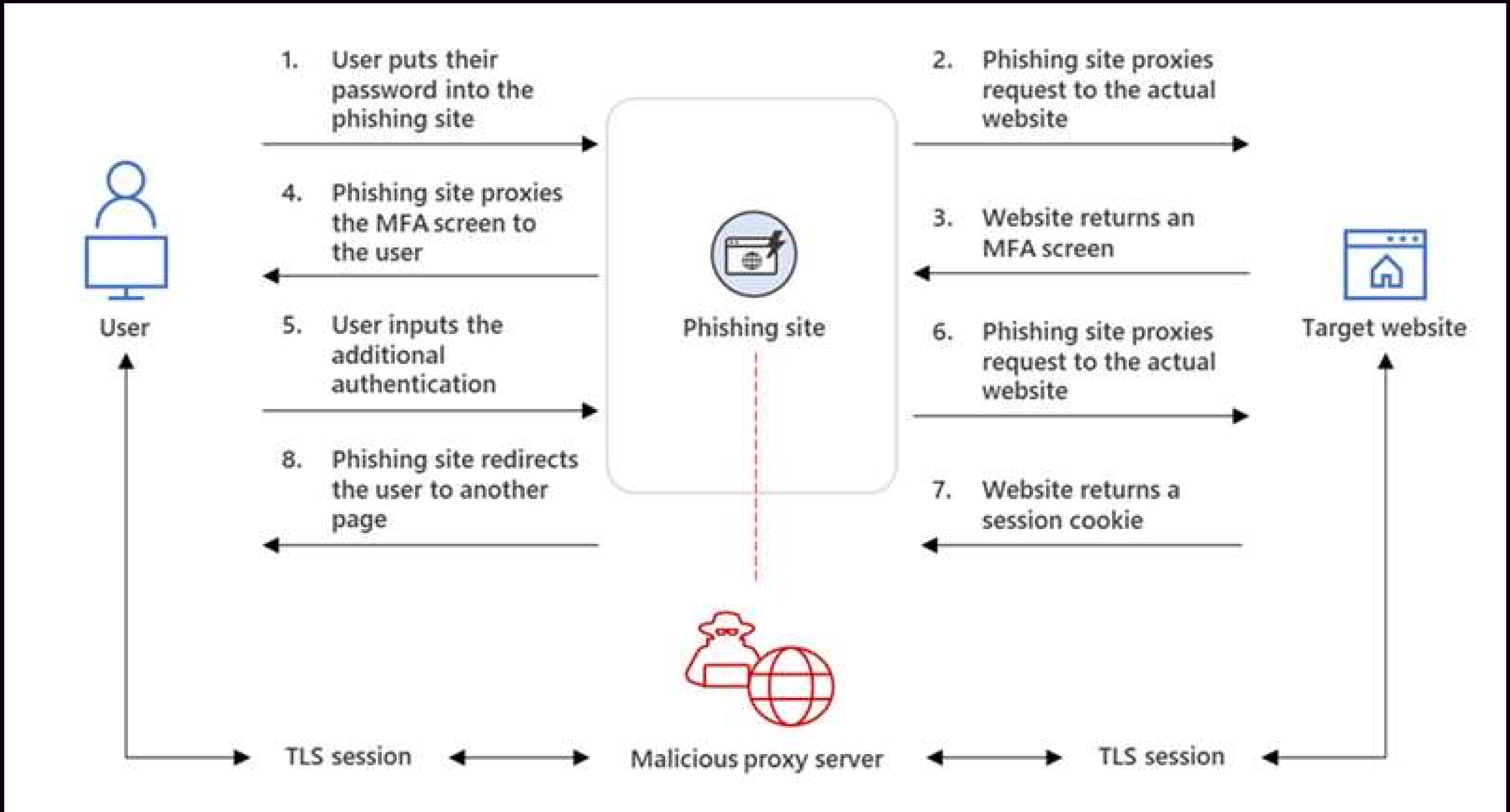
Super Secret Team

Super Secret Team

6 members

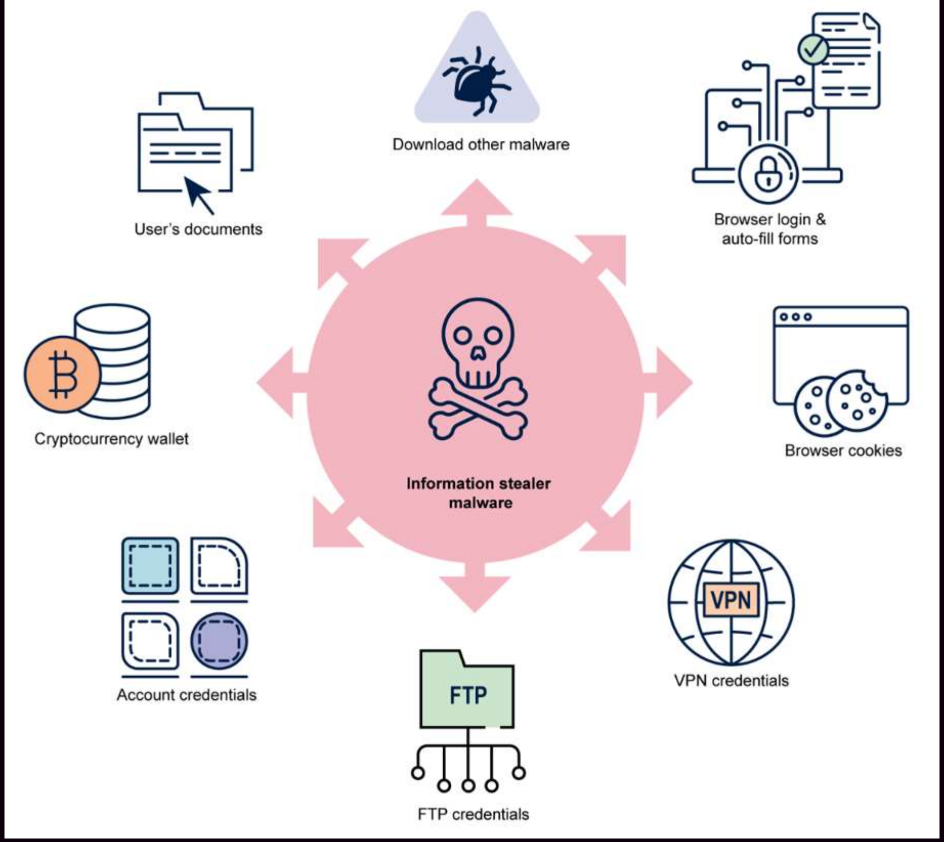
Use Device Code GY3TZG68L for access

AiTM – Adversary in The Middle

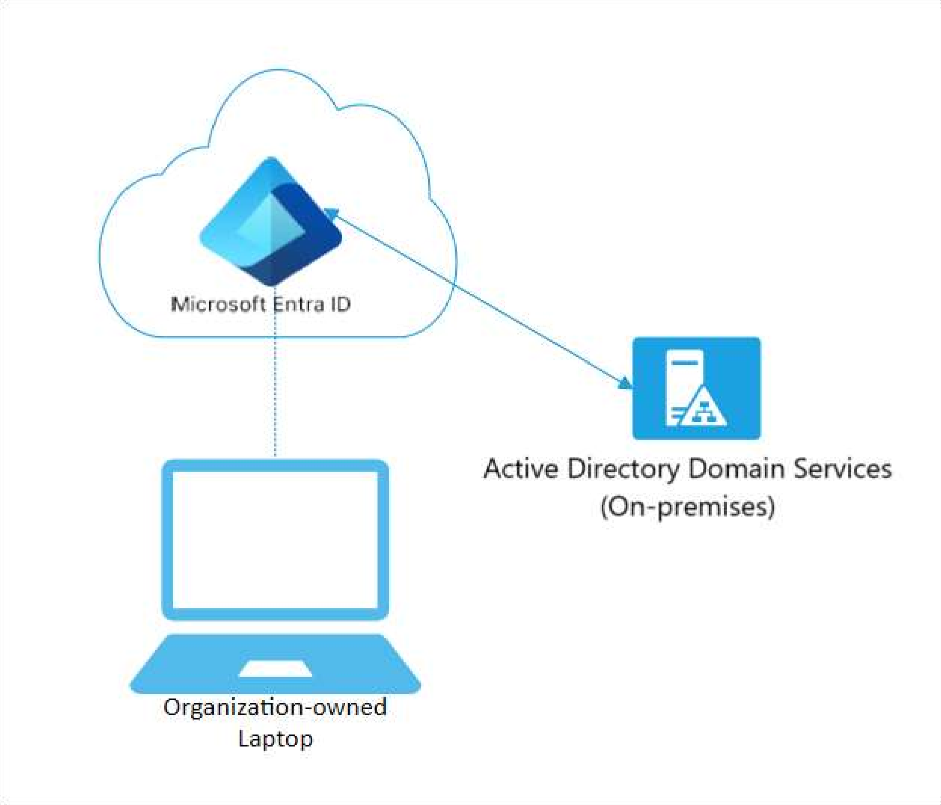


1. User puts their password into the phishing site
2. Phishing site proxies request to the actual website
3. Website returns an MFA screen
4. Phishing site proxies the MFA screen to the user
5. User inputs the additional authentication
6. Phishing site proxies request to the actual website
7. Website returns a session cookie
8. Phishing site redirects the user to another page

InfoStealer



Joining Devices to Entra ID



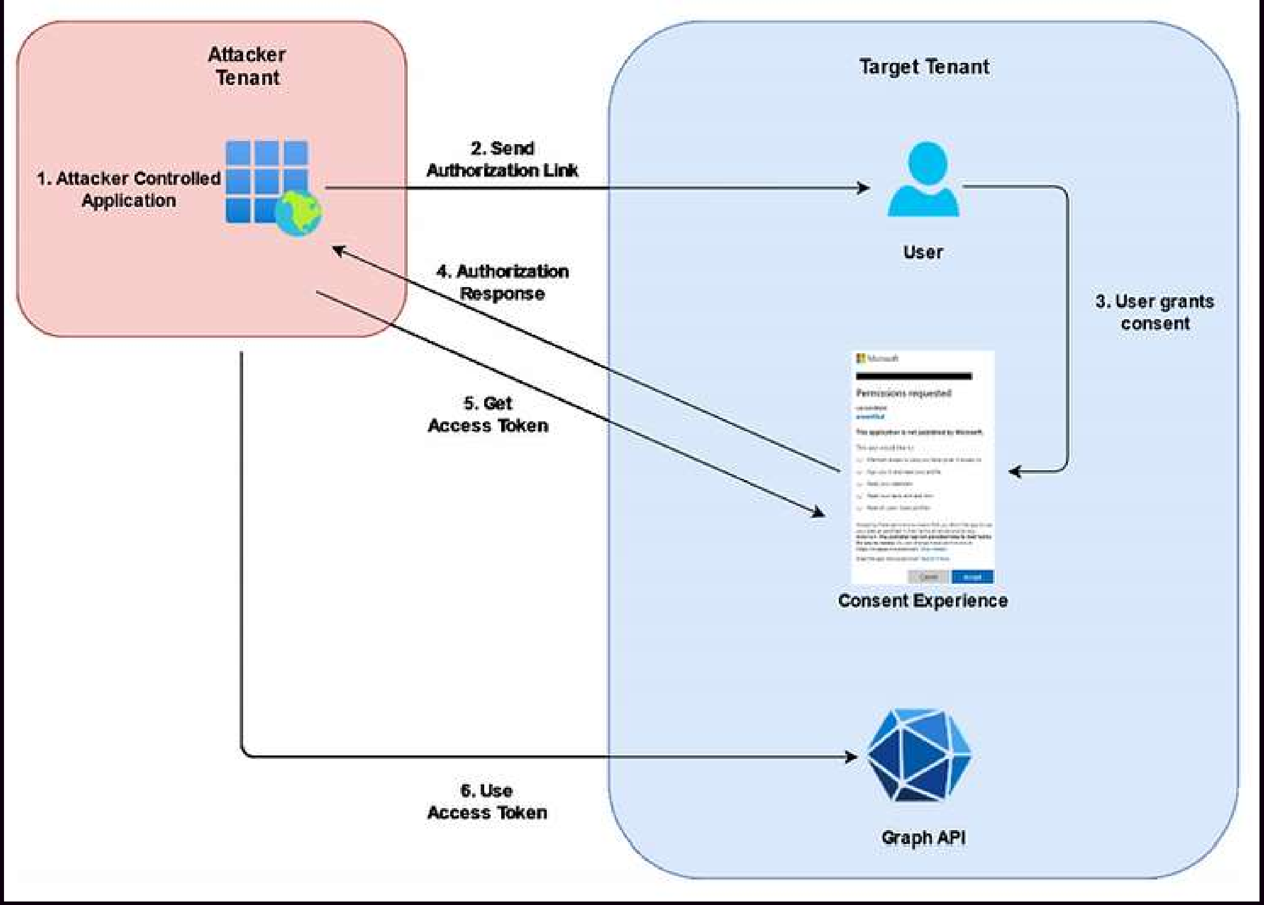
Joining Devices to Entra ID

- Can become compliant
- Gets a PRT
- Becomes “trusted”

Enterprise App Consent

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

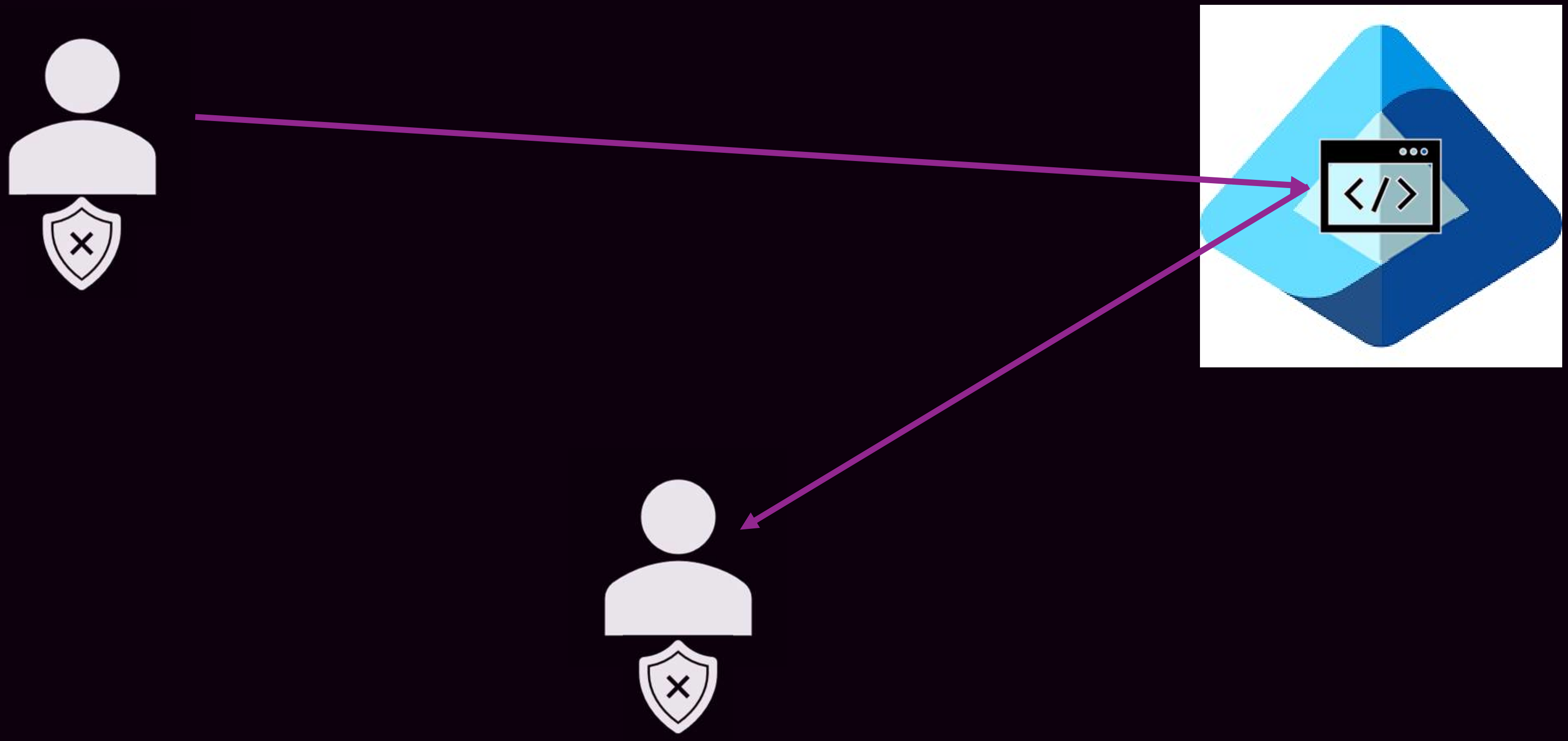
Enterprise App Consent Attack Flow



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

NIC
EMPOWER

Fear the FOCI

- Family of Client IDs:
- family-of-client-ids-research/known-foci-clients.csv at main · secureworks/family-of-client-ids-research · GitHub

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

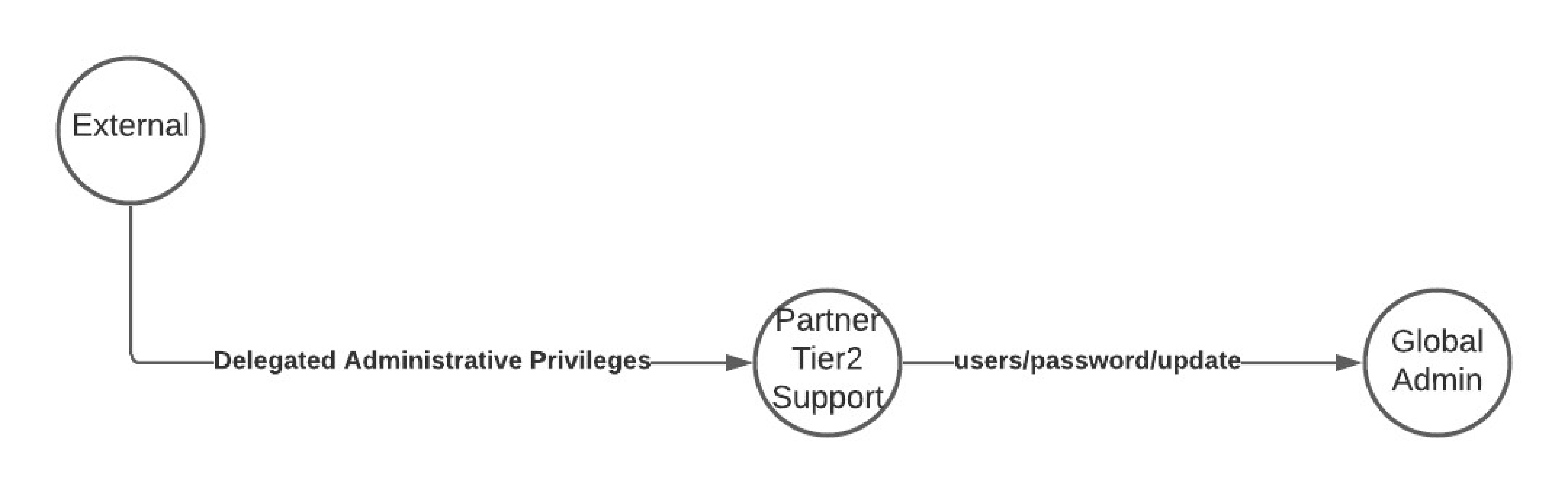
DEMO

Playing with Access Tokens

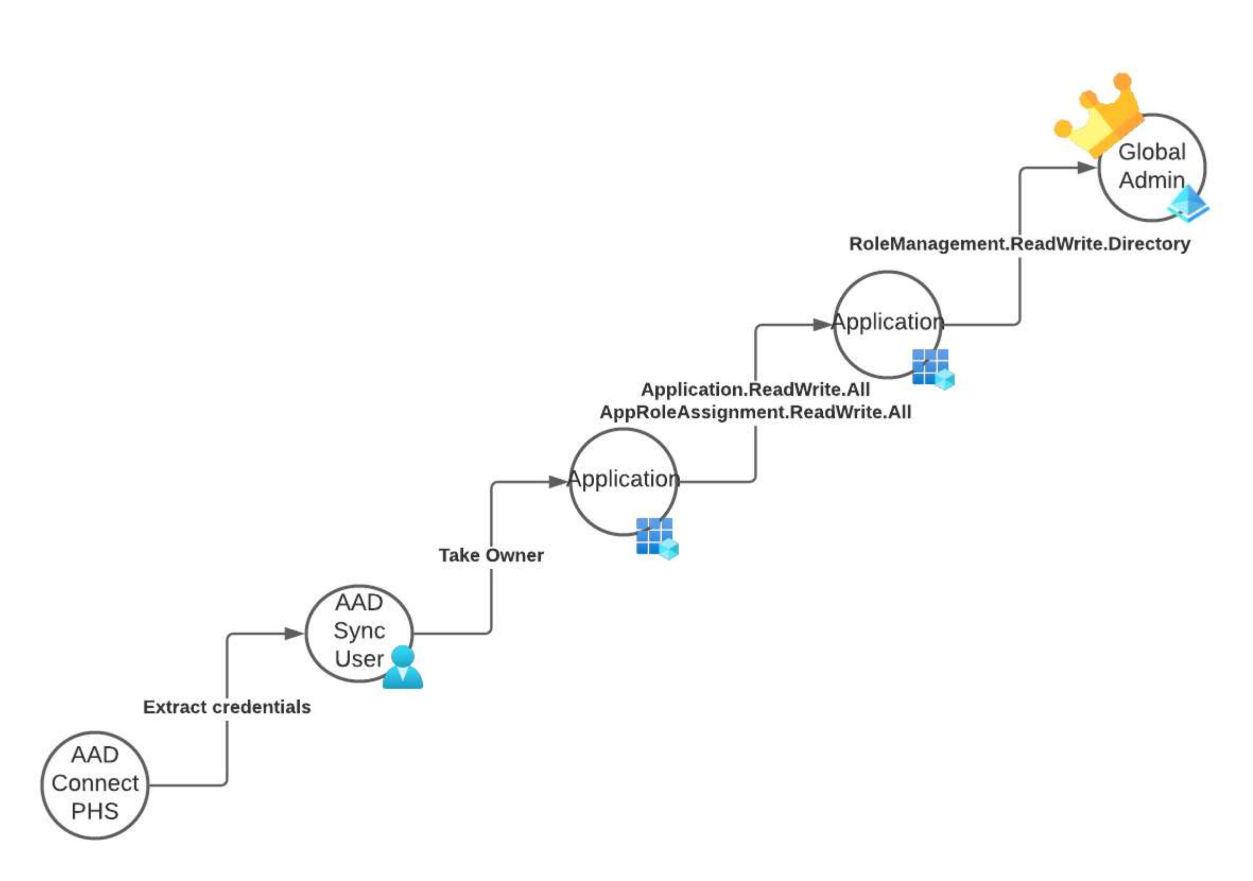
Privilege Escalation Paths

- Application Administrator -> Global Administrator
- Privileged Role/Authentication Administrator -> Global Administrator
- Entra ID Connect -> Global Administrator (patched with version
- DAP - > Global Adminstrator

DAP -> Global Admin



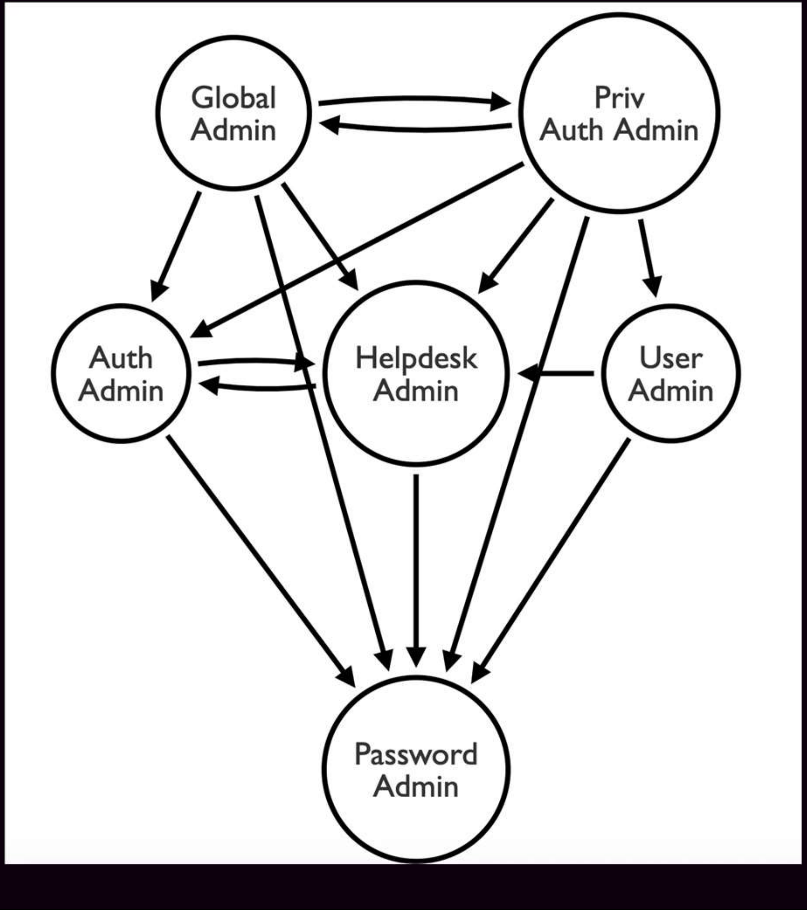
Entra ID Connect -> Global Admin



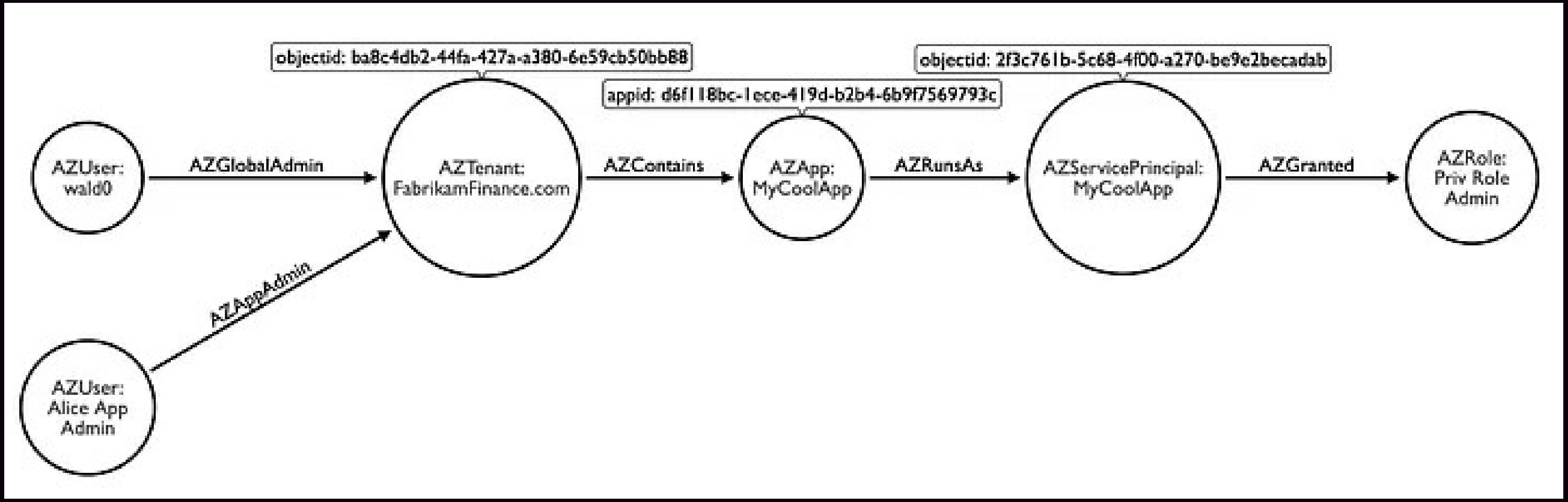
NIC

EMPOWER

Privileged Auth/Role Admin -> Global Admin



Application Administrator -> Global Admin


objectid: ba8c4db2-44fa-427a-a380-6e59cb50bb88
appid: d6f118bc-1ece-419d-b2b4-6b9f7569793c
objectid: 2f3c761b-5c68-4f00-a270-be9e2becadab
AZUser: wald0
AZGlobalAdmin
AZTenant: FabrikamFinance.com
AZContains
AZApp: MyCoolApp
AZRunsAs
AZServicePrincipal: MyCoolApp
AZGranted
AZRole: Priv Role Admin
AZAppAdmin
AZUser: Alice App Admin

NIC
EMPOWER

Mitigations

- For AAD Graph:
  - Register Azure Active Directory PowerShell 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

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

Mitigations

- Phishing Resistant Auth
  - FIDO
  - Yubikey
  - WHfB
- Only allow connection from trusted devices
- Require Authentication Strengths for registering MFA
- Require Authentication Strengths for Joining Devices to Entra ID