Martin Haller

⟨ Microsoft Entra ID Lateral movement & Persistence ⟩

PATRON ⟨IT⟩ OCHRANA A SPRÁVA SÍTÍ

Entra ID: Attackers' goals

Attackers' goals: Ransomware?

- On-prem AD
- Microsoft 365?
  - Sharepoint, OneDrive, Exchange – version history, local copies, double trash bin
  - Azure resources – SQL, storage, VMs
    - https://www.safebreach.com/resources/one-drive-double-agent-clouded-onedrive-turns-sides/
    - https://danielchronlund.com/2023/02/14/the-threat-of-microsoft-365-wiper-malware/
    - https://threatpost.com/office-365-opens-ransomware-attacks-on-onedrive-sharepoint/180010/

Attackers' goals: Business E-mail Compromise

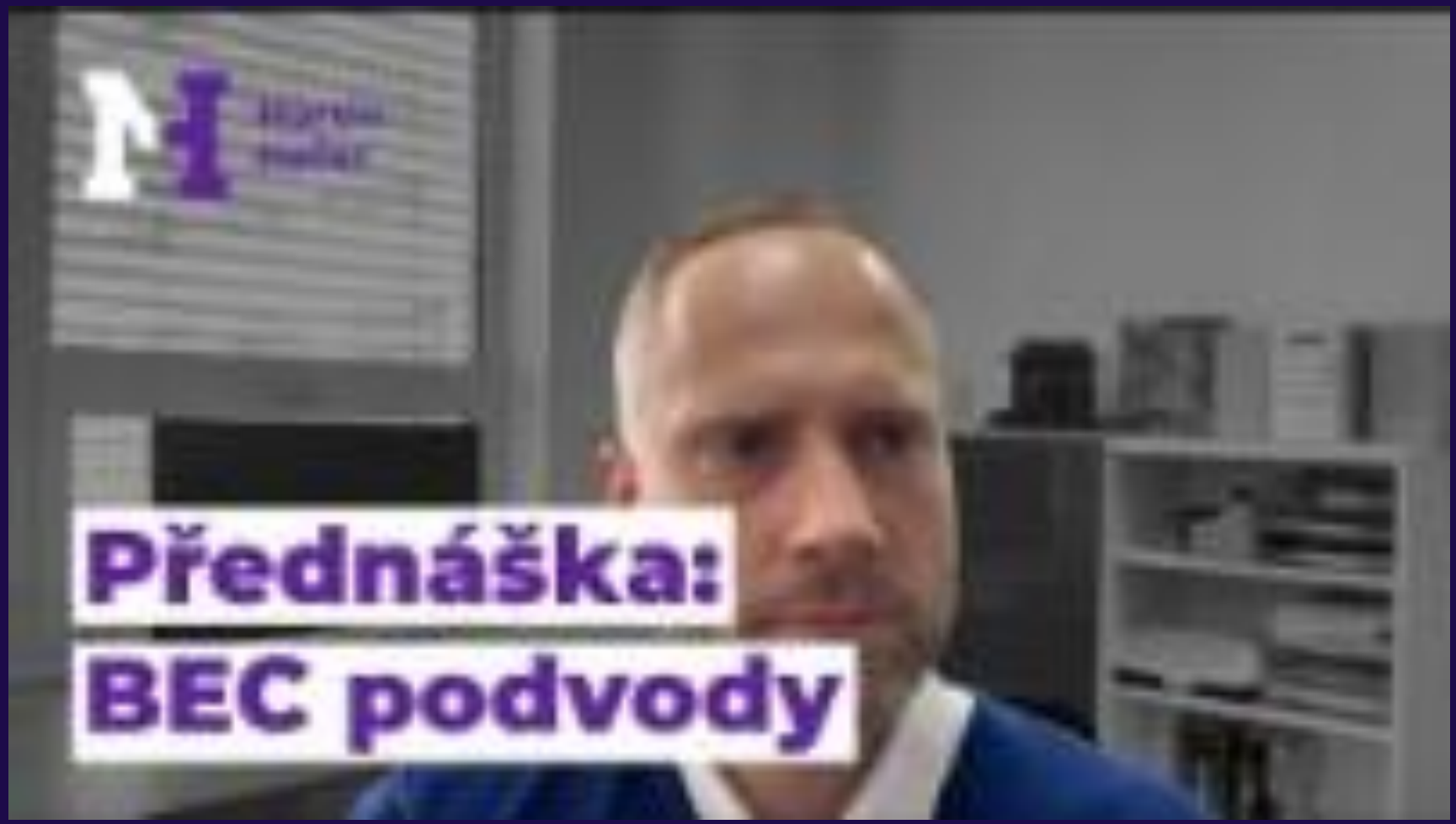
2022 CRIME TYPES continued

By Victim Loss

Crime Type	*Loss*	*Crime Type*	*Loss*
Investment	$3,311,742,206	Lottery/Sweepstakes/Inheritance	$83,602,376
BEC	$2,742,354,049	SIM Swap	$72,652,571
Tech Support	$806,551,993	Extortion	$54,335,128
Personal Data Breach	$742,438,136	Employment	$52,204,269
Confidence/Romance	$735,882,192	Phishing	$52,089,159
Data Breach	$459,321,859	Overpayment	$38,335,772
Real Estate	$396,932,821	Ransomware	*$34,353,237
Non-Payment/Non-Delivery	$281,770,073	Botnet	$17,099,378
Credit Card/Check Fraud	$264,148,905	Malware	$9,326,482
Government Impersonation	$240,553,091	Harassment/Stalking	$5,621,402
Identity Theft	$189,205,793	Threats of Violence	$4,972,099
Other	$117,686,789	IPR/Copyright/Counterfeit	$4,591,177
Spoofing	$107,926,252	Crimes Against Children	$577,464
Advanced Fee	$104,325,444		

Source: https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf

Attackers' goals: Business E-mail Compromise



Source: https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf

Attackers' goals: Data leak?

- Blackmailing (company, individual)
- Espionage

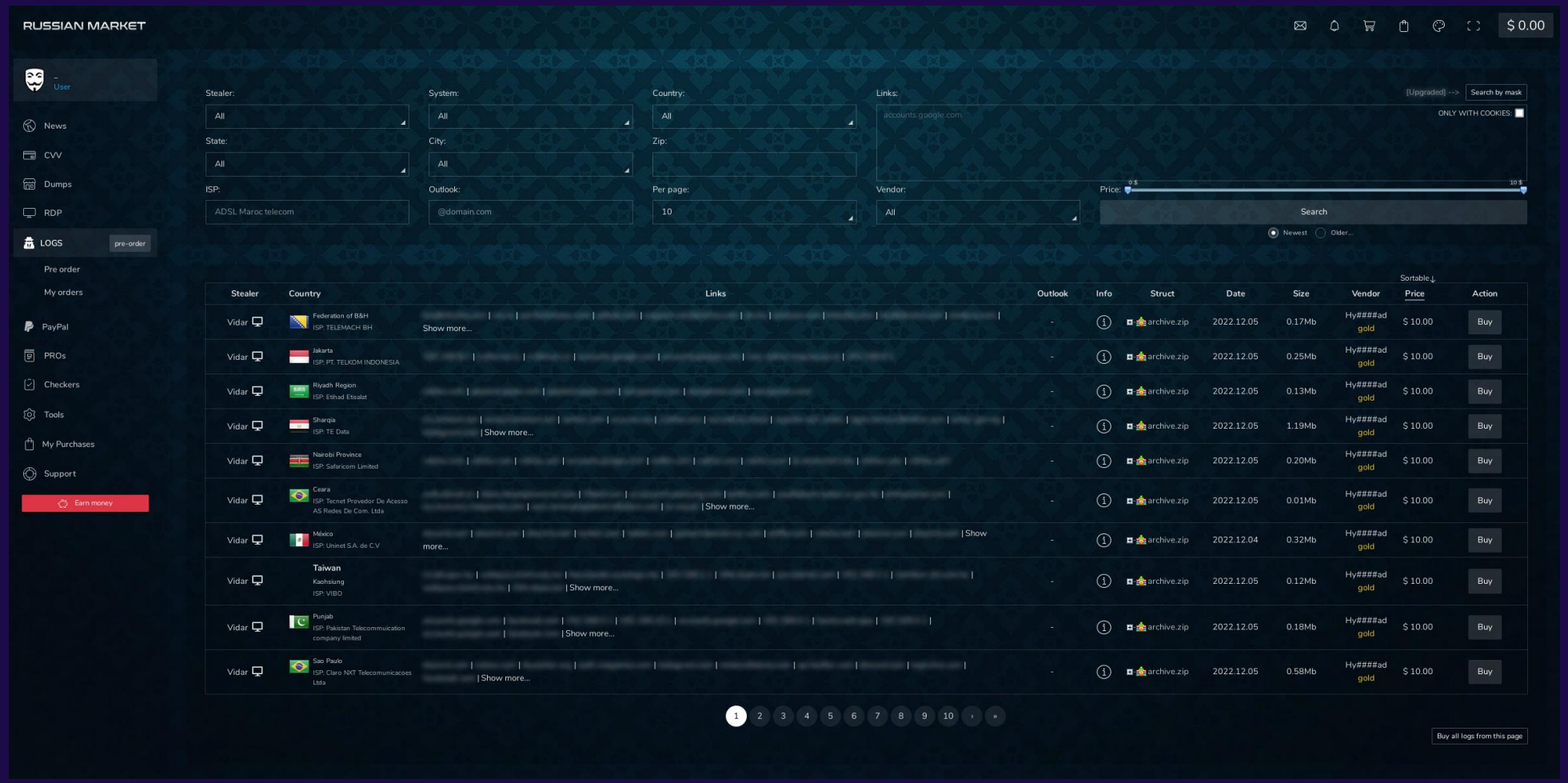
recent posts

last 200 posts

date	title	group
2023-08-18	tedpella.com	lockbit3
2023-08-18	mitchcointernational.com	lockbit3
2023-08-18	www.auda.org.au	noescape
2023-08-17	www.contact121.com.au	noescape
2023-08-17	umchealth.com	lockbit3
2023-08-17	Agriloja.pt demo-leak	everest
2023-08-17	sgl.co.th	lockbit3
2023-08-17	RIMSS	akira
2023-08-17	emerson.com	clop
2023-08-17	ricohacumen.com	clop
2023-08-17	vrm.de	clop
2023-08-17	umassmed.edu	clop
2023-08-17	mybps.us	lockbit3
2023-08-17	kriegerklatt.com	lockbit3
2023-08-17	www.alliancesolutionsgrp.com	blackbasta
2023-08-17	www.deutsche-leasing.com	blackbasta
2023-08-17	www.venauto.nl	blackbasta
2023-08-17	https://www.synquestlabs.com	blackbasta
2023-08-17	www.twintowerstrading.com	blackbasta
2023-08-17	Camino Nuevo Charter Academy	akira
2023-08-17	Smart-swgcrc.org	lockbit3
2023-08-17	SFJAZZ.ORG	lockbit3
2023-08-17	The Clifton Public S chools	akira
2023-08-17	https://dillonsupply.com	metaencryptor
2023-08-17	https://www.epicure.com	metaencryptor
2023-08-17	http://www.coswell.biz	metaencryptor
2023-08-17	https://bob-automotive.com	metaencryptor
2023-08-17	https://www.seoulsemicon.com	metaencryptor
2023-08-17	https://www.kraiburg-austria.com	metaencryptor
2023-08-17	https://www.autohaus-ebert.de	metaencryptor
2023-08-17	https://www.cvoantwerpen.be	metaencryptor
2023-08-17	https://www.iconcreativestudio.com	metaencryptor
2023-08-17	https://www.heilmann-ag.de	metaencryptor
2023-08-17	https://www.schwaelbchen-molkerei.de	metaencryptor

Result Number	Victim Name	Additional Info	Dates	Ransomware Group\Name	Icon
1	Cs Cargo Group	www.cscargo.cz	2023-07-11	Play News	
2	Algotech	www.algotech.cz	2023-06-27	Play News	
3	fosfa.cz	N\A	2023-04-13	LockBit 3.0	
4	stavinvest.cz	N\A	2023-03-19	LockBit 3.0	
5	stavbar.cz	N\A	2022-11-09	LockBit 3.0	
6	Gaben.Cz	N\A	2021-11-28	LV	
7	amista.cz	N\A	2021-09-29	LockBit 3.0	

Attackers' goals: Initial Access Brokers (IABs)



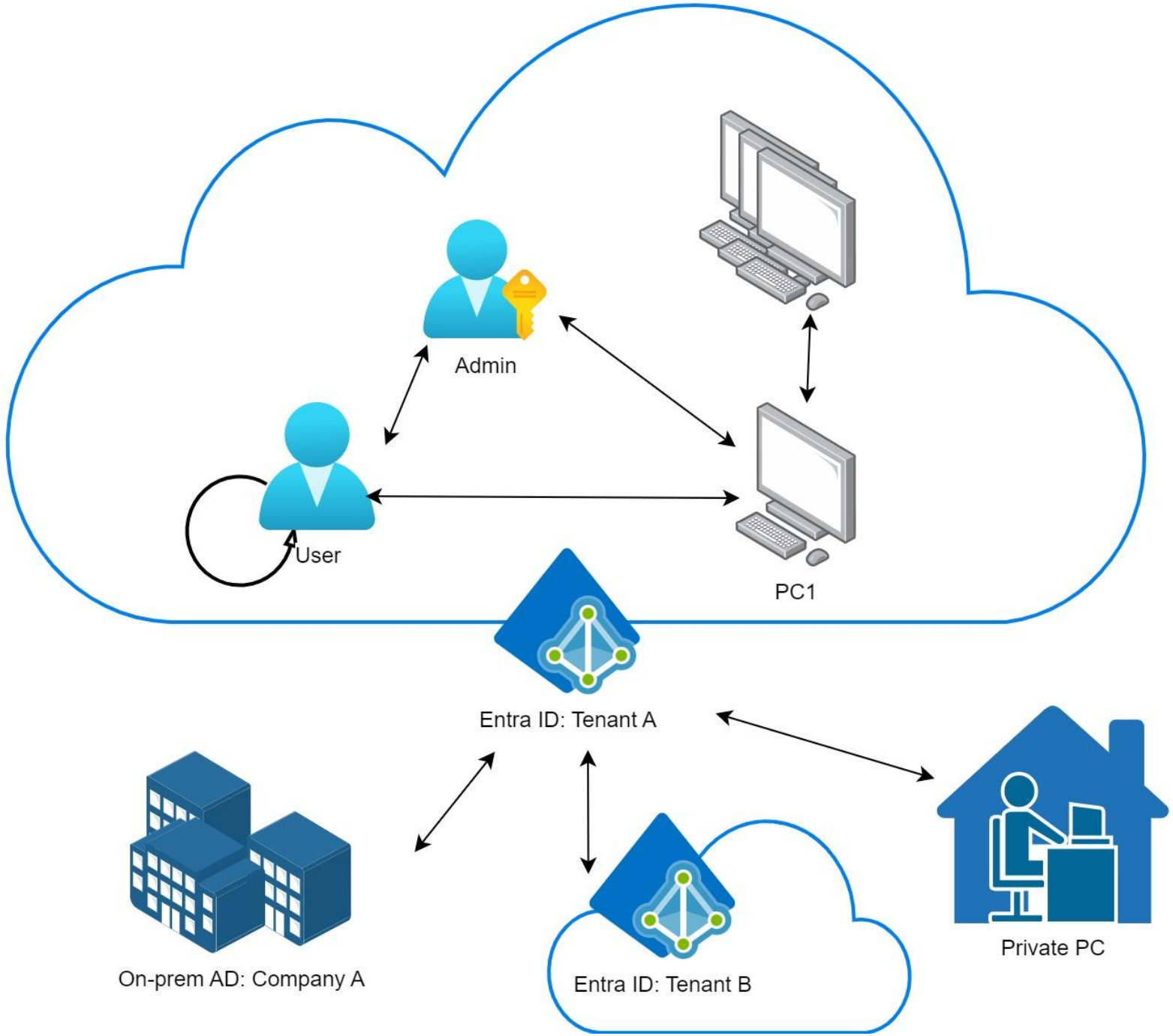
Source: https://securityboulevard.com/2023/01/threat-spotlight-top-illicit-sources-to-monitor-in-2023/

Attackers' goals : other

- Prestige
- Challenge
- Revenge
- Entertainment

Entra ID: Lateral movement

Lateral movement: why?

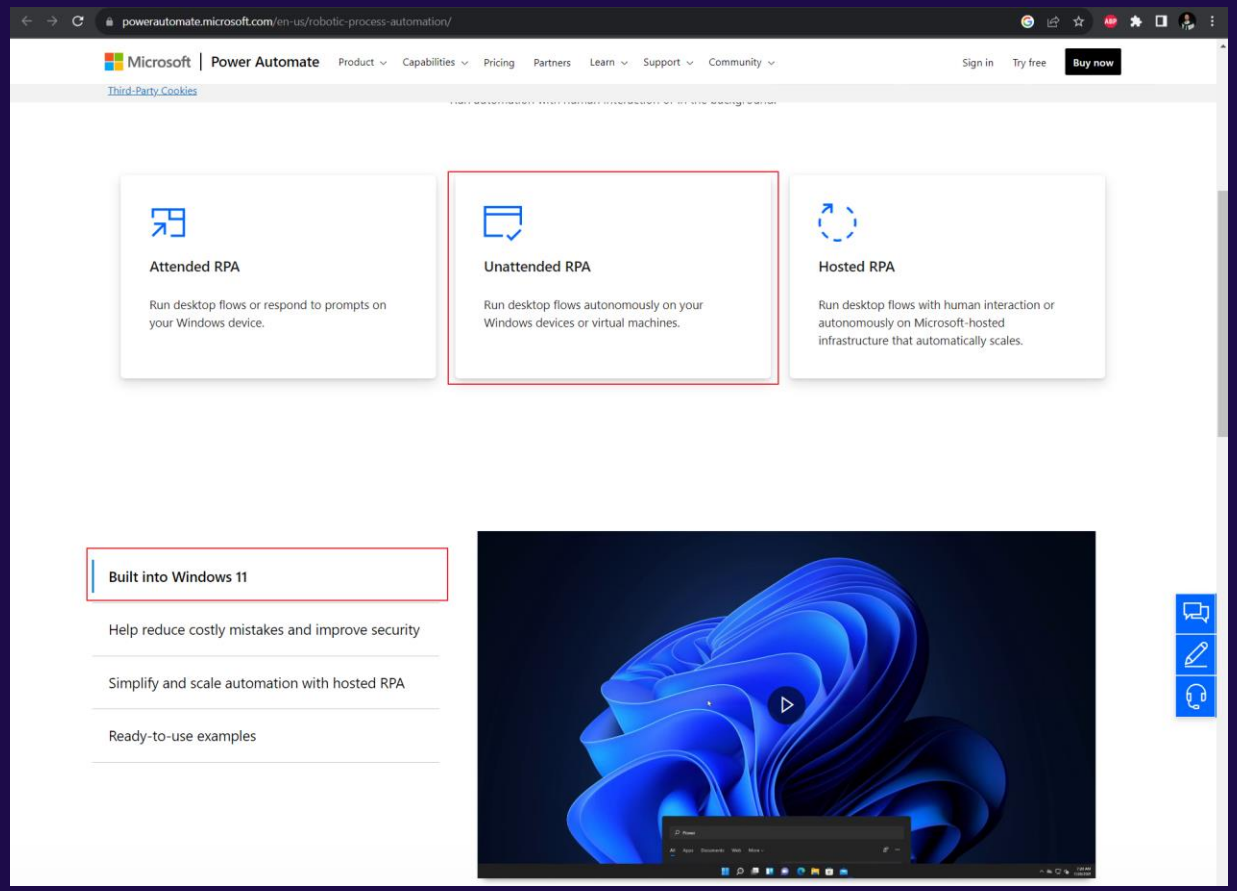

Admin
User
PC1
Entra ID: Tenant A
On-prem AD: Company A
Entra ID: Tenant B
Private PC

Lateral movement: User privilege escalation

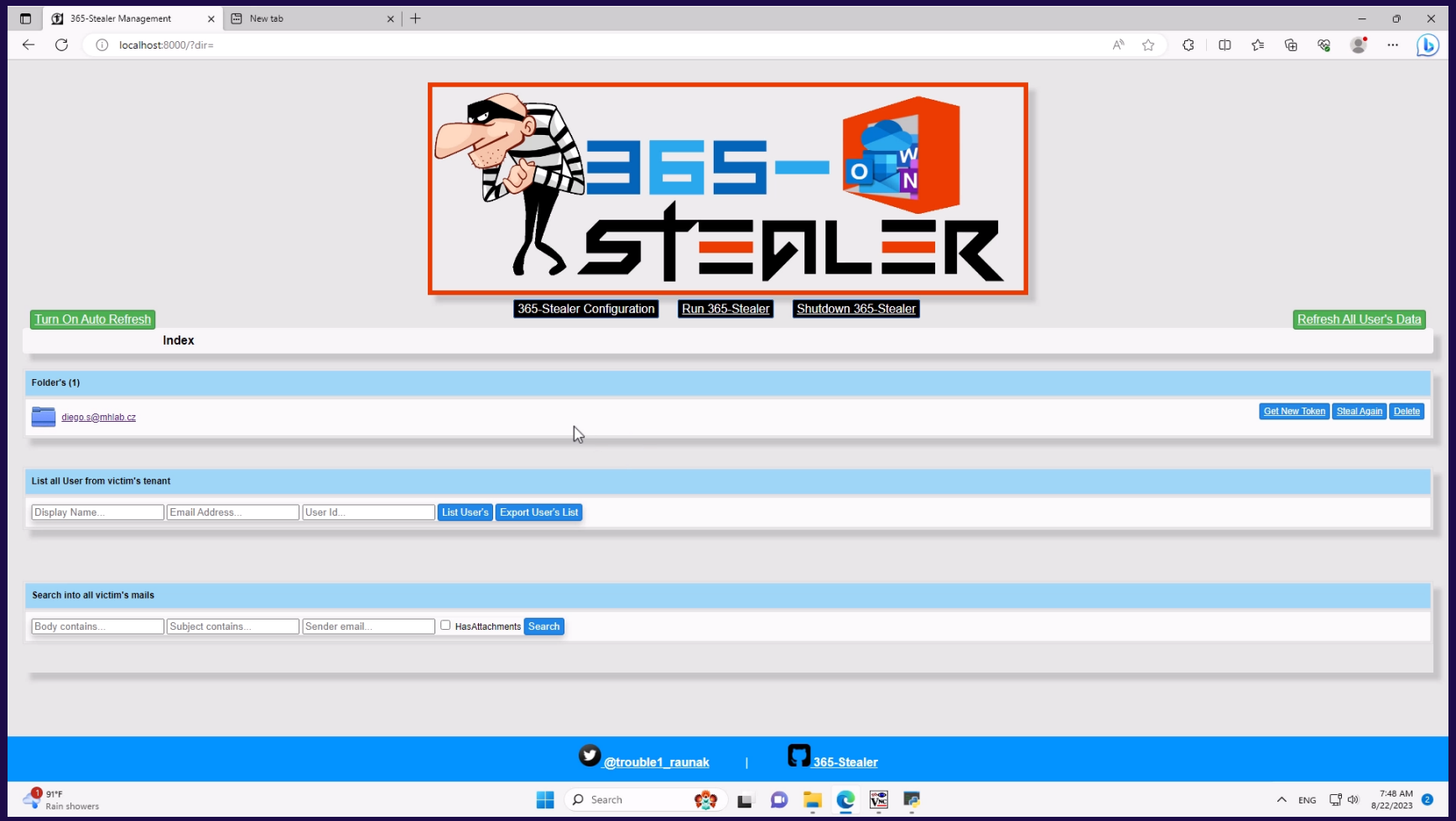
- FOCI (https://github.com/secureworks/family-of-client-ids-research)
- Looting (mail, OneDrive, Sharepoint)
- SSPR (Self-server password reset)
- Getting „Compliant device“(https://aadinternals.com/post/mdm/)

Lateral movement: User/Admin to PC

- OneDrive „poisoning“ (User ->)
- Microsoft Power Automate (User ->)
- RDP (User ->)
- Intune (Admin ->)



Lateral movement : OneDrive



Lateral movement: PC to User/Admin

- Cookies, PRT, RT, AT reuse (-> User, Admin)
  - Request admin help
- Application‘s secrets

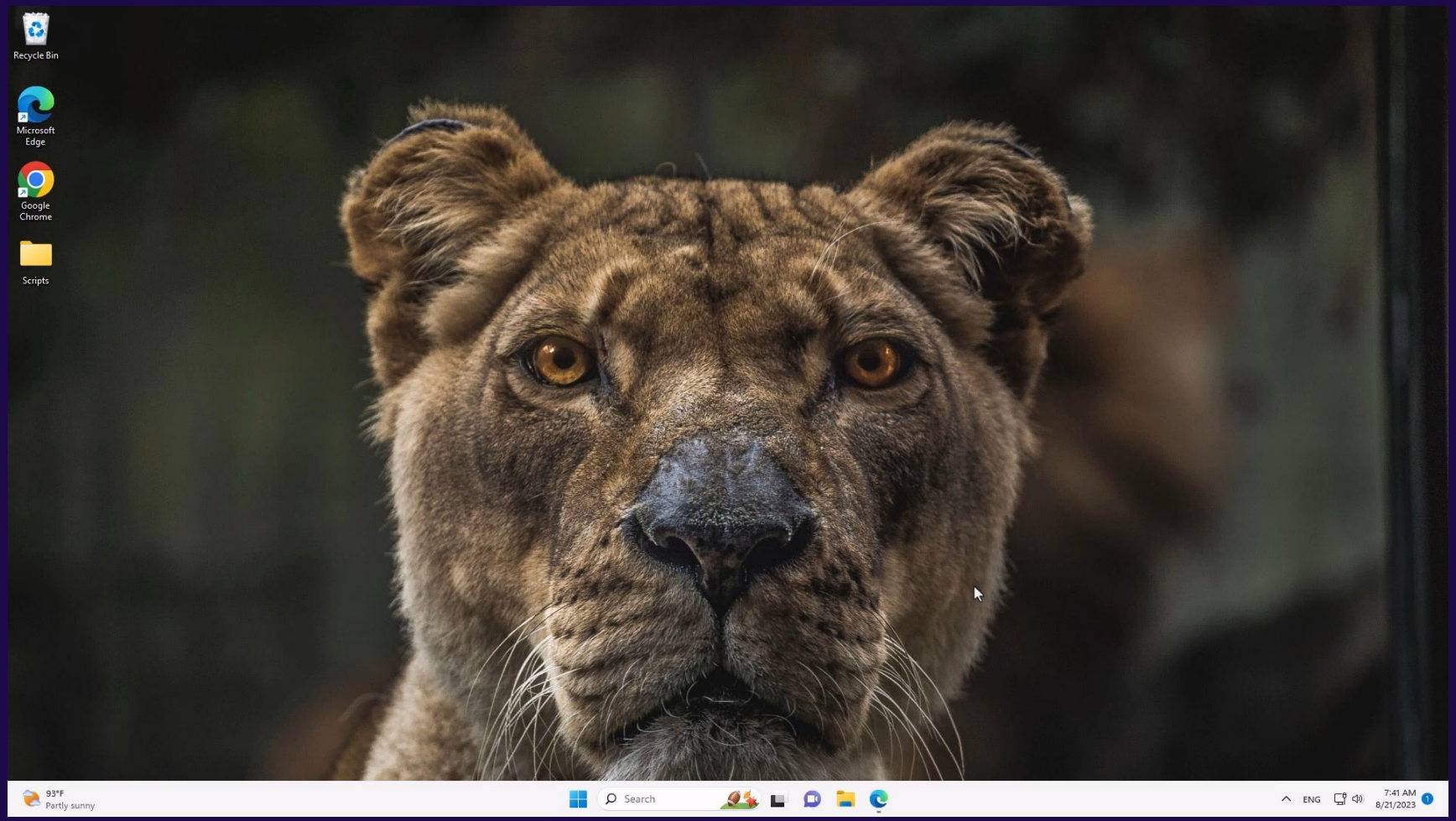
Lateral movement: PC to PC

- Misuse workstation admin account
  - No MFA/CA
  - PSExec (https://medium.com/@talthemaor/moving-laterally-between-azure-ad-joined-machines-ed1f8871da56)
  - NegoEx Relay (https://github.com/morRubin/NegoExRelay)

Lateral movement: User to User/Admin

- OneDrive „poisoning“ (-> User, Admin)
- Looting (mail, OneDrive, Sharepoint)
- Application rights missue (Owner, Application Admin -> Admin)
- Phishing

Lateral movement : Application misuse



Lateral movement: AAD to AD

- Cloud Kerberos Trust (https://dirkjanm.io/obtaining-domain-admin-from-azure-ad-via-cloud-kerberos-trust/)
- Password reset
- Intune (Local admin group, Application deployment)

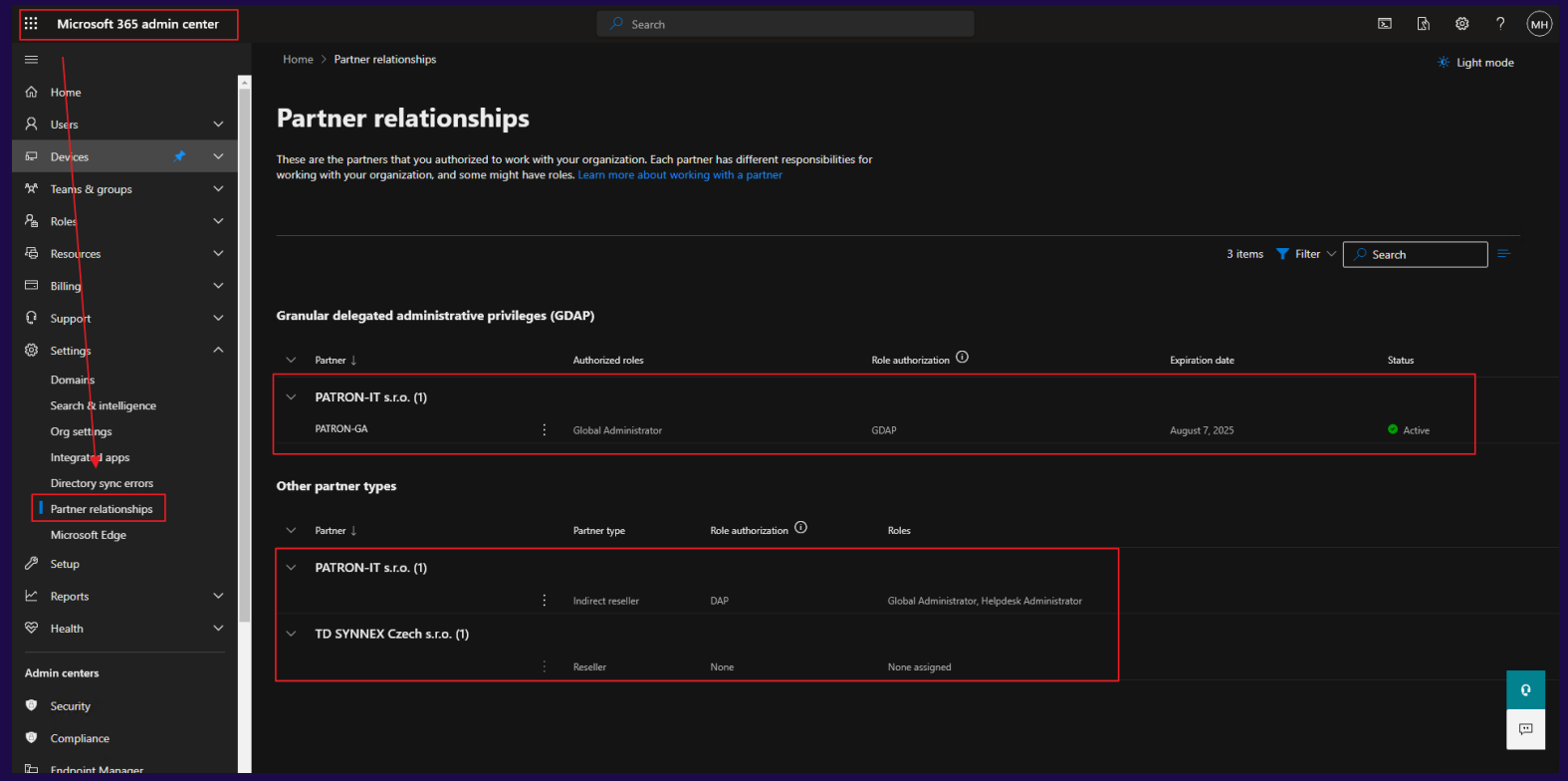
Lateral movement: AD to AAD

- Unnoticed sidekick: Getting access to cloud as an on-prem admin (https://aadinternals.com/post/on-prem_admin/)
- AAD Connect (local, hybrid users)
- AD FS (Golden SAML, MFA, hybrid+cloud users)
- Pass-through Authentication (PTA Agent) (only hybrid users)
- Seamless SSO (AZUREADSSOACC) (nedá MFA claim)

Lateral movement: Cloud to Cloud

» GDAP delegation (https://www.microsoft.com/en-us/security/blog/2021/10/25/nobelium-targeting-delegated-administrative-privileges-to-facilitate-broader-attacks/)

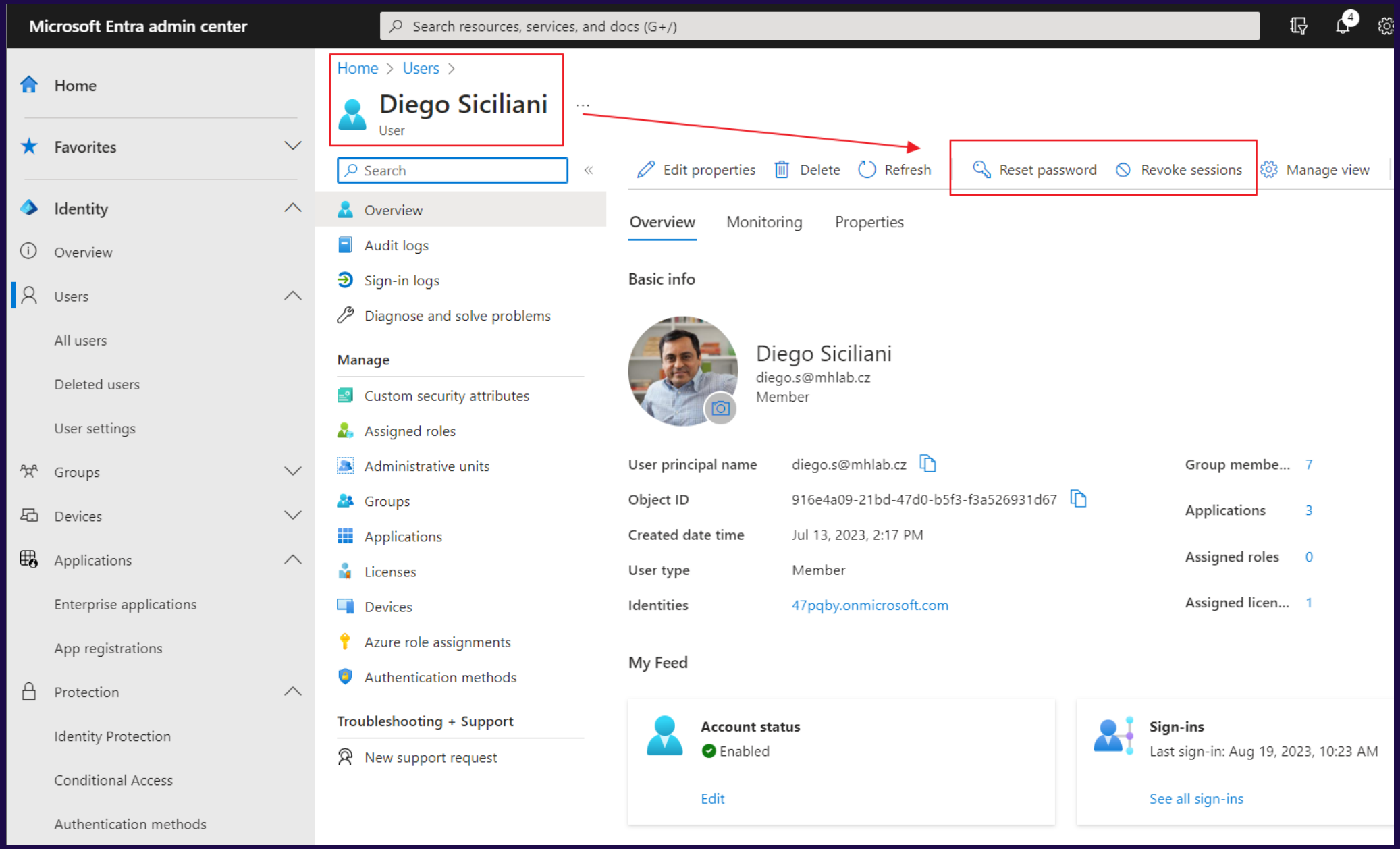
» AAD Cross-tenant sync (https://www.bleepingcomputer.com/news/security/new-microsoft-azure-ad-cts-feature-can-be-abused-for-lateral-movement/)



Entra ID: Persistence

Persistence: why?

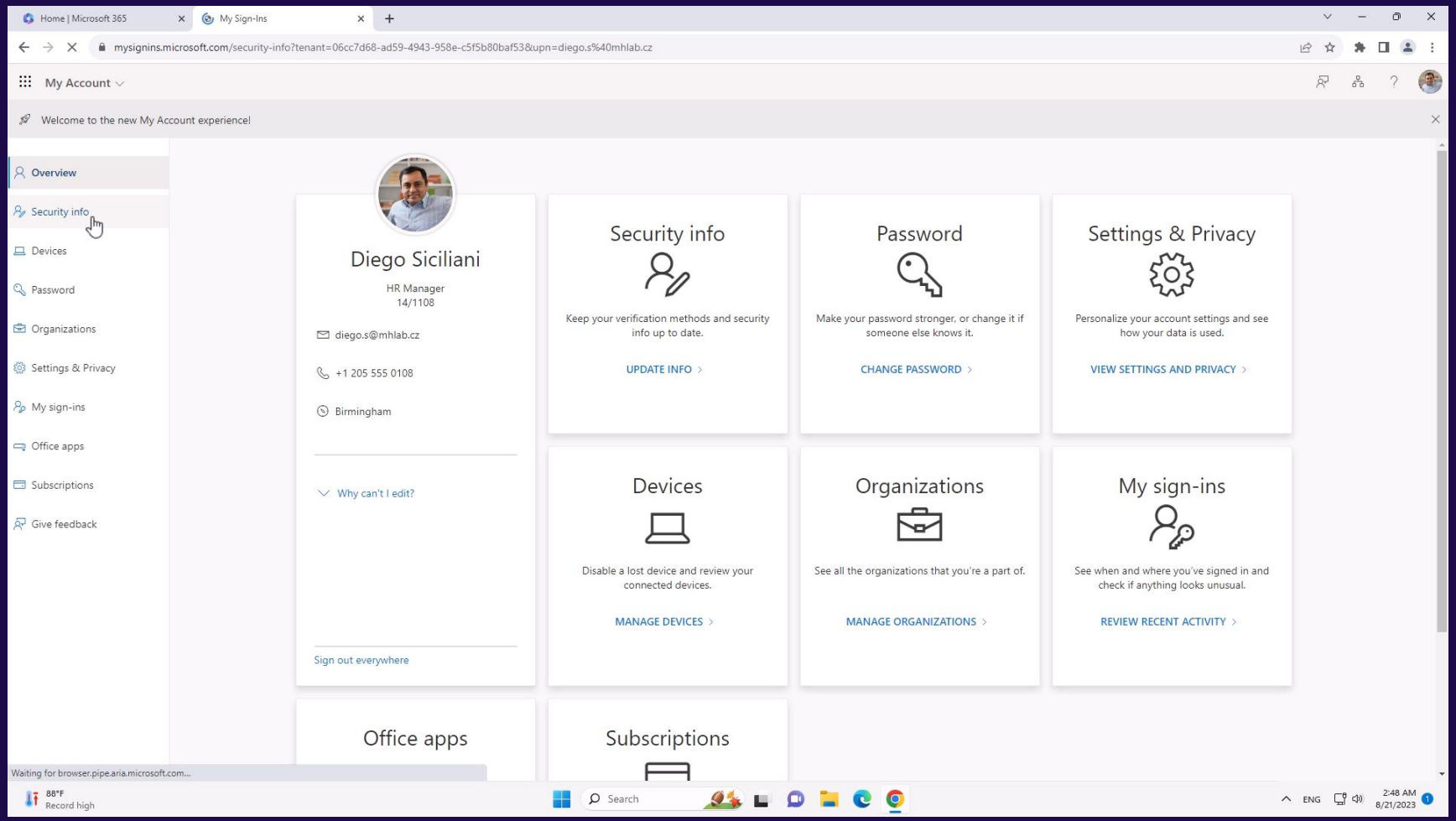
- Long-term espionage
- Time to find buyer (IAB)
- Blackmail better (ransomware)


Microsoft Entra admin center
Search resources, services, and docs (G+/)
Home
Favorites
Identity
Overview
Users
All users
Deleted users
User settings
Groups
Devices
Applications
Enterprise applications
App registrations
Protection
Identity Protection
Conditional Access
Authentication methods
Home > Users >
Diego Siciliani
User
Search
Overview
Audit logs
Sign-in logs
Diagnose and solve problems
Manage
Custom security attributes
Assigned roles
Administrative units
Groups
Applications
Licenses
Devices
Azure role assignments
Authentication methods
Troubleshooting + Support
New support request
Edit properties
Delete
Refresh
Reset password
Revoke sessions
Manage view
Overview
Monitoring
Properties
Basic info
Diego Siciliani
diego.s@mhlab.cz
Member
User principal name
diego.s@mhlab.cz
Object ID
916e4a09-21bd-47d0-b5f3-f3a526931d67
Created date time
Jul 13, 2023, 2:17 PM
User type
Member
Identities
47pqby.onmicrosoft.com
Group membe... 7
Applications 3
Assigned roles 0
Assigned licen... 1
My Feed
Account status
Enabled
Edit
Sign-ins
Last sign-in: Aug 19, 2023, 10:23 AM
See all sign-ins

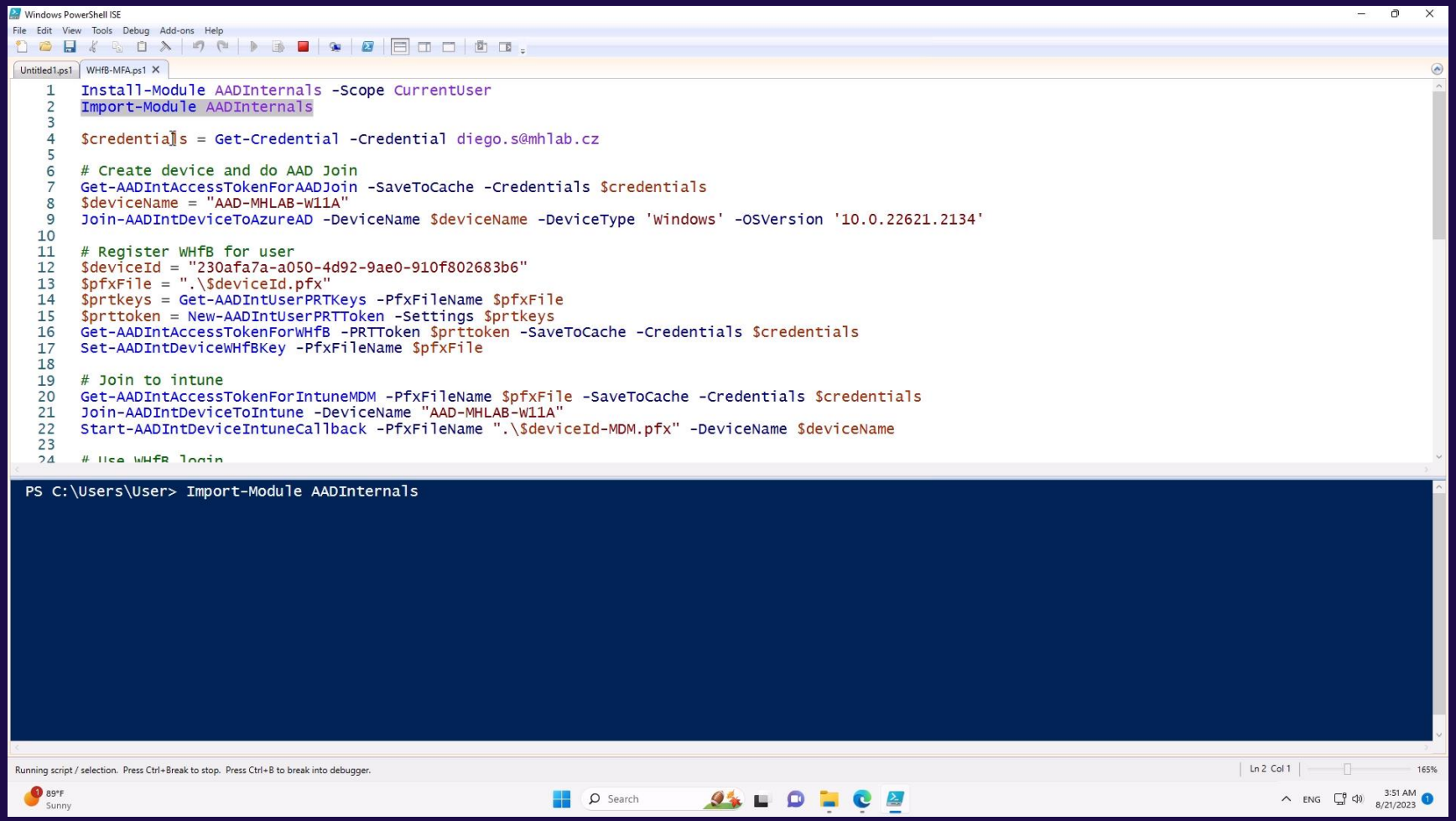
Change	Password-based cookie	Password-based token	Non-password-based cookie	Non-password-based token	Confidential client token
Password expires	Stays alive	Stays alive	Stays alive	Stays alive	Stays alive
Password changed by user	Revoked	Revoked	Stays alive	Stays alive	Stays alive
User does SSPR	Revoked	Revoked	Stays alive	Stays alive	Stays alive
Admin resets password	Revoked	Revoked	Stays alive	Stays alive	Stays alive
User revokes their refresh tokens	Revoked	Revoked	Revoked	Revoked	Revoked
Admin revokes all refresh tokens for a user	Revoked	Revoked	Revoked	Revoked	Revoked
Single sign-out	Revoked	Stays alive	Revoked	Stays alive	Stays alive

Source: https://learn.microsoft.com/en-us/azure/active-directory/develop/refresh-tokens

Persistence: Demo persistence on user



Persistence: Demo persistence on user CLI

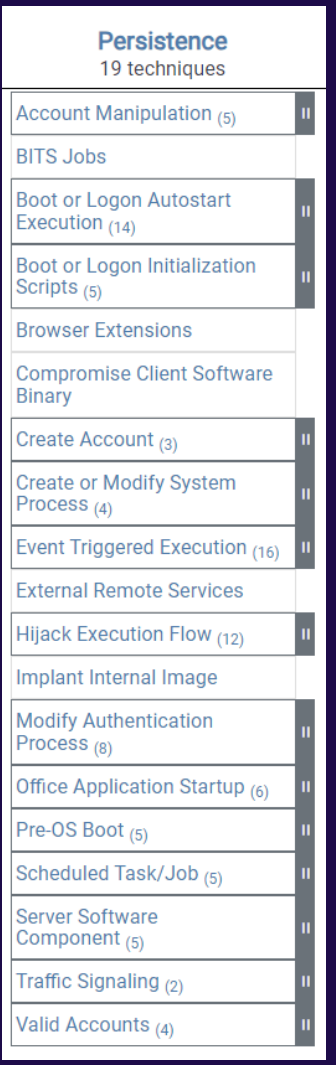


Persistence: on user

- Cookie, PRT, RT, application password
- Add of authentication method (WHfB, FIDO, Authenticator, MFA [SSPR])
- Mail-Flow rules
- PowerApps
  - DEF CON 30 - Michael Bargury - Low Code High Risk - Enterprise Domination via Low Code Abuse
  - https://www.zenity.io/hackers-abuse-low-code-platforms-and-turn-them-against-their-owners/

Persistence: PC

- Same as with on-prem PC
  - Malware (program, service, driver, DLL sideloading)
  - Scheduled task
  - User account
  - Legit RMM, or Remote Access app

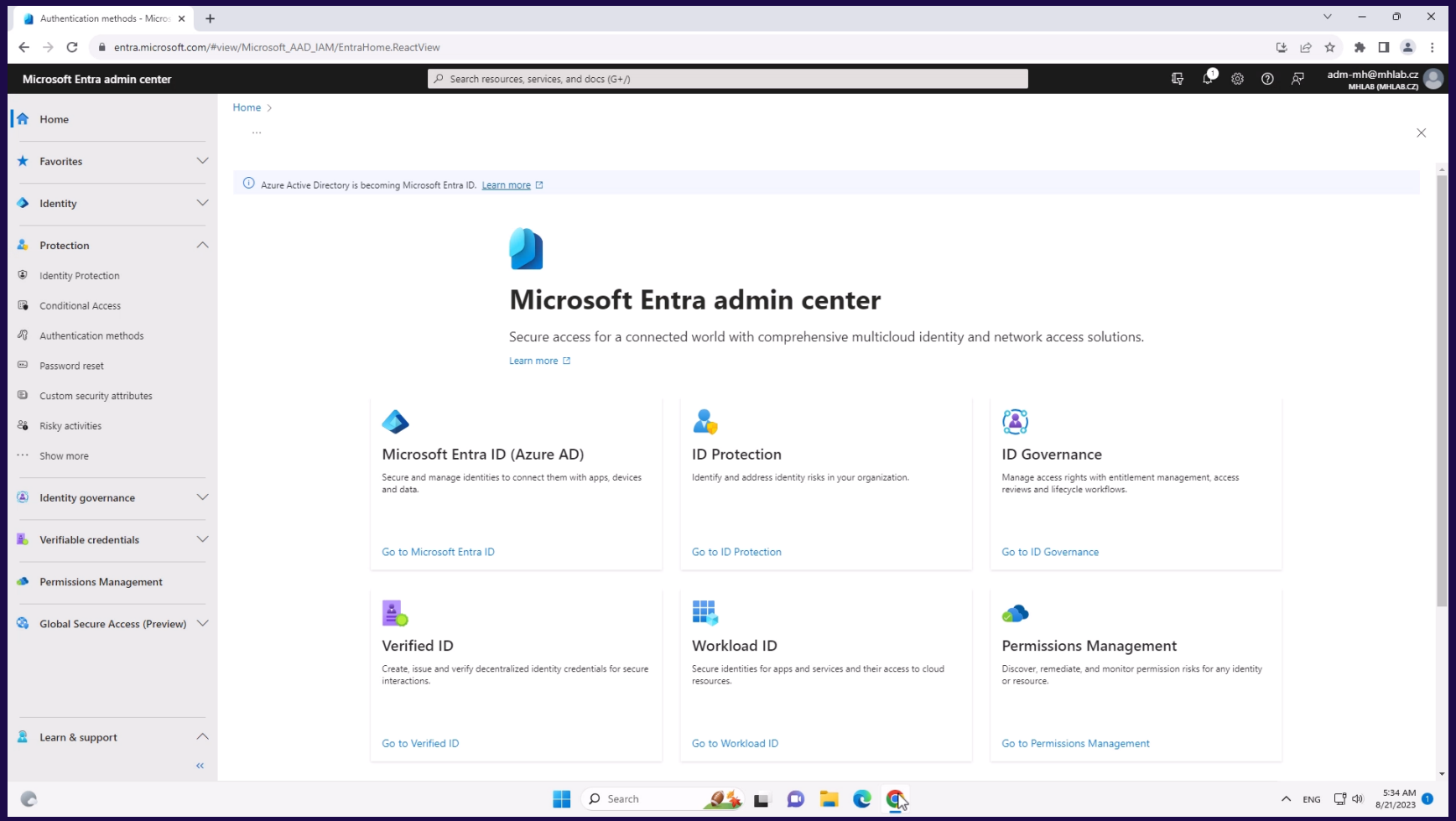


Source: https://attack.mitre.org/

Persistence: on tenant

- AD FS (https://aadinternals.com/post/aadbackdoor/) (including 2FA claim)
- Seamless SSO (https://aadinternals.com/post/kerberos/)
- AAD Connect account
- CA authentication (strong authentication)
  - https://entra.microsoft.com/#view/Microsoft_AAD_IAM/SecurityMenuBlade/~/CertificateAuthorities/menuId/IdentitySecureScore
  - https://posts.specterops.io/passwordless-persistence-and-privilege-escalation-in-azure-98a01310be3f
- Application – new/existing (bypasses MFA and Conditional Access)
  - (https://cyberdom.blog/2023/07/29/persistence-via-app-registration-in-entra-id/)
- Account with privileges (eg. LAPS)
- GDAP (https://www.microsoft.com/en-us/security/blog/2021/10/25/nobelium-targeting-delegated-administrative-privileges-to-facilitate-broader-attacks/)

Persistence: Demo persistence through CA



Other observations

- AAD will contain as same mess as AD
- Initial access: OneDrive share, GDAP
- DoS admin account

Summary

Summary

- Attacks are happening, it is just beginning
- It will depend on monetization scenarios
- GA (Global Admin) rights are not always needed
- Unknown unknown are the most dangerous
- The sooner the better to stop the attack

Hackers ask $120,000 for access to multi-billion auction house

72 by Ionut Ilascu / 2d

Hackers have breached the network of a major auction house and offered access to whoever was willing to pay $120,000. [...]

Source: https://www.bleepingcomputer.com/news/security/hackers-ask-120-000-for-access-to-multi-billion-auction-house/

Sources

Where to find more knowledge

- BlueHat Seattle 2019 || I'm in your cloud: A year of hacking Azure AD
- https://github.com/WillOram/AzureAD-incident-response/blob/main/README-OFFENSIVETECHNIQUES.md
- TR19: I'm in your cloud, reading everyone's emails - hacking Azure AD via Active Directory
- https://cloudbrothers.info/en/azure-attack-paths/
- https://aadinternals.com/

Thank ⟨YOU⟩