



Martin Haller

⟨ Microsoft Entra ID Lateral movement & Persistence ⟩

PATRON⟨IT⟩ OCHRANA
A SPRÁVA SÍTÍ

Entra ID: Attackers' goals

Attackers' goals: Ransomware?

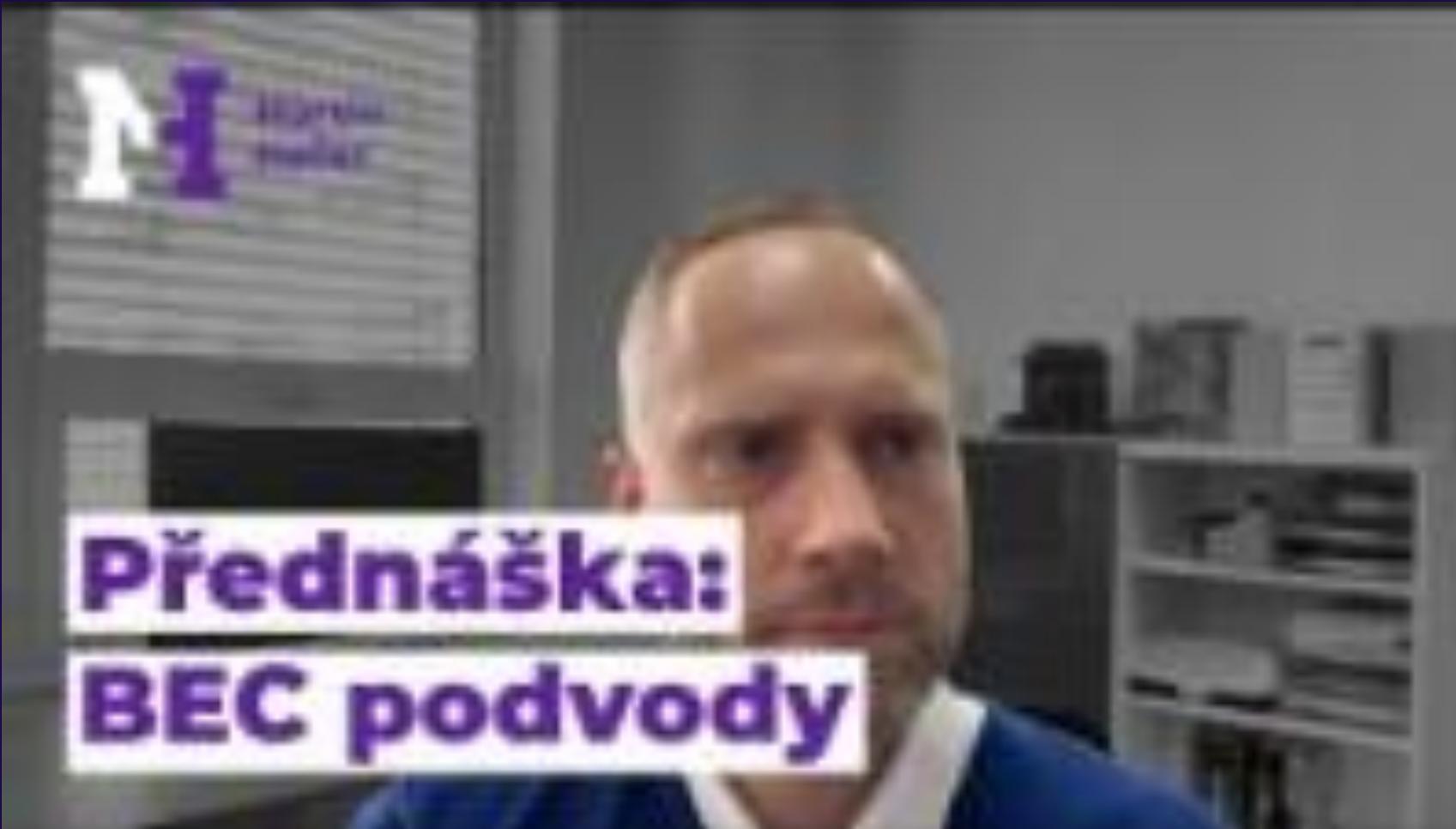
- » On-prem AD
- » Microsoft 365?
 - » Sharepoint, OneDrive, Exchange – version history, local copies, double trash bin
 - » Azure resources – SQL, storage, VMs
 - » <https://www.safebreach.com/resources/one-drive-double-agent-clouded-onedrive-turns-sides/>
 - » <https://danielchronlund.com/2023/02/14/the-threat-of-microsoft-365-wiper-malware/>
 - » <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			
date	title	group	
2023-08-18	tedbella.com	lockbit3	
2023-08-18	mitchcointernational.com	lockbit3	
2023-08-18	www.gude.org.au	noescane	
2023-08-17	www.contact121.com.au	noescane	
2023-08-17	unchealth.com	lockbit3	
2023-08-17	AgriLoja.pt_demo-leak	everest	
2023-08-17	sgil.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	mybox.us	lockbit3	
2023-08-17	kriegerklett.com	lockbit3	
2023-08-17	www.allianceolutionsgrp.com	blackbasta	
2023-08-17	www.deutsche-leasing.com	blackbasta	
2023-08-17	www.venauto.nl	blackbasta	
2023-08-17	https://www.synquestlaba.com	blackbasta	
2023-08-17	www.twintowerstrading.com	blackbasta	
2023-08-17	Camino_Nuevo_Charter_Academy	akira	
2023-08-17	Smart-wgcrc.org	lockbit3	
2023-08-17	SFJAZZ.ORG	lockbit3	
2023-08-17	The Clifton Public Schools	akira	
2023-08-17	https://dillionssupply.com	metaencryptor	
2023-08-17	https://www.policure.com	metaencryptor	
2023-08-17	http://www.coswell.biz	metaencryptor	
2023-08-17	https://bob-automotive.com	metaencryptor	
2023-08-17	https://www.seoulmemicon.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.evonterwerpen.be	metaencryptor	
2023-08-17	https://www.iconcreativestudio.com	metaencryptor	
2023-08-17	https://www.helmann-ag.de	metaencryptor	
2023-08-17	https://www.schweelbchen-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)

The screenshot shows a dark-themed web application interface titled "RUSSIAN MARKET". On the left, there is a sidebar with various menu items: News, CVV, Dumps, RDP, LOGS (which is currently selected), and pre-order. Below these are sections for My orders, PayPal, PROs, Checkers, Tools, My Purchases, and Support. A red button labeled "Earn money" is also visible.

The main content area features a search bar at the top with filters for Stealer, System, Country, Links, Outlook, Vendor, and Price. The search results table lists ten entries, each representing an IAB with details like Stealer, Country, Links, Outlook, Info, Struct, Date, Size, Vendor, Price, and an Action button. The entries include:

Stealer	Country	Links	Outlook	Info	Struct	Date	Size	Vendor	Price	Action
Vidar	Federation of B&H ISP TELEMACH BH	Show more...	-	(i)	archive.zip	2022.12.05	0.17Mb	Hy###ad gold	\$ 10.00	<button>Buy</button>
Vidar	Jakarta ISP PT. TELKOM INDONESIA	-	-	(i)	archive.zip	2022.12.05	0.25Mb	Hy###ad gold	\$ 10.00	<button>Buy</button>
Vidar	Riyadh Region ISP Ethad Etisalat	-	-	(i)	archive.zip	2022.12.05	0.13Mb	Hy###ad gold	\$ 10.00	<button>Buy</button>
Vidar	Sharqia ISP TE Data	Show more...	-	(i)	archive.zip	2022.12.05	1.19Mb	Hy###ad gold	\$ 10.00	<button>Buy</button>
Vidar	Nairobi Province ISP Safaricom Limited	-	-	(i)	archive.zip	2022.12.05	0.20Mb	Hy###ad gold	\$ 10.00	<button>Buy</button>
Vidar	Ceara ISP Tecnet Provedor De Acesso AS Redes De Com. Ltda	-	-	(i)	archive.zip	2022.12.05	0.01Mb	Hy###ad gold	\$ 10.00	<button>Buy</button>
Vidar	México ISP Uninet S.A. de C.V	more...	-	(i)	archive.zip	2022.12.04	0.32Mb	Hy###ad gold	\$ 10.00	<button>Buy</button>
Vidar	Taiwan Kaohsiung ISP VIBO	-	-	(i)	archive.zip	2022.12.05	0.12Mb	Hy###ad gold	\$ 10.00	<button>Buy</button>
Vidar	Punjab ISP Pakistan Telecommunication company limited	-	-	(i)	archive.zip	2022.12.05	0.18Mb	Hy###ad gold	\$ 10.00	<button>Buy</button>
Vidar	Sao Paulo ISP Claro NKT Telecomunicacoes Ltda	-	-	(i)	archive.zip	2022.12.05	0.58Mb	Hy###ad gold	\$ 10.00	<button>Buy</button>

At the bottom of the page, there is a navigation bar with numbers 1 through 10, a "Buy all logs from this page" button, and a small "Buy all logs from this page" link.

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

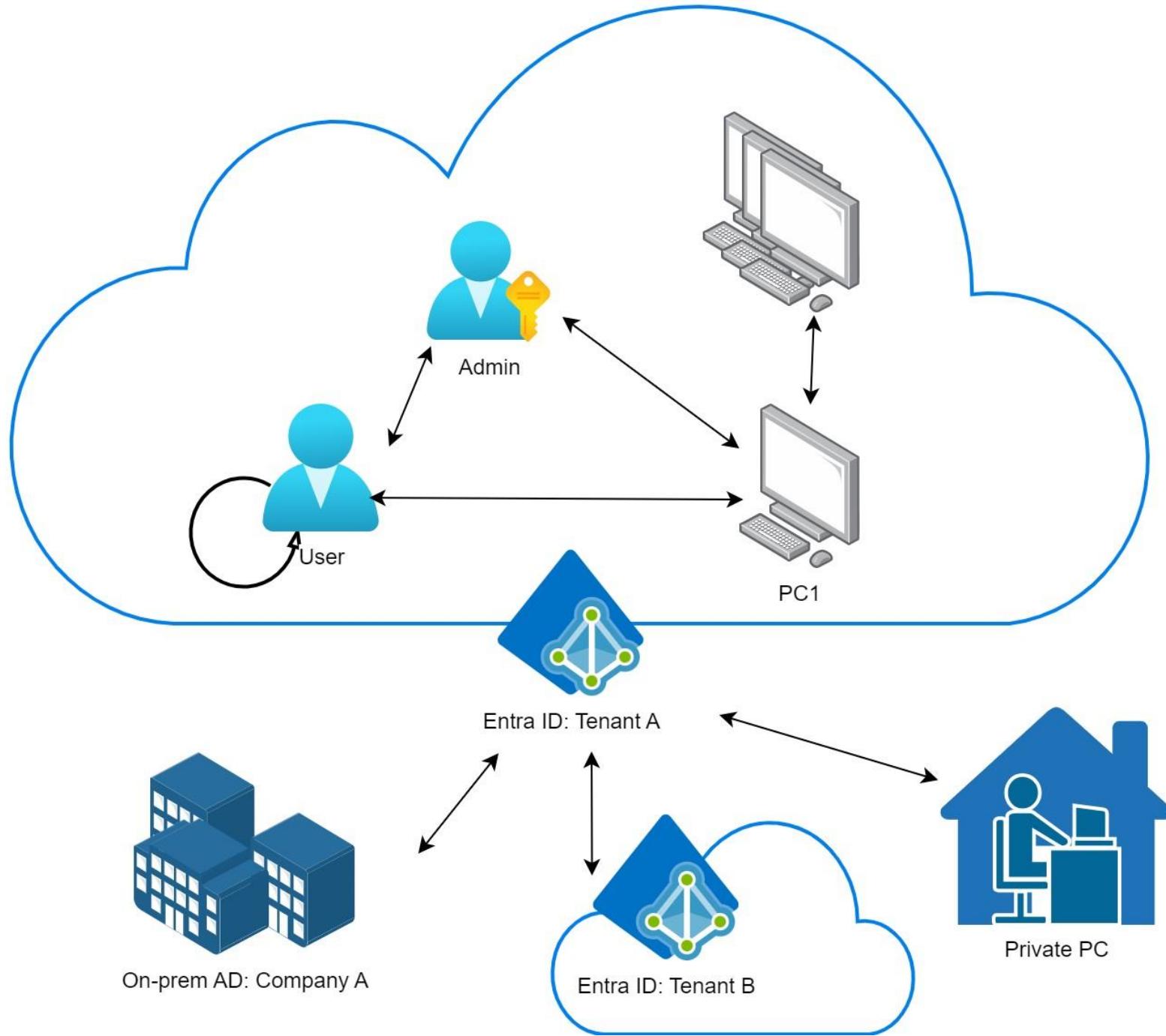
Attackers' goals : other

- » Prestige
- » Challenge
- » Revenge
- » Entertainment

Entra ID: Lateral movement

Lateral movement: why?



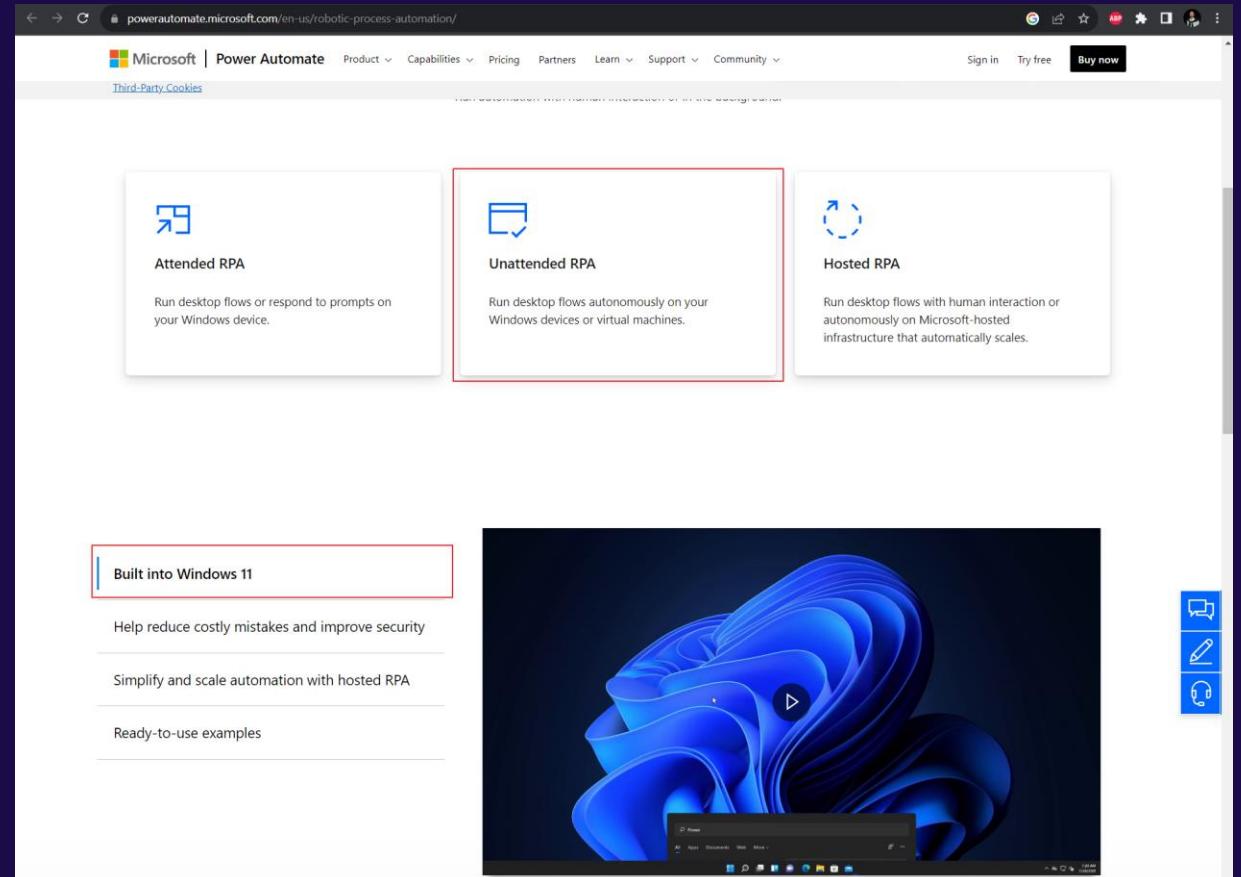


Lateral movement: User privilege escalation

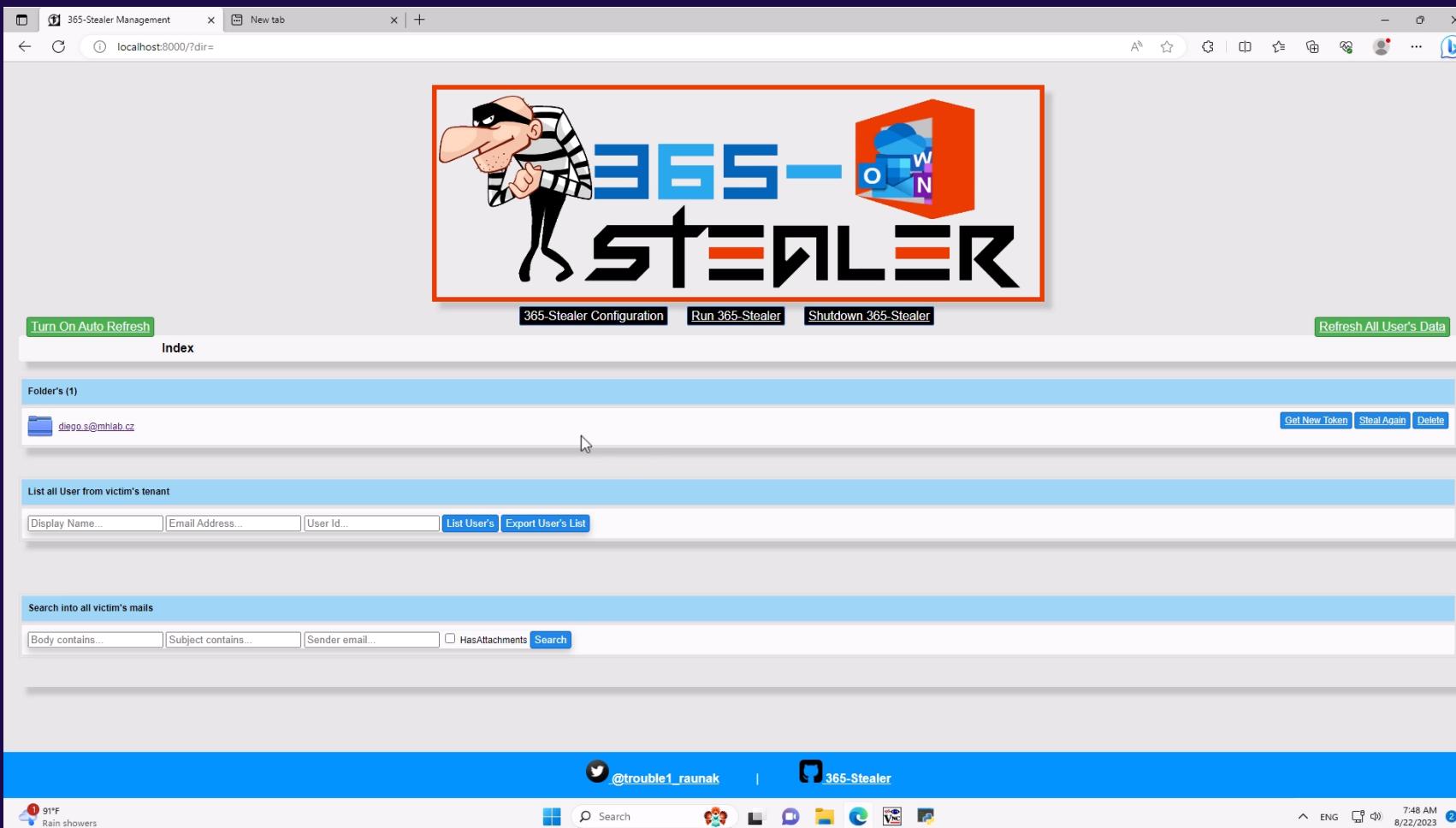
- » FOCI (<https://github.com/secureworks/family-of-client-ids-research>)
- » Looting (mail, OneDrive, Sharepoint)
- » SSPR (Self-server password reset)
- » Getting „Compliant device“ (<https://aadinternals.com/post/mdm/>)

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

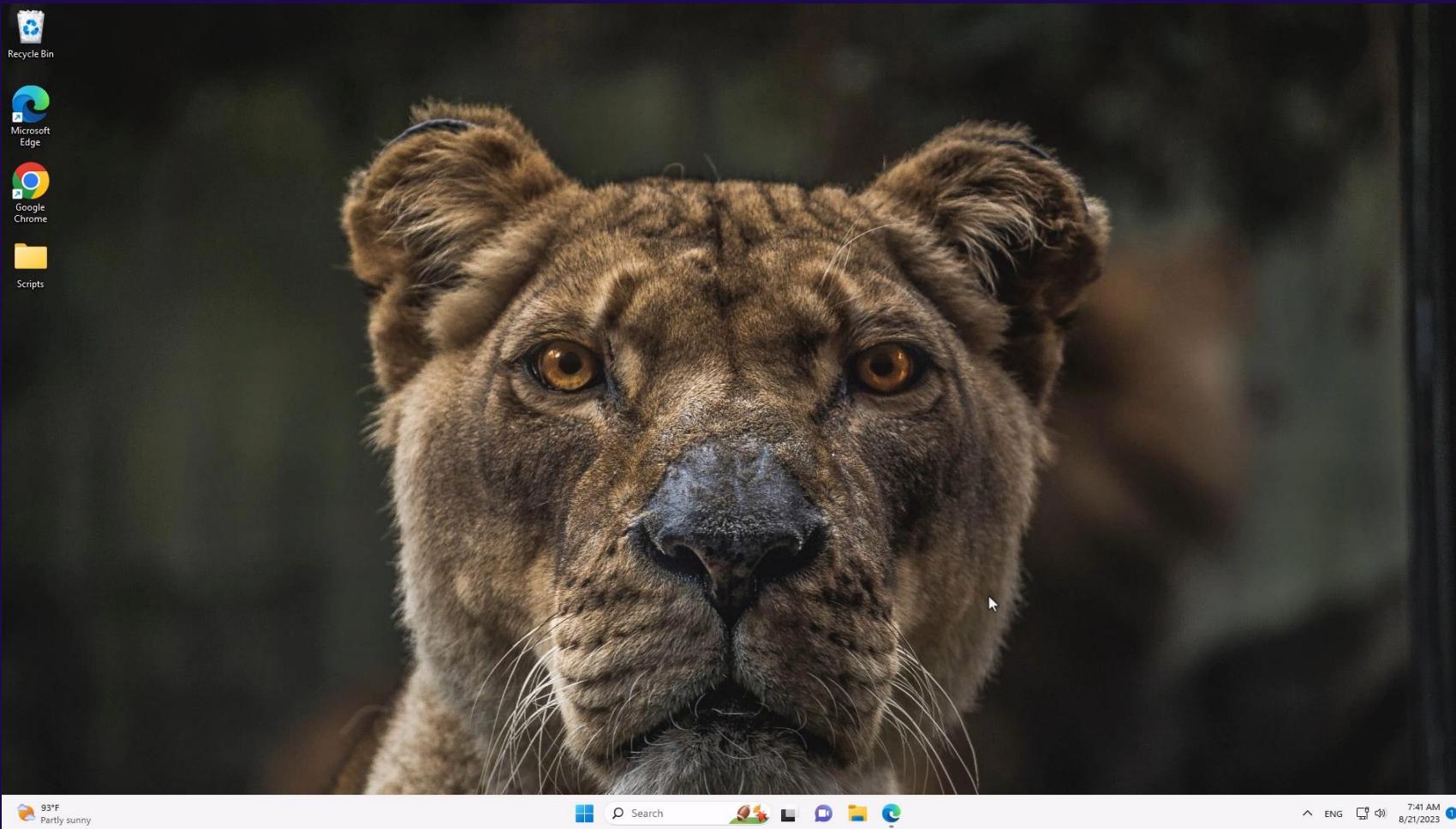
Lateral movement: PC to PC

- » 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 misuse (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/>)

The screenshot shows the Microsoft 365 Admin Center interface. The left sidebar has a red box around the 'Partner relationships' link under 'Admin centers'. The main content area is titled 'Partner relationships' and displays two entries:

Partner	Authorized roles	Role authorization	Expiration date	Status	
PATRON-IT s.r.o. (1)	PATRON-GA	Global Administrator	GDAP	August 7, 2025	Active

Below this, under 'Other partner types', there are two more entries:

Partner	Partner type	Role authorization	Roles
PATRON-IT s.r.o. (1)	Indirect reseller	DAP	Global Administrator, Helpdesk Administrator
TD SYNNEX Czech s.r.o. (1)	Reseller	None	None assigned

Entra ID: Persistence

Persistence: why?

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

Home > Users > **Diego Siciliani**

User

Search

Edit properties Delete Refresh

Reset password Revoke sessions Manage view

Overview Monitoring Properties

Basic info

Diego Siciliani
diego.s@mhlab.cz
Member

Custom security attributes

Assigned roles

Administrative units

Groups

Applications

Licenses

Devices

Azure role assignments

Authentication methods

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 members 7

Applications 3

Assigned roles 0

Assigned licenses 1

My Feed

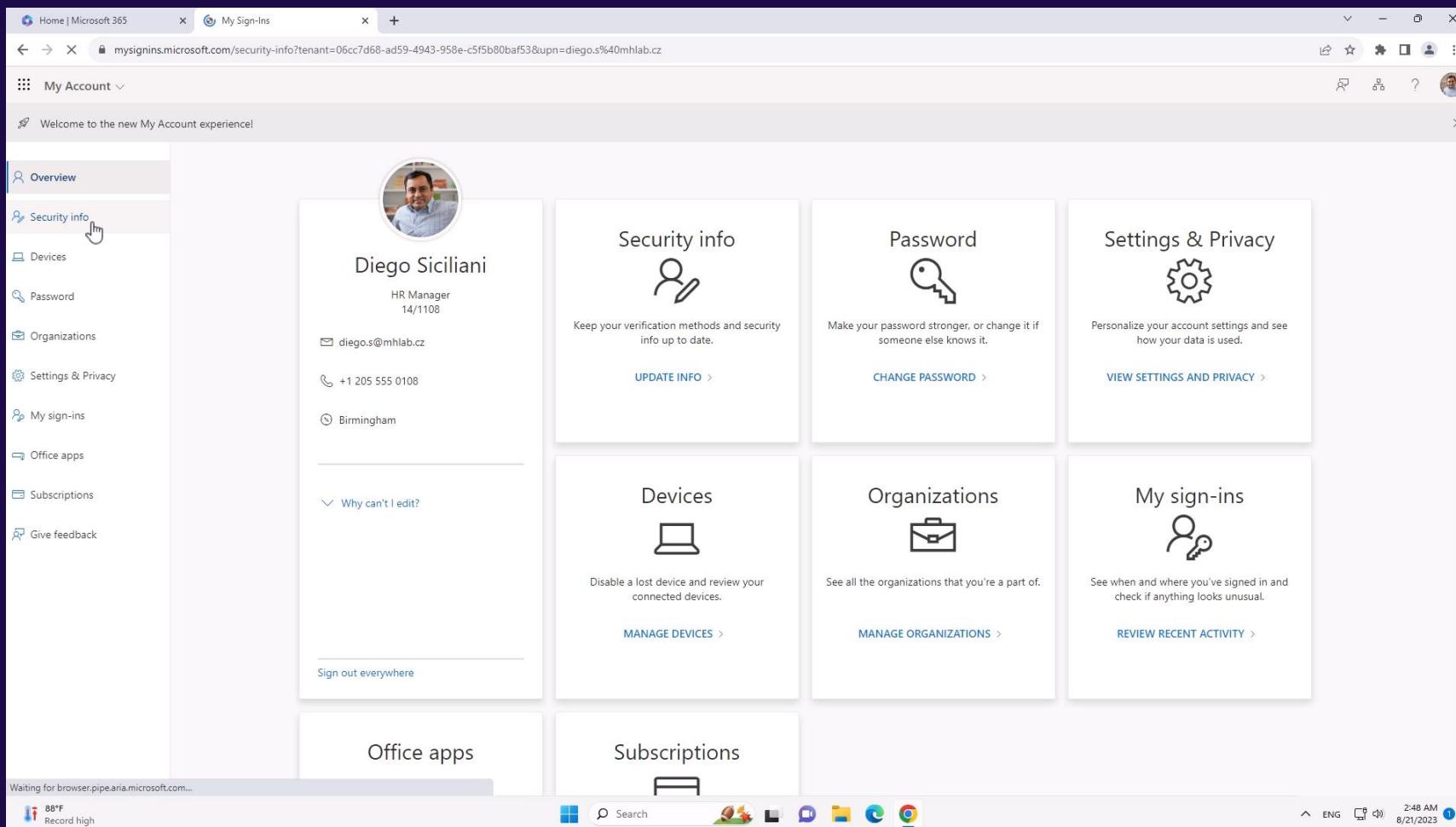
Account status Enabled

Sign-ins Last sign-in: Aug 19, 2023, 10:23 AM

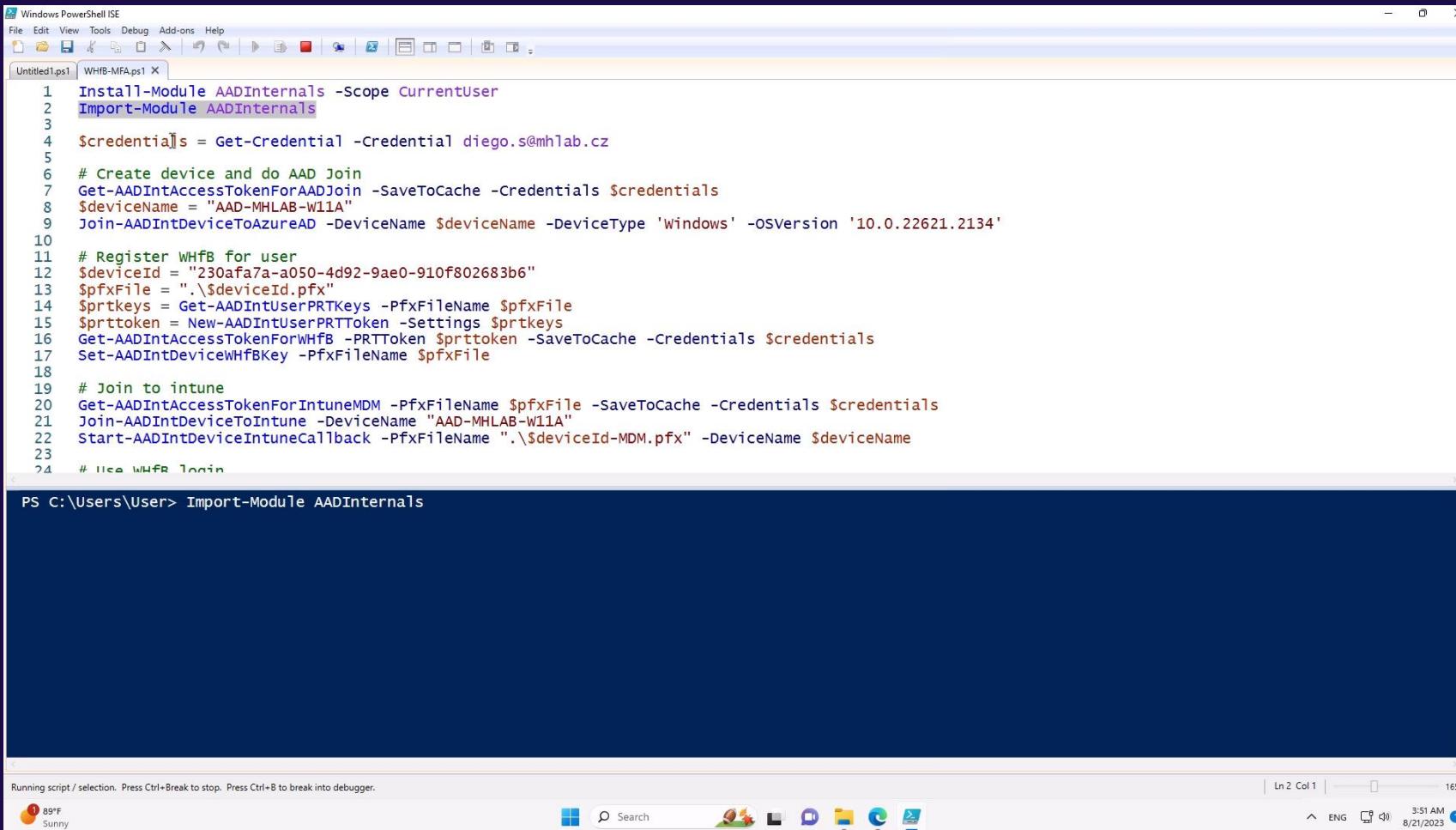
See all sign-ins

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

Persistence: Demo persistence on user



Persistence: Demo persistence on user CLI



The screenshot shows a Windows PowerShell ISE window with a script named `Untitled1.ps1` (renamed to `WHfB-MFA.ps1`). The script performs several steps to establish persistence:

- Install the `AADInternals` module.
- Import the `AADInternals` module.
- Get credentials for the user `diego.s@mhlab.cz`.
- Create a device and do AAD Join.
- Get an AAD access token for AAD Join.
- Join the device to Azure AD.
- Register WHfB for the user.
- Get the device ID.
- Get the PFX file for the device.
- Get the AAD Int User PRT keys.
- Create a new AAD Int User PRT token.
- Get an AAD access token for WHfB.
- Set the AAD Int Device WHfB key.
- Join the device to Intune.
- Get an AAD access token for Intune MDM.
- Join the device to Intune.
- Start the AAD Int Device Intune callback.
- Use WHfB login.

The PowerShell session at the bottom shows the command `Import-Module AADInternals` being run.

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

Persistence 19 techniques
Account Manipulation (5)
BITS Jobs
Boot or Logon Autostart Execution (14)
Boot or Logon Initialization Scripts (5)
Browser Extensions
Compromise Client Software Binary
Create Account (3)
Create or Modify System Process (4)
Event Triggered Execution (16)
External Remote Services
Hijack Execution Flow (12)
Implant Internal Image
Modify Authentication Process (8)
Office Application Startup (6)
Pre-OS Boot (5)
Scheduled Task/Job (5)
Server Software Component (5)
Traffic Signaling (2)
Valid Accounts (4)

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/menuld/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

The screenshot shows the Microsoft Entra admin center interface. The left sidebar contains a navigation menu with sections like Favorites, Identity, Protection, Identity governance, Verifiable credentials, Permissions Management, Global Secure Access (Preview), and Learn & support. The main content area features a banner about Azure Active Directory becoming Microsoft Entra ID, followed by a central heading "Microsoft Entra admin center" and a subtext: "Secure access for a connected world with comprehensive multicloud identity and network access solutions." Below this are six service cards arranged in a grid:

- Microsoft Entra ID (Azure AD)**: Secure and manage identities to connect them with apps, devices and data. [Go to Microsoft Entra ID](#)
- ID Protection**: Identify and address identity risks in your organization. [Go to ID Protection](#)
- ID Governance**: Manage access rights with entitlement management, access reviews and lifecycle workflows. [Go to ID Governance](#)
- Verified ID**: Create, issue and verify decentralized identity credentials for secure interactions. [Go to Verified ID](#)
- Workload ID**: Secure identities for apps and services and their access to cloud resources. [Go to Workload ID](#)
- Permissions Management**: Discover, remediate, and monitor permission risks for any identity or resource. [Go to Permissions Management](#)

The bottom of the screen shows a taskbar with icons for File, Home, Search, and other Microsoft applications, along with system status indicators.

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 unknowns 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**