

The Current State of Microsoft Identity Security: Common Security Issues and Misconfigurations



Sean Metcalf
Founder/CTO Trimarc
@PyroTek3
sean@trimarcsecurity.com



TRIMARC

About

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



Agenda

- Introduction
- The Identity Nexus
- Common Security Issues
 - Active Directory
 - Active Directory Certificate Services (ADCS)
 - Azure AD / Entra ID
- Cloud Security Risk
- Midnight Blizzard & Microsoft
- Okta Integration Concerns
- Attacks: MGM & Caesars
- Current State of Microsoft Identity Security
- Conclusion

The logo for The Experts Conference (TEC) features the letters 'TEC' in a large, bold, sans-serif font. The 'T' is orange, the 'E' is grey, and the 'C' is light blue. A vertical white line is positioned to the right of the 'C'.

The Experts Conference

Sponsored by Quest®



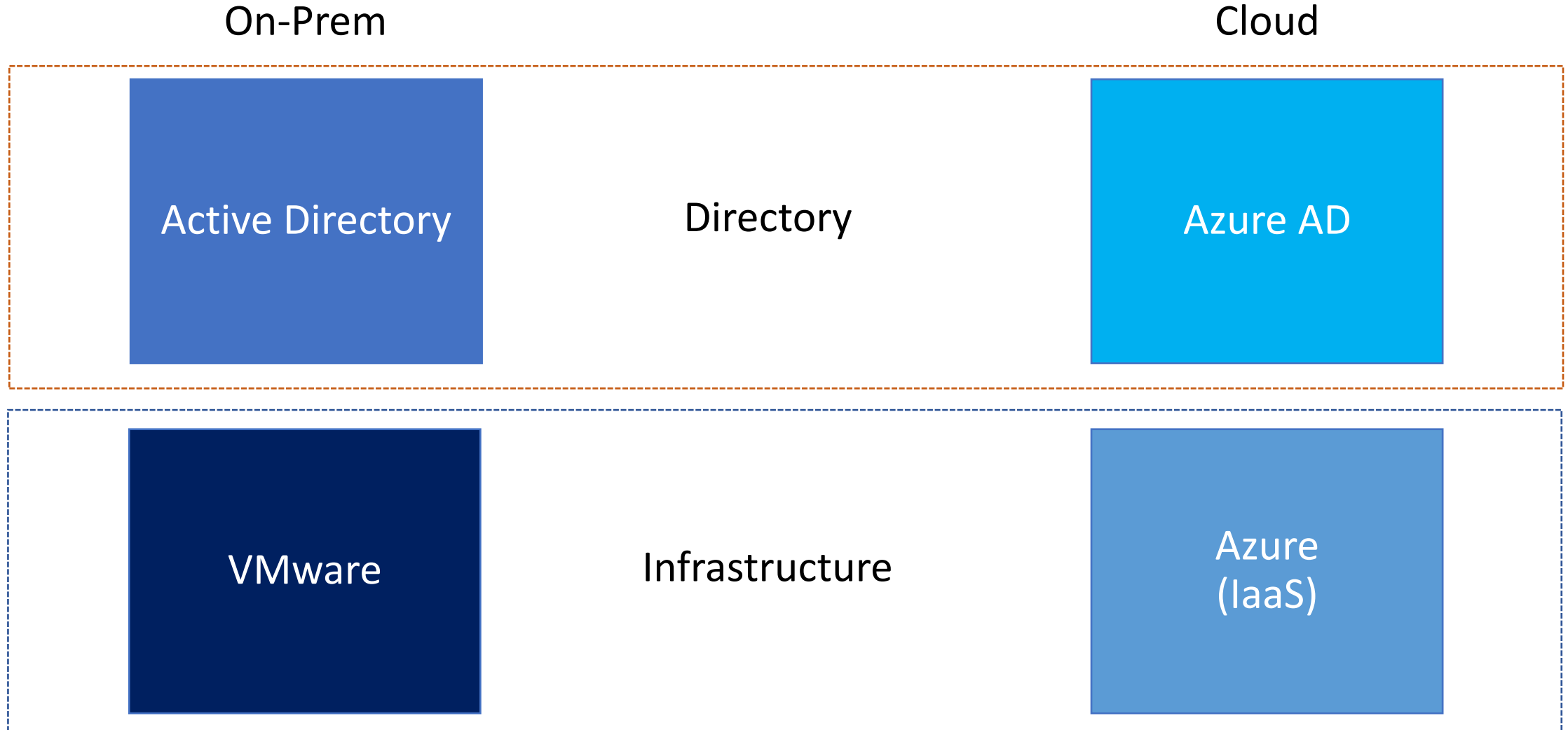
Sean Metcalf
Founder/CTO Trimarc

Defending the Identity Nexus

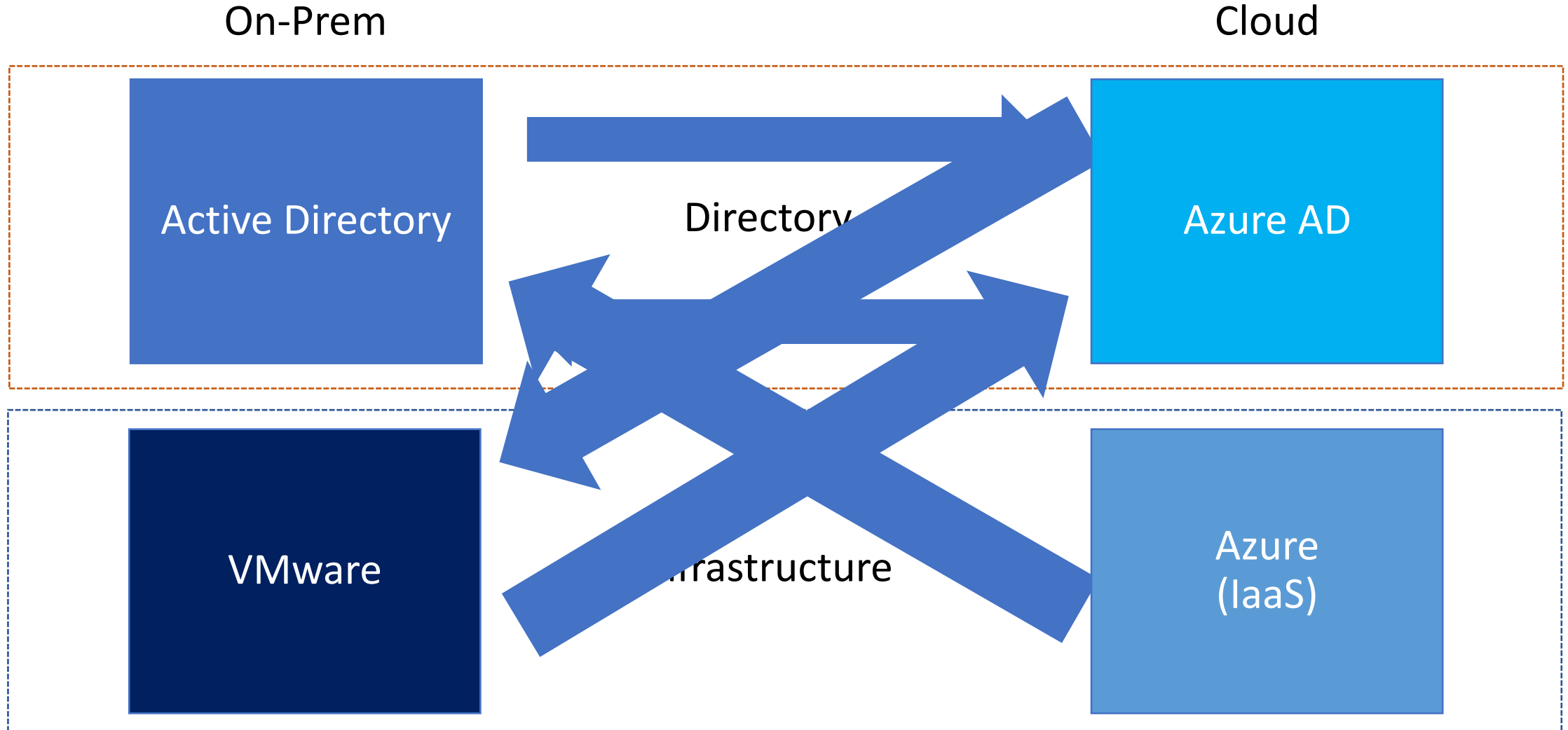
#TEC2022



The Identity Nexus



The Identity Nexus



Common Security Issues: Active Directory

2019: Avenues to Compromise



GPO permissions

Modify a GPO to own everything that applies it



AD Permissions

Delegation a decade ago is still in place, so are the groups



Improper group nesting

Group inception = innocuous groups with super powers



Over-permissioned accounts

Regular users are admins



Service account access

Domain Admins (of course!)



Kerberos Delegation

Who really knows what this means?



Password Vaults

Management issues (user accounts with admin rights, improper protection of server, etc)



Backup Process

What servers backup Active Directory? How is this backup data protected?

2024: Avenues to Compromise



GPO permissions

Modify a GPO to own everything that applies it



AD Permissions

Delegation a decade ago is still in place, so are the groups



Improper group nesting

Group inception = innocuous groups with super powers



Over-privileged accounts

Regular users are admins



Service account access

Domain Admins (of course!)



Kerberos Delegation

Who really knows what this means?



Password Vaults

Management issues (user accounts with admin rights, improper protection of server, etc)



Backup Process

What servers backup Active Directory? How is this backup data protected?

2019: State of Security

- Local Administrator Passwords Not Managed on Workstations or Servers
- Weak Domain Password Policy
- Regular Users in AD Admin Groups
- No Account Naming Standard
- Admin Group Nesting Issues
- Default Domain Controllers Policy is Default
- Service Accounts in Domain Admins
- Accounts with Delegated Rights to AD
- Kerberos Delegation
- Cross-Forest Administration
- Default Domain Administrator Account SPN
- Server GPOs Linked to DCs
- Modify Rights to GPOs at Domain /DC Level
- Domain Permission Delegation Issues
- AdminSDHolder Permission Delegation Issues
- Admins Use Regular Workstations for AD Administration
- DCs with minimal event auditing

2024: State of Security

- Local Administrator Passwords Not Managed on Workstations or Servers
- Weak Domain Password Policy
- Regular Users in AD Admin Groups
- No Account Naming Standard
- Admin Group Nesting Issues
- Default Domain Controllers Policy is Default
- Service Accounts in Domain Admins
- Accounts with Delegated Rights to AD
- Kerberos Delegation
- Cross-Forest Administration
- Default Domain Administrator Account SPN
- Server GPOs Linked to DCs
- Modify Rights to GPOs at Domain /DC Level
- Domain Permission Delegation Issues
- AdminSDHolder Permission Delegation Issues
- Admins Use Regular Workstations for AD Administration
- DCs with minimal event auditing

Common AD Security Issues:

Active Directory Admins



Admin accounts with old passwords



Kerberos Service Principal Names (SPNs)



Service Accounts



Account Usage

AD Admins with Old Passwords

- Ensure privileged account passwords change annually.
- Older passwords are typically poor and easier to guess.
- Password Spraying & Kerberoasting are popular attack methods for compromising accounts lacking strong passwords.



Lab.trimarcresearch.com AD Admins:

name	DistinguishedName	PasswordLastSet
admMBailey	CN=admMBailey,OU=Admin Accounts,OU=AD Management,DC=Lab,DC=trimarcresearch,DC=com	11/10/2019 11:26:46 PM
admEGray	CN=admEGray,OU=Admin Accounts,OU=AD Management,DC=Lab,DC=trimarcresearch,DC=com	11/10/2019 11:27:06 PM
VMWareAdmin	CN=VMWareAdmin,OU=Service Accounts,DC=trimarcresearch,DC=com	11/10/2019 11:57:14 PM
SharepointSVC	CN=SharepointSVC,OU=Service Accounts,DC=Lab,DC=trimarcresearch,DC=com	11/13/2019 9:18:33 AM
Administrator	CN=Administrator,CN=Users,DC=trimarcresearch,DC=com	2/11/2020 2:08:55 PM
Administrator	CN=Administrator,CN=Users,DC=Lab,DC=trimarcresearch,DC=com	5/19/2020 4:32:44 PM
SVC-LAB-GMSA1	CN=SVC-LAB-GMSA1,CN=Managed Service Accounts,DC=Lab,DC=trimarcresearch,DC=com	6/10/2020 8:15:07 AM

AD Admin Account Checks



```
Get-ADGroupMember Administrators -Recursive
```

- Passwords change regularly (every year)
- Disable inactive accounts
- Remove disabled accounts
- No SPNs on accounts associated with people
- Member of Protected Users group
- No computer accounts
- Scrutinize Service Accounts
 - What do they do?
 - Where do they run?
 - What computers do they authenticate to?
 - What rights are actually required?

Action: Improving AD Admin Account Security

(including Service Accounts)



Limit accounts in privileged AD admin groups.



Ensure AD admin accounts have passwords change annually (at a minimum).



Assume no service accounts need to be in AD admin groups.



Ensure all AD admin accounts have “sensitive” bit set and are members of the Protected Users group.

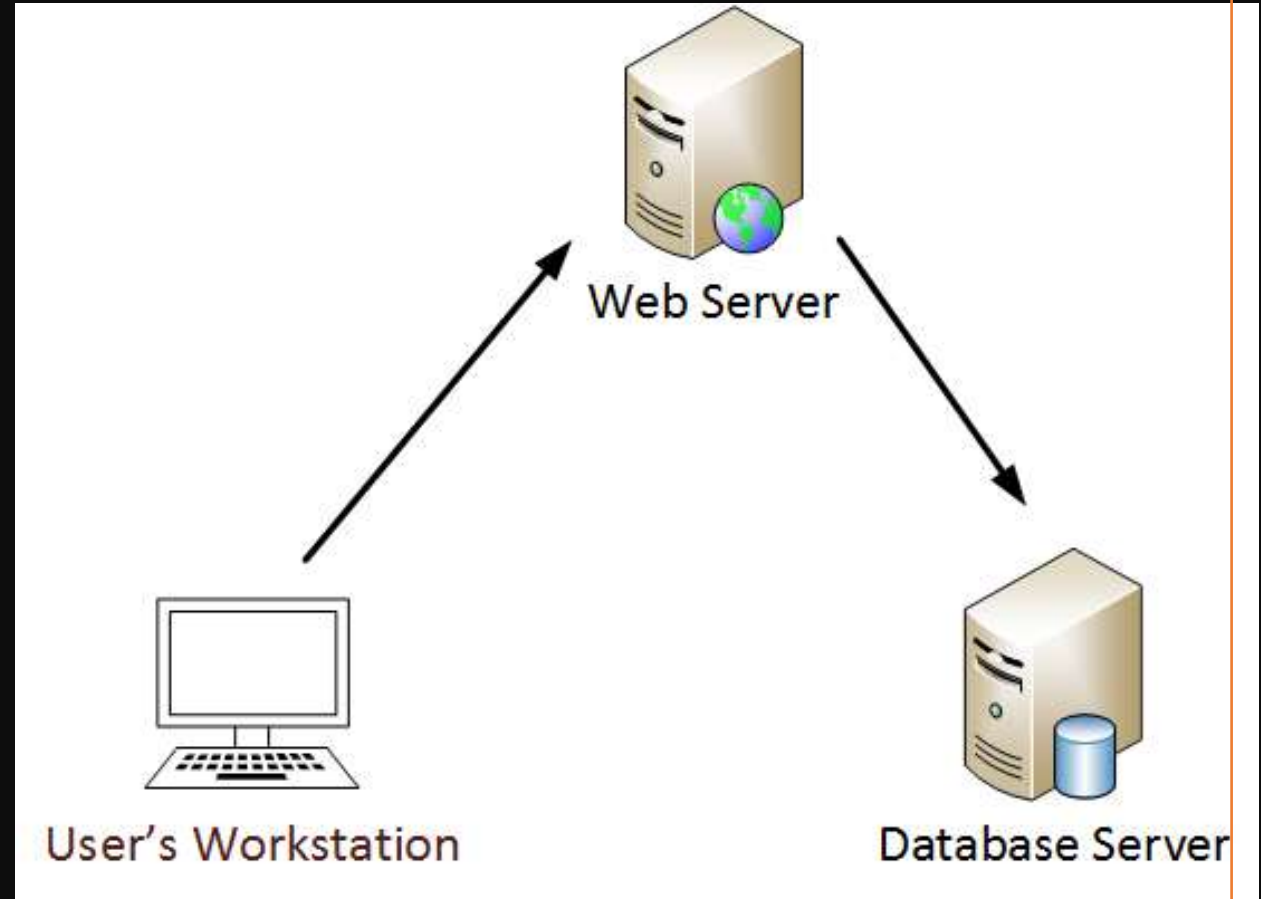


Ensure no AD admin accounts associated with people have Kerberos Service Principal Names (SPNs).



Disable accounts that are no longer in use (and eventually remove from privileged groups).

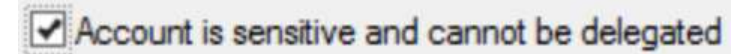
Common AD Security Issues: Kerberos Delegation



Action List: Kerberos Delegation

GOOD:

- Set all AD Admin accounts to: “Account is sensitive and cannot be delegated”
- Remove all delegation accounts that don’t have Kerberos SPNs



BEST:

- Add all AD Admin accounts to the “Protected Users” group.
- Convert Unconstrained delegation to Constrained delegation.
- Work to remove Kerberos delegation from accounts where no longer required.
- Ensure service accounts with Kerberos delegation have long, complex passwords (preferably group Managed Service Accounts).
- Don’t use Domain Controller SPNs when delegating.
- Restrict & monitor who has the ability to configure Kerberos delegation.

Limitation:

Service Accounts may not operate fully when added to Protected Users and may also experience issues with “Account is sensitive and cannot be delegated”

Common AD Security Issues: Custom Permissions

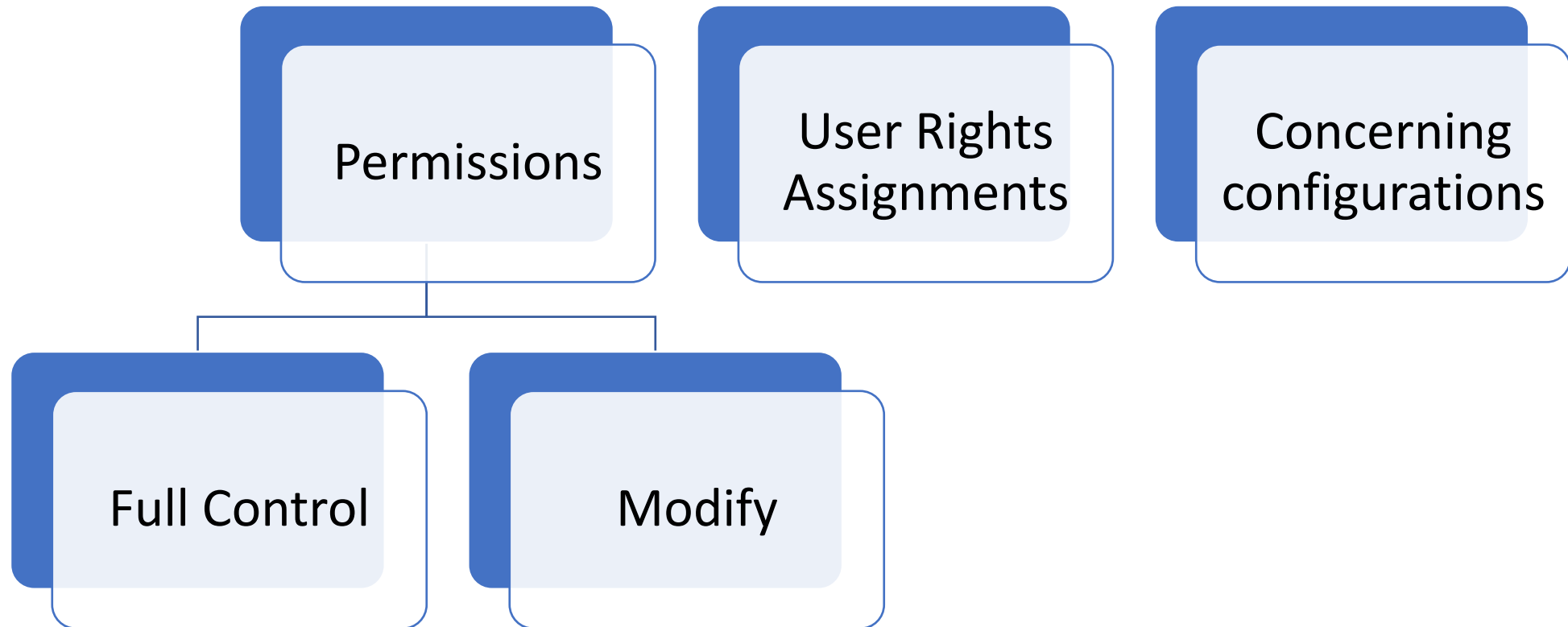
Domain

OUs

Group Policy Objects (GPOs)

Sensitive objects

Group Policy Misconfiguration



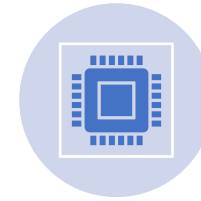
Common AD Security Issues: DCs



Print Spooler service running



Event auditing issues



User Rights Assignments applied to DCs (via GPO)



Installed applications and agents



Old version of VMware Tools



Insecure remote access tools



Still running Windows Server 2012 (or older!) on DCs

Domain Controller Security:

User Rights Assignment

- **Add workstations to domain**
 - Only AD Admins & specific groups/accounts should have this right
- **Allow log on locally & Allow log through Terminal Services (RDP)**
 - Only “Domain Admins” or “Administrators” should have this right
- **Debug programs**
 - Not required
- **Enable computer and user accounts to be trusted for delegation (Kerberos)**
 - Only “Domain Admins” or “Administrators” should have this right
- **Load and unload device drivers (can compromise DC)**
 - Not required
- **Manage auditing and security log (can clear security logs)**
 - AD Admins & Exchange groups only
- **Take ownership of files or other objects (become owner of AD objects)**
 - Only “Domain Admins” or “Administrators” should have this right

Domain Controller Security:

“Not on Domain Controllers” Applications List

SQL

ADFS

Azure AD Connect

Management Console (not the agent)

Firefox

Chrome

(old) Remote console software

Domain Controller Security:

Typical DC Agents

VMware Tools

- You are running the current version, right? (VMware Tools 12.4.0 - 03/21/2024)
- Versions older than 10.1.0 are vulnerable to a significant security issue (VIX API)

EDR

- Has live response capability (console) with system/admin rights on the DC

Management (SCCM)

- Can install/run code on the DC

Splunk Universal Forwarder

- Default install has the ability to run code

DCs: Only Run Supported Versions of Windows

Microsoft Server Operating System	Support Start Date	Mainstream Support End Date	Extended Support End Date
Windows Server 2022	11/2/2021	10/13/2026	10/14/2031
Windows Server 2019	11/13/2018	1/9/2024	1/9/2029
Windows Server 2016	10/15/2016	1/11/2022	1/23/2027
Windows Server 2012R2	11/25/2013	10/9/2018	10/10/2023
Windows Server 2012	10/30/2012	10/9/2018	10/10/2023
Windows Server 2008R2	10/22/2009	1/13/2015	1/14/2020

Action: DC Security

Ensure

Ensure Advanced Auditing is enabled & configured appropriately in DC-linked GPO

Ensure

Ensure DC User Rights Assignments are configured appropriately in DC-linked GPOs

Ensure

Ensure DCs are only operating as Domain Controllers with 0 unnecessary applications

Ensure

Ensure you are running the current VMWare Tools version on virtual DCs

Review

Review all agents on DCs and identify those that can install/run code

Ensure

Ensure DCs are running current Windows versions & keep patched

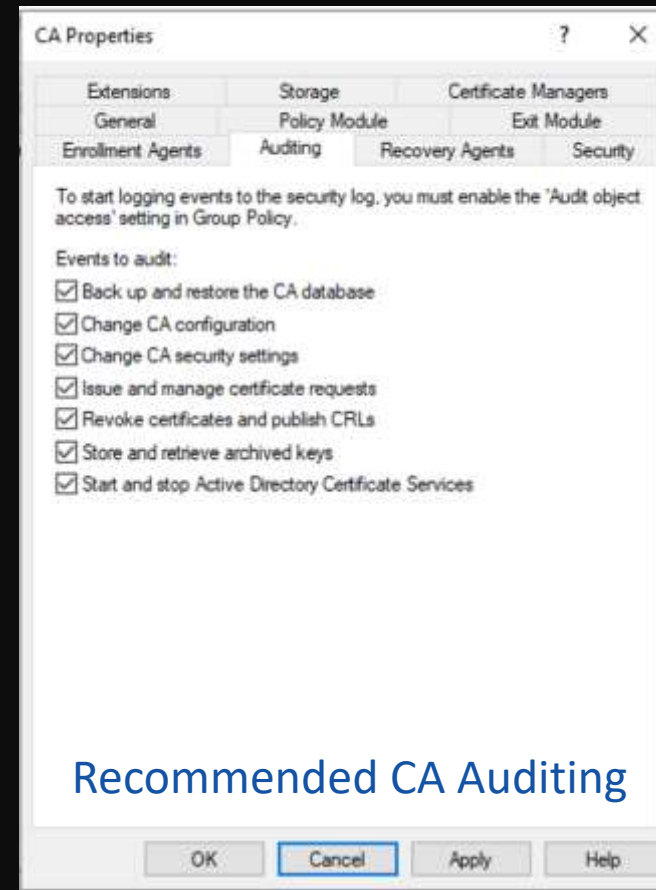
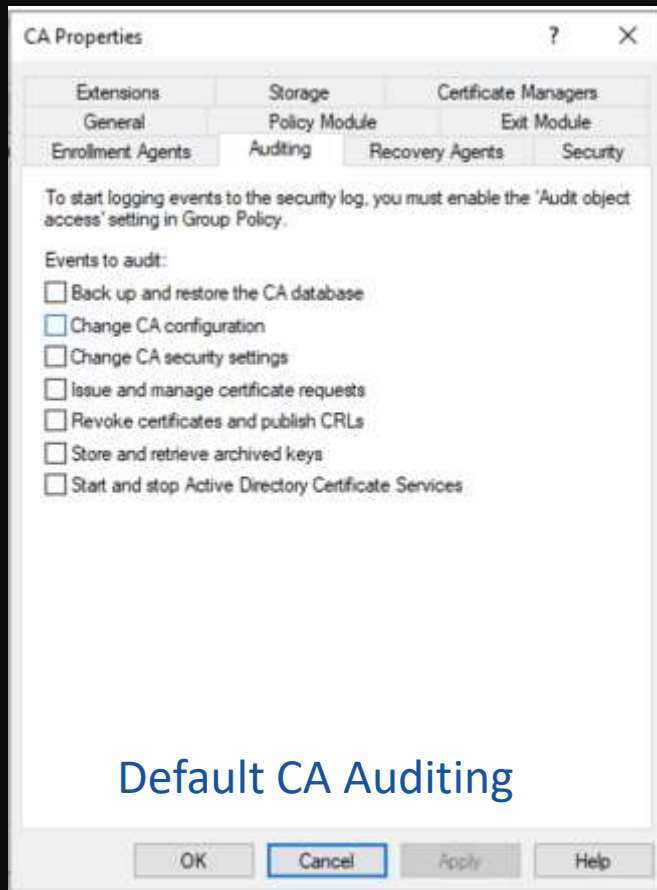
Common AD Security Issues

Active Directory Certificate Services (ADCS)

Active Directory Certificate Services (ADCS) Security Issues

- Auditing Issues
- Misconfigured Certificate Template
 - SAN without Manager Approval
 - SubCA certificate without Manager Approval
 - Overly-permissive AD Object ACLs (ex. auth users with GenericAll)
- Vulnerable PKI Object Access Control (AD permissions)
- EDITF_ATTRIBUTESUBJECTALTNAME2
- HTTP Enrollment Enabled

ADCS Auditing



Templates with Dangerous Configs



- Templates options include:
 - Who can enroll/auto-enroll
 - Certificate purpose(s)/approved use(s)
 - Who is this certificate for?
 - Is approval required?
- If a normal user can specify the subject of the certificate, that *user can request a certificate on behalf of any other entity in the domain including a Domain Admin or Domain Controller.*
- *Trimarc has found at least one certificate that matches this description in ~95% of the environments we've assessed.*

EDITF_ATTRIBUTESUBJECTALTNAME2

Controlling User Added Subject Alternative Names

An Active Directory® Certificate Services CA offers several methods to add subject alternative names (SANs) to a certificate:

1. **Add from known AD object attributes** – The CA can add alternative names from a defined subset of attributes when you choose to add the subject information from Active Directory®. The CA performs this addition, and the data is not specified by the user. Manipulation would require an attacker to be able to manipulate the values of attributes for a user in Active Directory®.
2. **Add as an extension in the certificate request** – If the template is configured for “supply in request”, the extensions requested will be honored by the CA if supported. The alternative names are provided by the requestor.
3. **Add as an attribute that accompanies the certificate request** – Requires the CA to allow user-specified alternative names via the EDITF_ATTRIBUTESUBJECTALTNAME2 flag. If this flag is set on the CA, any request (including when the subject is built from Active Directory®) can have user defined values in the subject alternative name.

Allowing users to define arbitrary alternative names poses risk to the PKI if it is not implemented with proper controls. Anytime you allow a user to define SANs, implement the following additional controls:

- Requests that may contain user-defined alternative names should be set to “pending” when submitted and reviewed by a Certificate Manager prior to issuance
- Do not allow a single person to have the ability to both add SANs and approve the request

EDITF_ATTRIBUTESUBJECTALTNAME2

It is strongly recommended not to enable the **EDITF_ATTRIBUTESUBJECTALTNAME2** flag on an enterprise CA. If this is enabled, alternative names are allowed for any Certificate Template issued, regardless of how the subject of the certificate is determined according to the Certificate Template. Using this feature, a malicious user could easily generate a certificate with an alternative name that would allow them to impersonate another user. For example, depending on the issuance requirements, it may be possible for a malicious user to request a new certificate valid for smart card logon and request a SAN which contains the UPN of a different user. Since smart card logon uses UPN mapping by default to map a certificate to a user account, the certificate could be used to log on interactively as a different user, which could be a domain administrator or other VIP account. If this flag is enabled, the CA should be limited to require Certificate Manager approval or limit enrollment permissions to only trusted accounts.

Secure Your HTTP Endpoints

Enforce & Enable

- Enforce HTTPS & Enable Extended Protection for Authentication (EPA)

Disable

- Disable NTLM auth on IIS on your AD CS servers

Disable

- Disable NTLM auth on your AD CS servers

Best Option:

- Remove all ADCS HTTP endpoints.

ACTION: ADCS Security Checks

- Lots of areas in default configs for attackers to take advantage of.
- Trimarc finds Critical issues in 99% of environments with ADCS.
- Perform the following to improve ADCS security:
 - Review CA auditing settings
 - Review certificate template configuration
 - Review AD PKI object permissions
 - Check for EDITF_ATTRIBUTESUBJECTALTNAME2
 - Secure ADCS HTTP endpoints

```
Administrator: Windows PowerShell
PS C:\Users\Administrator\Documents\Locksmith> Invoke-Locksmith

LOCKSMITH
v2023.9

Gathering AD CS Objects from horse.local...
Identifying auditing issues...
Identifying AD CS templates with dangerous configurations...
Identifying AD CS template and other objects with poor access control...
Identifying HTTP-based certificate enrollment interfaces...

##### Auditing Not Fully Enabled #####

Technique Name      Issue
-----
DETECT      CA      Auditing is not fully enabled. Current value is 0
DETECT      foal-CA  Auditing is not fully enabled. Current value is 0
```

Locksmith: <https://github.com/Trimarc/locksmith>

Run Locksmith!

[illegible]

A large crowd of grey umbrellas with one blue umbrella standing out in the center. The umbrellas are arranged in a dense field, creating a textured, geometric pattern. The blue umbrella is positioned slightly above the center, drawing the viewer's eye.

Common Security Issues: Azure AD/Entra ID

Azure AD / Entra ID Common Security Issues

Privileged Account Issues

- Standard user accounts are members
- Service Accounts / Service Principals are members
- Account(s) authenticate from user workstations
- Using PIM, but all/most are permanently active, not eligible.
- MFA not configured on highly privileged role members

Applications with Highly Privileged Permissions

- Highly privileged applications (Trimarc Level 0) with standard user account as owner
- Standard user account in Application Administrator and/or Cloud Application Administration role(s).


Group Nesting

- Role Assignable Groups in highly privileged roles (Trimarc Level 0)

Partner Access - Delegated Access Permissions




- Global Administrator
- Helpdesk Administrator

Highly Privileged Standard User Accounts

 **Global Administrator | Assignments** ...
Privileged Identity Management | Azure AD roles

« + Add assignments ⚙ Settings ↻ Refresh ↓ Export | 👤 Got feedback?

Manage

-  Assignments
-  Description
-  Role settings


Eligible assignments **Active assignments** Expired assignments

🔍 Search by member name or principal name

Name	Principal name	Type	Scope	Membership	State	St...	End time
Global Administrator							
Shayla Young	Shayla.Young@BigMegaCorp.com	User	Directory	Direct	Assigned	9/...	Permanent
Seana Brennan	Seana.Brennan@BigMegaCorp.com	User	Directory	Direct	Assigned	9/...	Permanent
Janeya Craig	Janeya.Craig@BigMegaCorp.com	User	Directory	Direct	Assigned	9/...	Permanent
Annalina Herman	Annalina.Herman@BigMegaCorp.com	User	Directory	Direct	Assigned	9/...	Permanent
Cadence Sparks	Cadence.Sparks@BigMegaCorp.onmicrosoft.com	User	Directory	Direct	Assigned	9/...	Permanent
Sean Metcalf	sean@bigmegacorp.com	User	Directory	Direct	Assigned	-	Permanent
Chrissa Bradley	Chrissa.Bradley@BigMegaCorp.com	User	Directory	Direct	Assigned	9/...	Permanent
Kenya Bryan	Kenya.Bryan@BigMegaCorp.com	User	Directory	Direct	Assigned	9/...	Permanent
Aafiyah Rodgers	Aafiyah.Rodgers@BigMegaCorp.com	User	Directory	Direct	Assigned	9/...	Permanent

Showing 1 - 9 of 9 results.

PIM Members are Permanent, Not Eligible

 **Global Administrator** | Assignments ...
Privileged Identity Management | Azure AD roles

« + Add assignments ⚙ Settings ↻ Refresh ↓ Export | 🗨 Got feedback?

Manage

- Assignments
- Description
- Role settings

Eligible assignments **Active assignments** Expired assignments

🔍 Search by member name or principal name

Name	Principal name	Type	Scope	Membership	State	St...	End time
Global Administrator							
Shayla Young	Shayla.Young@BigMegaCorp.com	User	Directory	Direct	Assigned	9/...	Permanent
Seana Brennan	Seana.Brennan@BigMegaCorp.com	User	Directory	Direct	Assigned	9/...	Permanent
Janeya Craig	Janeya.Craig@BigMegaCorp.com	User	Directory	Direct	Assigned	9/...	Permanent
Annalina Herman	Annalina.Herman@BigMegaCorp.com	User	Directory	Direct	Assigned	9/...	Permanent
Cadence Sparks	Cadence.Sparks@BigMegaCorp.onmicrosoft.com	User	Directory	Direct	Assigned	9/...	Permanent
Sean Metcalf	sean@bigmegacorp.com	User	Directory	Direct	Assigned	-	Permanent
Chrissa Bradley	Chrissa.Bradley@BigMegaCorp.com	User	Directory	Direct	Assigned	9/...	Permanent
Kenya Bryan	Kenya.Bryan@BigMegaCorp.com	User	Directory	Direct	Assigned	9/...	Permanent
Aafiyah Rodgers	Aafiyah.Rodgers@BigMegaCorp.com	User	Directory	Direct	Assigned	9/...	Permanent

Showing 1 - 9 of 9 results.

Admin Accounts without MFA

The Following ☐ Global Admin Account(s) have MFA Successfully Configured:

UserDisplayName	UserPrincipalName	IsMfaCapable	IsMfaRegistered	IsPasswordlessCapable	MethodsRegistered
Sean Metcalf	sean@bigmegacorp.com	True	True	True	{microsoftAuthenticatorPasswordless,

The Following 7 Global Admin Account(s) don't have MFA Configured:

- Cadence.Sparks@BigMegaCorp.onmicrosoft.com
- Kenya.Bryan@BigMegaCorp.com
- Janeya.Craig@BigMegaCorp.com
- Annalina.Herman@BigMegaCorp.com
- Seana.Brennan@BigMegaCorp.com
- Chrissa.Bradley@BigMegaCorp.com
- Shayla.Young@BigMegaCorp.com

There are 100 Entra ID Roles!

Role	Description
Application Administrator	Can create and manage all aspects of app registrations and enterprise apps.
Application Developer	Can create application registrations independent of the 'Users can register applications' setting.
Attack Payload Author	Can create attack payloads that an administrator can initiate later.
Attack Simulation Administrator	Can create and manage all aspects of attack simulation campaigns.
Attribute Assignment Administrator	Assign custom security attributes keys and values to supported Microsoft Entra objects.
Attribute Assignment Reader	Read custom security attributes keys and values for supported Microsoft Entra objects.
Attribute Definition Administrator	Define and manage the definition of custom security attributes.
Attribute Definition Reader	Read the definition of custom security attributes.
Attribute Log Administrator	Read audit logs and configure diagnostic settings for events related to custom security attributes.
Attribute Log Reader	Read audit logs related to custom security attributes.
Authentication Administrator	Can access to view, set and reset authentication method information for any non-admin user.
Authentication Extensibility Administrator	Customize sign in and sign up experiences for users by creating and managing custom authentication extensions.
Authentication Policy Administrator	Can create and manage the authentication methods policy, tenant-wide MFA settings, password protection policy, and v
Azure DevOps Administrator	Can manage Azure DevOps policies and settings.
Azure Information Protection Administrator	Can manage all aspects of the Azure Information Protection product.
B2C IEF Keyset Administrator	Can manage secrets for federation and encryption in the Identity Experience Framework (IEF).
B2C IEF Policy Administrator	Can create and manage trust framework policies in the Identity Experience Framework (IEF).
Billing Administrator	Can perform common billing related tasks like updating payment information.
Cloud App Security Administrator	Can manage all aspects of the Defender for Cloud Apps product.
Cloud Application Administrator	Can create and manage all aspects of app registrations and enterprise apps except application proxy.
Cloud Device Administrator	Limited access to manage devices in Microsoft Entra ID.
Compliance Administrator	Can read and manage compliance configurations and reports in Microsoft Entra ID and Microsoft 365.
Compliance Data Administrator	Creates and manages compliance content.
Conditional Access Administrator	Can manage Conditional Access capabilities.
Customer LockBox Access Approver	Can approve Microsoft support requests to access customer organizational data.
Desktop Analytics Administrator	Can access and manage Desktop management tools and services.
Directory Readers	Can read basic directory information. Commonly used to grant directory read access to applications and guests.
Directory Synchronization Accounts	Only used by Microsoft Entra Connect service.
Directory Writers	Can read and write basic directory information. For granting access to applications, not intended for users.
Domain Name Administrator	Can manage domain names in cloud and on-premises.
Dynamics 365 Administrator	Can manage all aspects of the Fabric and Power BI products.
Dynamics 365 Business Central Administrator	Can access Dynamics 365 Business Central environments and perform all administrative tasks on the environments.
Edge Administrator	Manage all aspects of Microsoft Edge.
Exchange Administrator	Can manage all aspects of the Exchange product.
Exchange Recipient Administrator	Can create or update Exchange Online recipients within the Exchange Online organization.
External ID User Flow Administrator	Can create and manage all aspects of user flows.
External ID User Flow Attribute Administrator	Can create and manage the attribute schemas available to all user flows.
External Identity Provider Administrator	Can configure identity providers for use in direct federation.
Fabric Administrator	Can manage all aspects of the Fabric and Power BI products.
Global Administrator	Can manage all aspects of Microsoft Entra ID and Microsoft services that use Microsoft Entra identities.
Global Reader	Can read everything that a Global Administrator can, but not update anything.
Global Secure Access Administrator	Create and manage all aspects of Microsoft Entra Internet Access and Microsoft Entra Private Access, including managin
Groups Administrator	Members of this role can create/manage groups, create/manage groups settings like naming and expiration policies, and v
Guest Inviter	Can invite guest users independent of the 'members can invite guests' setting.
Helpdesk Administrator	Can reset passwords for non-administrators and Helpdesk Administrators.
Hybrid Identity Administrator	Can manage Active Directory to Microsoft Entra cloud provisioning, Microsoft Entra Connect, Pass-through Authentica
Identity Governance Administrator	Manage access using Microsoft Entra ID for identity governance scenarios.
Insights Administrator	Has administrative access in the Microsoft 365 Insights app.
Insights Analyst	Access the analytical capabilities in Microsoft Viva Insights and run custom queries.
Insights Business Leader	Can view and share dashboards and insights via the Microsoft 365 Insights app.
Intune Administrator	Can manage all aspects of the Intune product.
Kaizala Administrator	Can manage settings for Microsoft Kaizala.
Knowledge Administrator	Can configure knowledge, learning, and other intelligent features.
Knowledge Manager	Can organize, create, manage, and promote topics and knowledge.
License Administrator	Can manage product licenses on users and groups.
Lifecycle Workflows Administrator	Can create and manage all aspects of management scenarios associated with Lifecycle Workflows in Microsoft Entra ID.
Message Center Privacy Reader	Can read security messages and updates in Office 365 Message Center only.
Message Center Reader	Can read messages and updates for their organization in Office 365 Message Center only.
Microsoft 365 Migration Administrator	Perform all migration functionality to migrate content to Microsoft 365 using Migration Manager.
Microsoft Entra Joined Device Local Administ	Users assigned to this role are added to the local administrators group on Microsoft Entra joined devices.
Microsoft Hardware Warranty Administrator	Create and manage all aspects warranty claims and entitlements for Microsoft manufactured hardware, like Surface and Ho
Microsoft Hardware Warranty Specialist	Create and read warranty claims for Microsoft manufactured hardware, like Surface and HoloLens.
Modern Commerce Administrator	Can manage commercial purchases for a company, department or team.
Network Administrator	Can manage network locations and review capabilities network design insights for Microsoft 365 Software as a Service ap
Office Apps Administrator	Can manage Office apps cloud services, including policy and settings management, and manage the ability to select, unsele
Organizational Branding Administrator	Manage all aspects of organizational branding in a tenant.
Organizational Messages Approver	Review, approve, or reject new organizational messages for delivery in the Microsoft 365 admin center before they are se
Organizational Messages Writer	Write, publish, manage, and review the organizational messages for end-users through Microsoft product surfaces.
Partner Tier1 Support	Do not use - not intended for general use.
Partner Tier2 Support	Do not use - not intended for general use.
Password Administrator	Can reset passwords for non-administrators and Password Administrators.
Permissions Management Administrator	Manage all aspects of Microsoft Entra Permissions Management.
Power Platform Administrator	Can create and manage all aspects of Microsoft Dynamics 365, Power Apps and Power Automate.
Printer Administrator	Can manage all aspects of printers and printer connectors.
Printer Technician	Can register and unregister printers and update printer status.
Privileged Authentication Administrator	Can access to view, set and reset authentication method information for any user (admin or non-admin).
Privileged Role Administrator	Can manage role assignments in Microsoft Entra ID, and all aspects of Privileged Identity Management.
Reports Reader	Can read sign-in and audit reports.
Search Administrator	Can create and manage all aspects of Microsoft Search settings.
Search Editor	Can create and manage the editorial content such as bookmarks, G and A's, locations, floorplan.
Security Administrator	Can read security information and reports, and manage configuration in Microsoft Entra ID and Office 365.
Security Operator	Creates and manages security events.
Security Reader	Can read security information and reports in Microsoft Entra ID and Office 365.
Service Support Administrator	Can read service health information and manage support tickets.
SharePoint Administrator	Can manage all aspects of the SharePoint service.
Skype for Business Administrator	Can manage all aspects of the Skype for Business product.
Teams Administrator	Can manage the Microsoft Teams service.
Teams Communications Administrator	Can manage calling and meetings features within the Microsoft Teams service.
Teams Communications Support Engineer	Can troubleshoot communications issues within Teams using advanced tools.
Teams Communications Support Specialist	Can troubleshoot communications issues within Teams using basic tools.
Teams Devices Administrator	Can perform management related tasks on Teams certified devices.
Tenant Creator	Create new Microsoft Entra or Azure AD B2C tenants.
Usage Summary Reports Reader	Read Usage reports and Adoption Score, but can't access user details.
User Administrator	Can manage all aspects of users and groups, including resetting passwords for limited admins.
Virtual Visits Administrator	Manage and share Virtual Visits information and metrics from admin centers or the Virtual Visits app.
Viva Goals Administrator	Manage and configure all aspects of Microsoft Viva Goals.
Viva Pulse Administrator	Can manage all settings for Microsoft Viva Pulse app.
Windows 365 Administrator	Can provision and manage all aspects of Cloud PCs.
Windows Update Deployment Administrator	Can create and manage all aspects of Windows Update deployments through the Windows Update for Business deploym
Yammer Administrator	Manage all aspects of the Yammer service.

Template ID
3b835d32-2cd3-44c7-3d02-68acd25ca5c3
c1c38e5-3621-4004-a7cb-878624dcd7c
3c6df0f2-1e7c-4dc3-b195-66dfbd24aa8f
c430b396-e653-46cc-36f3-db01b18bb62a
58b19e3c-e632-46ea-36cd-3e0d43cd1f9d
f482af5-364c-4653-3814-fc073ab5f8f8
8424-c6f0-1b33-433c-bb40-26c1753c96d4
1d336d2c-43e8-42ef-9711-b3604cc3fc2c
5b784334-f34b-471b-a387-c7219fc43ca2
3c9353d4-8186-4804-835f-fd5f1e3c2dcd
c4c39bd9-1100-46d3-8c65-bf160da0071f
25a516ed-2fa0-40ea-a2d0-12932a21473a
0526716b-113d-4c15-b22b-66cc3a2b3960
c09730dd-4987-439e-807b-ba8a2b1c7296
1435f4c4-34c4-4d15-a289-98788cc393fd
aa432336-0c0d-4d5f-883a-6355382ac081
3cdaf663-341e-4475-8f94-5c396ef6c070
b0f54661-2d74-4c50-af33-1cc803f12efe
892c5842-a9a6-463a-8041-72aa08cc3cf6
158c047a-c907-4556-b7ef-446551b6b5f7
7639a712-787b-4ac8-90ff-60d6b08af1d2
17075791-f02d-40b4-39cd-432062ccca18
6d4d23a3-da11-4bc4-3570-b0fc686067a7
b1b1c13e-b65d-4f19-8427-f6fa0d937fcb
5c4f9dcd-47dc-4c77-8c3a-3e4207cbfc31
38396431-2bdf-4b4c-8b6e-5d3d8abacta4
88d8c3c3-8f55-4a1e-953a-9b3836b8876b
d23b2b05-8046-44ba-8758-1c26182fcf32
3360fab5-f418-4ba9-8175-e2a00bac4301
6329533b-3180-4127-b345-745d3bc5f3f1
443671b3-b5b7-44c3-36a4-f757879796a
9637977b-cb3b-4cde-8cc3-58786332a3cf
3f1accde-1e04-4ffc-3b63-f0302cd849ef
29232cd2-3923-42fd-ade2-1d097af3e4de
31323ff6-586c-42d1-9346-c534152cc4e
6e591065-3bad-43cd-30f3-c3424366d2f0
0f971ee3-41eb-4569-a71e-57bb83off1e
b62f45f1-457d-42af-a06f-6c1ef63bc451
a9a3c936-b19d-4c14-9520-bddcf82626c
62c90334-6395-4237-8190-01271145c10
f2ef932c-3a7b-46b9-b7cf-a126ee74c451
ac434307-12b3-4f51-a708-88bf58cabcf1
fdd7a751-b60b-444a-984c-02652f8f9c1c
95c79103-95c0-4d8e-aeec-d01accf2d47b
729827c3-3c14-43f7-bb1b-3608f156bbb8
8ac3f64-6cc9-42ea-3e63-59147c6b0ab2
45d8d4c5-b02d-45d6-b32a-fd70b5c1e86e
ae1f448d-243a-41f0-9baf-d71dfe6c5f7c
254f335f-86ab-4119-b717-0f02dc2073c
31c933ad-3672-4736-9c2e-873181342d2d
3a2c62db-5318-420d-8d74-23affce5d9d5
74cf975b-6605-40af-5d2d-b353d83c3533
b5d8dcf3-03d5-43a3-a639-8c29af291470
744cc460-397e-42ad-a462-8b3f9747a02c
4d95c14f-3453-41d0-bef9-a3c0c569773a
3c3d4618-662b-457b-bca3e5c300b3500f
ac16-43a-7b2d-40c0-9c05-243f355ab5b
190cfb3-717d-4188-86a1-ef195c05c1b
8c8b803f-96c1-4123-3343-20738d9f3652
9f06204d-73c1-4d4c-880a-6ed3b060f1d8
1501b37f-7653-41f9-a4b5-203caf33784f
281ef777-fb20-41bb-b7a3-cccebc5b0d96
d24ef571-1500-4070-84db-2666f29cf966
c57138bd-07ff-441f-ba38-babaf66c4c22
2b745bd-f0803-4480-aaf5-822ca433d3ac
92cd40bf-c34a-4b62-9723-b793a7a4c178
c483382d-14bb-4074-8f31-4586725c205b
507f3c4-4c52-4077-abd3-d2e158b6e3d2
4ba33cc4-527c-433a-b33d-d3b43c50246
c00c864a-17c5-4a4b-3c06-f5b95a8d5bd8
366707d0-3269-4127-3ba2-8c3a10f13b3d
a7f9dc32-c74d-46f9-b44c-442855264665
f1648597-92b6-4ef9-c01e-bcaabb1b3dce
644cf478-c28f-4c28-b3dc-3fdac3a0b0ff
c8cc6ff1-44bd-4c38-bc07-4b8d950f4477
7bc44c8a-sdaf-4c2a-84d6-ab2643c08a13
c8611ab8-c189-46c8-34c1-60213ab1f814
4c5d8f65-41d4-4dc4-8368-c035b65333cf
0364bb5c-3bdb-4d7b-ac29-58c734862a40
8635291a-318c-41d7-a3cc-fa4390cf7d3
f84c4c4b-b126-4082-bd5b-f631b38097fd
57222b1-57c3-48ba-ba65-d4759ff1d6f
5d6b6bb7-dc71-4623-b4af-36380a352503
f023fd81-a637-4b56-95fd-731ac0226033
f28af50-f6c7-4571-818b-6a12f2af6b6c
75341003-915a-4863-ab07-631bff18273e
63091246-20c8-4a56-aad4-066075b2a7a8
ba3f7b3a-610a-454a-3e62-d9d1c5c8914b
f7053b30-fc10-4177-3a30-2178f6165737
fc9f9098-03a3-41a9-b3a9-f01cc886a12
37d62c5a-bb6c-433f-843c-f55c3ba2923d4
112ca1a2-15ad-4102-935c-45b0bc473a6a
7534031-6c7e-415a-39d7-48dbd43e875e
fc930be7-5e62-47db-31af-38c3a3a38b1
c300d3c7-4a2b-4235-3eff-f1c78b36cc38
32b086b3-c367-4af2-b863-1dc128b3866e
877b1bf7-1e42-4a9f-3acd-32a50038160
1a45f660-ae2d-45db-17d6-43d00125c13
3269e413-001a-462a-978c-c0f6b3e20d2
810a26d2-a034-447f-a5c8-41cc3378541

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

Trimarc Level 0 Entra ID Roles

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 (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
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.

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>

Admin Group Nesting

 **Global Administrator** | Assignments ...
Privileged Identity Management | Azure AD roles

« + Add assignments ⚙ Settings ↻ Refresh ↓ Export | 🗨 Got feedback?

Manage

-  Assignments
-  Description
-  Role settings

Eligible assignments Active assignments Expired assignments

🔍 Search by member name or principal name

Name	Principal name	Type	Scope	Membership	State	Start time	End time
Global Administrator							
Shayla Young	Shayla.Young@BigMegaCorp.com	User	Directory	Direct	Assigned	9/11/202...	Permanent
Seana Brennan	Seana.Brennan@BigMegaCorp.com	User	Directory	Direct	Assigned	9/11/202...	Permanent
Janeya Craig	Janeya.Craig@BigMegaCorp.com	User	Directory	Direct	Assigned	9/11/202...	Permanent
BigMegaCorp Global Admins	-	Group	Directory	Direct	Assigned	-	Permanent
Annalina Herman	Annalina.Herman@BigMegaCorp.com	User	Directory	Direct	Assigned	9/11/202...	Permanent
Cadence Sparks	Cadence.Sparks@BigMegaCorp.onmicrosoft.com	User	Directory	Direct	Assigned	9/11/202...	Permanent
Sean Metcalf	sean@bigmegacorp.com	User	Directory	Direct	Assigned	-	Permanent
Chrissa Bradley	Chrissa.Bradley@BigMegaCorp.com	User	Directory	Direct	Assigned	9/11/202...	Permanent
Kenya Bryan	Kenya.Bryan@BigMegaCorp.com	User	Directory	Direct	Assigned	9/11/202...	Permanent
Aafiyah Rodgers	Aafiyah.Rodgers@BigMegaCorp.com	User	Directory	Direct	Assigned	9/11/202...	Permanent

Showing 1 - 10 of 10 results.

Group Nesting

Home > BigMegaCorp Global Admins

BigMegaCorp Global Admins Members

Group

+ Add members × Remove ↺ Refresh | Bulk operations | Columns | Got feedback?







Overview
Diagnose and solve problems

Manage

Properties
Members
Owners
Roles and administrators
Administrative units
Group memberships
Assigned roles
Applications

Direct members All members

Search by name Add filters

	Name	Type	Email	User type
<input type="checkbox"/>	 Aadit White	User	Aadit.White@BigMegaCorp.com	Member
<input type="checkbox"/>	 Cadence Mclean	User	Cadence.Mclean@BigMegaCorp.com	Member
<input type="checkbox"/>	 Dane Pineda	User	Dane.Pineda@BigMegaCorp.com	Member
<input type="checkbox"/>	 Dirk Lester	User	Dirk.Lester@BigMegaCorp.com	Member
<input type="checkbox"/>	 Tyrek Miller	User	Tyrek.Miller@BigMegaCorp.com	Member
<input type="checkbox"/>	 Wilson Merritt	User	Wilson.Merritt@BigMegaCorp.com	Member

Group Owners

Role Assignable Group Owners can manage group membership

Home > BigMegaCorp Global Admins

BigMegaCorp Global Admins | Owners



Group

Overview
Diagnose and solve problems

Manage
Properties
Members
Owners

« + Add owners ✕ Remove ↺ Refresh ≡ Columns 🗨 Got feedback?

🔍 Search by name + Add filters

	Name	Type	Email	User type
<input type="checkbox"/>	 Kate Pena	User	Kate.Pena@BigMegaCorp.com	Member
<input type="checkbox"/>	 Robert Marquez	User	Robert.Marquez@BigMegaCorp.com	Member

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.

Reviewing Azure AD Permissions with PowerShell

```
PS C:\> Get-AzureADPSPermissions -ApplicationPermissions | Select ClientDisplayName,ResourceDisplayName,Permission
```

ClientDisplayName	ResourceDisplayName	Permission
Trimarc RD TestApp Windows Azure Active Directory	Device.ReadWrite.All	
Trimarc RD TestApp Windows Azure Active Directory	Member.Read.Hidden	
Trimarc RD TestApp Windows Azure Active Directory	Directory.ReadWrite.All	
Trimarc RD TestApp Windows Azure Active Directory	Domain.ReadWrite.All	
Trimarc RD TestApp Windows Azure Active Directory	Application.ReadWrite.OwnedBy	
Trimarc RD TestApp Windows Azure Active Directory	Application.ReadWrite.All	
Trimarc RD TestApp Office 365 Exchange Online	User.Read.All	
Trimarc RD TestApp Office 365 Exchange Online	Mail.ReadWrite	
Trimarc RD TestApp Office 365 Exchange Online	MailboxSettings.ReadWrite	
Trimarc RD TestApp Office 365 Exchange Online	Contacts.ReadWrite	
Trimarc RD TestApp Office 365 Exchange Online	Mailbox.Migration	
Trimarc RD TestApp Office 365 Exchange Online	Calendars.ReadWrite.All	
Trimarc RD TestApp Office 365 Exchange Online	Mail.Send	
Office 365 ASI App Office 365 Management APIs	ServiceHealth.Read	
Office 365 ASI App Office 365 Management APIs	ActivityFeed.Read	

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

Who are the Application Owners for TestApp?

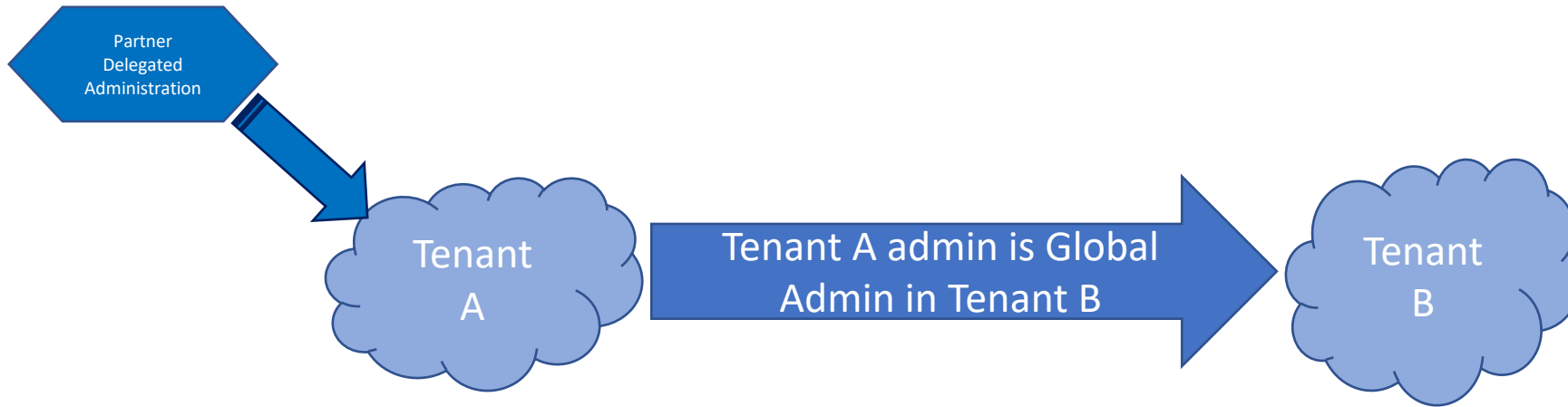
```
PS C:\> Get-AzureADApplication -Objectid $appid | select displayname,Objectid,appid
```

DisplayName	Objectid	AppId
-----	-----	-----
Trimarc RD TestApp	c8e9b6fe-cc98-4e90-8b7b-15fba500d49c	2f337e5f-8414-45a4-b48f-e0ec2014a1d4

```
PS C:\> Get-AzureADApplicationOwner -Objectid $AppId
```

Objectid	DisplayName	UserPrincipalName	UserType
-----	-----	-----	-----
71575fad-39b2-475a-b519-314dde65e7cf	Sean Metcalf	sean@trimarcrd.com	Member
13cf788e-baf0-4b1e-b9fa-46128a6468d0	Joe User	JoeUser@TrimarcRD.com	Member
f4d30f9e-0837-4e3f-974e-ef282a2fcef	Darth Vader	DarthVader@TrimarcRD.com	Member
f2a0fb99-bdaf-49ce-9192-9488ea5d3dae	Boba Fett	BobaFett@TrimarcRD.com	Member

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.

Delegated Admin

Home > Trimarc RD - BIG MEGA CORP

Trimarc RD - BIG MEGA CORP | Delegated admin partners ...

- Overview
- Preview features
- Diagnose and solve problems

Manage

- Users
- Groups
- External Identities
- Roles and administrators
- Administrative units
- Delegated admin partners

Got feedback?

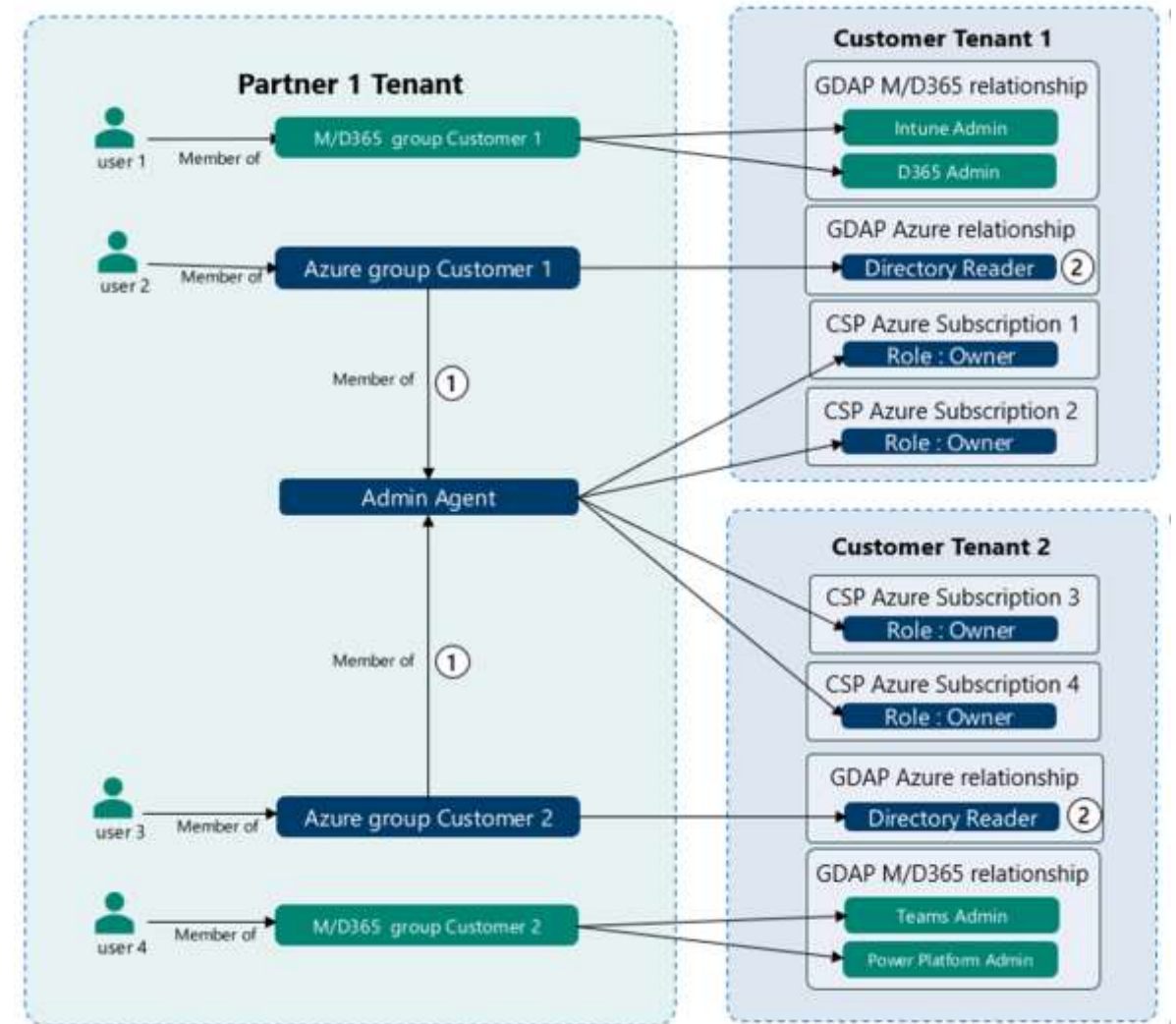
Delegated admin partners are Microsoft partners that you have authorized to administer Microsoft services in your tenant using delegated administration permission. [Learn about partners.](#)

Partner	Relationship type	Roles	Expiration
None			

Entra ID Menu Item: Delegated admin partners

https://portal.azure.com/#view/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/~/PartnerRelationships

Move to Granular Delegated Admin Privileges (GDAP)



Results of Major Technical Investigations for Storm-0558 Key Acquisition

MSEC / By MSEC / September 06, 2023 / 3 min read

On July 11, 2023, Microsoft published a [blog post](#) which details how the China-Based threat actor, Storm-0558, used an acquired Microsoft account (MSA) consumer key to forge tokens to access OWA and Outlook.com. Upon identifying that the threat actor had acquired the consumer key, Microsoft performed a comprehensive technical investigation into the acquisition of the Microsoft account consumer signing key, including how it was used to access enterprise email. Our technical investigation has concluded. As part of our commitment to transparency and trust, we are releasing our investigation findings.

Key acquisition

Microsoft maintains a highly isolated and restricted production environment. Controls for Microsoft employee access to production infrastructure include background checks, dedicated accounts, secure access workstations, and multi-factor authentication using hardware token devices. Controls in this environment also prevent the use of email, conferencing, web research and other collaboration tools which can lead to common account compromise vectors such as malware infections or phishing, as well as restricting access to systems and data using Just in Time and Just Enough Access policies.

Our corporate environment, which also requires secure authentication and secure devices, allows for email, conferencing, web research and other collaboration tools. While these tools are important, they also make users vulnerable to spear phishing, token stealing malware, and other account compromise vectors. For this reason - by policy and as part of our Zero-Trust and "assume breach" mindset - key material should not leave our production environment.

Our investigation found that a consumer signing system crash in April of 2021 resulted in a snapshot of the crashed process ("crash dump"). The crash dumps, which redact sensitive information, should not include the signing key. In this case, a race condition allowed the key to be present in the crash dump (this issue has been corrected). The key material's presence in the crash dump was not detected by our systems (this issue has been corrected).

We found that this crash dump, believed at the time not to contain key material, was subsequently moved from the isolated production network into our debugging environment on the internet connected corporate network. This is consistent with our standard debugging processes. Our credential scanning methods did not detect its presence (this issue has been corrected).

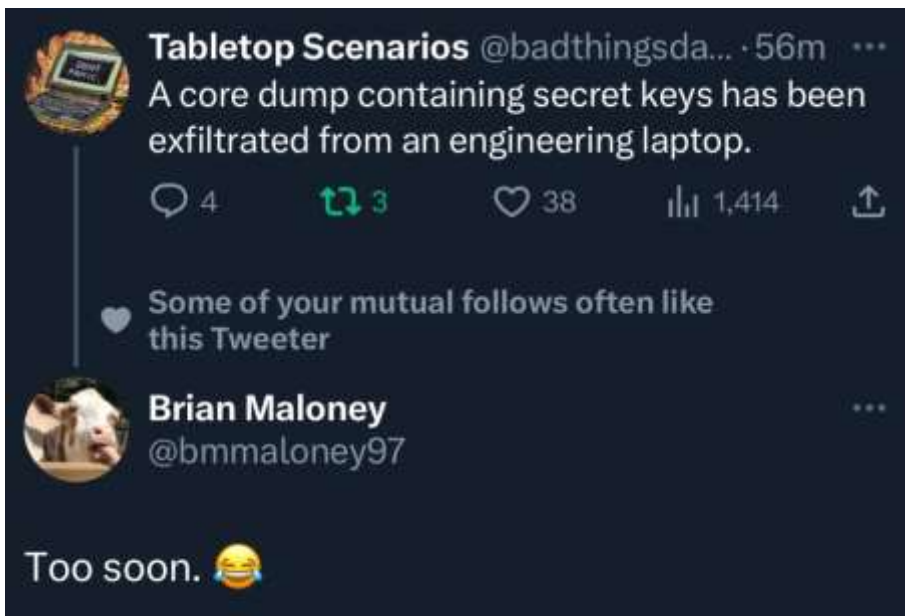
After April 2021, when the key was leaked to the corporate environment in the crash dump, the Storm-0558 actor was able to successfully compromise a Microsoft engineer's corporate account. This account had access to the debugging environment containing the crash dump which incorrectly contained the key. Due to log retention policies, we don't have logs with specific evidence of this exfiltration by this actor, but this was the most probable mechanism by which the actor acquired the key.

Why a consumer key was able to access enterprise mail

To meet growing customer demand to support applications which work with both consumer and enterprise applications, Microsoft [introduced](#) a common key metadata publishing endpoint in September 2018. As part of this converged offering, Microsoft updated documentation to clarify the requirements for key scope validation - which key to use for enterprise accounts, and which to use for consumer accounts.

As part of a pre-existing library of documentation and helper APIs, Microsoft provided an API to help validate the signatures cryptographically but did not update these libraries to perform this scope validation automatically (this issue has been corrected). The mail systems were updated to use the common metadata endpoint in 2022. Developers in the mail system incorrectly assumed libraries performed complete validation and did not add the required issuer/scope validation. Thus, the mail system would accept a request for enterprise email using a security token signed with the consumer key (this issue has been corrected using the updated libraries).

Post Incident Review



<https://msrc.microsoft.com/blog/2023/09/results-of-major-technical-investigations-for-storm-0558-key-acquisition/>

According to Microsoft, Storm-0558...

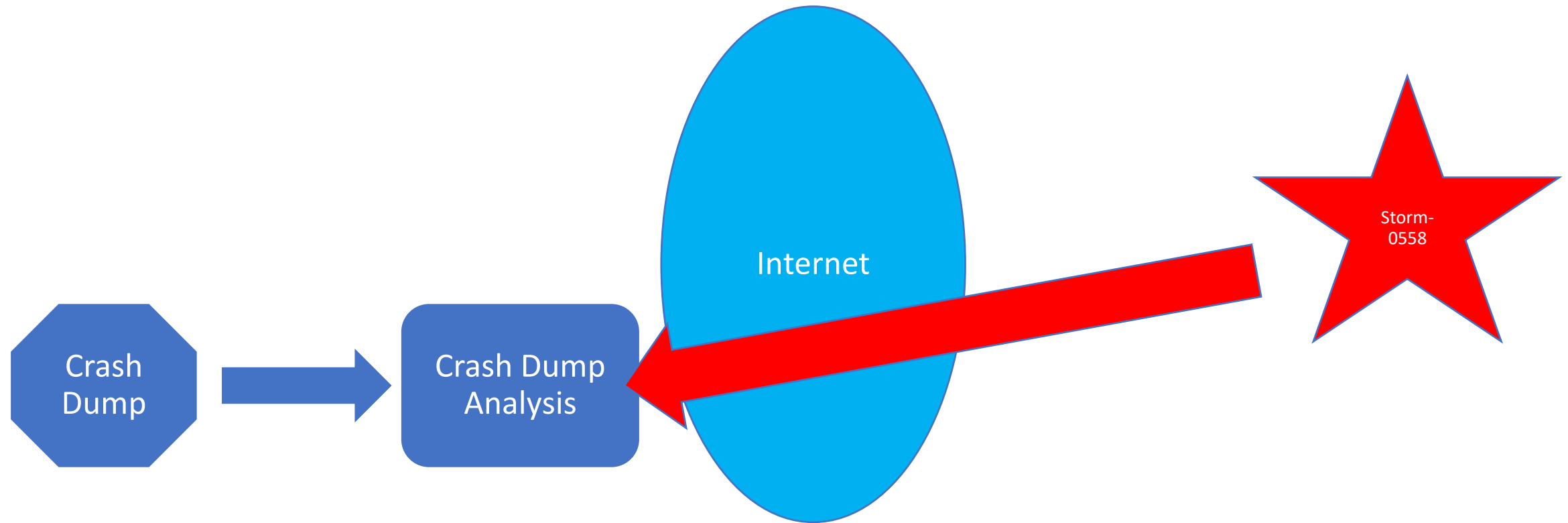
- is a **China-based threat actor** with activities and methods consistent with espionage objectives
- **primarily targeted US and European** diplomatic, economic, and legislative governing bodies, and individuals connected to Taiwan and Uyghur geopolitical interests
- displayed an interest in **targeting media companies, think tanks, and telecommunications equipment and service providers**
- Objective is to obtain **unauthorized access to email accounts** belonging to employees of targeted organizations
- pursues this objective through **credential harvesting, phishing campaigns, and OAuth token attacks**
- displayed an interest in OAuth applications, token theft, and token replay against Microsoft accounts since at least August 2021
- operates with a **high degree of technical tradecraft and operational security.**
- are keenly aware of the target's environment, logging policies, authentication requirements, policies, and procedures.
- **tooling and reconnaissance activity suggests the actor is technically adept, well resourced, and has an in-depth understanding of many authentication techniques and applications**

How Was This Possible? (According to Microsoft)

- Investigation found that a consumer signing system crash in April of 2021 resulted in a snapshot of the crashed process (“crash dump”).
- The crash dumps, which redact sensitive information, should not include the signing key.
- **In this case, a race condition allowed the key to be present in the crash dump** (this issue has been corrected).
- The **key material’s presence in the crash dump was not detected by our systems** (this issue has been corrected).
- We found that this crash dump, believed at the time not to contain key material, was subsequently **moved from the isolated production network into our debugging environment on the internet connected** corporate network. This is consistent with our standard debugging processes.
- **Our credential scanning methods did not detect its presence** (this issue has been corrected).
- **Due to log retention policies, we don’t have logs with specific evidence** of this exfiltration by this actor, but this was the most probable mechanism by which the actor acquired the key.
- To meet growing customer demand to support applications which work with both consumer and enterprise applications, Microsoft introduced a **common key metadata publishing endpoint** in September 2018.
- As part of a pre-existing library of documentation and helper APIs, Microsoft provided an API to help validate the signatures cryptographically **but did not update these libraries to perform this scope validation automatically** (this issue has been corrected).
- **Developers in the mail system incorrectly assumed libraries performed complete validation and did not add the required issuer/scope validation.** Thus, **the mail system would accept a request for enterprise email using a security token signed with the consumer key** (this issue has been corrected using the updated libraries).
- In-depth analysis of the Exchange Online activity discovered that in fact the actor was forging Azure AD tokens using an acquired Microsoft account (MSA) consumer signing key. **This was made possible by a validation error in Microsoft code**

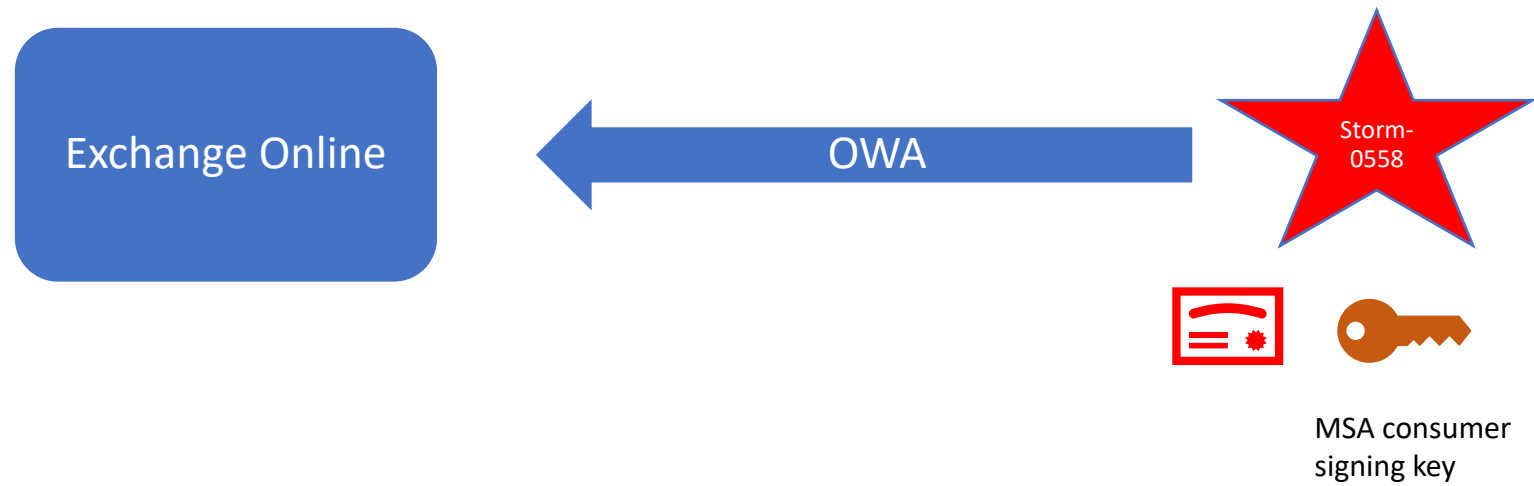
What Happened?

April 2021



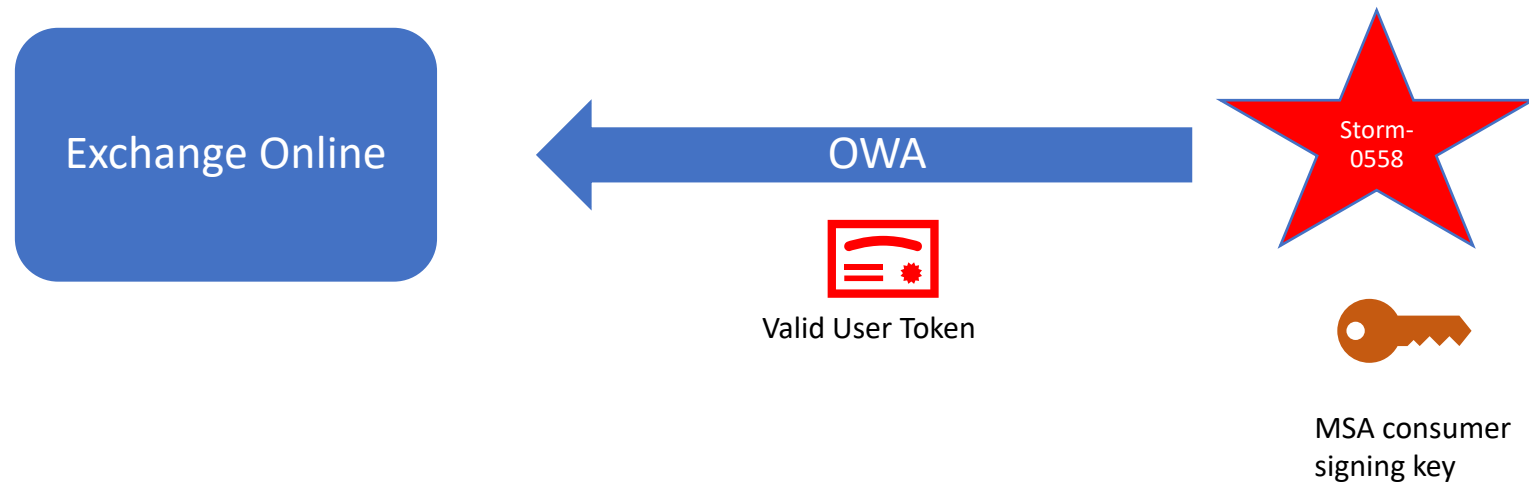
What Happened?

June 16, 2023



What Happened?

June 16, 2023



Gonna tell my kids this was Game of Thrones





CYBER SAFETY
REVIEW BOARD



Review of the Summer 2023 Microsoft Exchange Online Intrusion

March 20, 2024
Cyber Safety Review Board

https://www.cisa.gov/sites/default/files/2024-04/CSRB_Review_of_the_Summer_2023_MEO_Intrusion_Final_508c.pdf

When a hacking group associated with the government of the People's Republic of China, known as Storm-0558, compromised Microsoft's cloud environment last year, it struck the espionage equivalent of gold. The threat actors accessed the official email accounts of many of the most senior U.S. government officials managing our country's relationship with the People's Republic of China.

The Board finds that this intrusion was preventable and should never have occurred. The Board also concludes that Microsoft's security culture was inadequate and requires an overhaul, particularly in light of the company's centrality in the technology ecosystem and the level of trust customers place in the company to protect their data and operations.

The Board reaches this conclusion based on:

1. the cascade of Microsoft's avoidable errors that allowed this intrusion to succeed;
2. Microsoft's failure to detect the compromise of its cryptographic crown jewels on its own, relying instead on a customer to reach out to identify anomalies the customer had observed;
3. the Board's assessment of security practices at other cloud service providers, which maintained security controls that Microsoft did not;
4. Microsoft's failure to detect a compromise of an employee's laptop from a recently acquired company prior to allowing it to connect to Microsoft's corporate network in 2021;
5. Microsoft's decision not to correct, in a timely manner, its inaccurate public statements about this incident, including a corporate statement that Microsoft believed it had determined the likely root cause of the intrusion when in fact, it still has not; even though Microsoft acknowledged to the Board in November 2023 that its September 6, 2023 blog post about the root cause was inaccurate, it did not update that post until March 12, 2024, as the Board was concluding its review and only after the Board's repeated questioning about Microsoft's plans to issue a correction;

Throughout this review, the Board identified a series of Microsoft operational and strategic decisions that collectively point to a corporate culture that deprioritized both enterprise security investments and rigorous risk management.

State Department was the first victim to discover the intrusion when, on June 15, 2023, State's security operations center (SOC) detected anomalies in access to its mail systems.¹⁰ The next day, State observed multiple security alerts from a custom rule it had created, known internally as "Big Yellow Taxi,"¹¹ that analyzes data from a log known as MailltemsAccessed, which tracks access to Microsoft Exchange Online mailboxes. State was able to access the MailltemsAccessed log to set up these particular Big Yellow Taxi alerts because it had purchased Microsoft's government agency-focused G5 license that includes enhanced logging capabilities through a product called Microsoft Purview Audit (Premium).¹² The MailltemsAccessed log was not accessible without that "premium" service.¹³

Though the alerts showed activity that could have been considered normal—and, indeed, State had seen false positive Big Yellow Taxi detections in the past—State investigated these incidents and ultimately determined that the alert indicated malicious activity. State triaged the alert as a moderate-level event and, on Friday, June 16, 2023, its security team contacted Microsoft.^{14, 15} Microsoft opened and conducted an investigation of its own, and over the next 10 days, ultimately confirmed that Storm-0558 had gained entry to certain user emails through State's Outlook Web Access (OWA). Concurrently, Microsoft expanded its investigation to identify the 21 additional impacted organizations and 503 related users impacted by the attack and worked to identify and notify impacted U.S. government agencies.¹⁶

Microsoft began notifying potentially impacted organizations and individuals on or about June 19 and July 4, 2023, respectively.^{20, 21} As detailed below, this effort had varying degrees of success. Ultimately, Microsoft determined that Storm-0558 used an acquired MSA consumer token signing key to forge tokens to access Microsoft Exchange Online accounts for 22 enterprise organizations, as well as 503 related personal²² accounts, worldwide.²³ Of the 503 personal accounts reported by Microsoft, at least 391 were in the U.S. and included those of former government officials,²⁴ while others were linked to Western European, Asia-Pacific (APAC), Latin American, and Middle Eastern countries and associated victim organizations.^{25, 26, 27}



Midnight Blizzard

January 12, 2024

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.



ALERT

CISA Issues Emergency Directive 24-02: Mitigating the Significant Risk from Nation- State Compromise of Microsoft Corporate Email System

Release Date: April 11, 2024



Today, CISA publicly issued [Emergency Directive \(ED\) 24-02](#) to address the recent campaign by Russian state-sponsored cyber actor Midnight Blizzard to exfiltrate email correspondence of Federal Civilian Executive Branch (FCEB) agencies through a successful compromise of Microsoft corporate email accounts. This Directive <https://www.cisa.gov/news-events/directives/ed-24-02-mitigating-significant-risk-nation-state-compromise-microsoft-corporate-email-system> requires agencies to analyze the content of exfiltrated emails, reset compromised credentials, and take additional steps to secure privileged Microsoft Azure accounts.

While ED 24-02 requirements only apply to FCEB agencies, other organizations may also have been impacted by the exfiltration of Microsoft corporate email and are encouraged to contact their respective Microsoft account team for any additional questions or follow up. FCEB agencies and state and local government should utilize the distro MBFedResponse@Microsoft.com for any escalations and assistance with Microsoft. Regardless of direct impact, all organizations are strongly encouraged to apply stringent security measures, including strong passwords, multifactor authentication (MFA) and prohibited sharing of unprotected sensitive information via unsecure channels.

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."

Password spray investigation

Article • 11/07/2023 • 8 contributors

[Feedback](#)

In this article

[Prerequisites](#)

[Workflow](#)

[Checklist](#)

[Investigation steps](#)

[Show 6 more](#)

This article provides guidance on identifying and investigating password spray attacks within your organization and taking the required remediation actions to protect information and minimize further risks.

This article contains the following sections:

- **Prerequisites:** Covers the specific requirements you need to complete before starting the investigation. For example, logging that should be turned on, roles and permissions required, among others.
- **Workflow:** Shows the logical flow that you should follow to perform this investigation.
- **Checklist:** Contains a list of tasks for each of the steps in the flow chart. This checklist can be helpful in highly regulated environments to verify what you did or simply as a quality gate for yourself.
- **Investigation steps:** Includes a detailed step-by-step guidance for this specific investigation.
- **Recovery:** Contains high-level steps on how to recover/mitigate from a password spray attack.
- **References:** Contains more reading and reference materials.

Prerequisites

Before starting the investigation, make sure you have completed the setup for logs and alerts and other system requirements.

For Microsoft Entra monitoring, follow our recommendations and guidance in our [Microsoft Entra SecOps Guide](#).

Okta Integration

Okta

- Identity & Access Management (IAM) company
- IDP that competes with Azure AD
- AD Integration
 - **Delegated Access:** Allows users to sign into Okta using AD credentials
 - **Okta AD Agent:** Sync users & groups with Okta and also answering authentication requests from Okta as users log into the portal



Okta primarily targets enterprise businesses. Claimed customers as of 2020 include [Zoominfo](#), [JetBlue](#), [Nordstrom](#), [MGM Resorts International](#), and the [U.S. Department of Justice](#).^[11]

Okta for Red Teamers

Adam Chester (@_xpn_)

<https://www.trustedsec.com/blog/okta-for-red-teamers/>

September 18, 2023

By Adam Chester in [Red Team Adversarial Attack Simulation](#)

For a long time, Red Teamers have been preaching the mantra "Don't make Domain Admin the goal of the assessment" and it appears that customers are listening. Now, you're much more likely to see objectives focused on services critical to an organization, with many being hosted in the cloud.

With this shift in delegating some of the security burden to cloud services, it's commonplace to find Identity Providers (IDP) like Microsoft Entra ID or Okta being used. This means that our attention as attackers also needs to shift to encompass these services too.

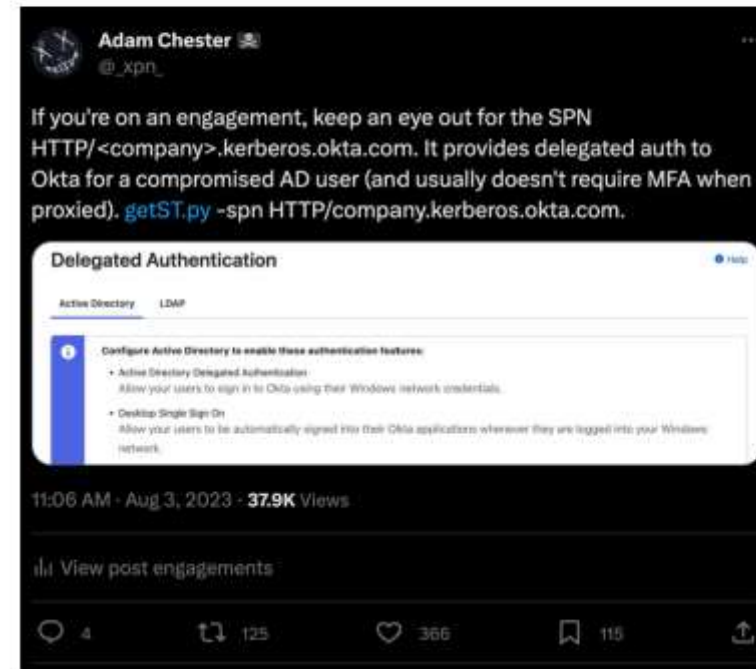
In this blog post, I'll discuss some of the post-exploitation techniques that I've found to be useful against one such provider, Okta, which has been one of the more popular solutions found in customer environments.

It should be noted that everything in this post is by design. You'll find no 0dayz here, and many of the techniques require administrative access to pull off. However, to say that the methods demonstrated in this post have been a helpful during engagements is an understatement. Let's dive in.

OKTA DELEGATED AUTHENTICATION

We'll start with a technology offered to users deploying their Okta tenant alongside traditional on-prem Active Directory (AD), and that is Delegated Authentication.

I recently Tweeted a method that I've found useful when compromising Delegated Authentication enabled tenants:



Attacking Okta: Delegated Access

- Compromise a User Account in AD
 - Leverage this to auth to Okta to SSO to other systems (typically with no MFA)
- Compromise the Okta service Account in AD
 - Auth to Okta as any AD user & SSO to other systems

```
> ticketer.py -domain-sid S-1-5-21-4170871944-1575468979-147100471 -domain lab.local -dc-ip DC01 -aesKey db22ab9c89f2f0d545024f9dfabbed44173397065d8f5b7e172200ca38ed4393 -user-id 1118 -spn HTTP/example.kerberos.okta.com testuser
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Creating basic skeleton ticket and PAC Infos
[*] Customizing ticket for lab.local/testuser
[*] PAC_LOGON_INFO
[*] PAC_CLIENT_INFO_TYPE
[*] EncTicketPart
[*] EncTGSRepPart
[*] Signing/Encrypting final ticket
[*] PAC_SERVER_CHECKSUM
[*] PAC_PRIVSVR_CHECKSUM
[*] EncTicketPart
[*] EncTGSRepPart
[*] Saving ticket in testuser.ccache
```

```
> ticketer.py -domain-sid S-1-5-21-4170871944-1575468979-147100471 -domain lab.local -dc-ip DC01 -aesKey db22ab9c89f2f0d545024f9dfabbed44173397065d8f5b7e172200ca38ed4393 -user-id 1118 -spn HTTP/example.kerberos.okta.com testuser
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Creating basic skeleton ticket and PAC Infos
[*] Customizing ticket for lab.local/testuser
[*] PAC_LOGON_INFO
[*] PAC_CLIENT_INFO_TYPE
[*] EncTicketPart
[*] EncTGSRepPart
[*] Signing/Encrypting final ticket
[*] PAC_SERVER_CHECKSUM
[*] PAC_PRIVSVR_CHECKSUM
[*] EncTicketPart
[*] EncTGSRepPart
[*] Saving ticket in testuser.ccache
```

Adam Chester (@_xpn_)

<https://www.trustedsec.com/blog/okta-for-red-teamers/>

Attacking Okta: Okta AD Agent

- Capture AD Credentials (clear-text username & password)
 - Compromise AD users who are authenticating to Okta
- Okta Skeleton Key (Fake AD Agent)
 - Leverage AD Admin rights

```
xml
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<action>
  <UserAuth actionId="rpc::app.active_directory.agent.reply.ok14-majoracs@2a.auw2-
ok14.internal//1670637714886//Y5PoJoeQQ3KDgHHzA11P9wAAC8g:e90888489-99ff-435a-943b-
b7dccc457cb5:">
    <type>USER_AUTH</type>
    <password>abc123</password>
    <useLdapGroupPasswordPolicy>false</useLdapGroupPasswordPolicy>
    <userName>[email protected]</userName>
  </UserAuth>
</action>
```

```
> python ./main.py --tenant-domain STENANT_DOMAIN --skeleton-key MibbleMobble99 oauth --machine-name DC03 --windows-d
omain lab.local --code uz9h7o1h
Cloud-Nine (OKTA Version)... by @_xpn_

[*] Creating Agent Token
[*] Token Created: 00e1Nz5
[*] Getting Domain ID
[*] Domain ID is 00
[*] Initialising AD Agent
[*] Agent ID is a51
[*] Sending Agent Checkin
[*] PING Received
[*] Username: test.user@lab.local
[*] Password: Password123
```

Adam Chester (@_xpn_)

<https://www.trustedsec.com/blog/okta-for-red-teamers/>

Okta investigating reports of possible digital breach

By Mary Kay Maloney, Andria Cambron and Sean Lyngass, CNN

Updated 4:09 PM EDT, Tue March 22, 2022



The Okta Inc. website on a laptop computer arranged in Dobbs Ferry, New York, U.S., on Sunday, Feb. 28, 2021.

Okta, an identity authentication service with more than 15,000 customers, said Tuesday that an attacker had access to a support engineer's laptop for five days in January. But the service itself was not breached, according to the company.

The Okta service that customers use to authenticate logins "has not been breached and remains fully operational," Okta Chief Security Officer David Bradbury said in a [blog post](#) Tuesday.

"The potential impact to Okta customers is limited to the access that support engineers have," Bradbury said, adding that these engineers are unable to download customer databases or create or delete users. "Support engineers are also able to facilitate the resetting of passwords and MFA factors for users, but are unable to obtain those passwords."

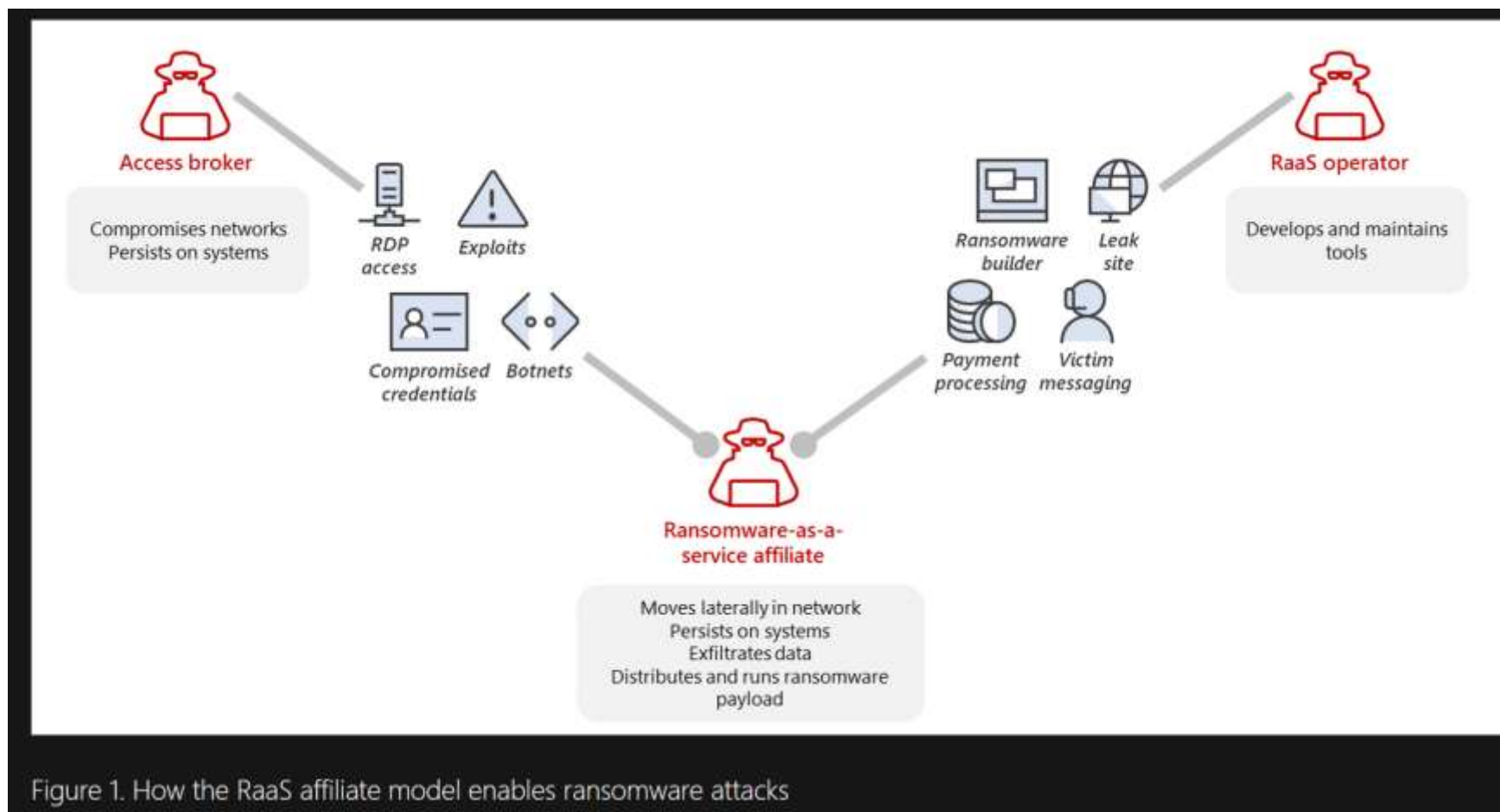
Lapsus\$ (LAPSUS\$)

*"The potential impact to Okta customers is limited to the access that support engineers have," Bradbury said, adding that these engineers are unable to download customer databases or create or delete users. **"Support engineers are also able to facilitate the resetting of passwords and MFA factors for users, but are unable to obtain those passwords."***

The Risk: Attackers

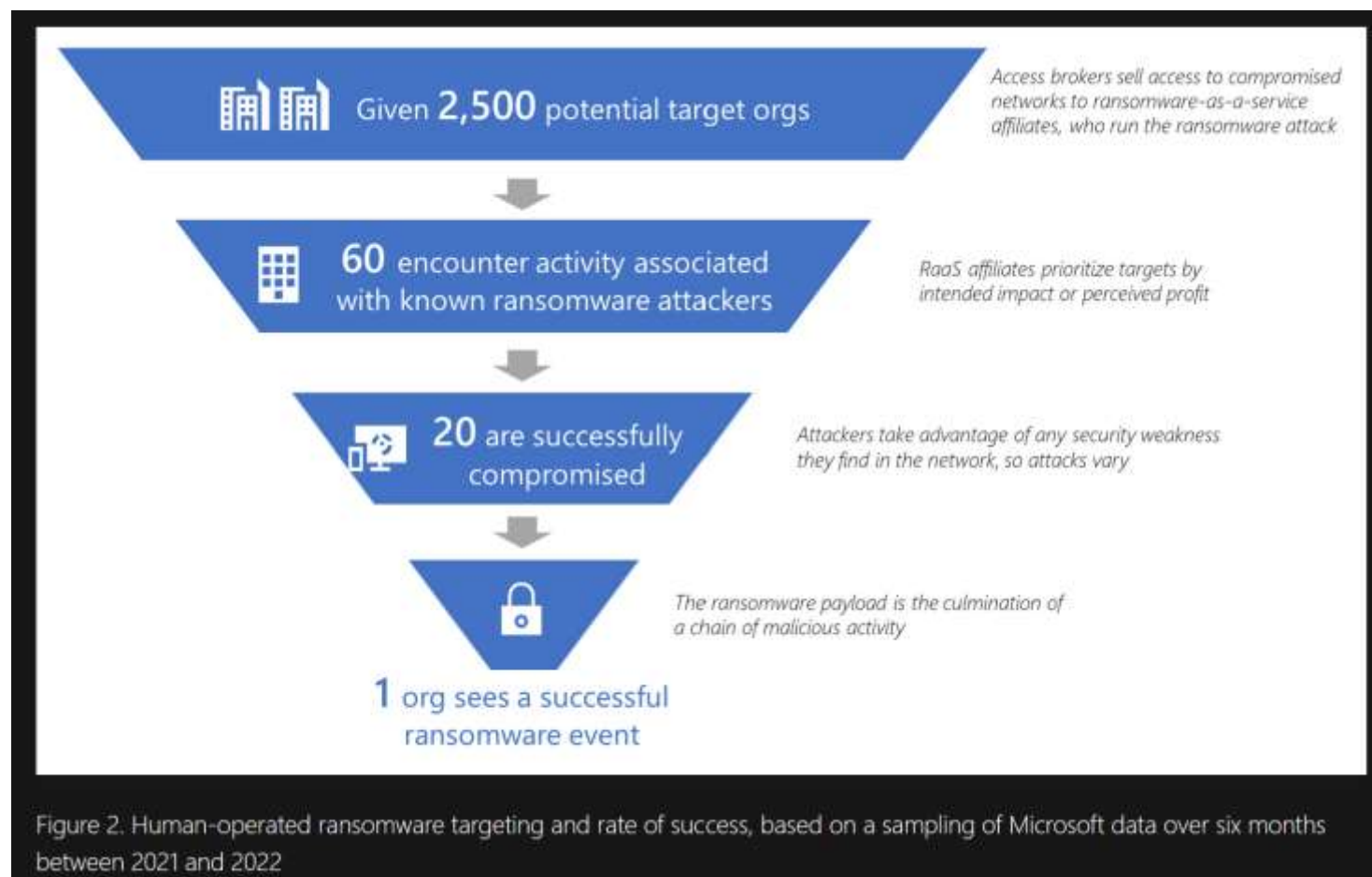


The Business of Cybercrime



<https://www.microsoft.com/en-us/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself/>

The Business of Cybercrime



A timeline of the MGM Resorts hack

September 7: A social engineering attack is launched against the IT support vendor employed by Caesar's Entertainment by hacking gang Scattered Spider. The hotelier pays around half of the \$30 million ransom to the hackers. This gang is later linked to the MGM Resorts cyber attack.

September 11: MGM Resorts puts out a statement saying a "cyber security incident" has affected some of the company's systems. An investigation into the cyber attack is launched and the relevant authorities contacted.

September 12: MGM Resorts makes a second statement reporting that all "resorts including dining, entertainment and gaming are still operational" and that its guests "continue to be able to access their hotel room and [its] Front Desk is ready to assist our guests as needed".

September 12: Guests report a number of issues with MGM Resorts' online booking system and casino. The company's main website is reported as being down.

September 13: VX Underground, host of "one of the largest collection of malware source code, samples, and papers on the internet", makes a post on X saying the MGM cyber attack was the result of vishing. VX Underground also reports that ransomware gang, ALPHV, were responsible for the attack.

September 13: Sources close to the cyber attack say that the hacking group, Scattered Spider, are responsible for the hack.

September 13: Financial services company Moody's says the cyber attack may negatively impact MGM's credit. The company also notes that the cyber security incident highlights "key risks" in MGM's reliance on technology.

September 18: Cyber security experts suggest that ALPHV and Scattered Spider were working together to launch the attack.

<https://www.cshub.com/attacks/news/a-full-timeline-of-the-mgm-resorts-cyber-attack#>



[Book a room](#)[Offers](#)[Entertainment](#)[Dining](#)[Pools](#)[Casino](#)[Spas & salons](#)[Nightlife](#)[MGM Rewards](#)

MGM Resorts recently identified a cybersecurity issue affecting some of the Company's systems. Promptly after detecting the issue, we quickly began an investigation with assistance from leading external cybersecurity experts. We also notified law enforcement and took prompt action to protect our systems and data, including shutting down certain systems.

Although the issue is affecting some of the Company's systems, the vast majority of our property offerings currently remain operational, and we continue to welcome tens of thousands of guests each day. We are ready to welcome you.

Below is additional information to assist you during your stay.

<https://www.mgmresorts.com/en/maintenance/faq.html>



vx-underground 

@vxunderground · [Follow](#)



All ALPHV ransomware group did to compromise MGM Resorts was hop on LinkedIn, find an employee, then call the Help Desk.

A company valued at \$33,900,000,000 was defeated by a 10-minute conversation.

8:45 PM · Sep 12, 2023



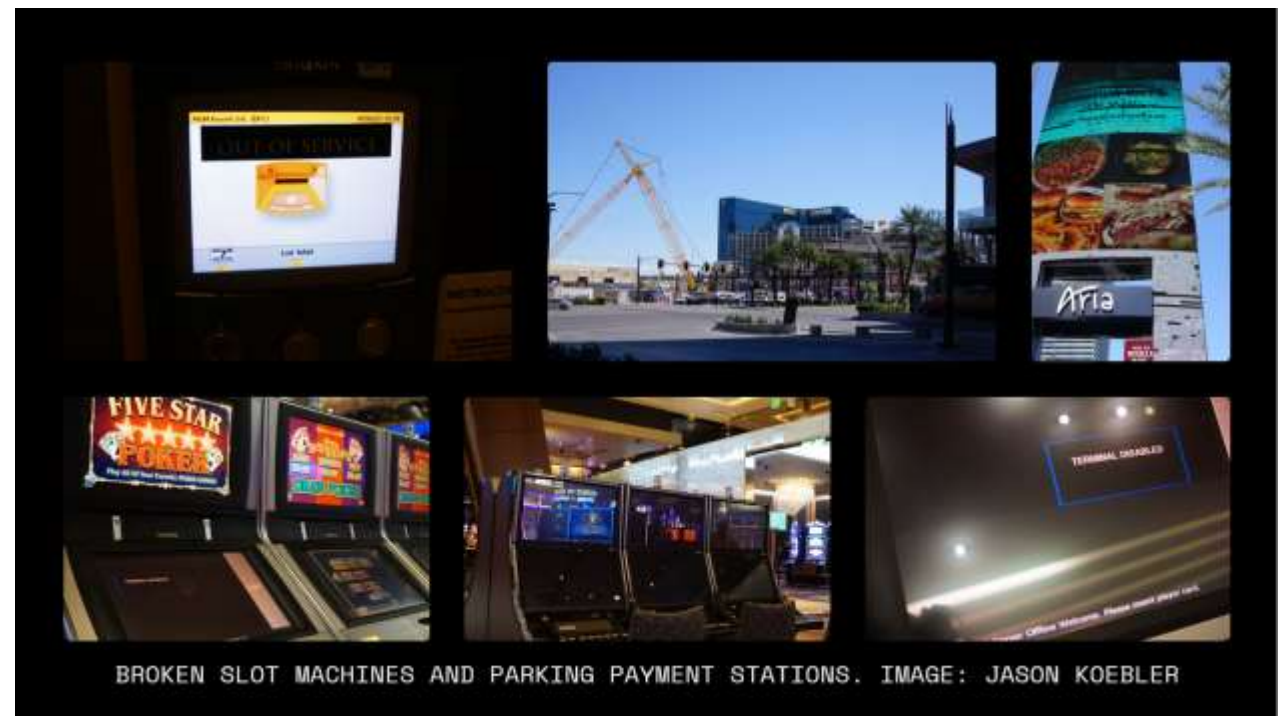
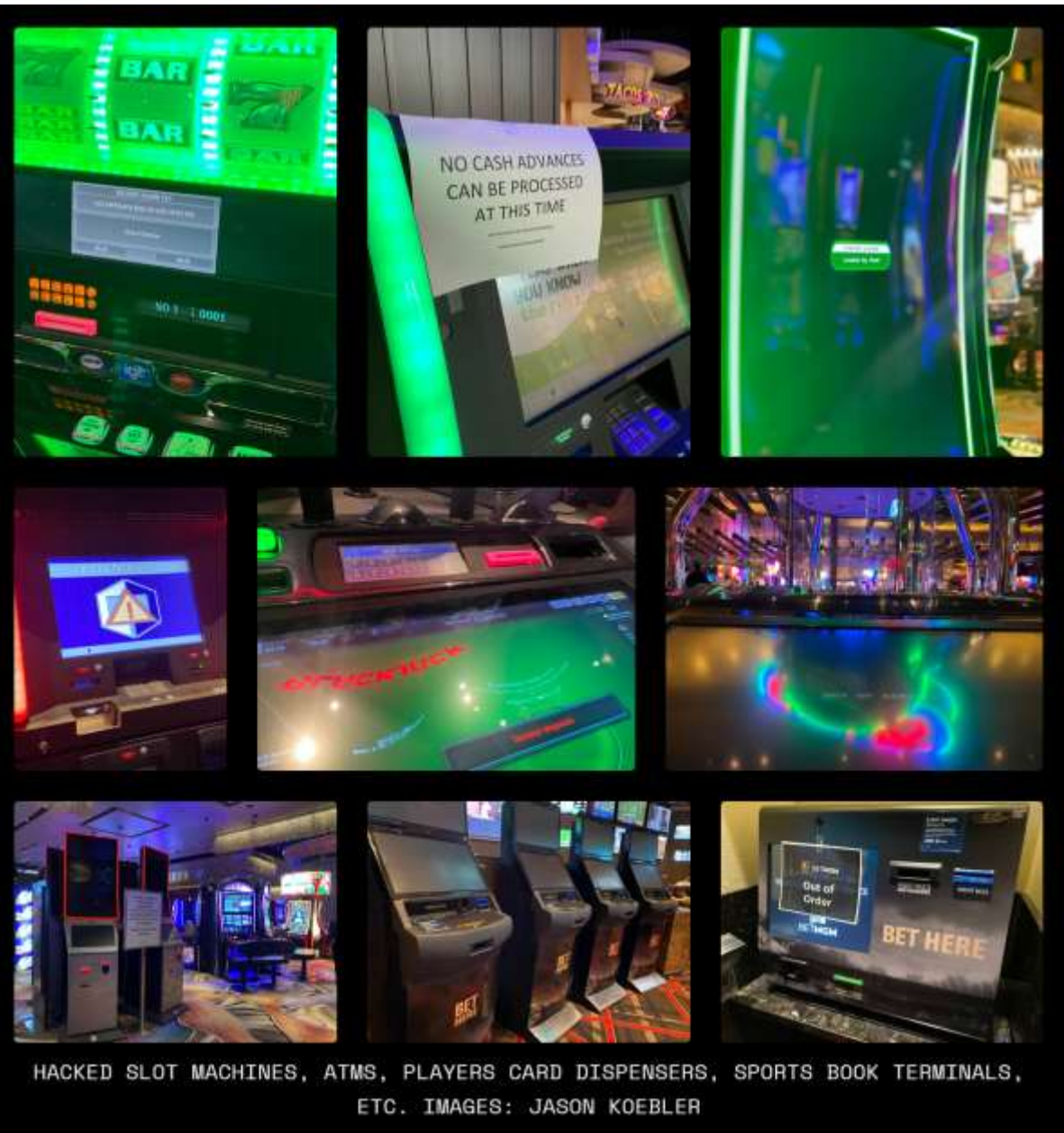
5.2K



Reply



Copy link



<https://www.404media.co/inside-mgms-hacked-casinos/>

MGM Attacker Notes

- We had been lurking on their **Okta Agent servers sniffing passwords of people whose passwords** couldn't be cracked from their domain controller hash dumps.
- We continued having **super administrator privileges to their Okta**
- Along with **Global Administrator privileges to their Azure tenant.**
- Their network has been infiltrated since Friday.
- We successfully **launched ransomware attacks against more than 100 ESXi hypervisors** in their environment on September 11th
- This was after they brought in external firms for assistance in containing the incident.

Caesars Entertainment SEC Filing

Item 8.01 Other Events.

Caesars Entertainment, Inc. (the "Company," "we," or "our") recently identified suspicious activity in its information technology network resulting from a social engineering attack on an outsourced IT support vendor used by the Company. Our customer-facing operations, including our physical properties and our online and mobile gaming applications, have not been impacted by this incident and continue without disruption.

After detecting the suspicious activity, we quickly activated our incident response protocols and implemented a series of containment and remediation measures to reinforce the security of our information technology network. We also launched an investigation, engaged leading cybersecurity firms to assist, and notified law enforcement and state gaming regulators. As a result of our investigation, on September 7, 2023, we determined that the unauthorized actor acquired a copy of, among other data, our loyalty program database, which includes driver's license numbers and/or social security numbers for a significant number of members in the database. We are still investigating the extent of any additional personal or otherwise sensitive information contained in the files acquired by the unauthorized actor. We have no evidence to date that any member passwords/PINs, bank account information, or payment card information (PCI) were acquired by the unauthorized actor.

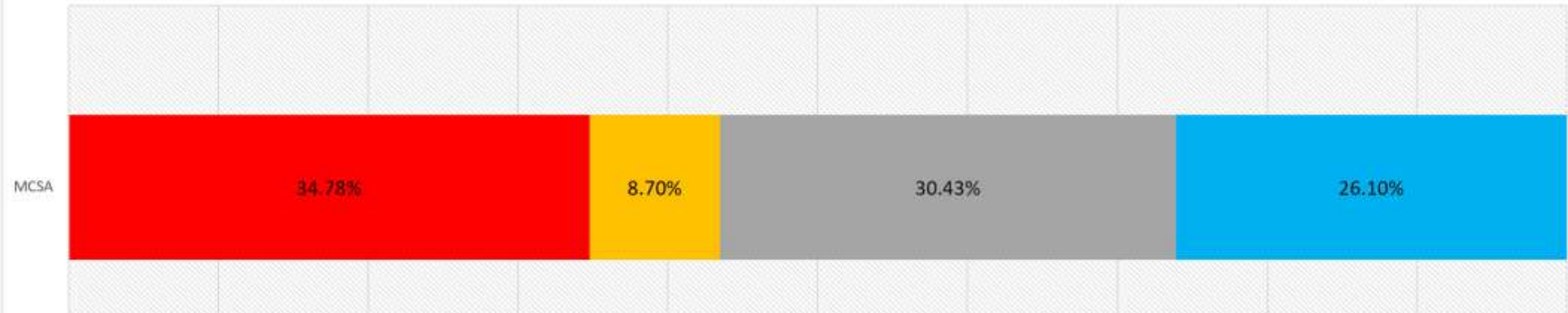
We have taken steps to ensure that the stolen data is deleted by the unauthorized actor, although we cannot guarantee this result. We are monitoring the web and have not seen any evidence that the data has been further shared, published, or otherwise misused. Nonetheless, out of an abundance of caution,

In September of this year, a social engineering attack on another casino operator and hotelier, Caesar's Entertainment, saw the company pay around US\$15 million to hackers. The malicious actors were able to gain access to and steal customer data including driver's license and potentially social security numbers by targeting the IT support vendor Caesar's Entertainment employs.

The background of the slide is a close-up, high-angle shot of a copper-colored printed circuit board (PCB). The board is covered in a complex network of white and gold-colored circuit traces. In the center-left of the frame, a silver-colored metal padlock is placed. The padlock's body is rectangular with rounded corners and features a keyhole. The surface of the padlock is engraved with various alphanumeric strings, including long sequences of binary digits (0s and 1s) and some standard alphanumeric characters. A small, circular blue logo is visible on the upper right portion of the padlock's body. The lighting is soft, creating subtle highlights and shadows that emphasize the textures of the metal padlock and the intricate patterns of the circuit board.

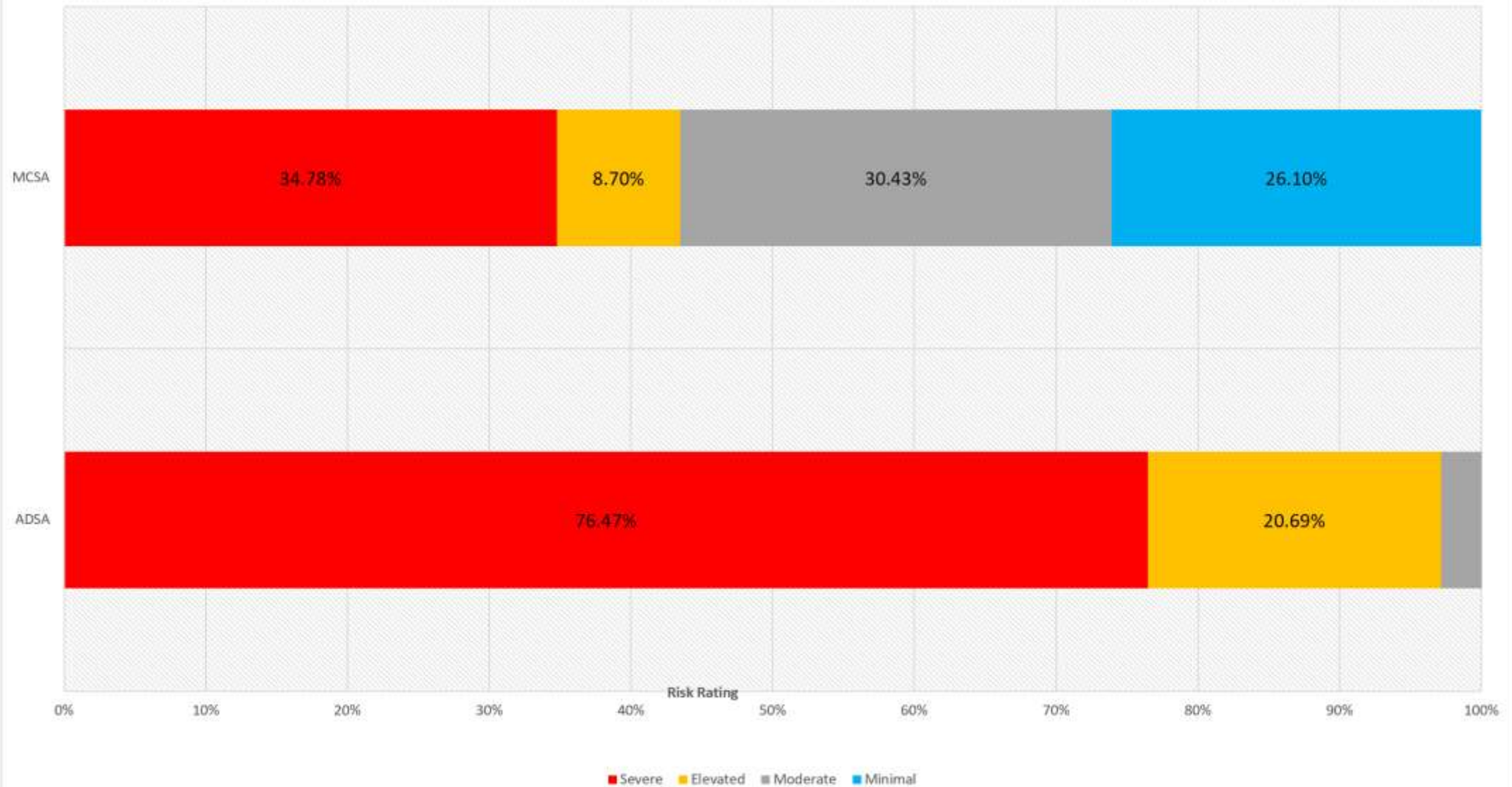
Current State of Microsoft Identity Security

Trimarc Risk Rating Per Assessment Type (2023)



■ Severe ■ Elevated ■ Moderate ■ Minimal

Trimarc Risk Rating Per Assessment Type (2023)



Fix Common Issues



Active Directory

Tool:

<https://github.com/Trimarc/Invoke-TrimarcADChecks>

Article:

<https://www.hub.trimarcsecurity.com/post/securing-active-directory-performing-an-active-directory-security-review>



ADCS

Locksmith Tool:

<https://github.com/Trimarc/locksmith>

Conclusion



There are typical security issues in most enterprise environments (AD & Azure AD/Entra ID)

Identifying common security issues and resolving them improves system security.

Fixing these issues provides improved breach resilience.



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

Sean Metcalf | @PyroTek3 | sean@trimarcsecurity.com



TRIMARC



Questions?