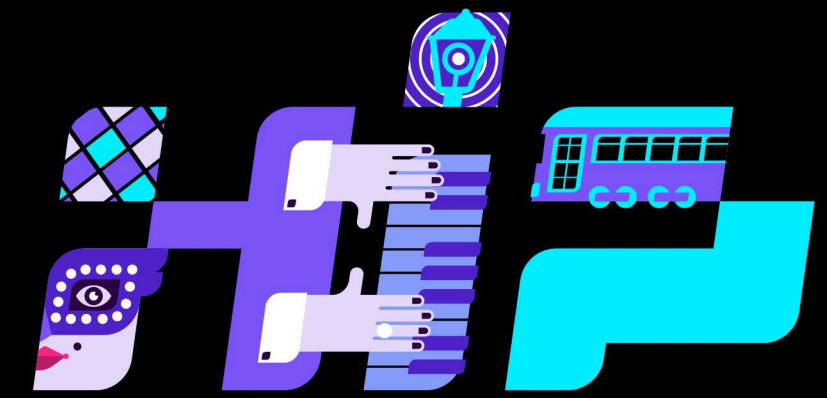
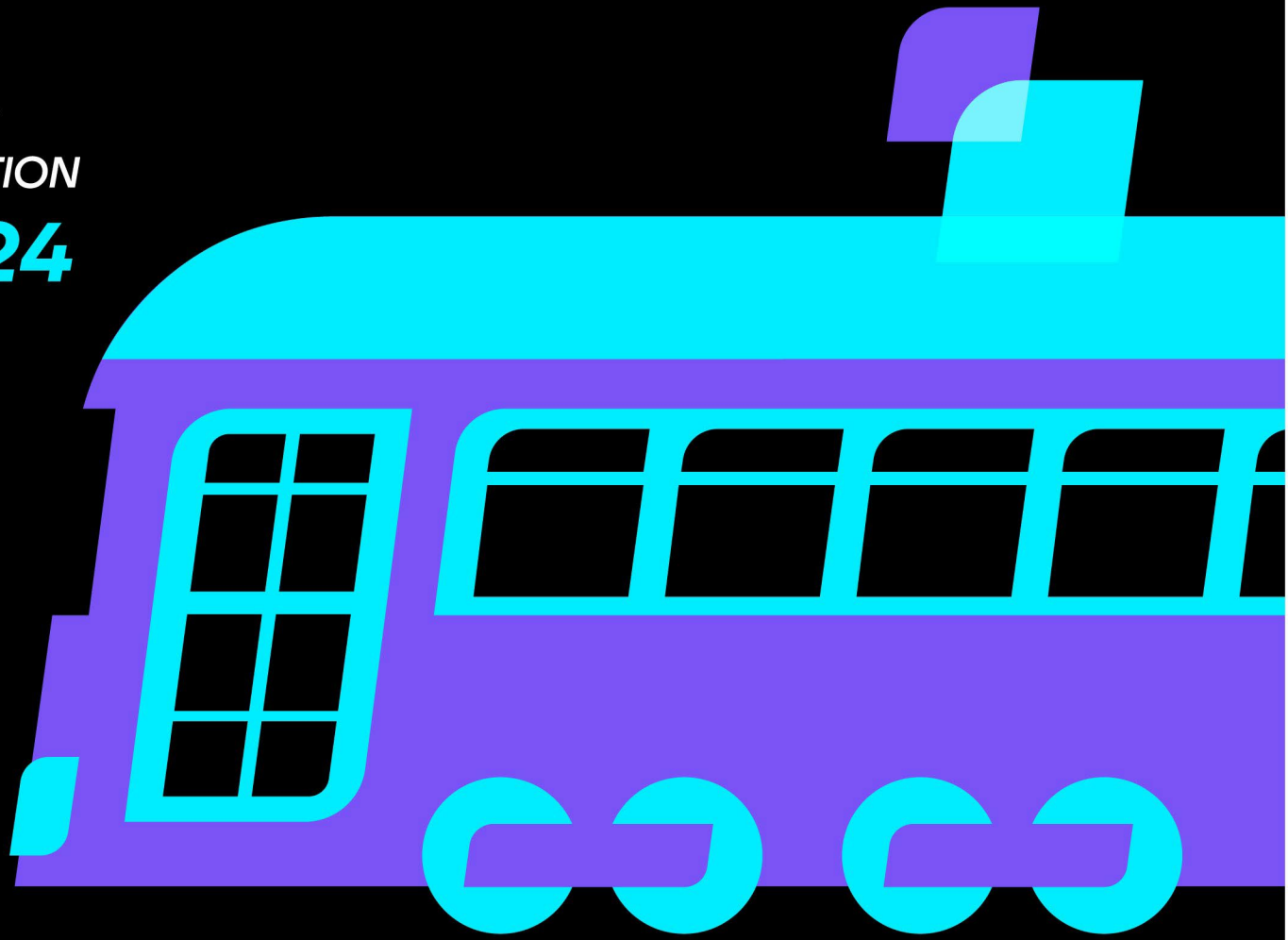


HYBRID
IDENTITY
PROTECTION

conf24

NEW ORLEANS



A Decade of Microsoft Identity Attacks: What We've Learned & What's Next

Sean Metcalf
Founder & CTO, Trimarc

About

- Founder & CTO @ Trimarc (Trimarc.co), a professional services company that helps organizations better secure their Microsoft Identity systems (Active Directory & Azure AD/Entra ID).
- Microsoft Certified Master (MCM) Directory Services
- Speaker: Black Hat, Blue Hat, Blue Team Con, BSides Charm, BSides DC, BSides PR, DEFCON, DerbyCon, TEC, Troopers
- Former Microsoft MVP
- Security Consultant / Researcher
- AD Enthusiast - Own & Operate ADSecurity.org (Microsoft identity security info)

I've Done Some Stuff

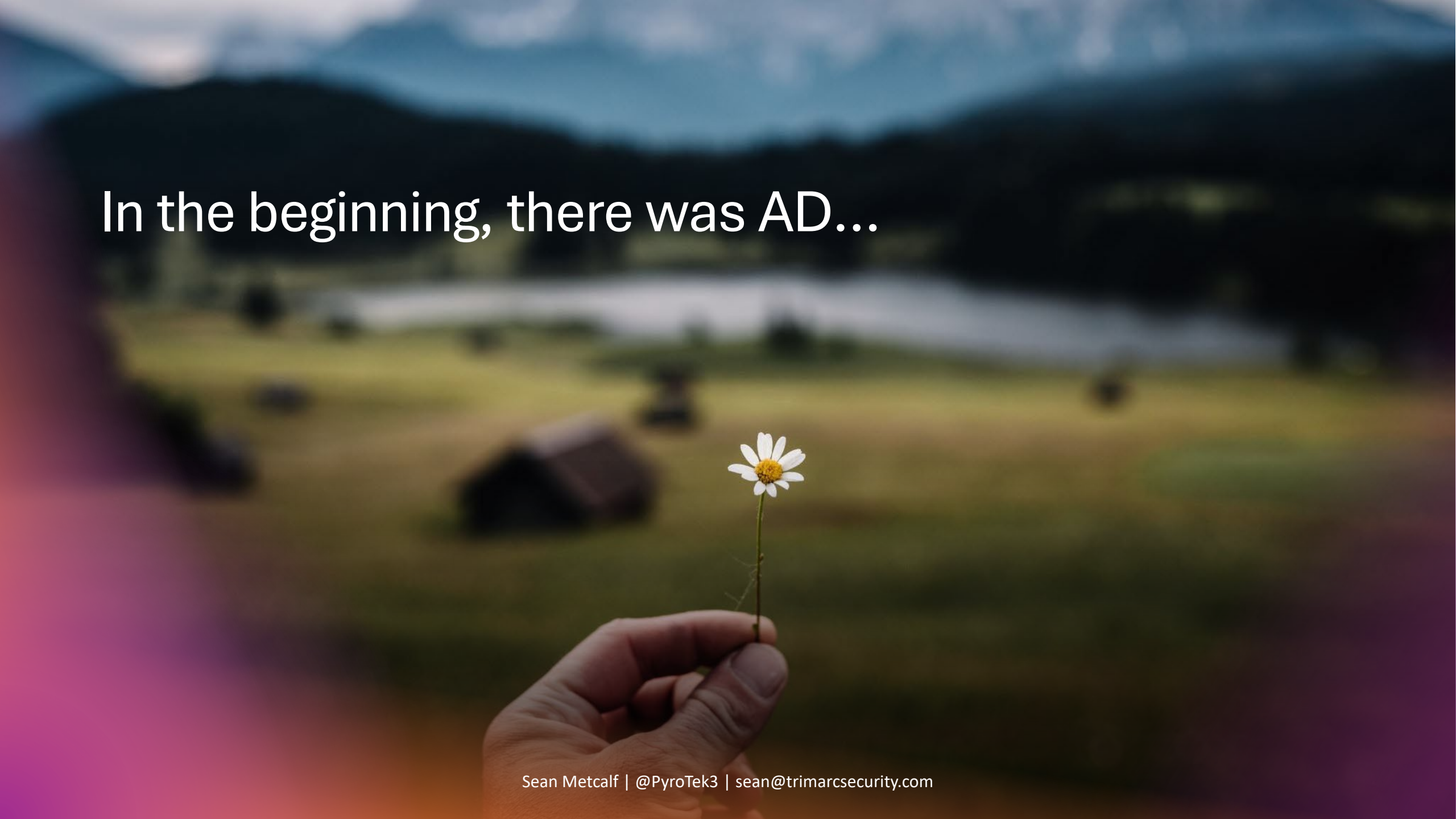
- 2015: Published original method to detect Golden Tickets
- 2015: Made Golden Tickets more effective by adding Enterprise Admins to SIDHistory in the ticket (extrasids) working with Benjamin Delpy
- 2015: Described what rights were necessary to DCSync, including initial detection guidance
- 2015: Described "SPN Scanning" – identifying services on a network without port scanning
- 2015: Identified how to use Silver Tickets to compromise AD (via DCs) for persistence
- 2015: Described how to pass-the-hash using the DC's DSRM password (with Benjamin Delpy)
- 2015: Described how to modify AdminSDHolder permissions for persistence
- 2016: Published methods to better detect PowerShell attack activity
- 2017: Published first effective detection of Kerberoasting with no false positives (still effective)
- 2017: Published Password Spray (AD) detection when attackers use Kerberos
- 2017: Discussed how to forge federation tokens (aka "GoldenSAML") & compromise AD through Azure AD Connect (on-prem)
- 2018: Described how most Read-Only Domain Controller deployments are vulnerable & how to improve
- 2018: Discussed how to bypass most enterprise password vault security
- 2019: Presented on Microsoft Cloud (Azure AD & Microsoft Office 365) attack & defense at BlackHat & DEFCON Cloud Security Village
- 2020: Published info on how to compromise Azure instances (VMs) from Azure AD / Microsoft Office 365
- 2021: 1 of 3 people thanked during CISA Director's BlackHat keynote for SolarWinds help
- "Stealth" contributor to Bloodhound
- Published lots of AD attack & defense techniques (conference talks & blog posts)

Sean Metcalf | @PyroTek3 | sean@trimarcsecurity.com

Agenda

- Introduction
- Active Directory Attack Timeline
  - “Baby Steps”(2000 – 2009)
  - “The Wonder Years” (2010 – 2014)
  - “The Third Age” (2020 – 2023)
- Structuring Effective AD Defenses
- Entra ID Attack Timeline
- Entra ID
  - Highly Privileged Roles & Applications
  - Conditional Access Policy & CAP Gaps
  - Attacking Azure AD/Entra ID
  - Securing Entra ID Administration
- Conclusion

In the beginning, there was AD…



Sean Metcalf | @PyroTek3 | sean@trimarcsecurity.com

Active Directory Attack Timelines

Note that dates may be inaccurate as I used the best available information on web sites and github to identify first use/publish date.

Sean Metcalf | @PyroTek3 | sean@trimarcsecurity.com

Active Directory Attack Timelines: "Baby Steps"(2000 – 2009)

1997

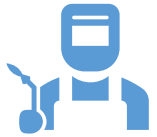
April: Paul Ashton posted to NTBugtraq about "'Pass the Hash' with Modified SMB Client" leveraging the username and LanMan hash against NT.

2001

March: Sir Dystic of Cult of the Dead Cow (cDc) releases SMBRelay and SMBRelay2

2007

NBNSpoof tool created by Robert Wesley McGrew (LLMNR/NBT-NS)



2008

July: Hernan Ochoa publishes the "Pass-the-Hash Toolkit" (later called WCE)

Active Directory Attack Timelines: "The Wonder Years" (2010 – 2014)

2010

March: Windows Credentials Editor (WCE) & RootedCon presentation by Hernan Ochoa

2011

May: First version of Mimikatz tool released by Benjamin Delpy

2012

Exploiting Windows 2008 Group Policy Preferences by Emilien Giraul

May: Chris Campbell's post on GPP Passwords

October: Responder v1 tool released by Laurent Gaffie

2013

October: Invoke-Mimikatz PowerShell module released by Joe Bialek

2014

August: "Abusing Microsoft Kerberos sorry you guys don't get it" Black Hat presentation by Benjamin Delpy & Skip Duckwell

- Golden Tickets
- Overpass-the-hash
- Pass-the-ticket

September: PAC Validation, The 20 Minute Rule and Exceptions (BHUSA 2014 part deux) blog post about Silver Tickets by Skip Duckwell

September: Kerberoast released by Tim Medin at DerbyCon

December: PowerView tool released by Will Schroeder

Active Directory Attack Timeline Summary (with Mitre ATT&CK): "The Wonder Years" (2010 – 2014)

Tools

Windows Credential Editor (WCE) (ID: S0005)

Mimikatz (ID: S0002)

Responder (ID: S0174)

PowerView

Privilege Escalation

Group Policy Preferences password (ID: T1552.006)

Pass the Ticket (ID: T1550.003)

Overpass-the-Hash

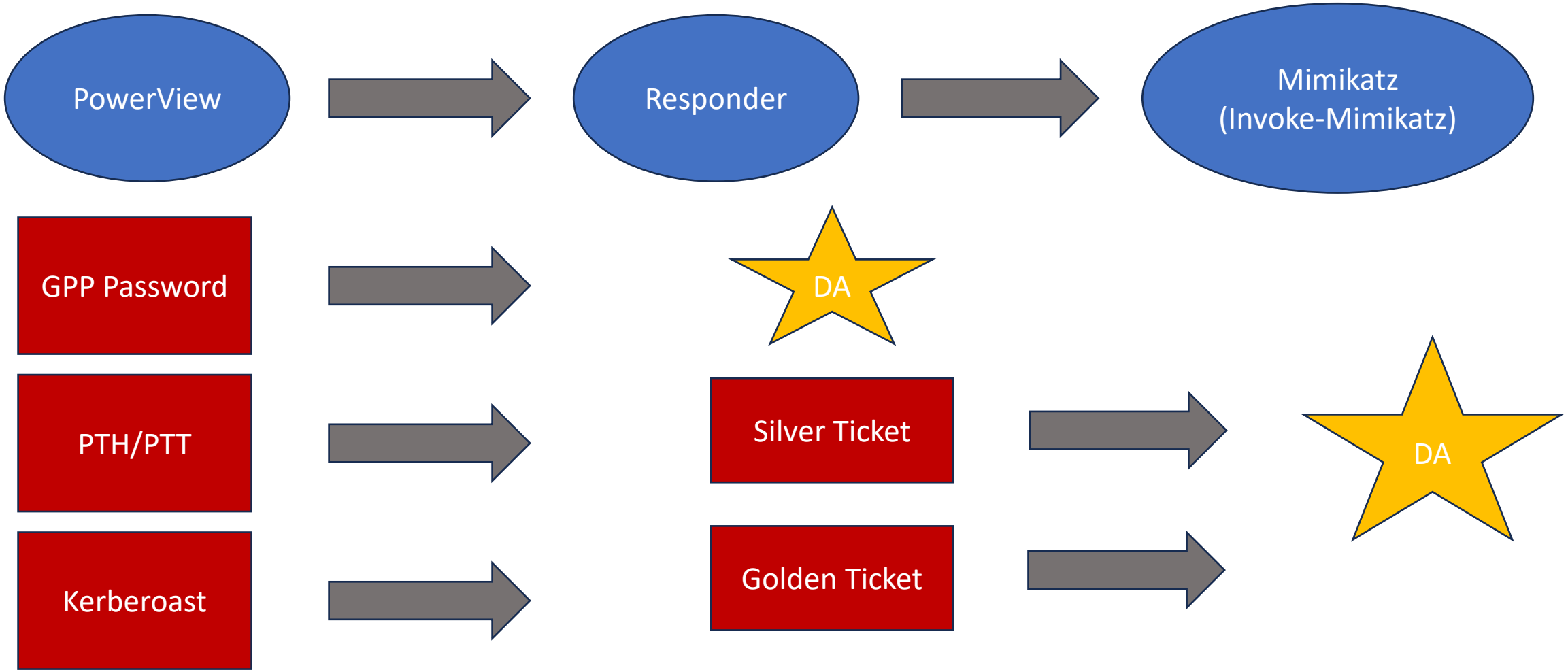
Kerberoast (ID: T1558.003)

Persistence

Golden Tickets (ID: T1558.001)

Silver Tickets (ID: T1558.002)

“The Wonder Years” (2010 – 2014) Conceptual Overview



Active Directory Attack Timelines: "The Golden Years" (2015 – 2019)

2015

DSInternals tool released by Michael Grafnetter
Kekeo tool released by Benjamin Delpy
PowerSploit toolset released by Matt Graeber
May: Impacket tool released by Alberto Solino (asolino)
May: Method to Detect Golden Tickets
August: PowerShell Empire released by Will @Hrmj0y & Justin Warner
August: DCSync update to Mimikatz by Vincent Le Toux & Benjamin Delpy

August: Black Hat 2015 presentation by Sean Metcalf: Unconstrained Delegation & Golden Tickets more powerful & Active Directory Persistence using AdminSDHolder

September: CrackMapExec v1.0.0 tool released by Marcello aka byt3bl33d3r

September: DerbyCon 2015 presentation by Sean Metcalf: Attacking DSRM

December: Attacking Group Managed Service Accounts (GMSAs) by Michael Grafnetter

2016

August: Bloodhound tool released at DEFCON 23 originally written by Will Schroeder, Rohan Vazarkar, & Andy Robbins

2017

May: DNSAdmin to Domain Admin by Shay Ber

May: Death Star python script released by byt3bl33d3r

May: Ntlmrelayx tool released by Fox-IT

August: ACE up the Sleeve Black Hat 2017 presentation by Andy Robbins and Will Schroeder

September: Sharphound tool release

2018

February: Bloodhound.py tool released by Dirk-jan Molema (Python based Bloodhound ingester)

July: GhostPack released as a collection of C# ports of popular PowerShell tools and collects these tools together

August: DCShadow attack by Vincent Le Toux & Benjamin Delpy

September: Rubeus tool released by Will Schroeder (port of Kekeo and added to GhostPack)

October: "Printer Bug" AD priv esc talk at DerbyCon by Will Schroeder, Lee Christensen, & Matt Nelson
Ldapdomaindump tool released by Dirk-jan Molema

2019

January: PrivExchange tool released by Dirk-jan Molema

January: Wagging the Dog: Abusing Resource-Based Constrained Delegation to Attack Active Directory article "Wagging the Dog" by Elad Shamir

Active Directory Attack Timeline Summary (with Mitre ATT&CK): "The Golden Years" (2015 – 2019)

Tools

DSInternals

Kekeo

PowerSploit (ID: S0194)

Impacket (ID: S0357)

PowerShell Empire (ID: S0363)

DCSync added to Mimikatz (ID: T1003.006)

CrackMapExec (ID: S0488)

Bloodhound (ID: S0521)

DeathStar.py

NTLMRelayX

SharpHound

GhostPack

Rubeus (ID: S1071)

Privilege Escalation

DNSAdmin to Domain Admin

AD Permissions

"Printer Bug"

Resource-Based Constrained Delegation

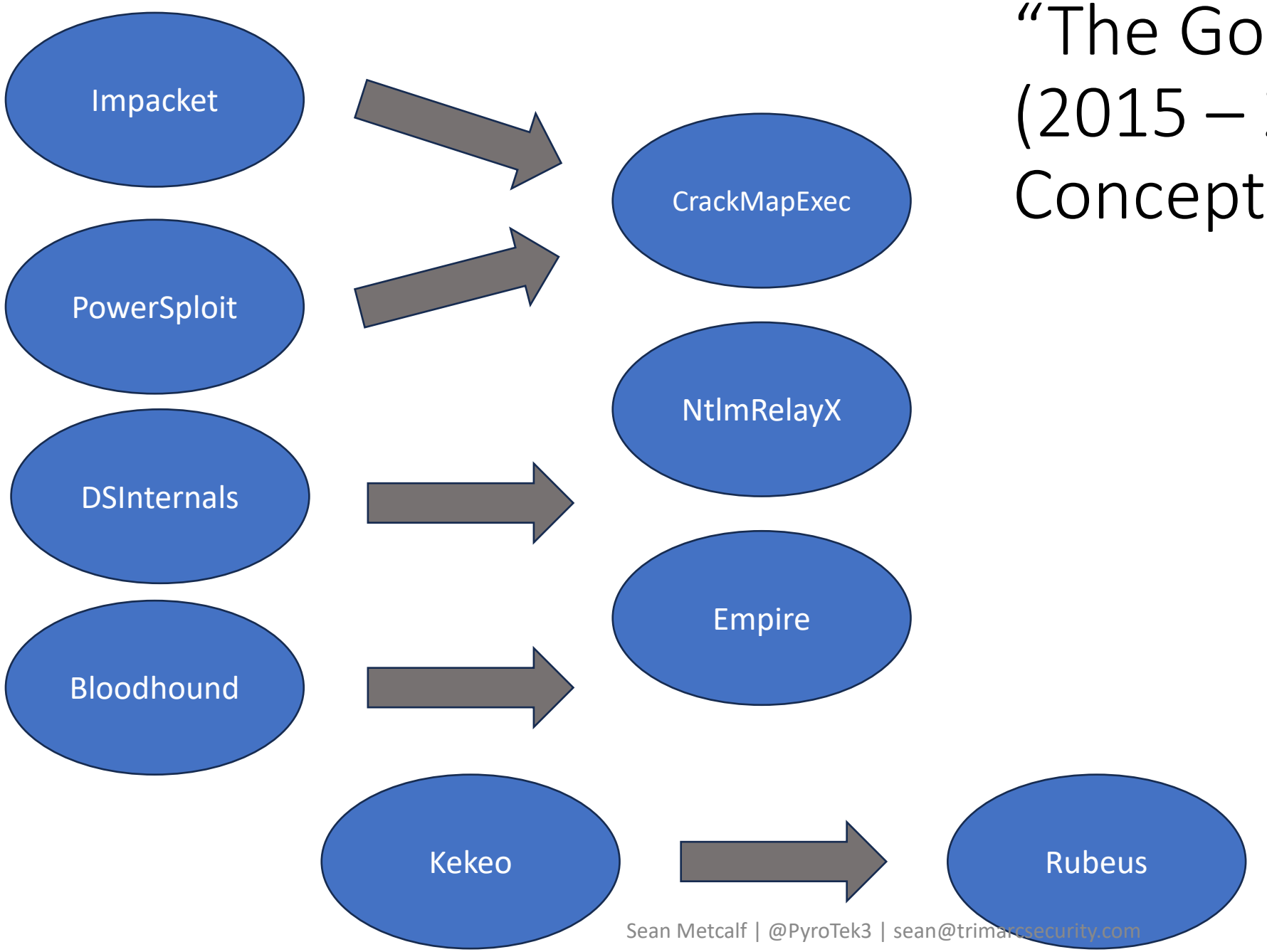
Persistence

AD Permissions

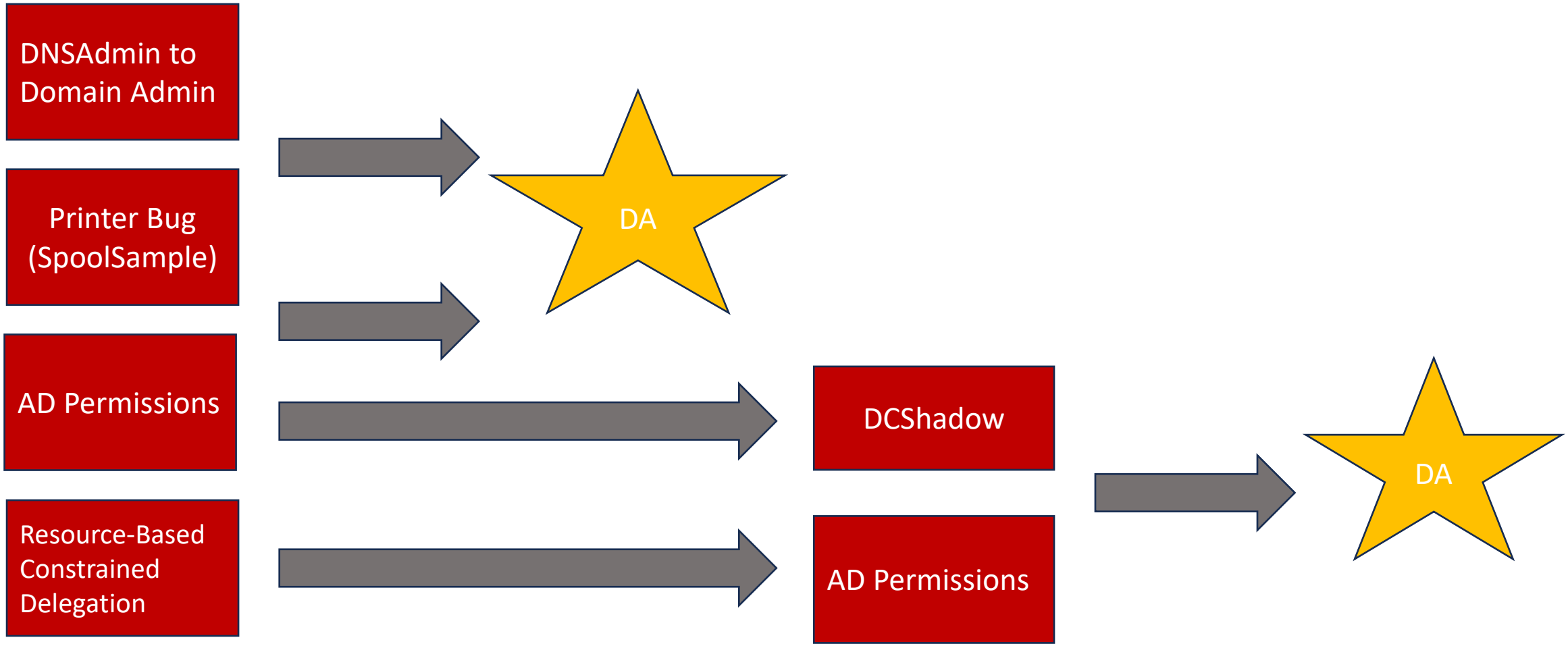
DCShadow (ID: T1207)

Sean Metcalf | @PyroTek3 | sean@trimarcsecurity.com

“The Golden Years” (2015 – 2019) Tools Conceptual Overview



“The Golden Years” (2015 – 2019) Conceptual Flow



Active Directory Attack Timelines: "The Third Age" (2020 – 2023)

2020

- December: Adalanche tool released by Lars Karlslund

2021

- April: RemotePotato0 tool released by antonioCoco & article by Antonio Cocomazzi and Andrea Pierini
- July: PetitPotam tool released
- August: Certified Pre-Owned (ADCS Attacks) Black Hat talk by Will Schroeder & Lee Christensen whitepaper download
- August: Certify ADCS tool released by Will Schroeder & Lee Christensen (in GhostPack)
- October: Kerberos Relay Attack by James Forshaw
- October: Certipy tool released by Oliver Lyak (ly4k) - Python port of the Certify tool
- November: "Is This My Domain Controller" Black Hat talk by Sagi Sheinfeld (@sagish1233), Eyal Karni (@eyal_karni), & Yaron Zinar (@YaronZi)

2022

- April: KrbRelayUp tool released by Dec0ne

2023

- October: CrackMapExec continues as NetExec (nxc)!

Active Directory Attack Timeline Summary (with Mitre ATT&CK): "The Third Age" (2020 – 2023)

Tools

RemotePotato0

PetitPotam

Certify

Certipy

KrbRelayUp

CrackMapExec continues as NetExec (nxc)

Privilege Escalation

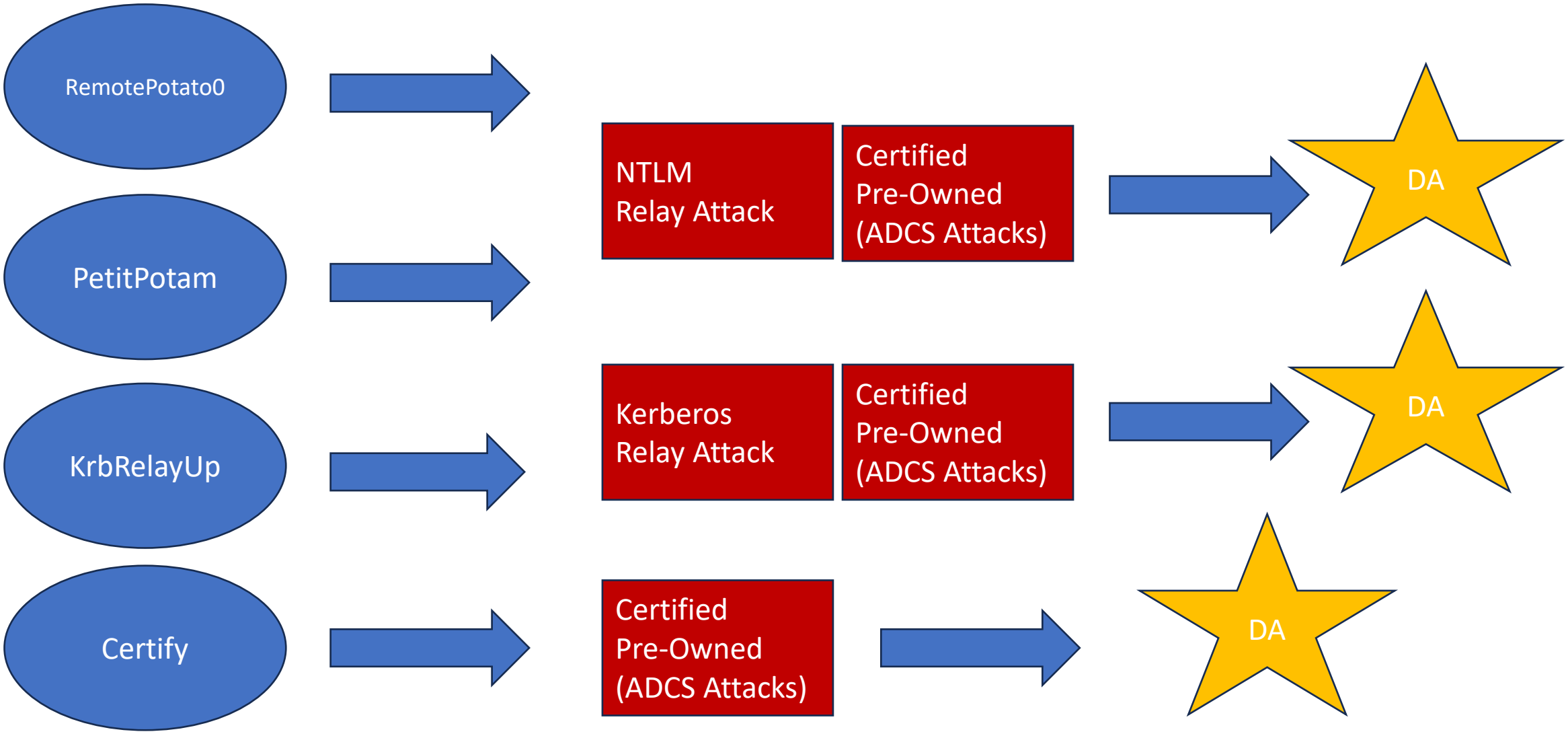
Certified Pre-Owned (ADCS Attacks)

Kerberos Relay Attack

Persistence

Certified Pre-Owned (ADCS Attacks)

“The Third Age” (2020 – 2023) Conceptual Overview



Structuring Effective Active Directory Defenses

Sean Metcalf | @PyroTek3 | sean@trimarcsecurity.com

Breaking Recon

Administrative Group/Account Enumeration

- Remove Authenticated Users from having rights on the groups (add a new “auditing” group so it can view the members).
- Place admin accounts/groups into secured OU that Authenticated Users can’t view.

GPO Security Permission/Setting Enumeration

- Remove Authenticated Users (this also prevents GPO from applying).
- Add new computer group that needs to apply the GPO.

Allow Blue Team & Auditors Recon/Review

Ensure there is a custom group that can view all objects where default permissions have changed.

Recommend different groups to enable different read access:

- Secure OU
- AD Privileged Groups (AdminSDHolder)
- Local Administrators Group Membership
- GPO View Access

Adding audit accounts to these group enables Bloodhound/Recon type access.

Effective Windows System Defense

- Disable LLMNR via Group Policy
- Disable NetBIOS via Group Policy
- Disable WPAD via Group Policy
- Disable LM & NTLMv1
- Disable SMBv1
- Enable PowerShell constrained language mode
- Control Microsoft Office macros via Group Policy
- Deploy Microsoft LAPS (or similar) to ensure all local Administrator passwords are unique
- Set GPO to prevent local accounts from connecting over network to computers
- Deny access to this computer from the network: Domain Admins, Enterprise Admins, other custom admin groups
- Ensure all admins only log onto approved admin workstations & servers
- Restrict workstation to workstation communication with host firewalls - AD clients don't need special rules, default block All inbound works.

Active Directory Administrative Security

- Admin accounts set to “sensitive & cannot be delegated”
- Ensure all Active Directory admin accounts associated with people are members of the Protected Users groupComplete separation of administration
- ADAs never logon to other security tiers
- ADAs should only logon to a DC from an admin workstation or admin server
- Ideally ADAs use time-based, temporary group membership
- Change the KRBTGT account password (twice) every year & when an AD admin leaves
- Implement network segmentation

Service Account Security

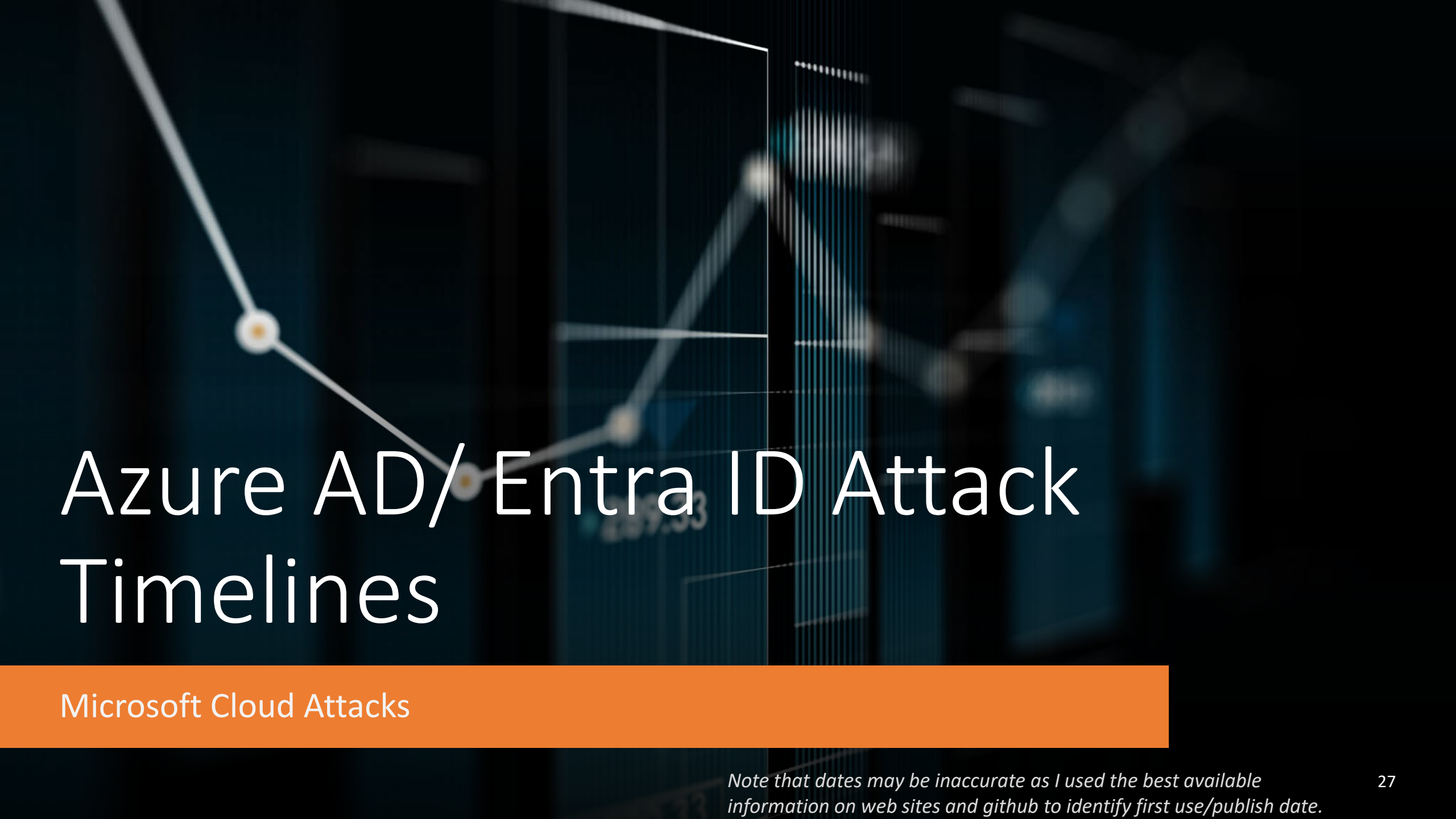
- Leverage “(Group) Managed Service Accounts”
- Implement Fine-Grained Password Policies
- Limit SAs to systems of the same security level, not shared between workstations & servers (for example)
- Ensure passwords are >25 characters
- Disable logon interactive capability
- No Domain Admin service accounts on non-DCs

Domain Controller Security

- Ensure DCs are physically secure
- Ensure the server is fully patched before running DCPromo
- Remove all unnecessary software, agents, and services
- Ensure IIS is not running on any DCs (IIS_USR account)
- Limit admin logon to DCs
- Update all Domain Controllers to a current supported Windows OS version.
- Scrutinize scheduled tasks
- Monitor logon events
- Audit use of backup & restore
- Enable Audit Subcategories
- Regularly change the DSRM account password on all DCs
- Limit management protocol access on DCs to admin subnets (RDP, WMI, WinRM, etc.)

Effective NTLM Relay Defenses

- Configure SMB auditing
- Configure NTLM auditing
- Add all AD Admin accounts to the Protected Users security group
- Enforce SMB signing
- Configure LDAP channel binding and LDAP signing
- Disable NTLM authentication where possible
- Enable Credential Guard



Azure AD/ Entra ID Attack Timelines

Microsoft Cloud Attacks

Note that dates may be inaccurate as I used the best available information on web sites and github to identify first use/publish date.

Azure AD/Entra ID Attack Timelines: “Baby Steps”(2016 – 2023)

2016

September: MailSniper Tool released by Beau Bullock

2017

January: Exploiting AAD Seamless Single Sign-On Article by Michael Grafnetter

May: original evilginx tool released by Kuba Gretzky (kgretzky)

August: Hacking the Cloud DEFCON Talk by Gerald Steere (Taya) & Sean Metcalf which identifies what later becomes known as the “Golden SAML Attack” and security concerns with Azure AD Connect

Golden SAML tool released

2018

July: evilginx2 tool released by Kuba Gretzky (kgretzky)

July: Microburst series of tools first released by Karl Fosaaen (kfosaaen)

October: AADInternals PowerShell module tool published by Dr Nestori Syynimaa (@DrAzureAD)

2019

February: Azure AD Connect for Red Teams by Adam Chester

August: Attacking & Defending the Microsoft Cloud (Azure AD & Office 365) Black Hat Talk by Mark Morowczynski & Sean Metcalf

August: Dirk-jan Mollema’s DEF CON 27 talk “I’m In Your Cloud Pwning Your Azure Environment”

adconnectdump tool released by Dirk-Jan Molema

MSOLSpray tool released by Beau Bullock

MFASweep Tool released by Beau Bullock

2020

ROADTools tool released by Dirk-Jan Molema

Invoke-AzureAdPasswordSprayAttack tool by Daniel Chronlund

2022

August: Midnight Blizzard MagicWeb ADFS hack

December: “Leveraging Microsoft Teams for Initial Access” article by Andrea Santese

2023

April: TeamsEnum tool released by Bastian Kanbach (bka-dev)

June: “Advisory: IDOR in Microsoft Teams Allows for External Tenants to Introduce Malware” article by Max Corbridge

July: TeamsPhisher tool released by Octoberfest7

Azure AD/Entra ID Attack Timelines: “Baby Steps”(2016 – 2023)

Tools

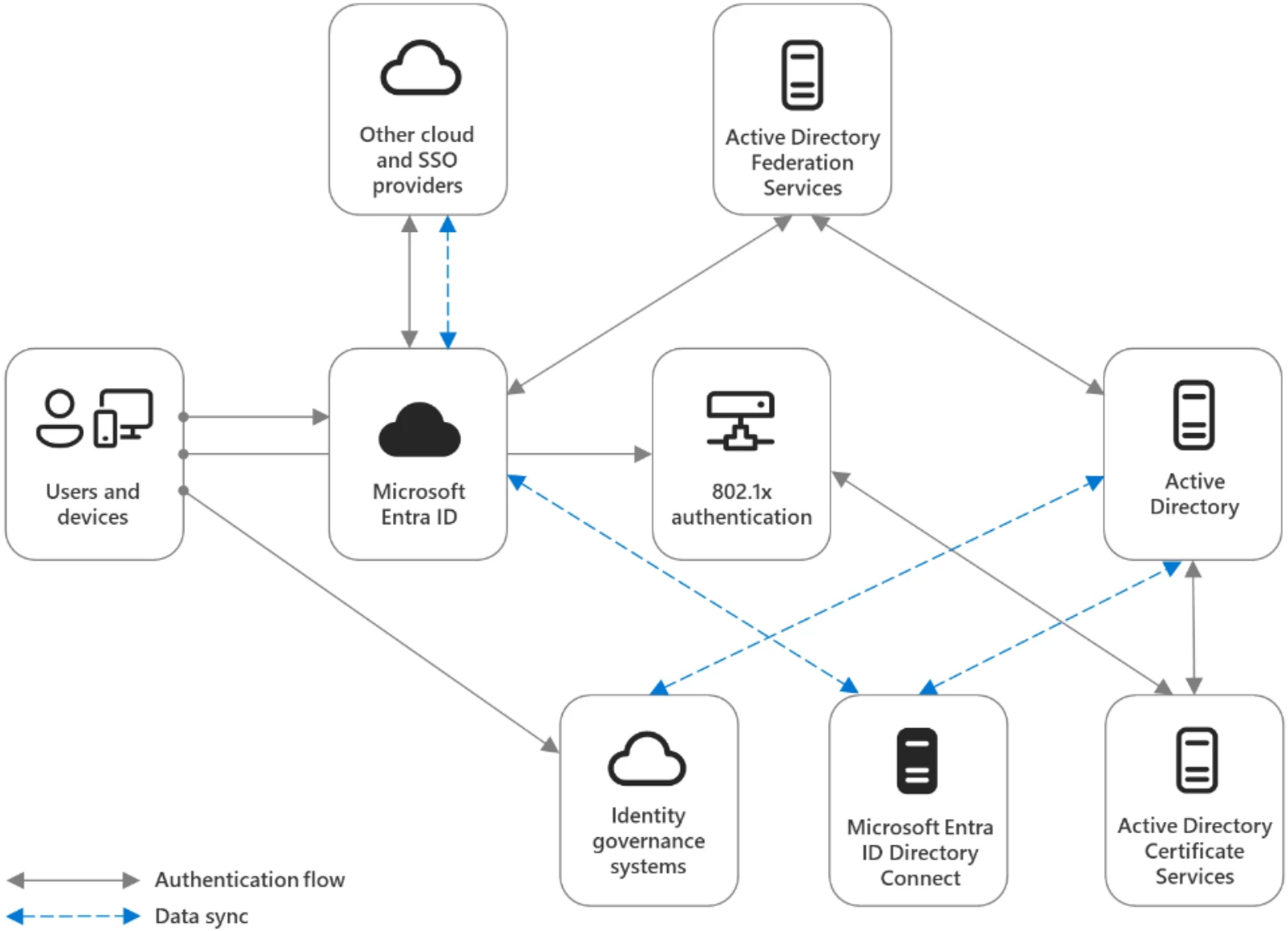
MailSniper
Evilginx
GoldenSAML
Evilginx2
Microburst
AADInternals
Aadconnectdump
MSOLSpray
MFASweep
ROADTools

Privilege Escalation

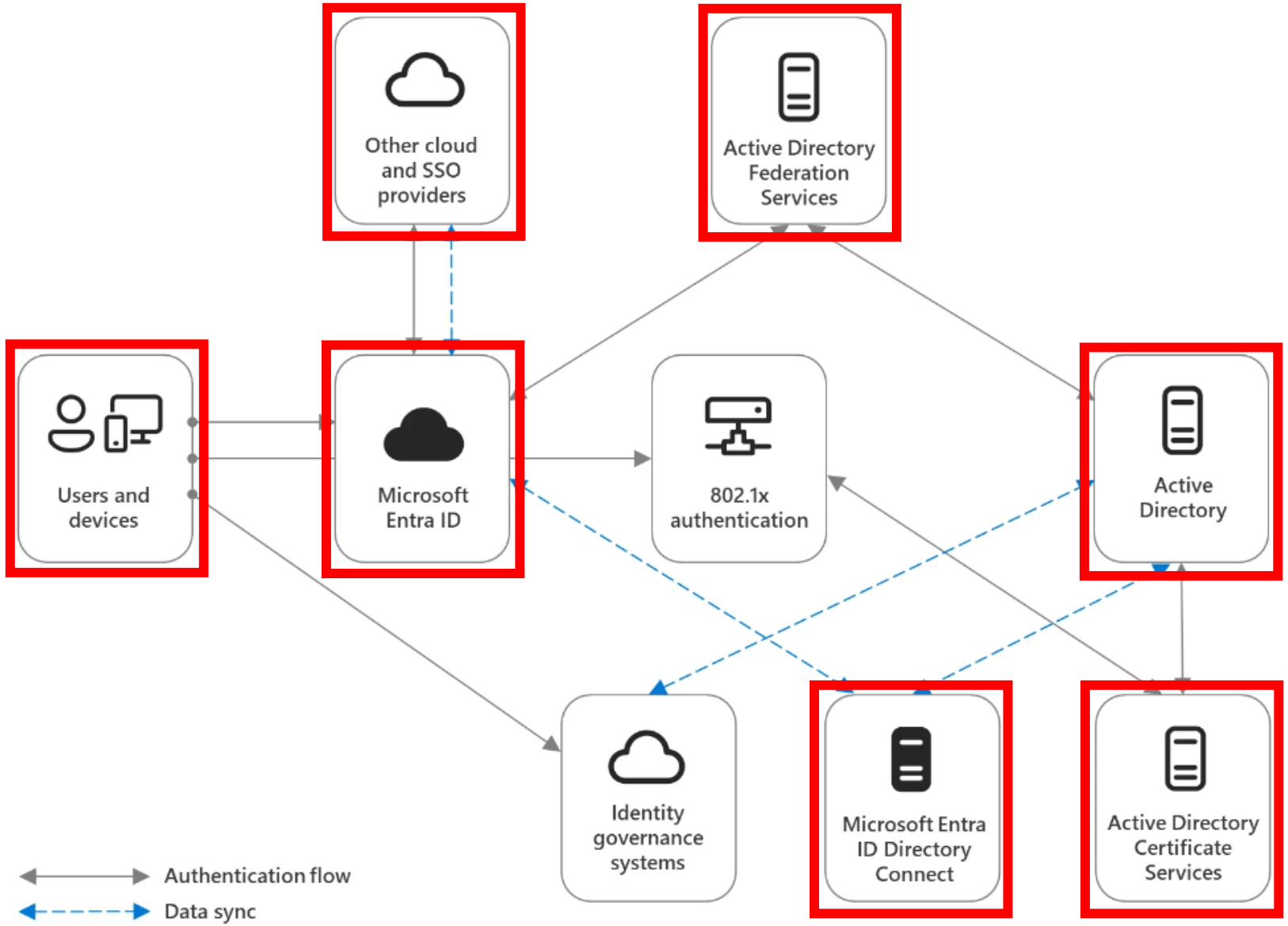
Evilginx
AADInternals
Aadconnectdump
ROADTools
MagicWeb

Persistence

GoldenSAML
AADInternals
MagicWeb



Microsoft Incident Response lessons on preventing cloud identity compromise | Microsoft Security Blog
https://www.microsoft.com/en-us/security/blog/2023/12/05/microsoft-incident-response-lessons-on-preventing-cloud-identity-compromise/



Microsoft Incident Response lessons on preventing cloud identity compromise | Microsoft Security Blog
https://www.microsoft.com/en-us/security/blog/2023/12/05/microsoft-incident-response-lessons-on-preventing-cloud-identity-compromise/

Entra ID Level 0

Like Tier 0, but Different!

Sean Metcalf | @PyroTek3 | sean@trimarcsecurity.com

There are **100+** Entra ID Roles!

Role	Description	Template ID
Application Administrator	Can create and manage all aspects of app registrations and enterprise apps.	9b895d92-2cd3-44c7-9d02-a6ac2d5ea5c3
Application Developer	Can create application registrations independent of the 'Users can register applications' setting.	cf1c38e5-3621-4004-a7cb-879624dced7c
Attack Payload Author	Can create attack payloads that an administrator can initiate later.	9c6df0f2-1e7c-4dc3-b195-66dfbd24aa8f
Attack Simulation Administrator	Can create and manage all aspects of attack simulation campaigns.	c430b396-e693-46cc-96f3-db01bf8bb62a
Attribute Assignment Administrator	Assign custom security attribute keys and values to supported Microsoft Entra objects.	58a13ea3-c632-46ae-9ee0-9c0d43cd7f3d
Attribute Assignment Reader	Read custom security attribute keys and values for supported Microsoft Entra objects.	ffd52fa5-98dc-465c-991d-fc073eb59f8f
Attribute Definition Administrator	Define and manage the definition of custom security attributes.	8424c6f0-a189-499e-bbd0-26c1753c96d4
Attribute Definition Reader	Read the definition of custom security attributes.	1d336d2c-4ae8-42ef-9711-b3604ce3fc2c
Attribute Log Administrator	Read audit logs and configure diagnostic settings for events related to custom security attributes.	5b784334-f94b-471a-a387-e7219fc49ca2
Attribute Log Reader	Read audit logs related to custom security attributes.	9c39539d-8186-4804-835f-fd51ef9e2dcd
Authentication Administrator	Can access to view, set and reset authentication method information for any non-admin user.	c4e39bd9-1100-46d3-8c65-fb160da0071f
Authentication Extensibility Administrator	Customize sign in and sign up experiences for users by creating and managing custom authentication extensions.	25a516ed-2fa0-40ea-a2d0-12923a21473a
Authentication Policy Administrator	Can create and manage the authentication methods policy, tenant-wide MFA settings, password protection policy, and vc	0526716b-113d-4c15-b2c8-68e3c22b9f80
Azure DevOps Administrator	Can manage Azure DevOps policies and settings.	e3973bdf-4987-49ae-837a-ba8e231c7286
Azure Information Protection Administrator	Can manage all aspects of the Azure Information Protection product.	7495fdc4-34c4-4d15-a289-98788ce399fd
B2C IEF Keyset Administrator	Can manage secrets for federation and encryption in the Identity Experience Framework (IEF).	aaf43236-0c0d-4d5f-883a-6955382ac081
B2C IEF Policy Administrator	Can create and manage trust framework policies in the Identity Experience Framework (IEF).	3edaf663-341e-4475-9f94-5c338ef6c070
Billing Administrator	Can perform common billing related tasks like updating payment information.	b0f54661-2d74-4c50-afa3-1ec803f12efe
Cloud App Security Administrator	Can manage all aspects of the Defender for Cloud Apps product.	892c5842-a9a6-463a-8041-72aa08ca3cf6
Cloud Application Administrator	Can create and manage all aspects of app registrations and enterprise apps except application proxy.	158c047a-c907-4556-b7ef-446551a6b5f7
Cloud Device Administrator	Limited access to manage devices in Microsoft Entra ID.	7698a772-787b-4ac8-901f-60d6b08affd2
Compliance Administrator	Can read and manage compliance configuration and reports in Microsoft Entra ID and Microsoft 365.	17315797-102d-40b4-93e0-432062caca18
Compliance Data Administrator	Creates and manages compliance content.	e6d1a23a-da11-4be4-9570-befc86d067a7
Conditional Access Administrator	Can manage Conditional Access capabilities.	b1be1c3e-b65d-4f19-8427-f6fa0d97feb9
Customer LockBox Access Approver	Can approve Microsoft support requests to access customer organizational data.	5c4f9dcd-47dc-4cf7-8c9a-9e4207cbfc91
Desktop Analytics Administrator	Can access and manage Desktop management tools and services.	38a96431-2bdf-4b4c-8b6e-5d3d8abac1a4
Directory Readers	Can read basic directory information. Commonly used to grant directory read access to applications and guests.	88d8e3e3-8f55-4a1e-953a-9b9898b8876b
Directory Synchronization Accounts	Only used by Microsoft Entra Connect service.	d29b2b05-8046-44ba-8758-1e26182fcf32
Directory Writers	Can read and write basic directory information. For granting access to applications, not intended for users.	9360feb5-f418-4baa-8175-e2a00bac4301
Domain Name Administrator	Can manage domain names in cloud and on-premises.	8329153b-31d0-4727-b945-745eb3bc5f31
Dynamics 365 Administrator	Can manage all aspects of the Dynamics 365 product.	44367163-eba1-44c3-98af-f5787879f96a
Dynamics 365 Business Central Administrator	Can access Dynamics 365 Business Central environments and perform all administrative tasks on the environments.	963797fb-eb3b-4cde-8ce3-5878b3f32a3f
Edge Administrator	Manage all aspects of Microsoft Edge.	3f1acade-1e04-4fbc-9b63-f0302cd84aef
Exchange Administrator	Can manage all aspects of the Exchange product.	29232cdf-9323-42fd-ade2-1d097af3e4de
Exchange Recipient Administrator	Can create or update Exchange Online recipients within the Exchange Online organization.	31392ffb-586c-42d1-9346-e59415a2cc4e
External ID User Flow Administrator	Can create and manage all aspects of user flows.	6e591065-9bad-43ed-90f3-e9424366d2f0
External ID User Flow Attribute Administrator	Can create and manage the attribute schema available to all user flows.	0f971eea-41eb-4569-a71e-57bb8a3eff1e
External Identity Provider Administrator	Can configure identity providers for use in direct federation.	be2f45a1-457d-42af-a067-6ec1fa63bc45
Fabric Administrator	Can manage all aspects of the Fabric and Power BI products.	a9ea8996-122f-4c74-9520-8edcd192826c
Global Administrator	Can manage all aspects of Microsoft Entra ID and Microsoft services that use Microsoft Entra identities.	62e90394-69f5-4237-9190-012177145e10
Global Reader	Can read everything that a Global Administrator can, but not update anything.	f2ef992c-3afb-46b9-b7cf-a126ee74c451
Global Secure Access Administrator	Create and manage all aspects of Microsoft Entra Internet Access and Microsoft Entra Private Access, including managin	ac434307-12b9-4fa1-a708-88bf58caabc1
Groups Administrator	Members of this role can create/manage groups, create/manage groups settings like naming and expiration policies, and v	fdd7a751-b60b-444a-984c-02652fe8fa1c
Guest Inviter	Can invite guest users independent of the 'members can invite guests' setting.	95e79109-95c0-4d8e-aee3-d01accf2d47b
Helpdesk Administrator	Can reset passwords for non-administrators and Helpdesk Administrators.	729827e3-9c14-49f7-bb1b-9608f156bbb8
Hybrid Identity Administrator	Can manage Active Directory to Microsoft Entra cloud provisioning, Microsoft Entra Connect, Pass-through Authenticat	8ac3fc64-6eca-42ea-9e69-59f4c7b60eb2
Identity Governance Administrator	Manage access using Microsoft Entra ID for identity governance scenarios.	45d8d3c5-c802-45c6-b32a-1d70b5e1e86e
Insights Administrator	Has administrative access in the Microsoft 365 Insights app.	eb1f4a8d-243a-41f0-9fbd-c7cdf6c5ef7c
Insights Analyst	Access the analytical capabilities in Microsoft Viva Insights and run custom queries.	25df335f-86eb-4119-b717-0ff02de207e9
Insights Business Leader	Can view and share dashboards and insights via the Microsoft 365 Insights app.	31e939ad-9672-4796-9c2e-873181342d2d
Intune Administrator	Can manage all aspects of the Intune product.	3a2c62db-5318-420d-8d74-23affee5d9d5
Kaizala Administrator	Can manage settings for Microsoft Kaizala.	74ef975b-6605-40af-a5d2-b9539d836353
Knowledge Administrator	Can configure knowledge, learning, and other intelligent features.	b5a8dcf3-09d5-43a9-a639-8e29ef291470
Knowledge Manager	Can organize, create, manage, and promote topics and knowledge.	744ec460-397e-42ad-a462-8b3f9747a02c
License Administrator	Can manage product licenses on users and groups.	4d6ac14f-3453-41d0-bef9-a3e0c569773a
Lifecycle Workflows Administrator	Create and manage all aspects of workflows and tasks associated with Lifecycle Workflows in Microsoft Entra ID.	59d46f88-662b-457b-bceb-5c3803e5908f
Message Center Privacy Reader	Can read security messages and updates in Office 365 Message Center only.	ac16e43d-7b2d-40e0-ac05-243ff356ab5b
Message Center Reader	Can read messages and updates for their organization in Office 365 Message Center only.	790c1fb3-7f7d-4f88-86a1-ef1f95c05c1b
Microsoft 365 Migration Administrator	Perform all migration functionality to migrate content to Microsoft 365 using Migration Manager.	8c8b803f-96e1-4129-9349-20738d9f9652
Microsoft Entra Joined Device Local Administ	Users assigned to this role are added to the local administrators group on Microsoft Entra joined devices.	9f06204d-73c1-4d4c-880a-6edb90606fd8
Microsoft Hardware Warranty Administrator	Create and manage all aspects warranty claims and entitlements for Microsoft manufactured hardware, like Surface and Hc	1501b917-7653-4ff9-a4b5-203eaf33784f
Microsoft Hardware Warranty Specialist	Create and read warranty claims for Microsoft manufactured hardware, like Surface and HoloLens.	281fe777-fb20-4fbb-b7a3-ccebce5b0d96
Modern Commerce Administrator	Can manage commercial purchases for a company, department or team.	d24aef57-1500-4070-84db-2666f29cf966
Network Administrator	Can manage network locations and review enterprise network design insights for Microsoft 365 Software as a Service ap	d37c8bed-0711-4417-ba38-b4abe66ce4c2
Office Apps Administrator	Can manage Office apps cloud services, including policy and settings management, and manage the ability to select, unsele	2b745bdf-0803-4d80-aa65-822c4493daac
Organizational Branding Administrator	Manage all aspects of organizational branding in a tenant.	92ed04bf-c94a-4b82-9729-b799a7a4c178
Organizational Messages Approver	Review, approve, or reject new organizational messages for delivery in the Microsoft 365 admin center before they are se	e48398e2-f4bb-4074-8f31-4586725e205b
Organizational Messages Writer	Write, publish, manage, and review the organizational messages for end-users through Microsoft product surfaces.	507f53e4-4e52-4077-abd3-d2e1558b6ea2
Partner Tier1 Support	Do not use - not intended for general use.	4ba39ca4-527c-499a-b93d-d9b492c50246
Partner Tier2 Support	Do not use - not intended for general use.	e00e864a-17c5-4a4b-9c06-f5b95a8d5bd8
Password Administrator	Can reset passwords for non-administrators and Password Administrators.	966707d0-3269-4727-9be2-8c3a10f19b9d
Permissions Management Administrator	Manage all aspects of Microsoft Entra Permissions Management.	af78dc32-cf4d-46f9-ba4e-4428526346b5
Power Platform Administrator	Can create and manage all aspects of Microsoft Dynamics 365, Power Apps and Power Automate.	11648597-926c-4cf3-9c36-bcebb0ba8dcc
Printer Administrator	Can manage all aspects of printers and printer connectors.	644ef478-e28f-4e28-b9dc-3fdde9aa0b1f
Printer Technician	Can register and unregister printers and update printer status.	e8cef6f1-e4bd-4ea8-bc07-4b8d950f4477
Privileged Authentication Administrator	Can access to view, set and reset authentication method information for any user (admin or non-admin).	7be44c8a-adaf-4e2a-84d6-ab2649e08a13
Privileged Role Administrator	Can manage role assignments in Microsoft Entra ID, and all aspects of Privileged Identity Management.	e8611ab8-c189-46e8-94e1-60213ab1f814
Reports Reader	Can read sign-in and audit reports.	4a5d8f65-41da-4de4-8968-e035b65339cf
Search Administrator	Can create and manage all aspects of Microsoft Search settings.	0964bb5e-9bdb-4d7b-ac29-58e794862a40
Search Editor	Can create and manage the editorial content such as bookmarks, Q and As, locations, floorplan.	8835291a-918c-4fd7-a9ce-faa49f0cf7d9
Security Administrator	Can read security information and reports, and manage configuration in Microsoft Entra ID and Office 365.	194ae4cb-b126-40b2-bd5b-6091b380977d
Security Operator	Creates and manages security events.	5f2222b1-57c3-48ba-8ad5-d4759f1fde6f
Security Reader	Can read security information and reports in Microsoft Entra ID and Office 365.	5d6b6bb7-de71-4623-b4af-96380a352509
Service Support Administrator	Can read service health information and manage support tickets.	f023fd81-a637-4b56-95fd-791ac0226033
SharePoint Administrator	Can manage all aspects of the SharePoint service.	f28a1f50-f6e7-4571-818b-6a12f2af6b6c
Skype for Business Administrator	Can manage all aspects of the Skype for Business product.	75941009-915a-4869-abe7-691bff18279e
Teams Administrator	Can manage the Microsoft Teams service.	69091246-20e8-4a56-aa4d-066075b2a7a8
Teams Communications Administrator	Can manage calling and meetings features within the Microsoft Teams service.	baf37b3a-610e-45da-9e62-d9d1e5e8914b
Teams Communications Support Engineer	Can troubleshoot communications issues within Teams using advanced tools.	f70938a0-fc10-4177-9e90-2178f8765737
Teams Communications Support Specialist	Can troubleshoot communications issues within Teams using basic tools.	fcf91098-03e3-41a9-b5ba-6f0ec8188a12
Teams Devices Administrator	Can perform management related tasks on Teams certified devices.	3d762c5a-1b6c-493f-843e-55a3b42923d4
Tenant Creator	Create new Microsoft Entra or Azure AD B2C tenants.	112ca1a2-15ad-4102-995e-45b0bc479a6a
Usage Summary Reports Reader	Read Usage reports and Adoption Score, but can't access user details.	75934031-6c7e-415a-99d7-48dbd49e875e
User Administrator	Can manage all aspects of users and groups, including resetting passwords for limited admins.	fe930be7-5e62-47db-91af-98c3a49a38b1
Virtual Visits Administrator	Manage and share Virtual Visits information and metrics from admin centers or the Virtual Visits app.	e300d9e7-4a2b-4295-9eff-f1c78b36cc98
Viva Goals Administrator	Manage and configure all aspects of Microsoft Viva Goals.	92b086b3-e367-4ef2-b869-1de128fb986e
Viva Pulse Administrator	Can manage all settings for Microsoft Viva Pulse app.	87761b17-1ed2-4af3-9acd-92a150038160
Windows 365 Administrator	Can provision and manage all aspects of Cloud PCs.	11451d60-acb2-45eb-a7d6-43d0f0125c13
Windows Update Deployment Administrator	Can create and manage all aspects of Windows Update deployments through the Windows Update for Business deploym	32696413-001a-46ae-978c-ce0f6b3620d2
Yammer Administrator	Manage all aspects of the Yammer service.	810a2642-a034-447f-a5e8-41beaa378541

Microsoft's Privileged Entra ID Roles List [PRIVILEGED]

- Application Administrator
- Application Developer
- Authentication Administrator
- Authentication Extensibility Administrator
- B2C IEF Keyset Administrator
- Cloud Application Administrator
- Cloud Device Administrator
- Conditional Access Administrator
- Directory Synchronization Accounts
- Directory Writers
- Domain Name Administrator
- External Identity Provider Administrator
- Global Administrator
- Global Reader
- Helpdesk Administrator
- Hybrid Identity Administrator
- Intune Administrator
- Partner Tier1 Support
- Partner Tier2 Support
- Password Administrator
- Privileged Authentication Administrator
- Privileged Role Administrator
- Security Administrator
- Security Operator
- Security Reader
- User Administrator

As of:
4/22/2024

26 roles: https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/permissions-reference

Microsoft's Privileged Entra ID Roles List [PRIVILEGED]

- *Application Administrator*
- Application Developer
- Authentication Administrator
- Authentication Extensibility Administrator
- B2C IEF Keyset Administrator
- *Cloud Application Administrator*
- Cloud Device Administrator
- Conditional Access Administrator
- Directory Synchronization Accounts
- **Directory Writers**
- Domain Name Administrator
- External Identity Provider Administrator
- **Global Administrator**
- Global Reader
- Helpdesk Administrator
- **Hybrid Identity Administrator**
- Intune Administrator
- Partner Tier1 Support
- **Partner Tier2 Support**
- Password Administrator
- **Privileged Authentication Administrator**
- **Privileged Role Administrator**
- Security Administrator
- Security Operator
- Security Reader
- User Administrator

As of: 4/22/2024

26 roles: https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/permissions-reference

Trimarc Level 0 Entra ID Roles (5)

Effective Full Admin Rights or Capability to Gain Full Admin to Entra ID

- **Global Administrator**
  - Full admin rights to the Entra ID, Microsoft 365, and 1-click full control of all Azure subscriptions
    From Azure AD to Active Directory (via Azure) – An Unanticipated Attack Path (2020)
- **Hybrid Identity Administrator**
  - *"Can create, manage and deploy provisioning configuration setup from Active Directory to Microsoft Entra ID using Cloud Provisioning as well as manage Microsoft Entra Connect, Pass-through Authentication (PTA), Password hash synchronization (PHS), Seamless Single Sign-On (Seamless SSO), and **federation settings**."*
    https://medium.com/tenable-techblog/roles-allowing-to-abuse-entra-id-federation-for-persistence-and-privilege-escalation-df9ca6e58360
- **Partner Tier2 Support**
  - *"The Partner Tier2 Support role can reset passwords and invalidate refresh tokens for all non-administrators and administrators (including Global Administrators). "*

    "not quite as powerful as Global Admin, but the role does allow a principal with the role to promote themselves or any other principal to Global Admin."
    The Most Dangerous Entra Role You've (Probably) Never Heard Of
- **Privileged Authentication Administrator**
  - *Microsoft: "do not use."*
    "Set or reset any authentication method (including passwords) for any user, including Global Administrators. …
    Force users to re-register against existing non-password credential (such as MFA or FIDO) and revoke remember MFA on the device, prompting for MFA on the next sign-in of all users."
- **Privileged Role Administrator**
  - *"Users with this role can manage role assignments in Microsoft Entra ID, as well as within Microsoft Entra Privileged Identity Management. …*
    This role grants the ability to manage assignments for all Microsoft Entra roles including the Global Administrator role. "

https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/permissions-reference

Trimarc Level 1 Entra ID Roles (1 of 2)

Highly Privileged Rights that have Privilege Escalation Potential Depending on Tenant Configuration or ability to reconfigure the security posture of the tenant

Role	Microsoft Description
Application Administrator	This is a privileged role. Users in this role can create and manage all aspects of enterprise applications, application registrations, and application proxy settings.
Authentication Administrator	This is a privileged role. Set or reset any authentication method (including passwords) for non-administrators and some roles. Require users who are non-administrators or assigned to some roles to re-register against existing non-password credentials (for example, MFA or FIDO), and can also revoke remember MFA on the device, which prompts for MFA on the next sign-in. Perform sensitive actions for some users.
Domain Name Administrator	This is a privileged role. Users with this role can manage (read, add, verify, update, and delete) domain names. Can be used in federation attacks.
Microsoft Entra Joined Device Local Administrator	During Microsoft Entra join, this group is added to the local Administrators group on the device.
Cloud Application Administrator	This is a privileged role. Users in this role have the same permissions as the Application Administrator role, excluding the ability to manage application proxy. This role grants the ability to create and manage all aspects of enterprise applications and application registrations.
Conditional Access Administrator	This is a privileged role. Users with this role have the ability to manage Microsoft Entra Conditional Access settings.
Directory Synchronization Accounts	This is a privileged role. Do not use. This role is automatically assigned to the Microsoft Entra Connect service, and is not intended or supported for any other use. Privileged rights: Update application credentials, Manage hybrid authentication policy in Microsoft Entra ID, Update basic properties on policies, & Update credentials of service principals
Directory Writers	This is a privileged role. Users in this role can read and update basic information of users, groups, and service principals. Privileged rights: Create & update OAuth 2.0 permission grants, add/disable/enable users, Force sign-out by invalidating user refresh tokens, & Update User Principal Name of users.

https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/permissions-reference

Trimarc Level 1 Entra ID Roles (2 of 2)

Highly Privileged Rights that have Privilege Escalation Potential Depending on Tenant Configuration or ability to reconfigure the security posture of the tenant

Role	Microsoft Description
Exchange Administrator	Users with this role have global permissions within Microsoft Exchange Online. Trimarc flags this role since it is a role that threat actors target.
External Identity Provider Administrator	This is a privileged role. This administrator manages federation between Microsoft Entra organizations and external identity providers. With this role, users can add new identity providers and configure all available settings (e.g. authentication path, service ID, assigned key containers). This user can enable the Microsoft Entra organization to trust authentications from external identity providers.
Helpdesk Administrator	This is a privileged role. Users with this role can change passwords, & invalidate refresh tokens, Invalidating a refresh token forces the user to sign in again.
Intune Administrator	This is a privileged role. Users with this role have global permissions within Microsoft Intune Online, when the service is present. Additionally, this role contains the ability to manage users and devices in order to associate policy, as well as create and manage groups. Privileged rights: Read Bitlocker metadata and key on devices
Password Administrator	This is a privileged role. Users with this role have limited ability to manage passwords.
Partner Tier1 Support	This is a privileged role. Do not use. The Partner Tier1 Support role can reset passwords and invalidate refresh tokens for only non-administrators. Privileged rights: Update application credentials, Create and delete OAuth 2.0 permission grants, & read and update all properties
Security Administrator	This is a privileged role. Users with this role have permissions to manage security-related features in the Microsoft 365 Defender portal, Microsoft Entra ID Protection, Microsoft Entra Authentication, Azure Information Protection, and Microsoft Purview compliance portal.
User Administrator	This is a privileged role. Can reset passwords for users.

https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/permissions-reference

Azure Privilege Escalation via Service Principal Abuse

Andy Robbins · Follow

Published in Posts By SpecterOps Team Members · 10 min read · Oct 12, 2021

Can a User with Role in Column A reset a password for a user with a Role in Row 2?

	(No Role)	Global Administrator	Privileged Authentication Administrator	Helpdesk Administrator	Authentication Administrator	User Administrator	Password Administrator	Directory Readers	Guest Inviter	Message Center Reader	Privileged Role Administrator	Reports Reader	Groups Administrator	(Any Other Role)
Global Administrator	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Privileged Authentication Administrator	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Helpdesk Administrator	Yes	No	No	Yes	Yes	No	No	Yes	Yes	Yes	No	Yes	No	No
Authentication Administrator	Yes	No	No	Yes	Yes	No	No	Yes	Yes	Yes	No	Yes	No	No
User Administrator	Yes	No	No	Yes	No	Yes	No	Yes	Yes	Yes	No	Yes	No	No
Password Administrator	Yes	No	No	No	No	No	Yes	Yes	Yes	No	No	No	No	No

https://posts.specterops.io/azure-privilege-escalation-via-service-principal-abuse-210ae2be2a5

From TEC 2022

Background

Highly Sensitive Application Permissions:

- **Directory.ReadWrite.All**: Effective Global Admin rights to AAD
- **RoleManagement.ReadWrite.Directory**: Ability to add members to Global Administrator and other roles
- **Application.ReadWrite.All**: Provides full rights to applications which could result in compromise if there are apps with highly privileged permissions
- **AppRoleAssignment.ReadWrite.All**: Provides the application the right to grant additional permissions to itself!

https://learn.microsoft.com/en-us/graph/permissions-reference

Trimarc Level 0 Applications

Effective Full Admin Rights or Capability to Gain Full Admin to Entra ID

Directory.ReadWrite.All	• "Directory.ReadWrite.All grants access that is broadly equivalent to a global tenant admin." *
AppRoleAssignment.ReadWrite.All	• Allows the app to manage permission grants for application permissions to any API & application assignments for any app, on behalf of the signed-in user. **This also allows an application to grant additional privileges to itself, other applications, or any user.**
RoleManagement.ReadWrite.Directory	• Allows the app to read & manage the role-based access control (RBAC) settings for the tenant, without a signed-in user. This includes instantiating directory roles & **managing directory role membership**, and reading directory role templates, directory roles and memberships.
Application.ReadWrite.All	• Allows the calling app to create, & manage (read, update, update application secrets and delete) applications & service principals without a signed-in user. This also allows an application to act as other entities & use the privileges they were granted.

Sean Metcalf | @PyroTek3 | sean@trimarcsecurity.com

Conditional Access Policies

… and the Gaps therein

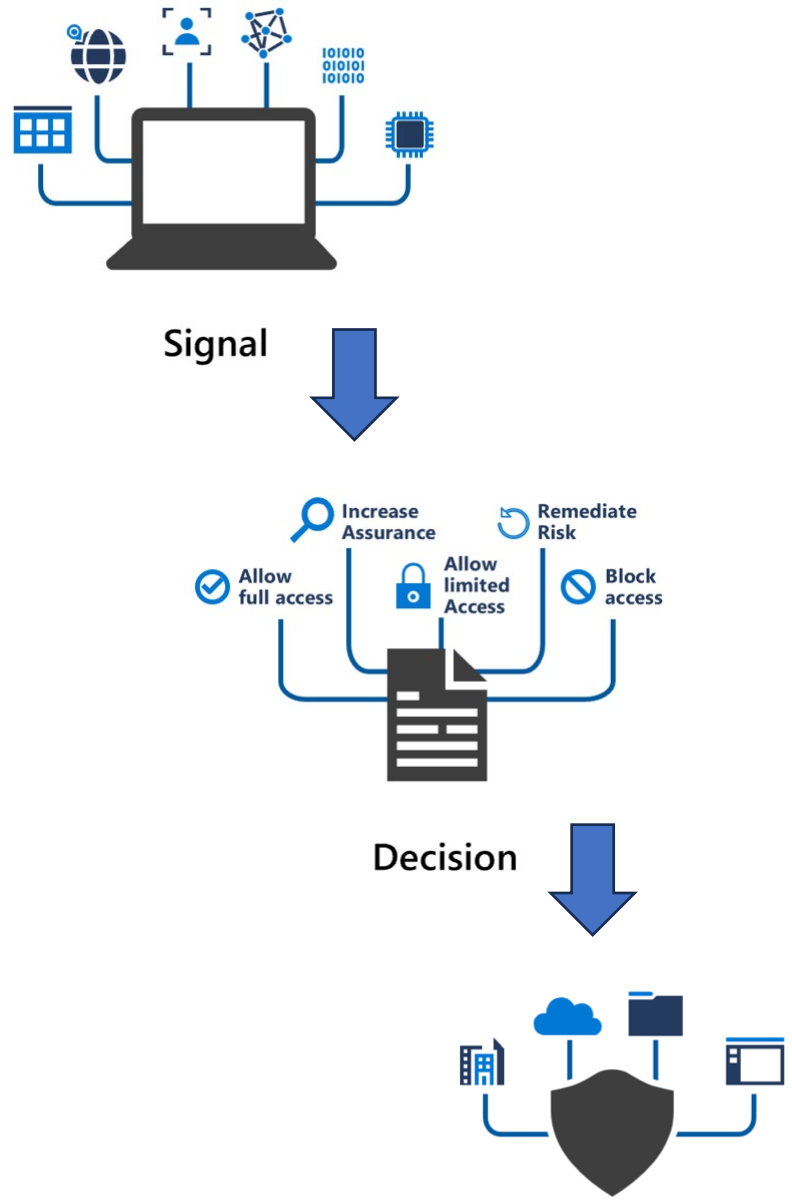
Conditional Access Policies

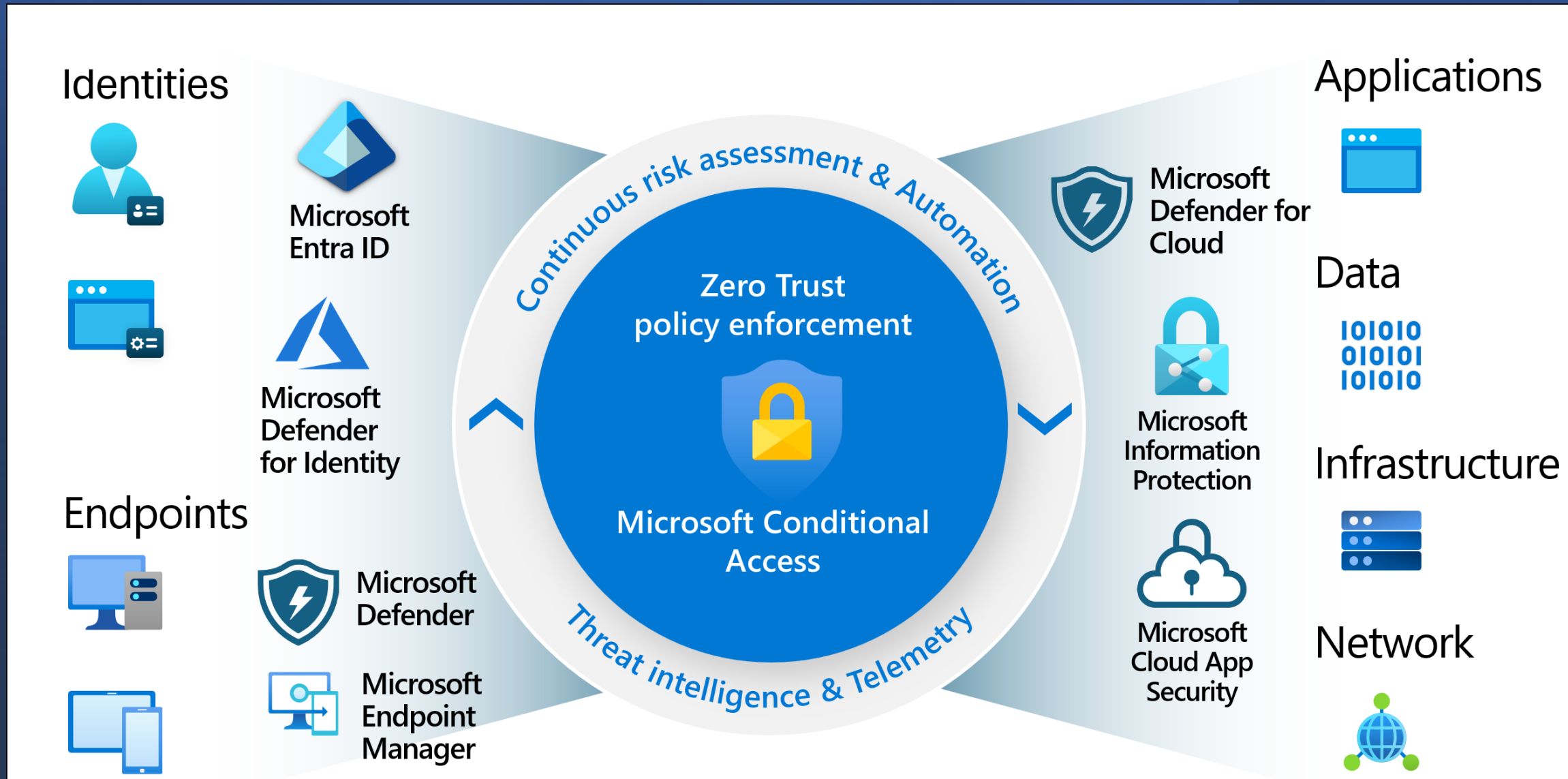
Policies apply after (first-factor) authentication

Requires P1 licensing

Rules based on:

- Who is connecting?
- Where are they connecting (from)?
- What app and/or device is connecting?
- When does this apply?




Identities
Microsoft Entra ID
Microsoft Defender for Identity
Endpoints
Microsoft Defender
Microsoft Endpoint Manager
Continuous risk assessment & Automation
Zero Trust policy enforcement
Microsoft Conditional Access
Threat intelligence & Telemetry
Microsoft Defender for Cloud
Microsoft Information Protection
Microsoft Cloud App Security
Applications
Data
Infrastructure
Network

Conditional Access | Policies

Microsoft Entra ID

- Overview
- Policies
- Insights and reporting
- Diagnose and solve problems
- Manage
  - Named locations
  - Custom controls (Preview)
  - Terms of use
  - VPN connectivity
  - Authentication contexts
  - Authentication strengths
  - Classic policies
- Monitoring
- Troubleshooting + Support

Microsoft Entra Conditional Access policies are used to apply access controls to keep your organization secure. Learn more

All policies

8

Total

Microsoft-managed policies

0

out of 8

Search

Add filter

8 out of 8 policies found

Policy name	State	Creation date	Modified date
CA001: Require multi-factor authentication for admins	Report-only	5/29/2022, 11:10:03 PM	5/29/2022, 11:19:17 PM
CA003: Block legacy authentication	Report-only	5/29/2022, 11:10:15 PM	
CA005: Require multi-factor authentication for guest access	Report-only	5/29/2022, 11:10:28 PM	
CA007: Require multi-factor authentication for risky sign-ins	Report-only	5/29/2022, 11:10:39 PM	
Require compliant or hybrid Azure AD joined device or multifactor authentic...	Report-only	1/19/2024, 3:13:25 PM	
Require multifactor authentication for Azure management	Report-only	1/19/2024, 3:13:13 PM	
Require multifactor authentication for all users	Report-only	1/19/2024, 3:12:52 PM	
Securing security info registration	Report-only	1/19/2024, 3:12:31 PM	

Common Conditional Access Policies

Require users to use MFA when connecting outside of the corporate network

Require MFA for users with certain administrative roles

Block legacy authentication (username & password auth)

Block/Grant access from specific locations

CA Policy Gap #1:
Users Require MFA Outside of Corp Network

- CAP requires users to MFA when they are working remotely (not on the corporate network or connected via VPN)
- Assumes no attacker would be on the corporate network
- Attacker can use username/password without having to MFA
- Fun Fact: Attackers love SSO!

CA Policy Gap #2: Admins don't require MFA

- MFA is required for certain users to access specific applications
- However, there is no CAP that requires MFA for Admins
- Or… CAP only requires members of a few roles use MFA
- Attacker can use username/password without having to MFA
- Fun Fact: Attackers love SSO!

CA Policy Gap #3: Exclusions

- CAP includes several security controls
  - MFA required
  - AAD Joined &Compliant device
  - Location based access
- However, there are exclusions:
  - Admins
  - VIPs
  - Executives
  - HR
  - Etc
- This creates a significant gap in security posture
- Attackers love being excluded from security controls!

Microsoft Provided Conditional Access Policies

Baseline Policies

Conditional Access Templates

Microsoft Managed Policies

Baseline Policies

Policy Name	State
Baseline policy: Require MFA for admins (Preview)	On
Baseline policy: End user protection (Preview)	On
Baseline policy: Block legacy authentication (Preview)	On
Baseline policy: Require MFA for Service Management (...	On

Security Defaults

Security defaults

Security defaults are basic identity security mechanisms recommended by Microsoft. When enabled, these recommendations will be automatically enforced in your organization. Administrators and users will be better protected from common identity-related attacks.

Learn more

Your organization is protected by security defaults.

Manage security defaults

Microsoft Provided Conditional Access Policies

~~Baseline Policies~~

Conditional Access Templates

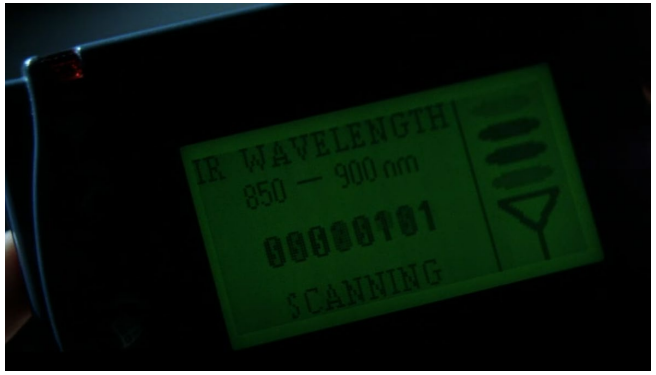
Microsoft Managed Policies

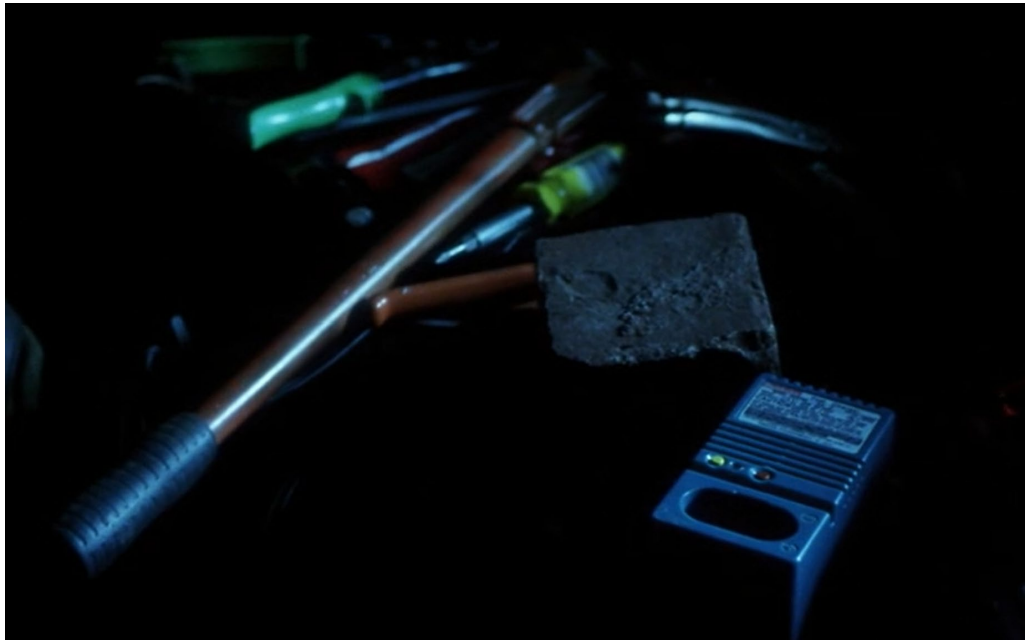
Microsoft Managed Policies (MMP)

- Deployed automatically in reporting mode
- Modification is limited:
  - Exclude users
  - Turn on or set to Report-only mode
  - Can't rename or delete any Microsoft-managed policies
  - Can duplicate the policy to make custom versions
- Microsoft might update these policies in the future
- MMPs turn on (set to enabled) 90 days after introduced to the tenant
- Currently focuses on 3 areas:
  - MFA for admins accessing Microsoft Admin Portals
  - MFA for per-user MFA configured on users
  - MFA and reauthentication for risky sign-ins

https://learn.microsoft.com/en-us/entra/identity/conditional-access/managed-policies

Attacking Azure AD/Entra ID





Phishing for Admins

Re: Office 365 Licenses Expired. - Message (HTML)

FILE MESSAGE

https://www.bleepingcomputer.com/news/security/phishers-target-office-365-admins-with-fake-admin-alerts/

Fri 4/12/2019 1:55 PM

Customer Support <xbox_.live.ww.00.en.vmc.rmd.ts.t03.spt.ua.pi@outlook.com>

Re: Office 365 Licenses Expired.

To [redacted]

This message was sent with High importance.

Office 365 Microsoft

®Office 365- Check Your Payment Information

Sign in to the Office 365 Admin center To Check Your Payment Information

View this message in the Office 365 message center

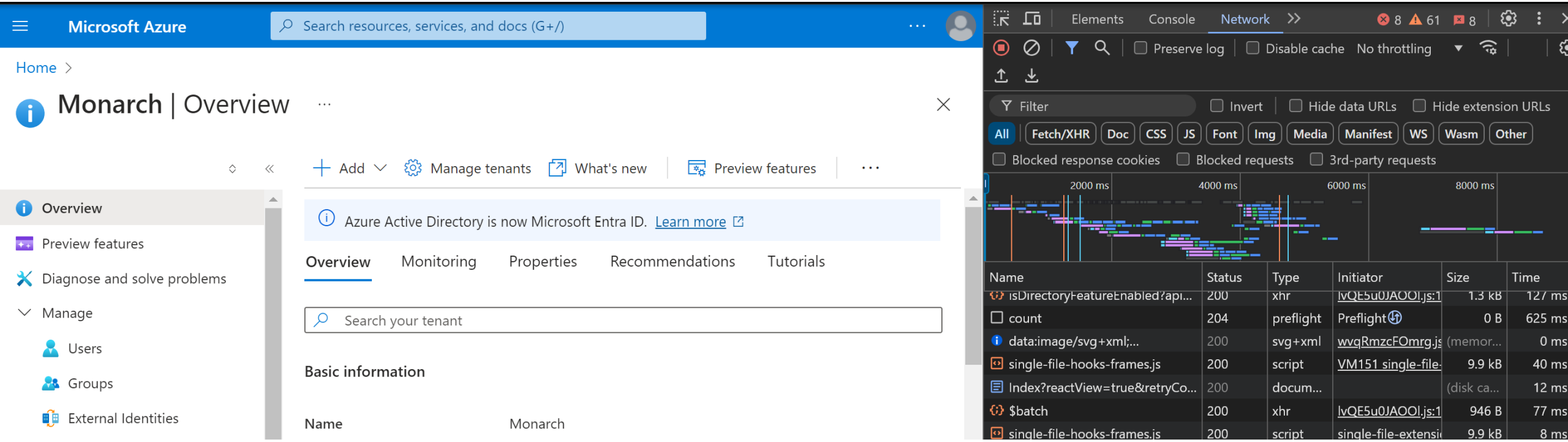
To customize what's included in this email, who gets it, or to unsubscribe, set your Message center preferences.

Edit release preferences
Choose the release track for your organization. Use these settings to join First Release if you haven't already.

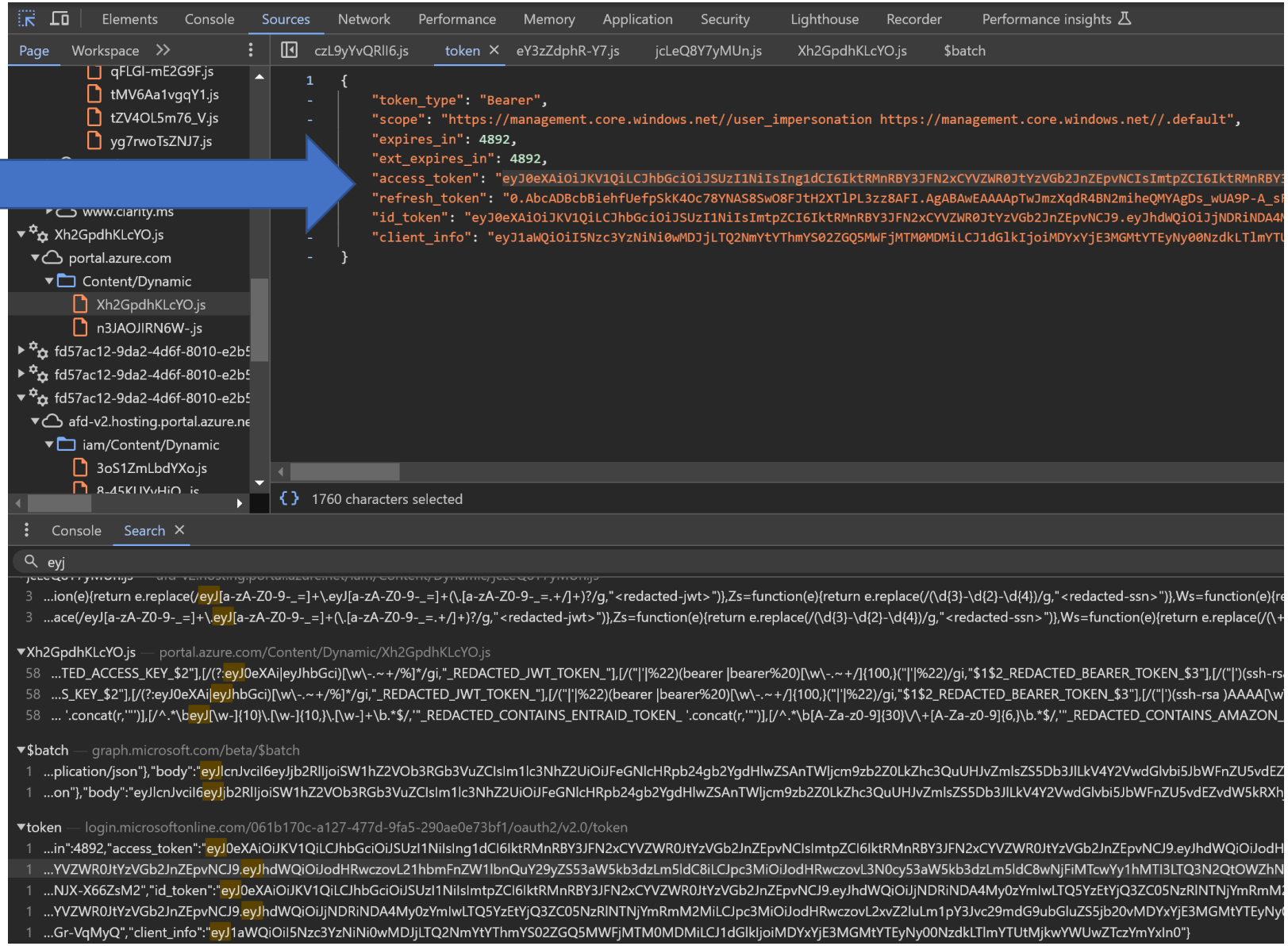
Microsoft respects your privacy. To learn more, please read our Privacy Statement.

Microsoft Corporation
One Microsoft Way
Redmond, WA, USA 98052

Stealing Tokens from the Web Browser



Stealing Tokens from the Web Browser



Stealing Access Token from the Web Browser

jwt.ms

Decoded Token | Claims


```
{
  "typ": "JWT",
  "alg": "RS256",
  "x5t": "KQ2tAcrE7lBaVVGBmc5Fob                ",
  "kid": "KQ2tAcrE7lBaVVGBmc5F                 "
}.{
  "aud": "https://management.core.windows.net/",
  "iss": "https://sts.windows.net/061b170c-a127-477d-9fa5-290ae0e73bf1/",
  "iat": 1723060777,
  "nbf": 1723060777,
  "exp": 1723065970,
  "acr": "1",
  "aio": "AVQAq/8XAAAAIqLZWy2NuIy
  "amr": [
    "pwd",
    "mfa"
  ],
  "appid": "c44b4083-3bb0-                              ",
  "appidacr": "0",
  "groups": [
    "fe1bc310-                                  "
  ],
  "idtyp": "user",
  "ipaddr": "136.179.21.70",
  "name": "Sean Metcalf",
  "oid": "9777c3b6-002c-46                                ",
  "puid": "100320037D4                ",
  "rh": "0.AbcADBcbBiehfUefpSkK4Oc7                                          .",
  "scp": "user_impersonation",
  "sub": "bT0T7_pKncPMRCvZbs-WtRw                                          ",
  "tid": "061b170c-a127-477d-9fa5-
  "unique_name": "sean@monarchsciences.org",
  "upn": "sean@monarchsciences.org",
  "uti": "QTkBIWbMpE                ",
```

That’s It!
Now we have the Access Token

Stealing Tokens from the Web Browser

AADInternals.com

The ultimate Entra ID (Azure AD) / Microsoft 365 hacking and admin toolkit

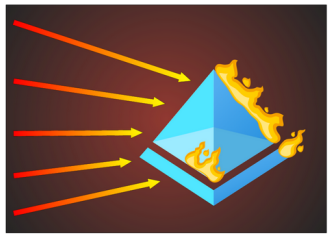
AAD KILL CHAIN | DOCUMENTATION | LINKS | OSINT | TALKS | TOOLS

Exfiltrating NTHashes by abusing Microsoft Entra Domain Services

January 13, 2024 (Last Modified: January 14, 2024)

Last year I gave a presentation titled **Dumping NTHashes from Azure AD** at TROOPERS conference. The talk was about how the **Microsoft Entra Domain Services** (formerly Azure AD Domain Services) works and how it enabled dumping NTHashes from Entra ID (formerly Azure AD).

In this blog, I'll show how Microsoft Entra Domain Services (MEDS) can be (ab)used to exfiltrate NTHashes from on-prem Active Directory.



DoSing Azure AD

July 02, 2023

My recent talk at the great **T2** conference on DoSing Azure AD gained a lot of attention. Unfortunately, the talk was not recorded, so I decided to write a blog for those who couldn't attend. So here we go!

Deploying users with pre-registered MFA

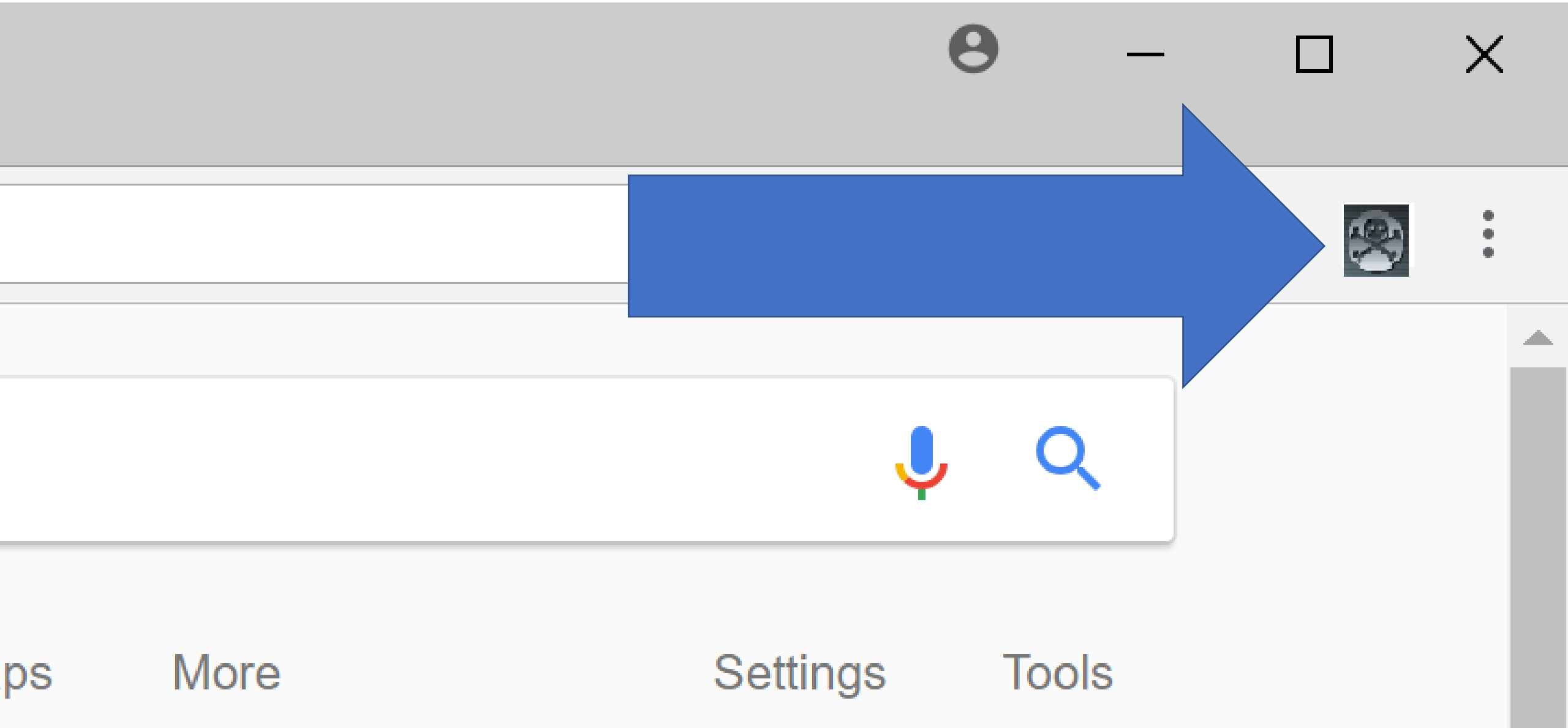
May 23, 2023 (Last Modified: May 24, 2023)

A couple of weeks ago a friend of mine asked would it be possible to pre-register MFA for users in Azure AD. For short, yes it is!

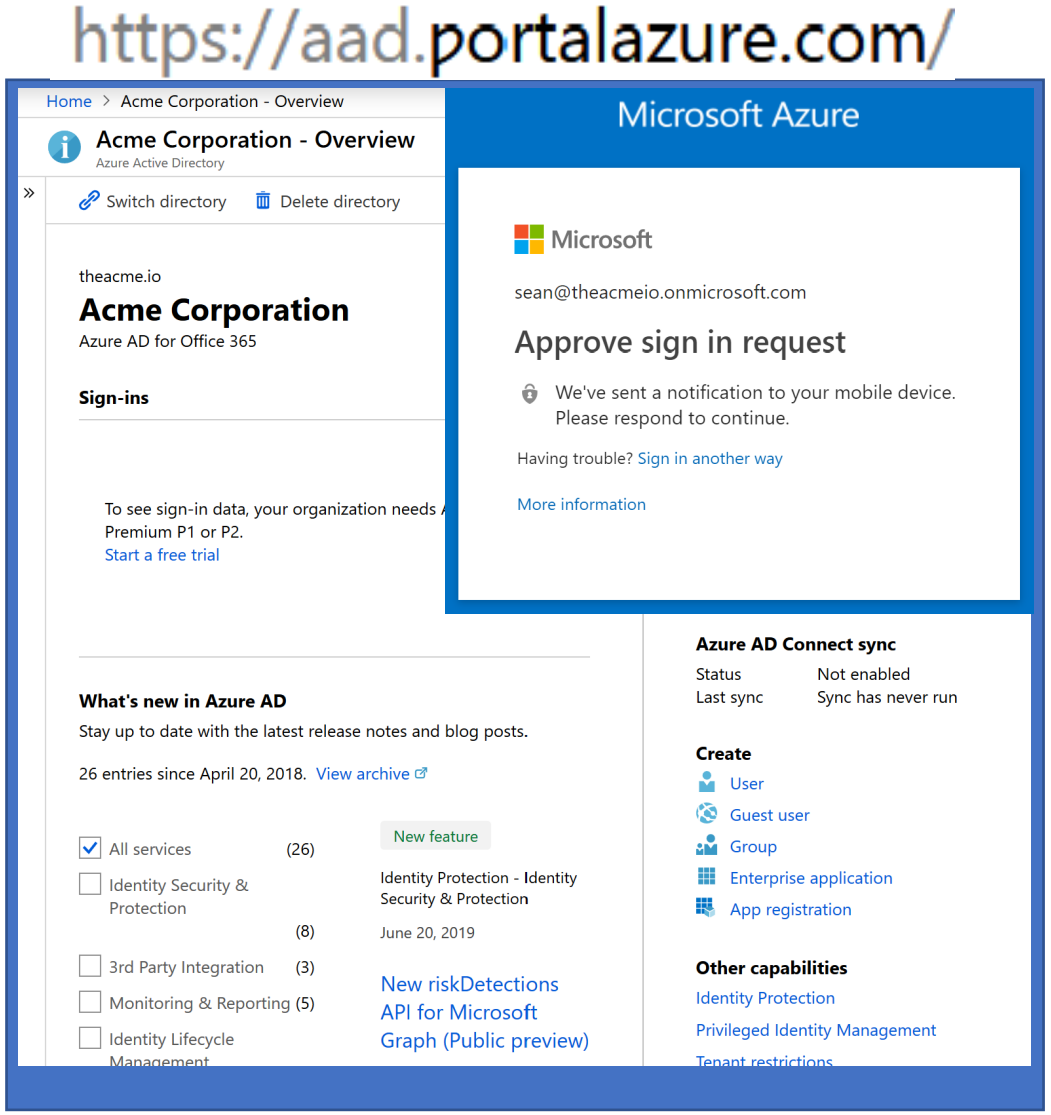
In this blog, I'll show how to pre-register **OTP** and **SMS** MFA methods using **AADInternals'** **Register-AADIntMFAApp** and **Set-AADIntUserMFA**.

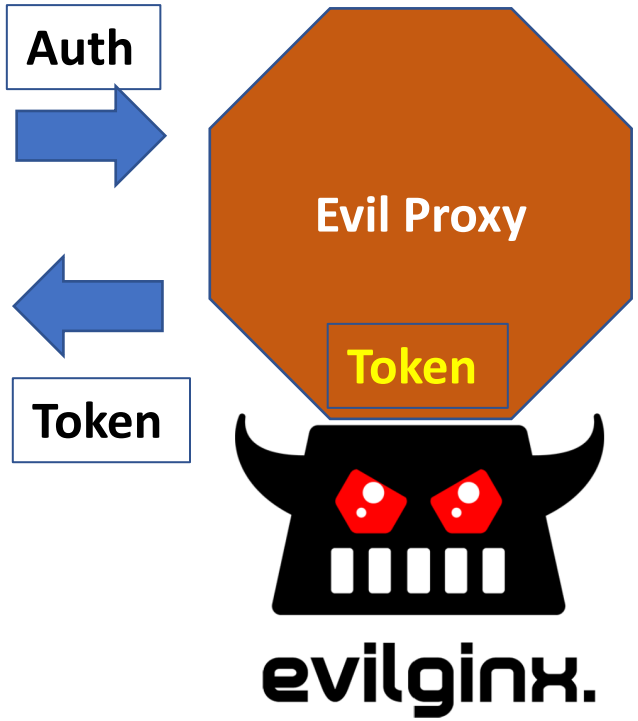
Special THANK YOU to DrAzureAD himself, Dr. Nestori Syynimaa for his help with this section!

Token Theft with Browser Extension

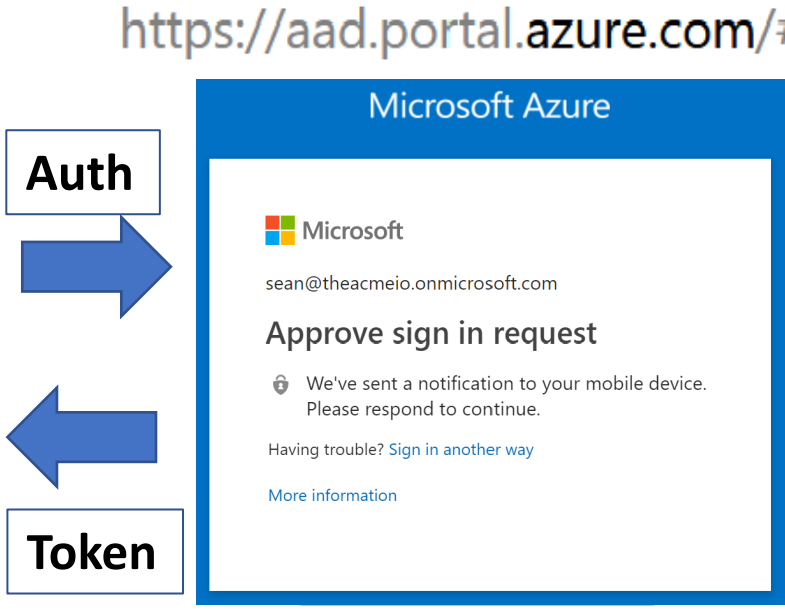


Token Theft with evilginx

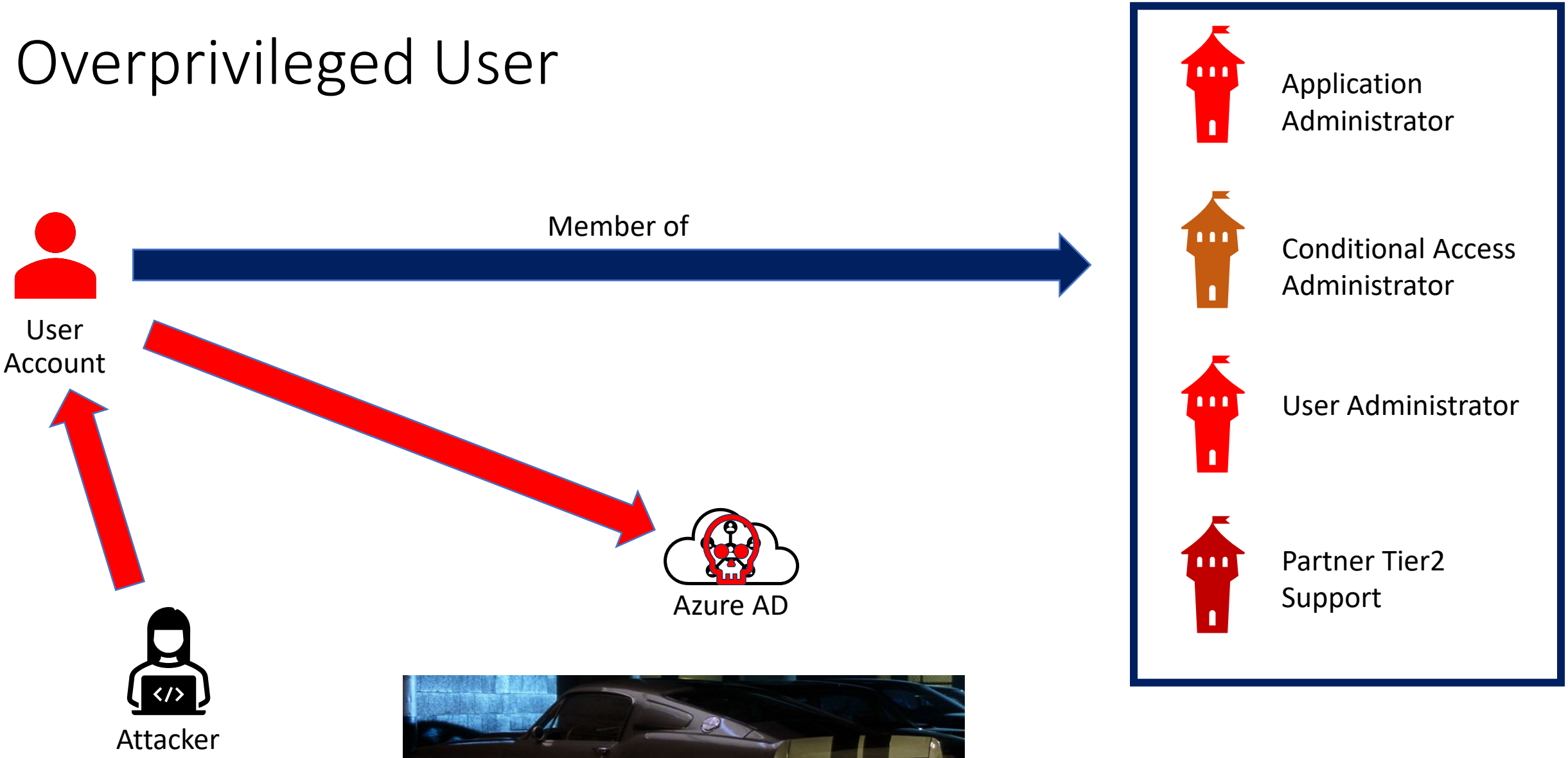




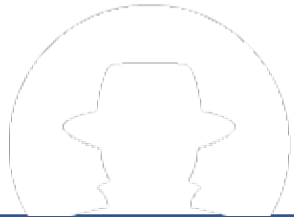
https://github.com/kgretzky/evilginx2



Overprivileged User



Application Escalation



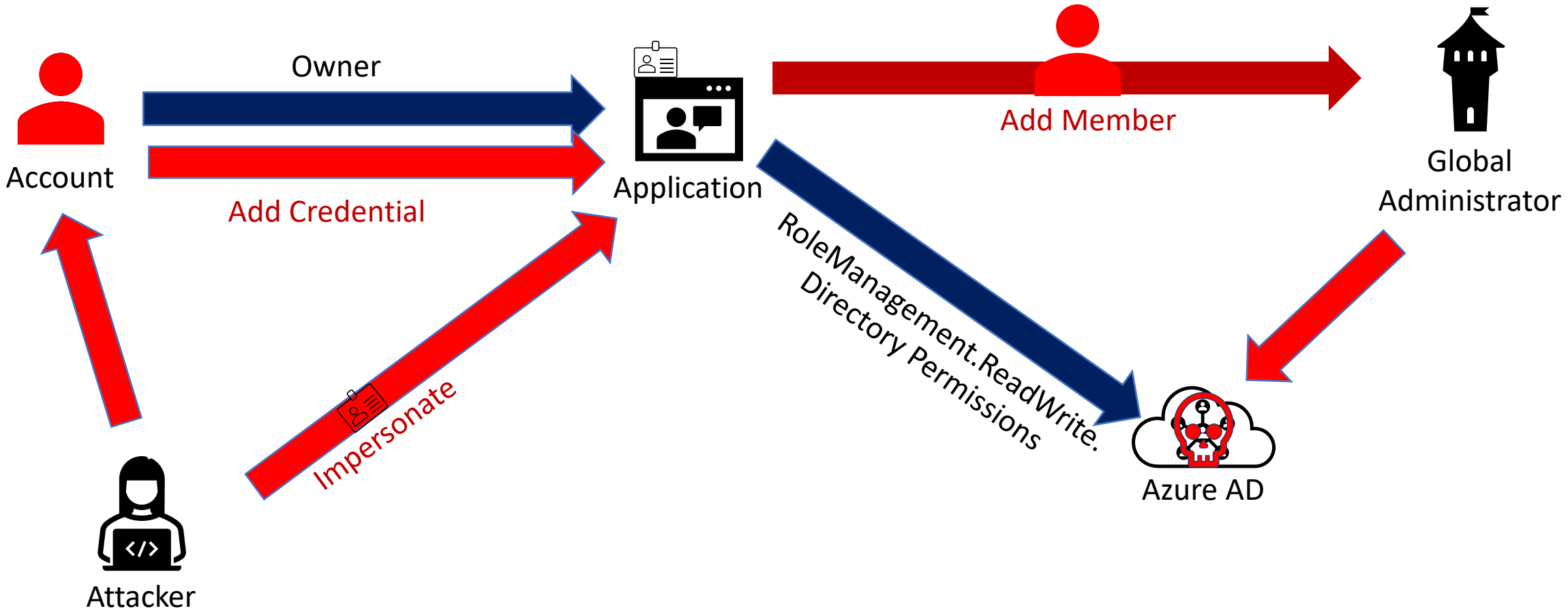
```
PS C:\Data\_MCSA> get-azureadpspermissions -ApplicationPermissions|select ClientObjectID,ClientDisplayName,ResourceDisplayName,Permission

ClientObjectId                       ClientDisplayName      ResourceDisplayName Permission
--------------                       -----------------      ------------------- ----------
9211cb77-c065-4fd9-a80b-bb3a3015caee Lots 'o Privs!         Microsoft Graph     DelegatedPermissionGrant.ReadWrite.All
9211cb77-c065-4fd9-a80b-bb3a3015caee Lots 'o Privs!         Microsoft Graph     Directory.ReadWrite.All
01438f2c-8d6d-4f11-9f76-f179fd3246fa Overpermissioned App   Microsoft Graph     Application.ReadWrite.All
01438f2c-8d6d-4f11-9f76-f179fd3246fa Overpermissioned App   Microsoft Graph     AppRoleAssignment.ReadWrite.All
01438f2c-8d6d-4f11-9f76-f179fd3246fa Overpermissioned App   Microsoft Graph     DelegatedPermissionGrant.ReadWrite.All
01438f2c-8d6d-4f11-9f76-f179fd3246fa Overpermissioned App   Microsoft Graph     Directory.ReadWrite.All
01438f2c-8d6d-4f11-9f76-f179fd3246fa Overpermissioned App   Microsoft Graph     RoleManagement.ReadWrite.Directory
```

https://gist.github.com/psignoret/9d73b00b377002456b24fcb808265c23

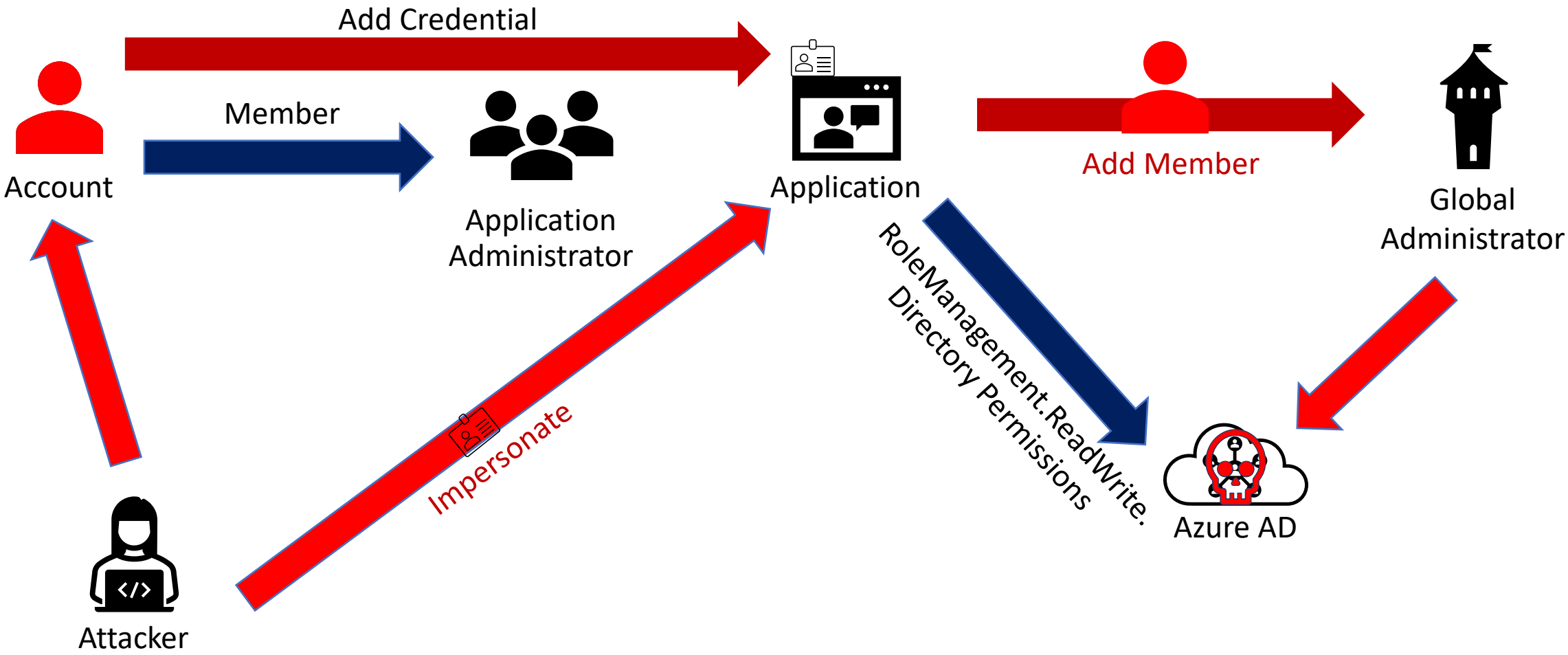
Application Escalation: Find the App Owner

```
PS C:\Data\_MCSA> Get-AzureADApplication -SearchString 'overpermissioned'

ObjectId                             AppId                                DisplayName
--------                             -----                                -----------
fbe4ea6c-0ae4-46b2-a6f0-5f96e3f4858f 5e356a56-f302-4987-923a-0e282ea31d39 Overpermissioned App



PS C:\Data\_MCSA> get-azureadapplicationowner -ObjectId 'fbe4ea6c-0ae4-46b2-a6f0-5f96e3f4858f'

ObjectId                             DisplayName    UserPrincipalName                          UserType
--------                             -----------    -----------------                          --------
ab2365a7-24a1-4ac0-9cd0-2d529d759323 Kenyatta Yoder Kenyatta.Yoder@BigMegaCorp.onmicrosoft.com Member
70d9a5f5-7190-4452-a743-4f2bede82c06 Shayla Santana Shayla.Santana@BigMegaCorp.com            Member
7d8afa78-d799-4bdc-8e33-3dff42fbbac3 Cadence Mclean Cadence.Mclean@BigMegaCorp.com            Member
```

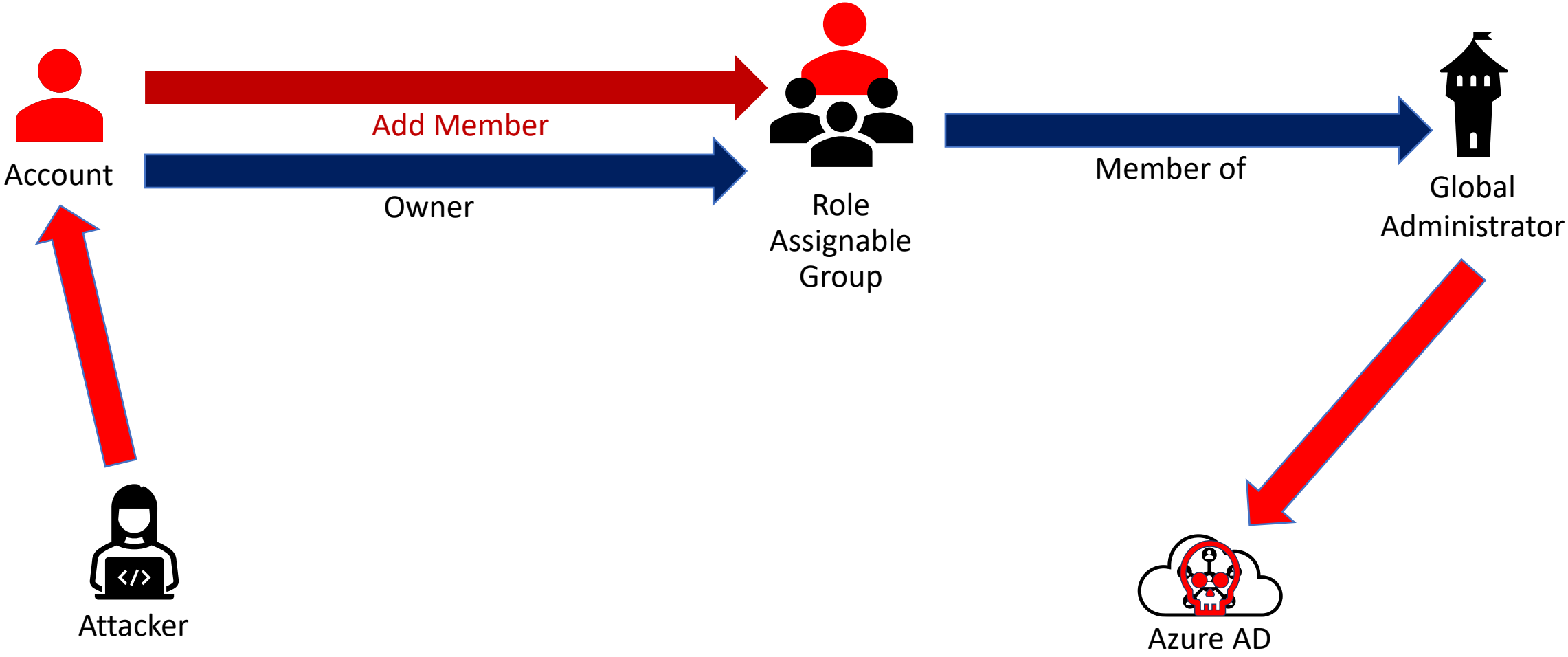
Compromise Azure AD through Application Permissions



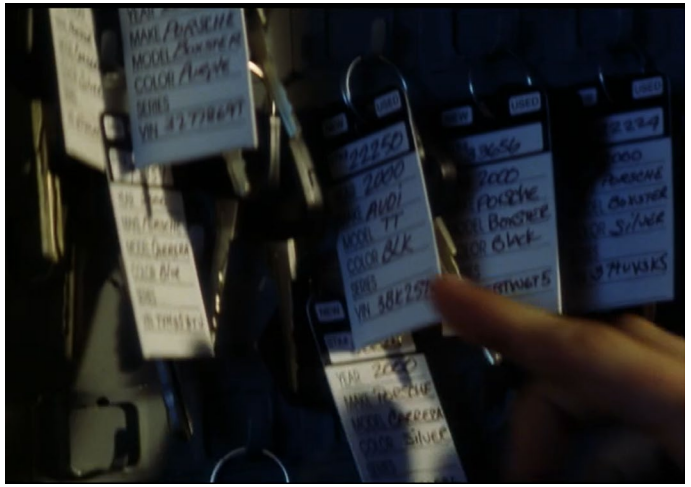
Compromise Azure AD through Application Permissions

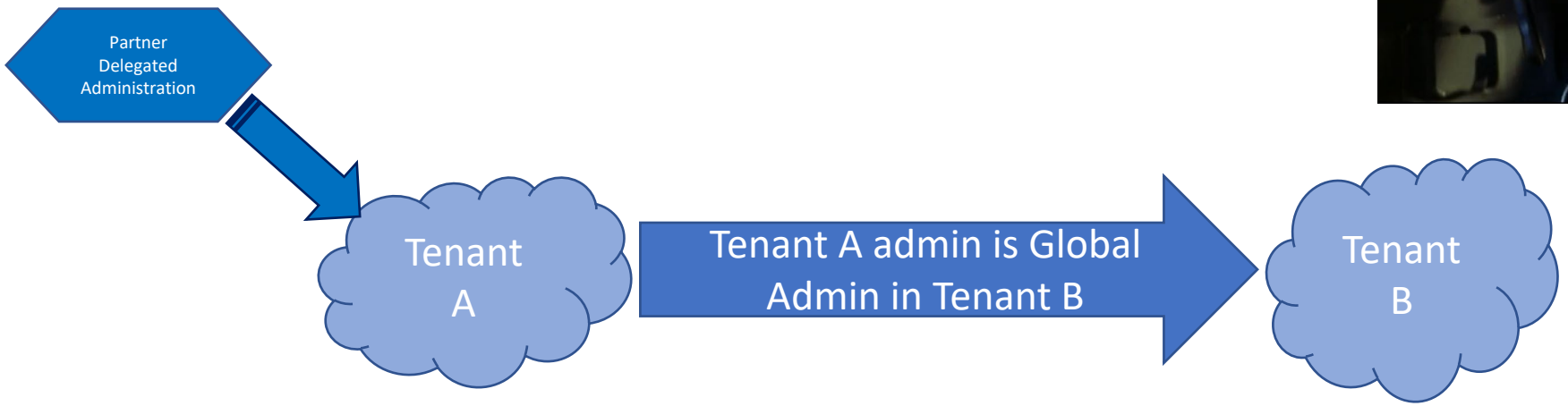


Compromise Azure AD through Role Assignable Group Owner Rights



Solarigate “Tenant Hopping”





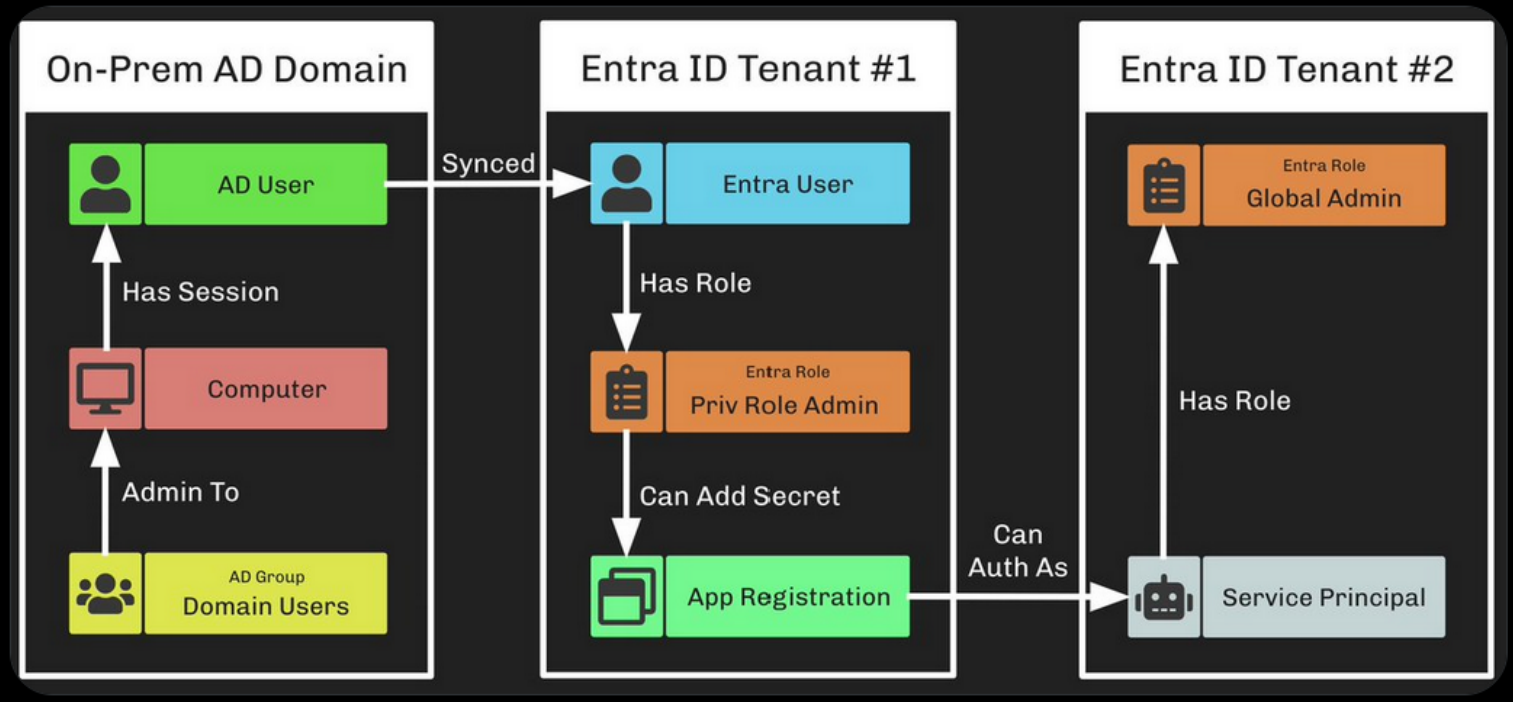
- Tenant Hopping (patent pending 😉) is when an attacker compromises one tenant to jump to another, often with privileged rights.
- Similar to trust hopping in Active Directory.
- Solarigate attackers leveraged partner connections.

What about Admins Synchronized from On-Prem AD?

Andy Robbins
@_wald0

From Domain User to Global Admin. A real example from a real environment.

We found this path with free and open source BloodHound Community Edition: medium.com/p/335652a164df



https://posts.specterops.io/hybrid-attack-paths-new-views-and-your-favorite-dog-learns-an-old-trick-335652a164df?gi=543e6e7a310d

Yeah,
don’t do that

Midnight Blizzard

January 12, 2024

Microsoft

Sean Metcalf | @PyroTek3 | sean@trimarcsecurity.com

Midnight Blizzard

January 12, 2024

Microsoft

Sean Metcalf | @PyroTek3 | sean@trimarcsecurity.com

Microsoft Actions Following Attack by Nation State Actor Midnight Blizzard

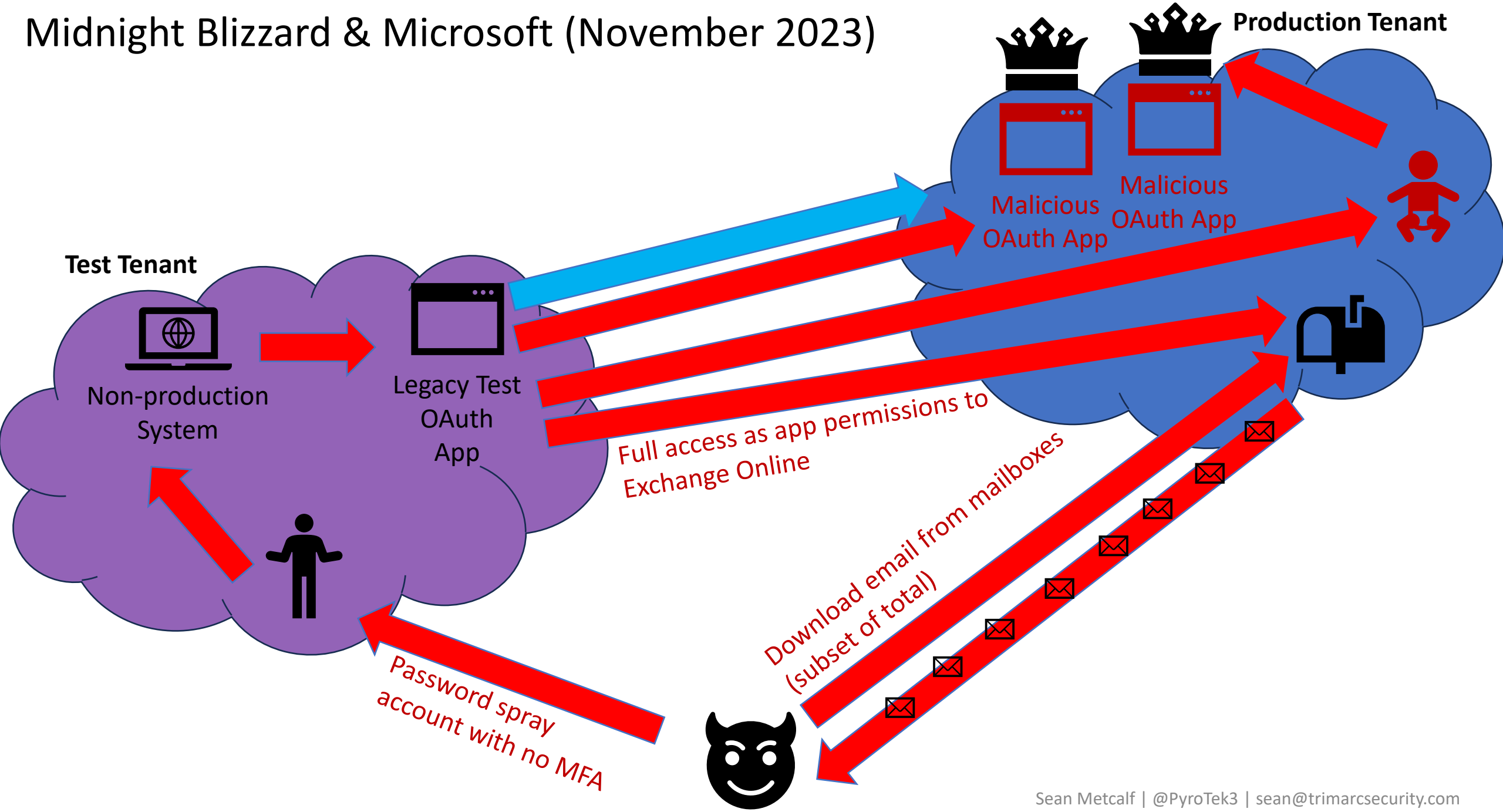
/ By MSRC / January 19, 2024 / 2 min read

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.

The attack was not the result of a vulnerability in Microsoft products or services. To date, there is no evidence that the threat actor had any access to customer environments, production systems, source code, or AI systems. We will notify customers if any action is required.

Midnight Blizzard & Microsoft (November 2023)



What We Know

- Midnight Blizzard – a Moscow-supported espionage team also known as APT29 or Cozy Bear – "**utilized password spray attacks that successfully compromised a legacy, non-production test tenant account that did not have multifactor authentication (MFA) enabled**."
- After gaining initial access to a **non-production** Microsoft system, the intruders **compromised a legacy test OAuth application that had access to Microsoft's corporate IT environment**.
- The actor **created additional malicious OAuth applications**.
- **They created a new user account to grant consent in the Microsoft corporate environment to the actor controlled malicious OAuth applications**.
- The threat actor then used the **legacy test OAuth application to grant them the Office 365 Exchange Online full_access_as_app role, which allows access to mailboxes**.
- They then used this access to **steal emails and other files from corporate inboxes belonging to top Microsoft executives and other staff**.
- They used residential broadband networks as proxies to make their traffic look like it was all legitimate traffic from work-from-home staff, since it was coming from seemingly real users' IP addresses.
- This **all happened in late November, Microsoft didn't spot the intrusion until January 12**, and the compromised email accounts included those of senior leadership and cybersecurity and legal employees.
- "If the same team were to deploy the legacy tenant today, mandatory Microsoft policy and workflows would ensure MFA and our active protections are enabled to comply with current policies and guidance, resulting in better protection against these sorts of attacks."

https://www.theregister.com/2024/01/27/microsoft_cozy_bear_mfa/

https://msrc.microsoft.com/blog/2024/03/update-on-microsoft-actions-following-attack-by-nation-state-actor-midnight-blizzard/

Update on Microsoft Actions Following Attack by Nation State Actor Midnight Blizzard

MSRC / By MSRC / March 08, 2024 / 2 min read

This blog provides an update on the nation-state attack that was detected by the Microsoft Security Team on January 12, 2024. As we shared, on January 19, the security team detected this attack on our corporate email systems and immediately activated our response process. The Microsoft Threat Intelligence investigation identified the threat actor as Midnight Blizzard, the Russian state-sponsored actor also known as NOBELIUM.

As we said at that time, our investigation was ongoing, and we would provide additional details as appropriate.

In recent weeks, we have seen evidence that Midnight Blizzard is using information initially exfiltrated from our corporate email systems to gain, or attempt to gain, unauthorized access. This has included access to some of the company's source code repositories and internal systems. To date we have found no evidence that Microsoft-hosted customer-facing systems have been compromised.

It is apparent that Midnight Blizzard is attempting to use secrets of different types it has found. Some of these secrets were shared between customers and Microsoft in email, and as we discover them in our exfiltrated email, we have been and are reaching out to these customers to assist them in taking mitigating measures. Midnight Blizzard has increased the volume of some aspects of the attack, such as password sprays, by as much as 10-fold in February, compared to the already large volume we saw in January 2024.

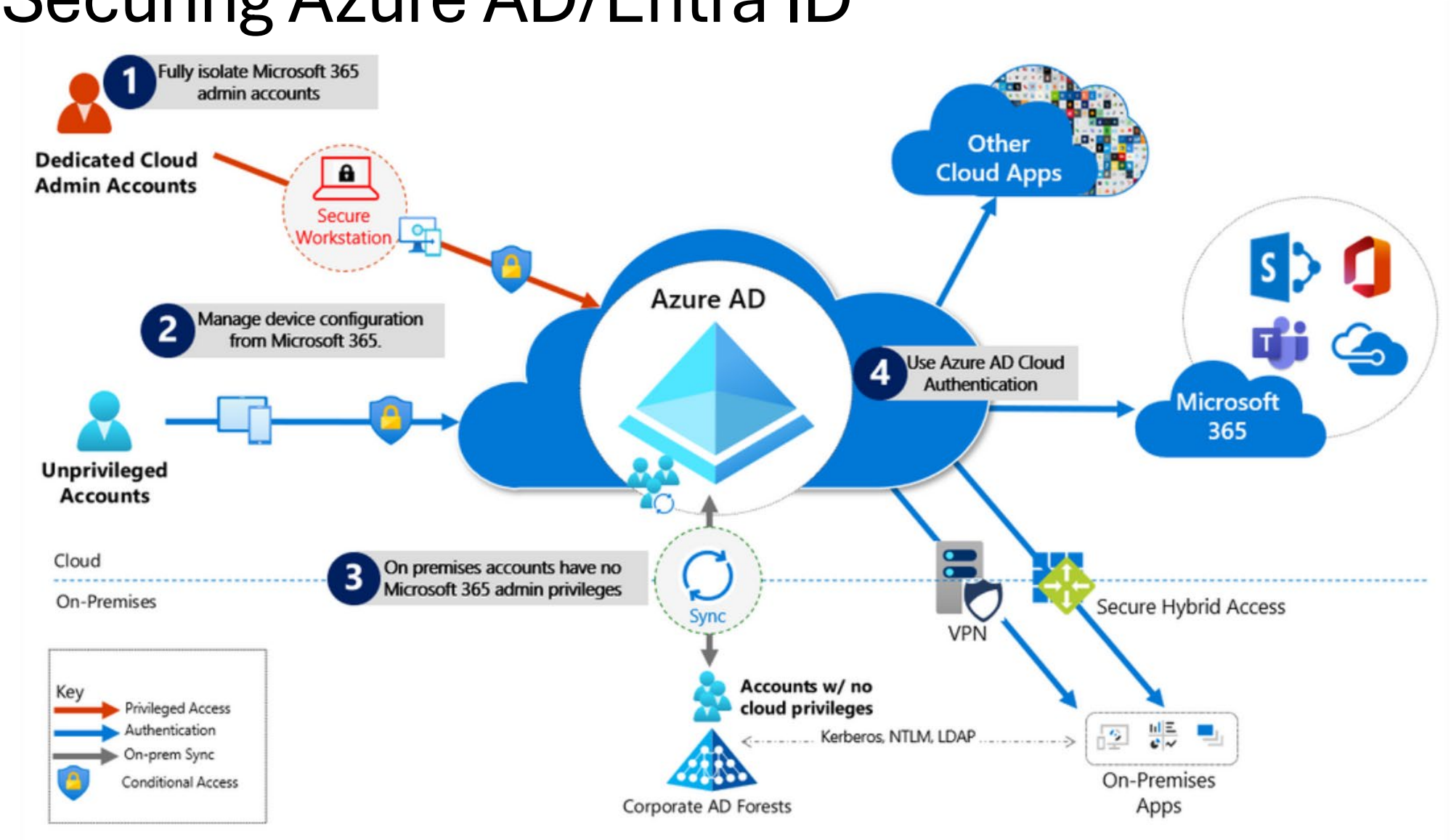
Midnight Blizzard's ongoing attack is characterized by a sustained, significant commitment of the threat actor's resources, coordination, and focus. It may be using the information it has obtained to accumulate a picture of areas to attack and enhance its ability to do so. This reflects what has become more broadly an unprecedented global threat landscape, especially in terms of sophisticated nation-state attacks.

Across Microsoft, we have increased our security investments, cross-enterprise coordination and mobilization, and have enhanced our ability to defend ourselves and secure and harden our environment against this advanced persistent threat. We have and will continue to put in place additional enhanced security controls, detections, and monitoring.

Our active investigations of Midnight Blizzard activities are ongoing, and findings of our investigations will continue to evolve. We remain committed to sharing what we learn.

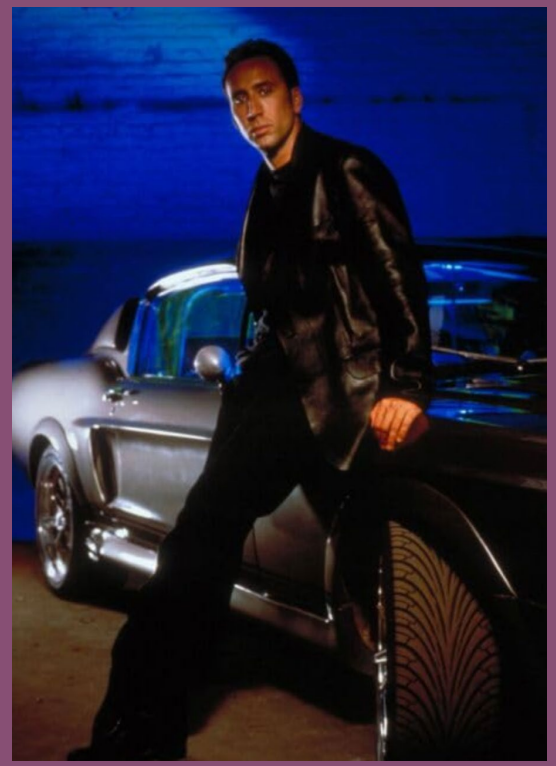
Securing Entra ID Administration

Securing Azure AD/Entra ID



https://techcommunity.microsoft.com/t5/azure-active-directory-identity/protecting-microsoft-365-from-on-premises-attacks/ba-p/1751754

Securing Azure AD/Entra ID - Microsoft Summary



Fully Isolate Azure AD / Microsoft Office 365 admin accounts

They should be:

1. Created in Entra ID.
2. Required to use Multi-factor authentication (MFA).
3. Secured by conditional access.
4. Accessed only by using Azure Managed Workstations.

There should be no on-prem accounts with highly privileged Azure AD/Entra ID rights.

Sean Metcalf | @PyroTek3 | sean@trimarcsecurity.com

Securing Azure AD/Entra ID - Microsoft Summary

Manage from Cloud controlled Devices
Use Azure AD Join and cloud-based mobile device management (MDM) to eliminate dependencies on your on-premises device management infrastructure, which can compromise device and security controls.

No on-prem account has Azure AD / Microsoft Office 365 privileges
Privileged on-premises software must not be capable of impacting Azure AD privileged accounts or roles.

Use Azure AD cloud authentication to eliminate on-prem credential dependencies**.**
Always use strong authentication, such as Windows Hello, FIDO, the Microsoft Authenticator, or Azure AD MFA.

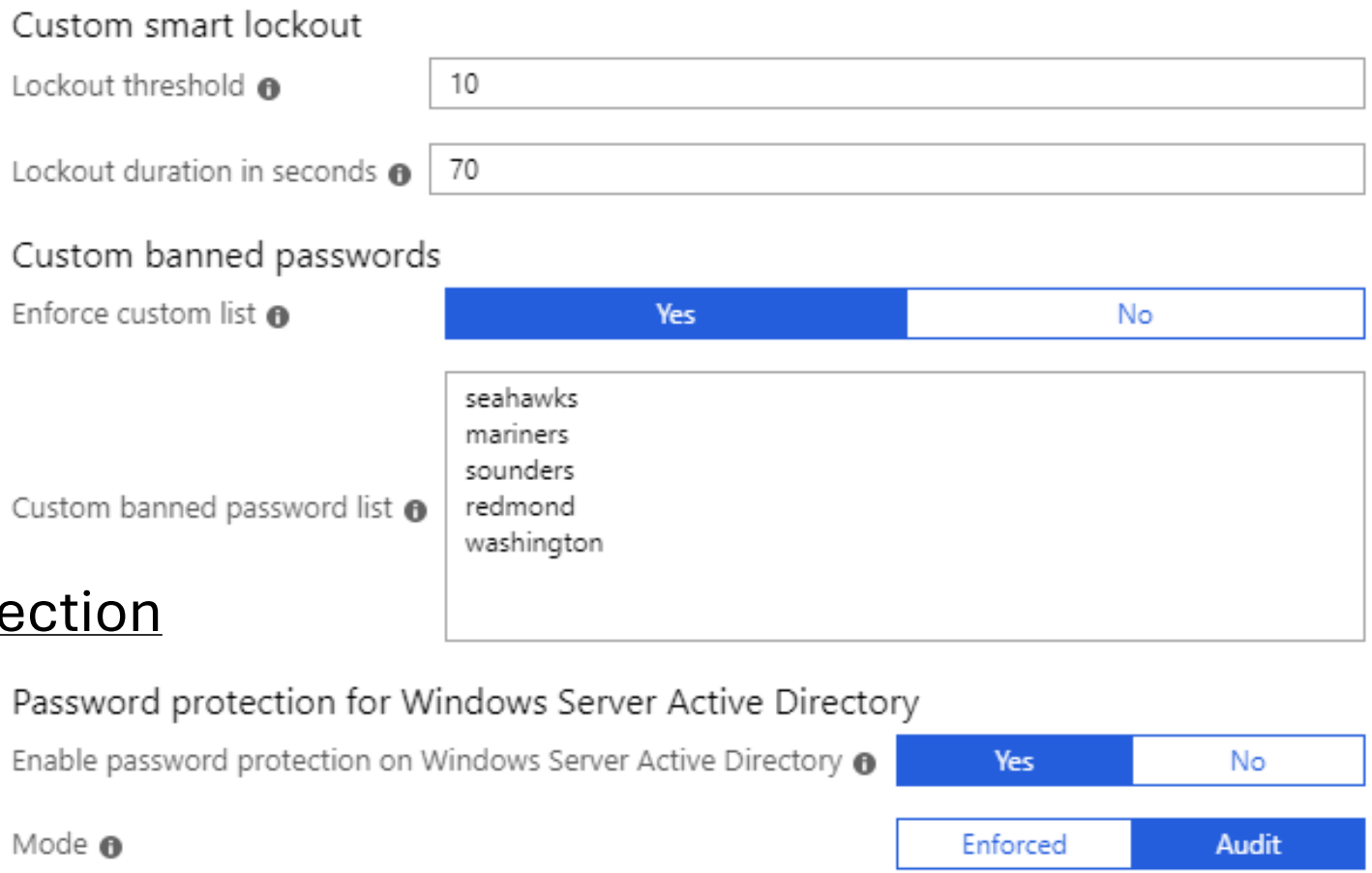
https://techcommunity.microsoft.com/t5/azure-active-directory-identity/protecting-microsoft-365-from-on-premises-attacks/ba-p/1751754

Sean Metcalf | @PyroTek3 | sean@trimarcsecurity.com

On-Prem: Entra Password Protection

- Prevent users from selecting known bad passwords
- Start in audit mode to get an idea how bad it is

https://aka.ms/deploypasswordprotection



Phishing Defensive Layers

Require Users to MFA, preferably FIDO2

- Authenticator App recommended. Better performance and less prompts (behaves as authentication token broker)

Conditional Access Policy

- MFA,Location, App, etc

Risk Based Policy

- Only prompt when Risk detected

People will fall to Phishing no matter what so we must monitor…

Key Cloud Administration Security Controls

- Use admin systems for cloud administration
- Enforce FIDO2 for Trimarc Level 0 & 1 roles
- FIDO2 keys for Emergency “Break Glass” Accounts
- Leverage Conditional Access policies to enforce MFA for admins from all locations

Sean Metcalf | @PyroTek3 | sean@trimarcsecurity.com

Common Persistence Method Checks

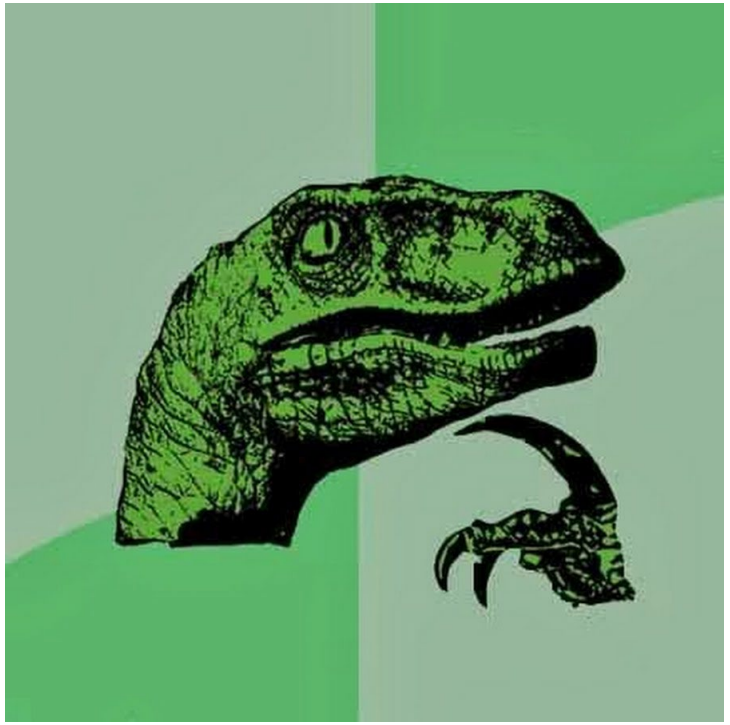
Review Illicit Consent Grants
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/detect-and-remediate-illicit-consent-grants?view=o365-worldwide

Review Exchange Forms/Rules for potentially malicious settings.
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/detect-and-remediate-outlook-rules-forms-attack?view=o365-worldwide

Review Exchange Online mailbox permissions for unusual/unintended configuration (Get-ExoMailboxPermission)
https://docs.microsoft.com/en-us/powershell/module/exchange/powershell-v2-module/get-exomailboxpermission?view=exchange-ps

Conclusion

Sean Metcalf | @PyroTek3 | sean@trimarcsecurity.com



- Attackers are targeting the cloud
- Identifying common security issues and resolving them improves system security.
- Fixing these issues provides improved breach resilience.

Slides, Video & Security Articles:
Hub.TrimarcSecurity.com

TRIMARC

linktr.ee/Trimarc

Questions?

HYBRID IDENTITY PROTECTION conf24 NEW ORLEANS

Questions?