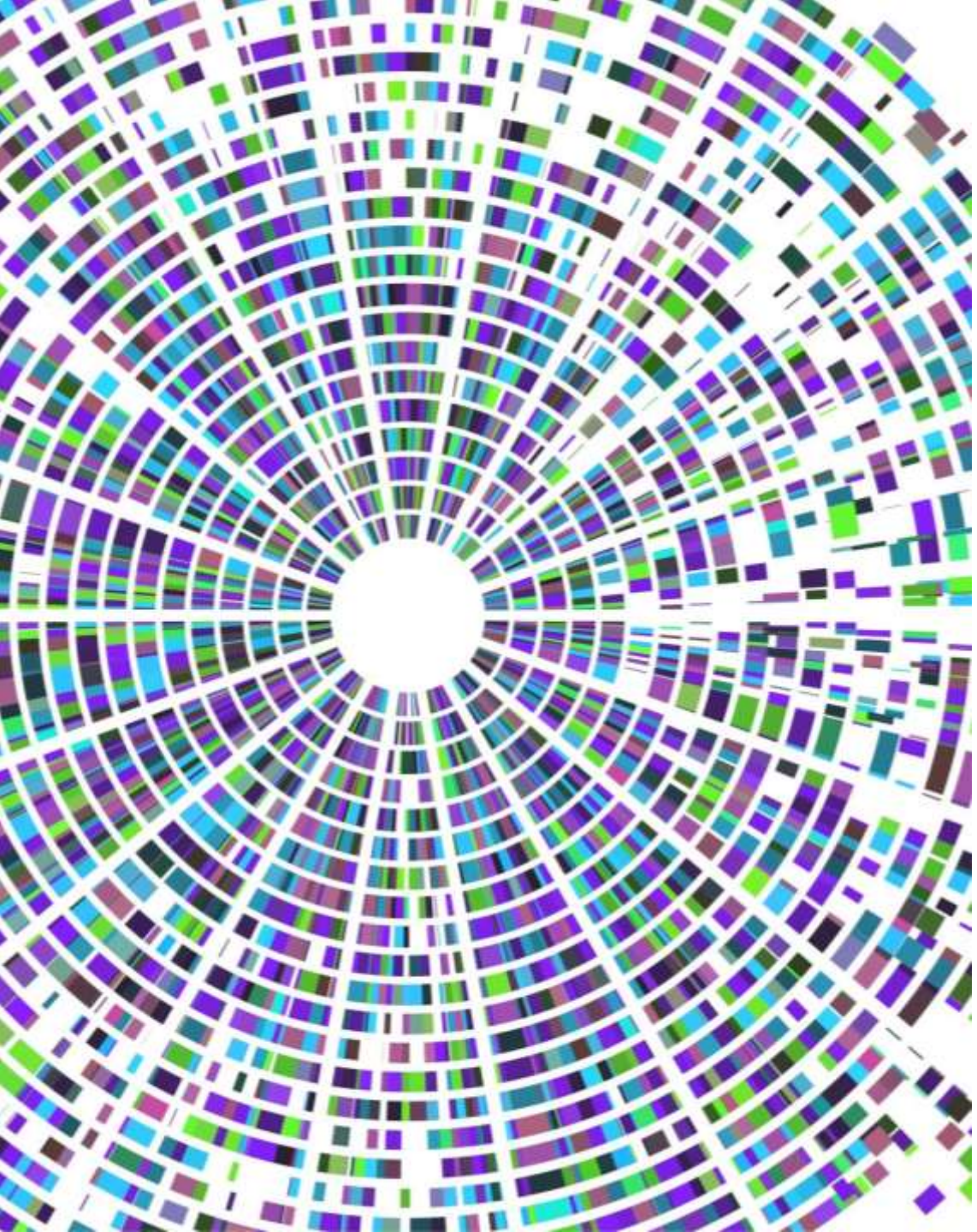


The Current State of Microsoft Identity Security: Common Security Issues and Misconfigurations

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, & 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

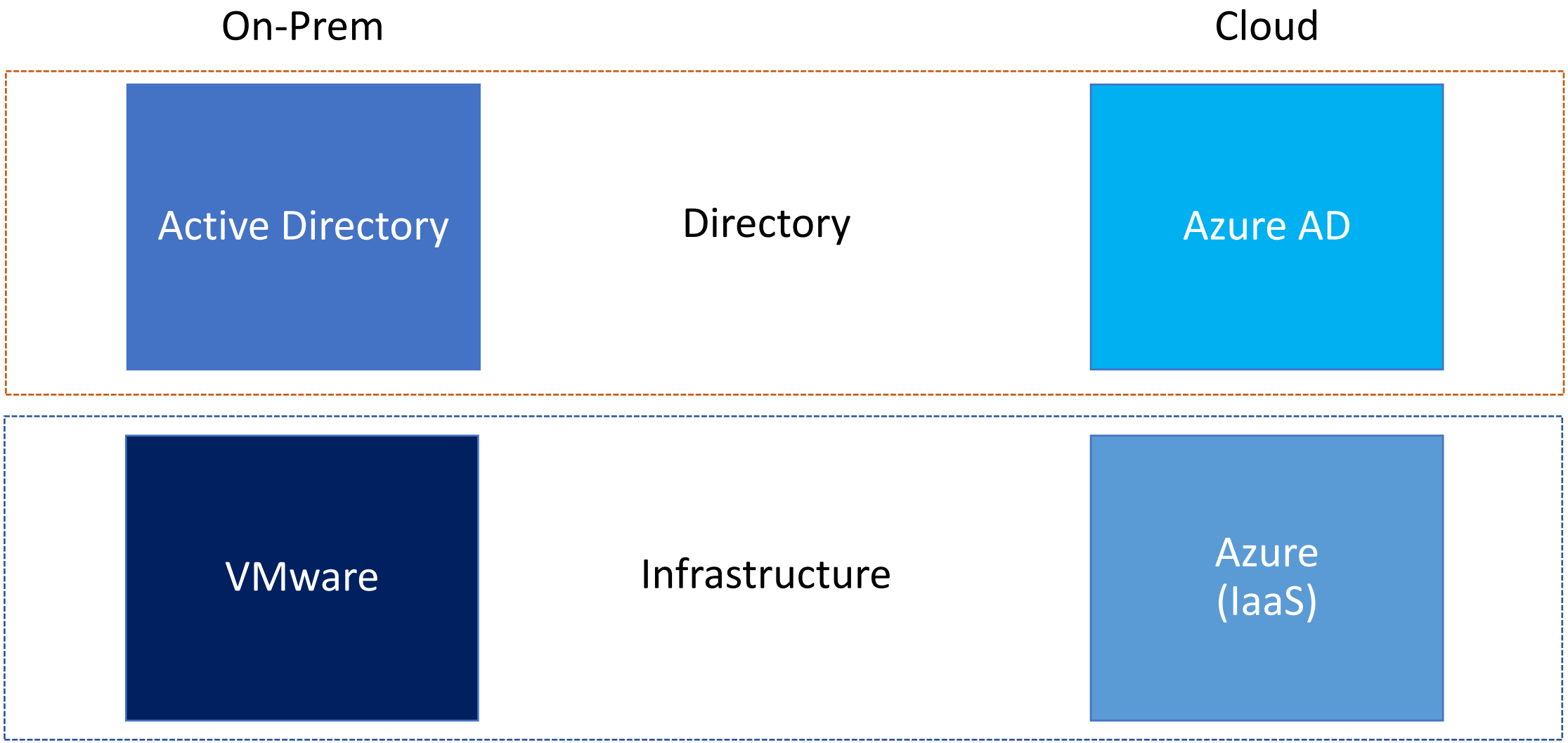
- Introduction
- The Identity Nexus
- Common Security Issues
  - Active Directory
  - Active Directory Certificate Services (ADCS)
  - Azure AD / Entra ID
  - Okta Integration
- Attacks: Caesars & MGM
- Cloud Risks
- Current State of Microsoft Identity Security
- Conclusion

Sean Metcalf
Founder/CTO Trimarc

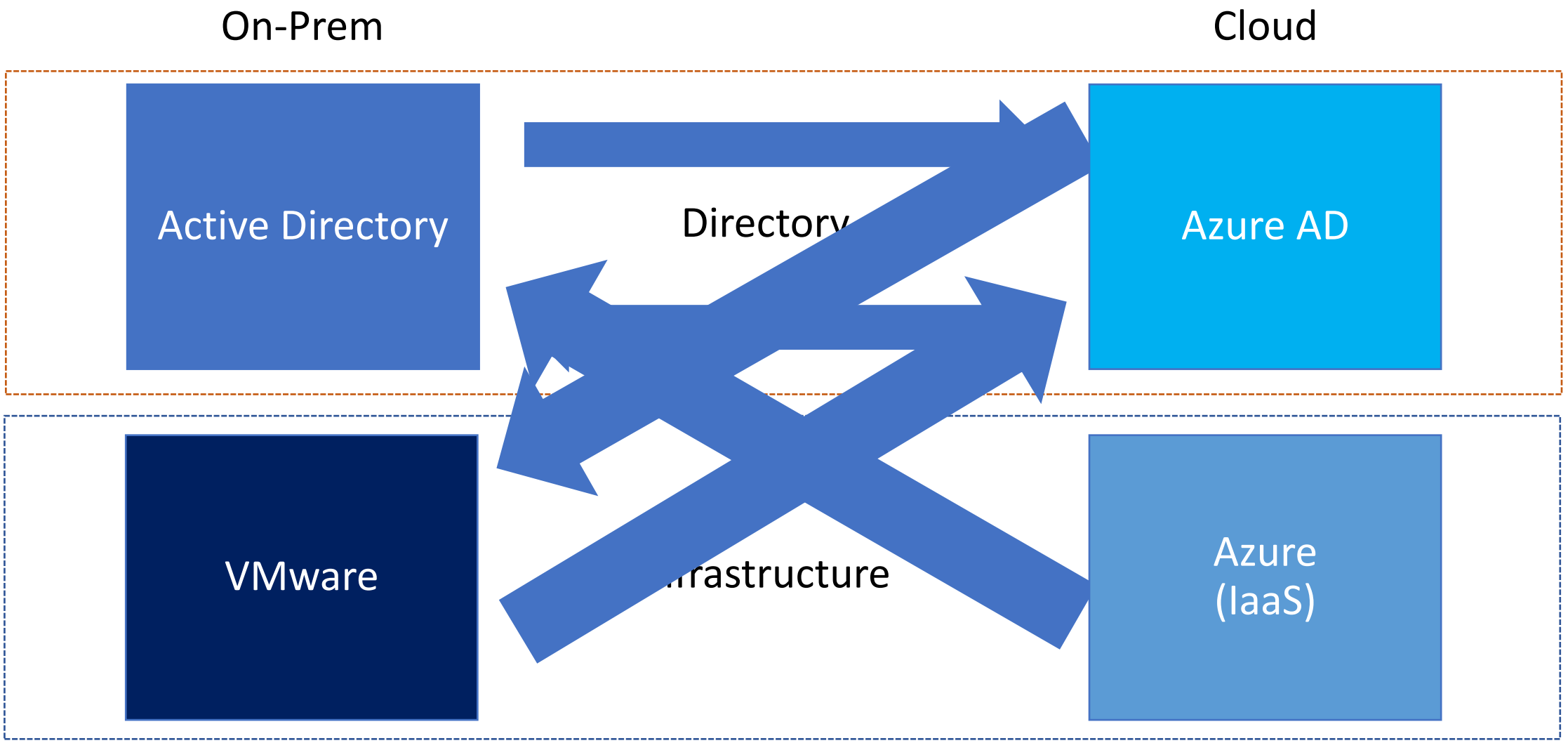
Defending the Identity Nexus

#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-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?

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

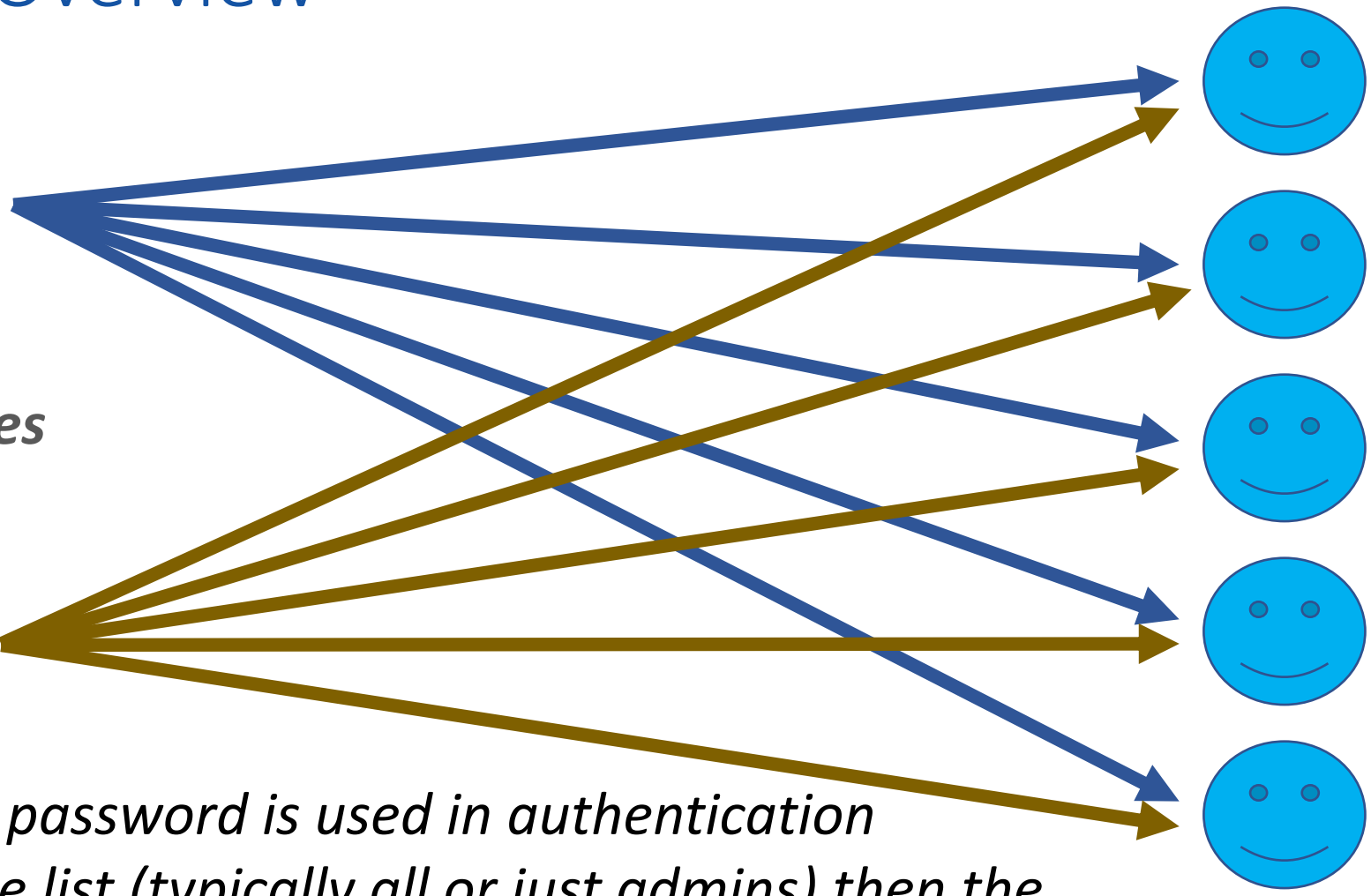
Account Usage

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
```

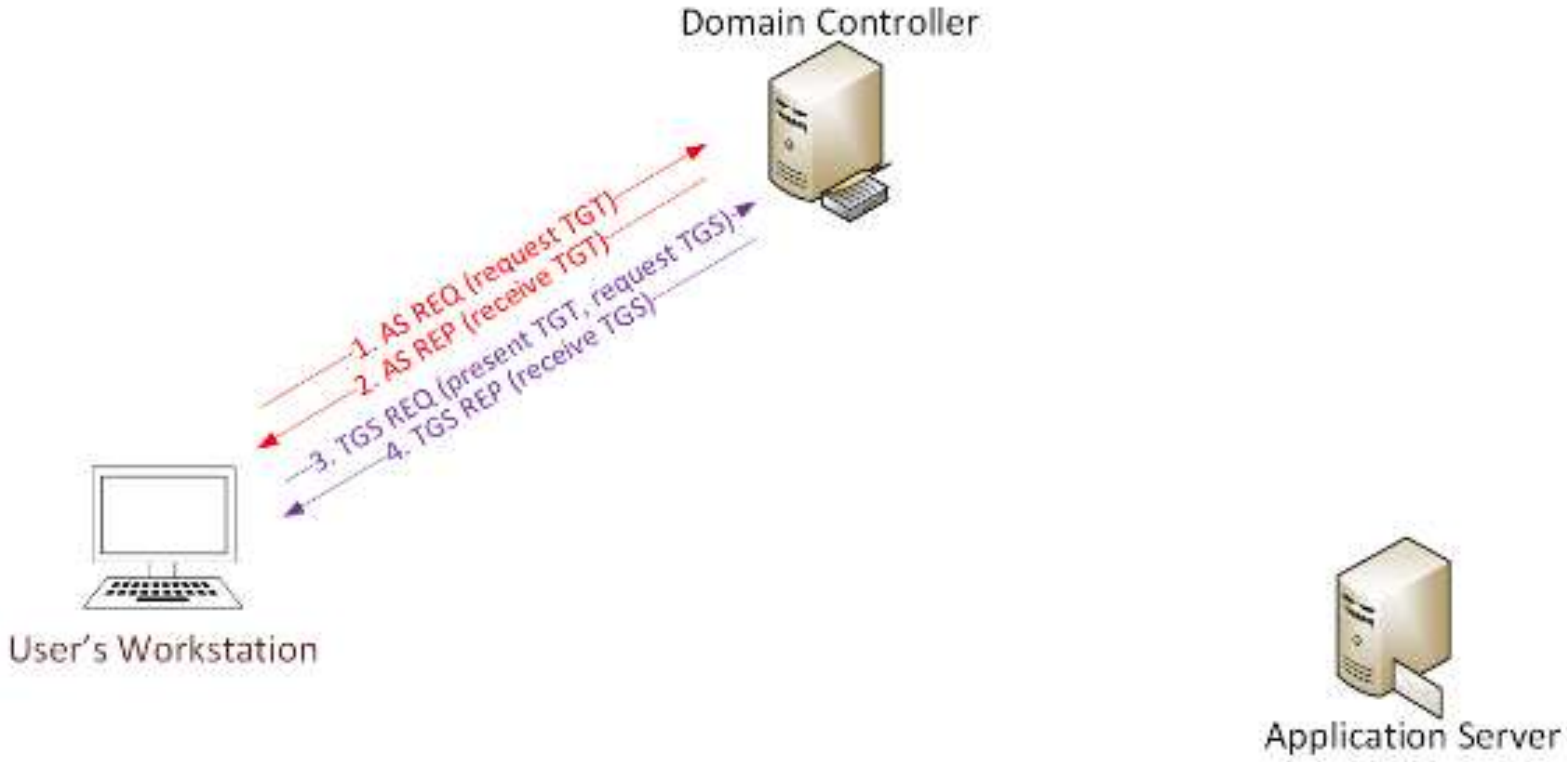
Password Spraying Overview



No account lockout since 1 password is used in authentication attempt for each user in the list (typically all or just admins) then the password spray tool pauses before moving onto the next password.

Cracking Service Account Passwords (Kerberoast)

Request/Save TGS service tickets & crack offline.



- User requests service tickets for targeted service account.
- No elevated rights required.
- No traffic sent to target.

Action: Limit Password Attack Capability

Password Spraying

Implement a Password filter to reduce “bad passwords” in the environment.

Domain Password Policy should be set to 12 characters or more (preferably 15).

Fine-Grained Password Policies (FGPP) provide flexibility.

Kerberoast

Ensure service accounts have passwords >25 characters.

Leverage Group Managed Service Accounts (GMSAs) where possible.

Create honeypot account & monitor for Kerberos Authentication.

https://www.hub.trimarcsecurity.com/post/trimarc-research-detecting-kerberoasting-activity

Check Default Domain Administrator Account for Issues

- Account Enabled?
- Password changed recently?
- Account has a SPN?
- Recent logon?
  Account should be reserved as an emergency account (aka “break glass)

```
lab.trimarcresearch.com Default Domain Administrator Account:


Name          Enabled Created              PasswordLastSet      LastLogonDate        ServicePrincipalName
----          ------- -------              ---------------      -------------        --------------------
Administrator    True 11/10/2019 3:36:51 PM 5/19/2020 4:32:44 PM 5/11/2020 1:16:56 PM {MSSQLSvc/GammaDB23:1434, MSSQLSvc/GammaDB14:1434, MSSQLSvc/Gamm
```

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?

https://Trimarc.co/ADCheckScript

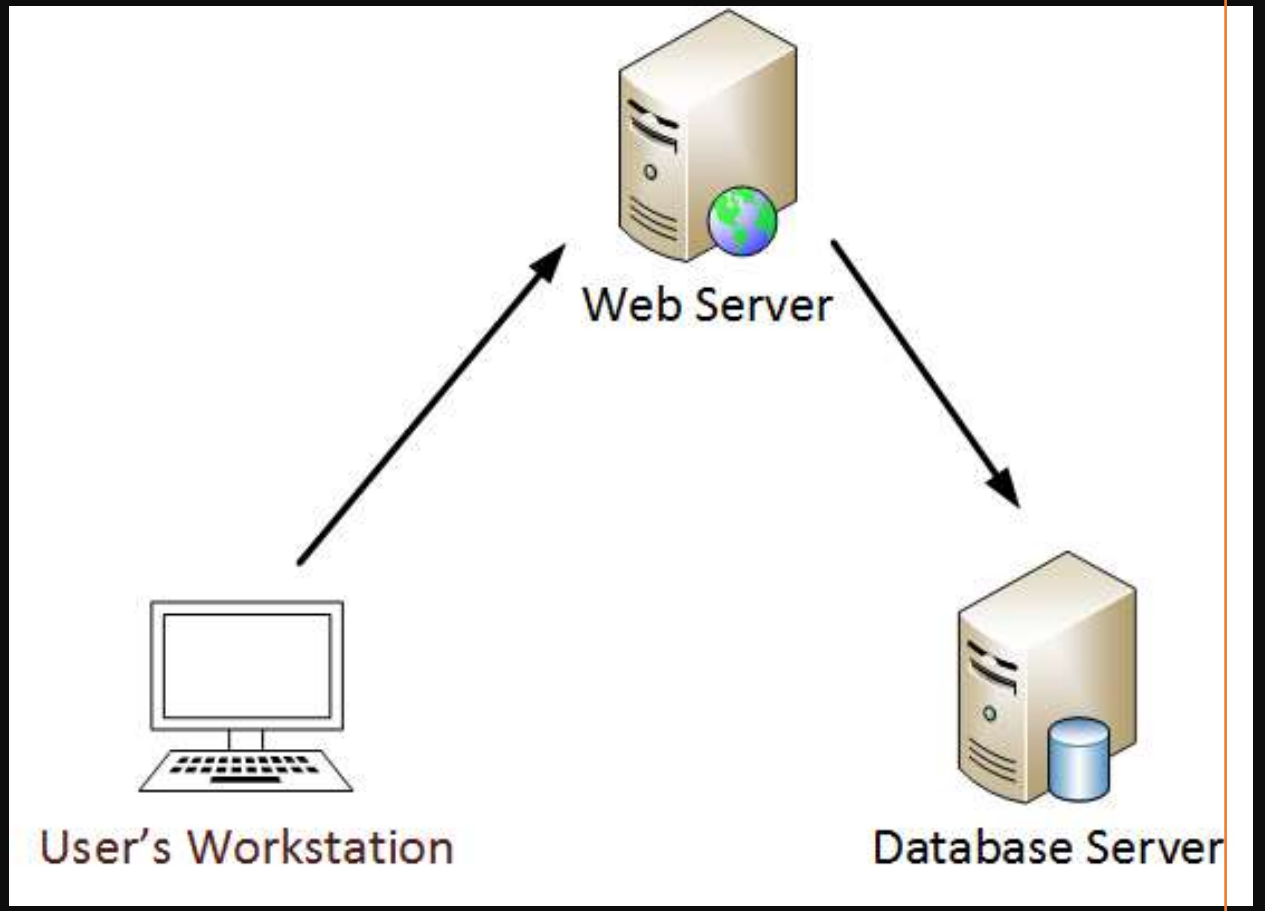
Action: Improving AD Admin Account Security

- 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).

Action: Reducing Service Account Rights

- Determine rights actually required.
- Delegate only these rights.
- Remove from AD Admin groups (Domain Admins, Enterprise Admins, domain Administrators, etc).
- Leverage Group Managed Service Account (GMSA) to manage account password automatically.
- Limit service account access & location (especially if highly privileged).
- Prevent Interactive logon capability

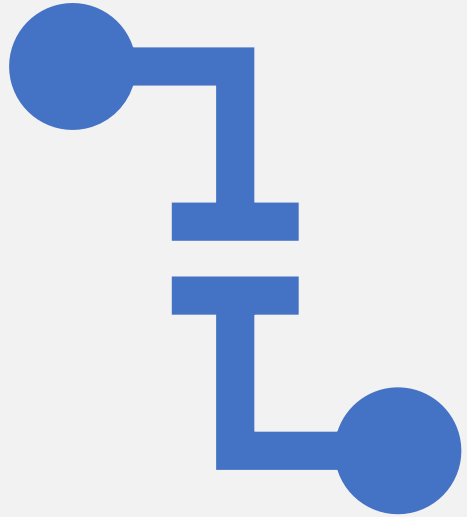
Common AD Security Issues:
Kerberos Delegation



Kerberos Delegation

Delegation = Impersonation

- **Unconstrained:**
  Impersonate users connecting to service to ANY Kerberos service.
- **Constrained:**
  Impersonate authenticated users connecting to service to SPECIFIC Kerberos services on servers.
- **Constrained with Protocol Transition:**
  Impersonate any user to SPECIFIC Kerberos services on servers. (aka “Kerberos Magic”)
- **Resource-based Constrained Delegation:**
  Enables delegation configured on the resource instead of the account.



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

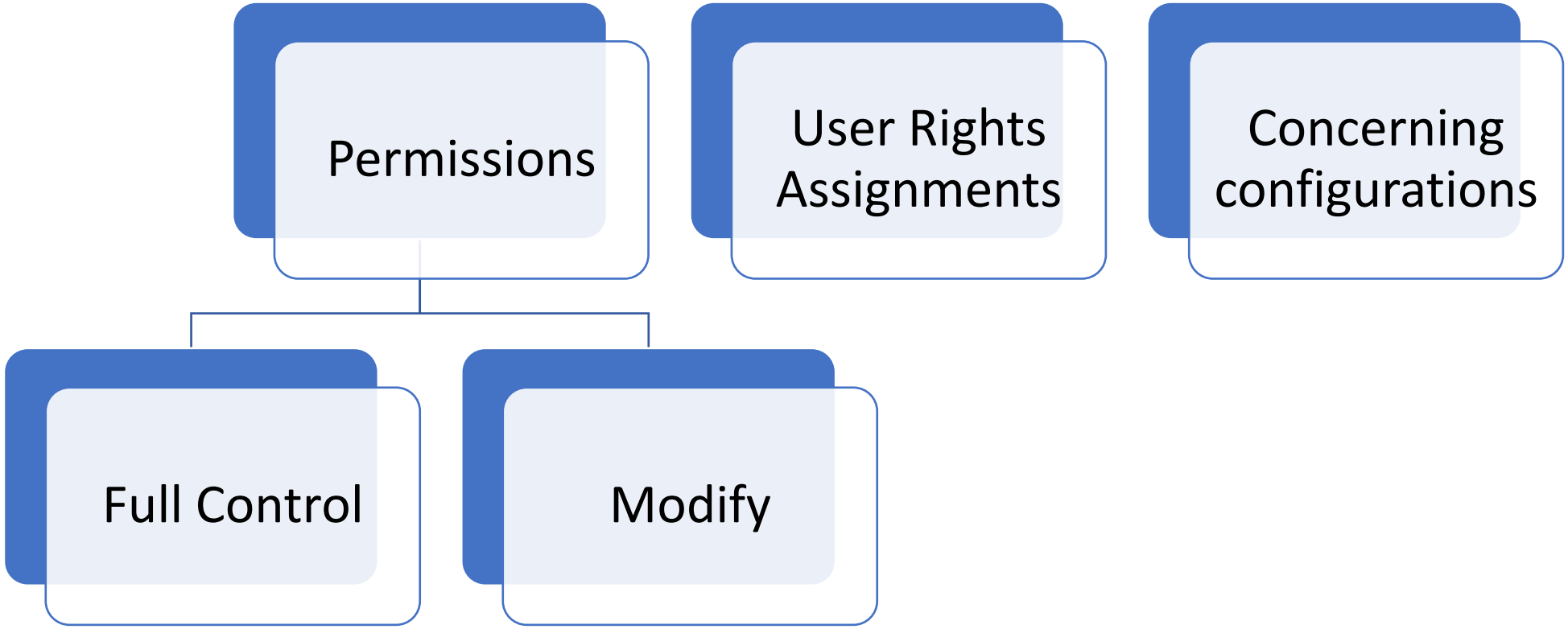
Domain Permission Delegation Issues

```
Domain                : lab.trimarcresearch.com
IdentityReference     : TRDLAB\Domain Computers
ActiveDirectoryRights : Full Control
ObjectAttribute       : user All
InheritedObjectClass  : user
ObjectClass           : All
AccessControlType     : Allow
IsInherited           : False
ObjectFlags           : InheritedObjectAceTypePresent
InheritanceFlags      : ContainerInherit
PropagationFlags      : InheritOnly
FlaggedForReview      : True
```

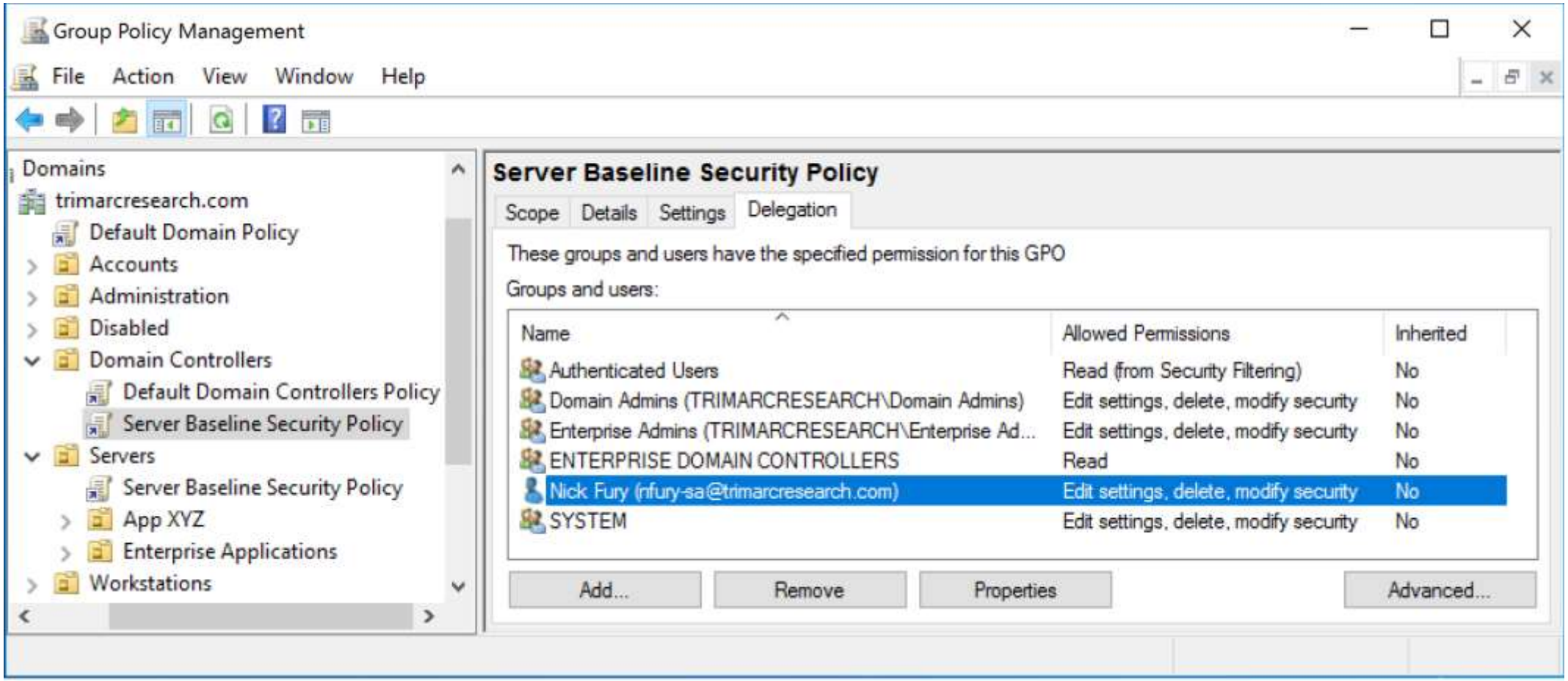
Domain Permission Delegation Issues

```
Domain                : lab.trimarcresearch.com
IdentityReference     : TRDLAB\ServerAdmins
ActiveDirectoryRights : ReadProperty, WriteProperty, ExtendedRight, GenericExecute
ObjectAttribute       : computer All
InheritedObjectClass  : computer
ObjectClass           : All
AccessControlType     : Allow
IsInherited           : False
ObjectFlags           : InheritedObjectAceTypePresent
InheritanceFlags      : ContainerInherit
PropagationFlags      : InheritOnly
FlaggedForReview      : False
```

Group Policy Misconfiguration



Modify Rights to GPOs at Domain or DC Level

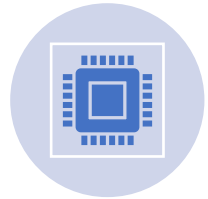


Only AD Admins should have modify rights on GPOs linked to the Domain/Domain Controllers.

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

Print Spooler Service Issues

PrinterBug/SpoolSample is a no-fix vuln in print spooler notification that can be used to coerce authentication that can be captured or relayed.

There's also attack surface left over from the PrintNightmare series of vulnerabilities if everything isn't configured absolutely perfectly.

Security researchers are still actively looking into the Print Spooler service due to its legacy and anticipated volume of remaining issues

Recommend disabling the Print Spooler service on all DCs and servers that don’t actually use it.

Most Important DC Auditing Settings

- Account Logon
  - Audit Credential Validation: S&F
  - Audit Kerberos Authentication Service: S&F
  - **Audit Kerberos Service Ticket Operations: Success**
  - Account Logon: Audit Other Account Logon Events: S&F
- Account Management
  - Audit Computer Account Management: S&F
  - Audit Other Account Management Events: S&F
  - Audit Security Group Management: S&F
  - Audit User Account Management: S&F
- Detailed Tracking
  - Audit DPAPI Activity: S&F
  - Audit Process Creation: S&F
- DS Access
  - *Audit Directory Service Access*: S&F
  - Audit Directory Service Changes: S&F
- Privilege Use
  - Audit Sensitive Privilege Use: S&F
- Logon and Logoff
  - Audit Account Lockout: Success
  - Audit Logoff: Success
  - Audit Logon: S&F
  - **Audit Special Logon: Success & Failure**
  - Audit Other Logon/Logoff Events
- Object Access
  - Audit File System: Failure
  - Audit Registry: Failure
- Policy Change
  - Audit Audit Policy Change : S&F
  - Audit Authentication Policy Change : S&F
  - Audit MPSSVC Rule-Level Policy Change: Success
- System
  - Audit IPSec Driver: S&F
  - Audit Other System Events: S&F
  - Audit Security State Change : S&F
  - Audit Security System Extension : S&F
  - Audit System Integrity : S&F

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 12.3.5 - 10/26/2023)
- 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

Domain Controller Security: OS Version & Patching

Ensure DCs are running current, supported Windows versions

Should be 2019/2022 since 2012/2012R2 left extended support October 2023.

Ensure DCs are regularly patched

Action: DC Security

Ensure	Ensure	Ensure	Ensure	Review	Ensure
Ensure Advanced Auditing is enabled & configured appropriately in DC-linked GPO	Ensure DC User Rights Assignments are configured appropriately in DC-linked GPOs	Ensure DCs are only operating as Domain Controllers with 0 unnecessary applications	Ensure you are running the current VMWare Tools version on virtual DCs	Review all agents on DCs and identify those that can install/run code	Ensure DCs are running current Windows versions & keep patched

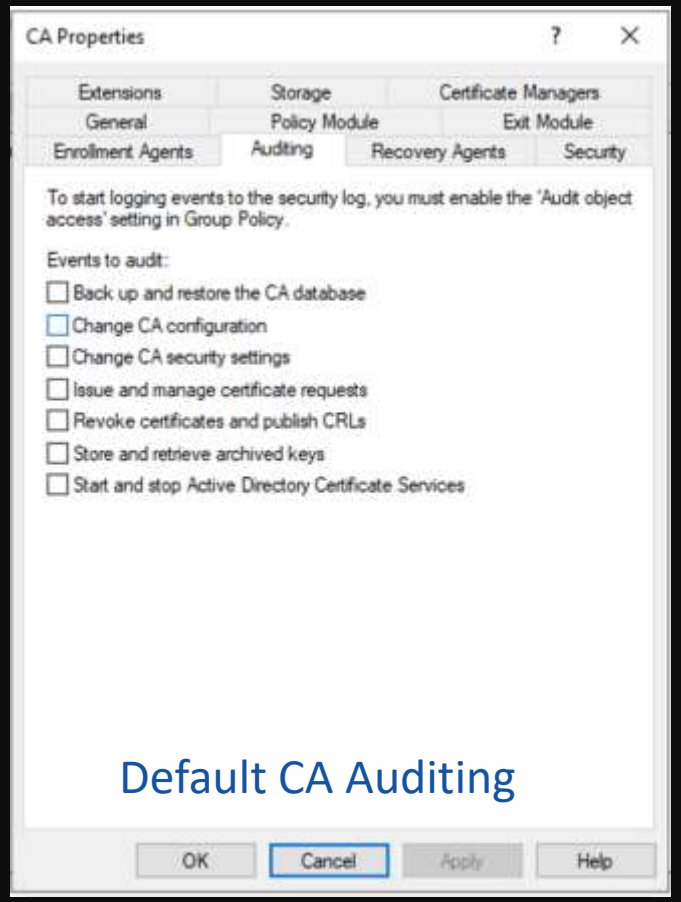
Common AD Security Issues

Active Directory Certificate Services (ADCS)

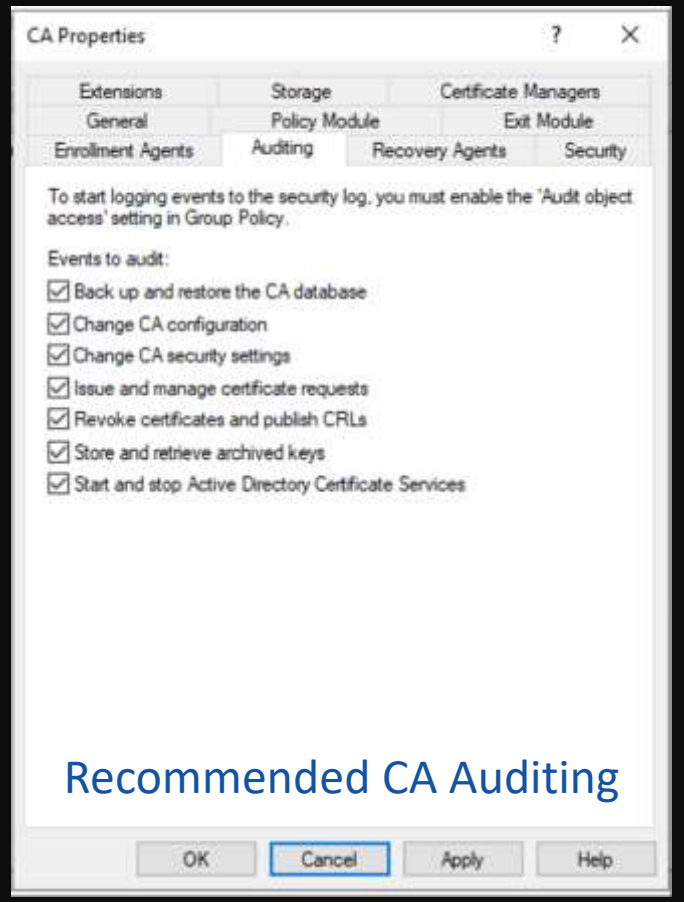
Active Directory Certificate Services (ADCS) Security Issues

- 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



Default CA Auditing



Recommended CA 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

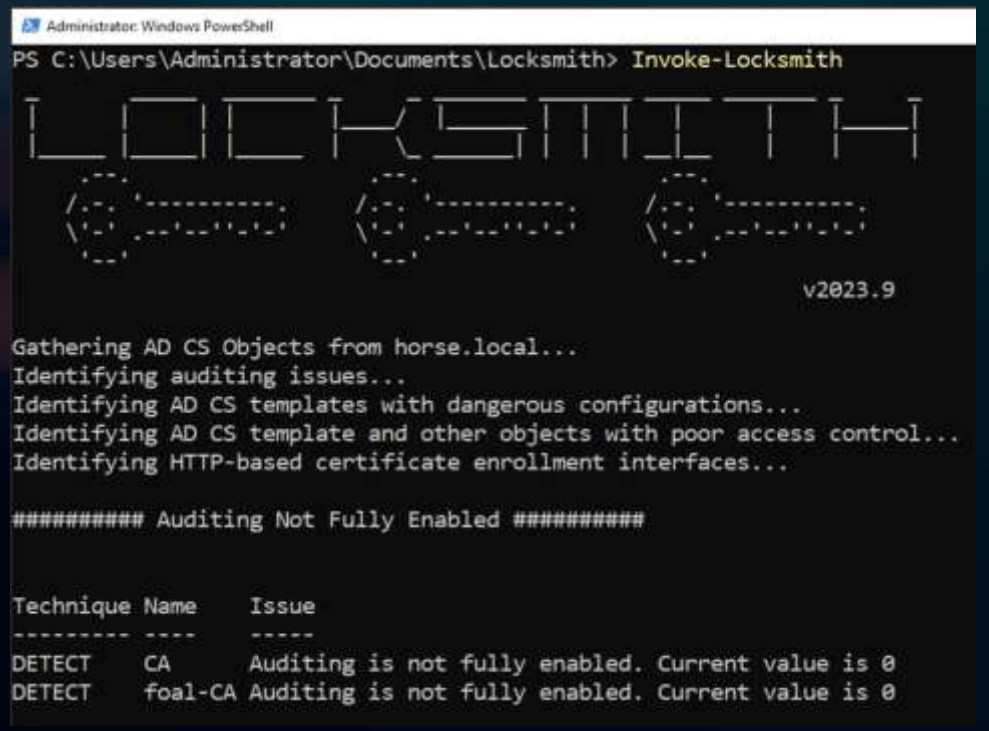
It is strongly recommended not to enable the **EDITF_ATTRIBUTESUBJECALTNAME2 flag** on an enterprise CA. If this is enabled, alternative names are allowed for any Certificate Template issued, regardless of how the subject of the certificate is determined according to the Certificate Template. Using this 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

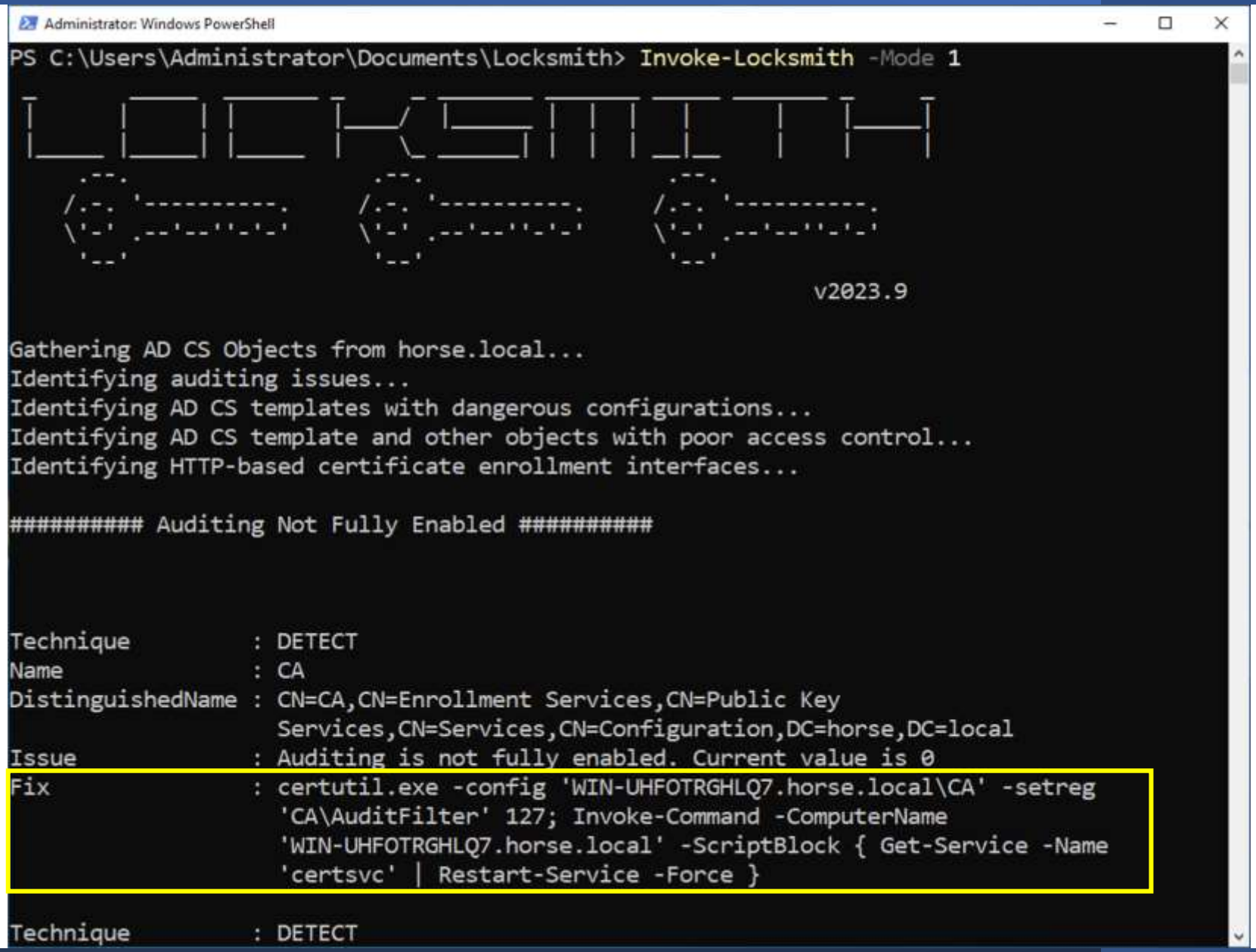
Enforce & Enable	• Enforce HTTPS & Enable Extended Protection for Authentication (EPA)
Disable	• Disable NTLM auth on IIS on your AD CS servers
Disable	• Disable NTLM auth on your AD CS servers
Best Option:	• Remove all ADCS HTTP endpoints.

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



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



https://github.com/Trimarc/locksmith

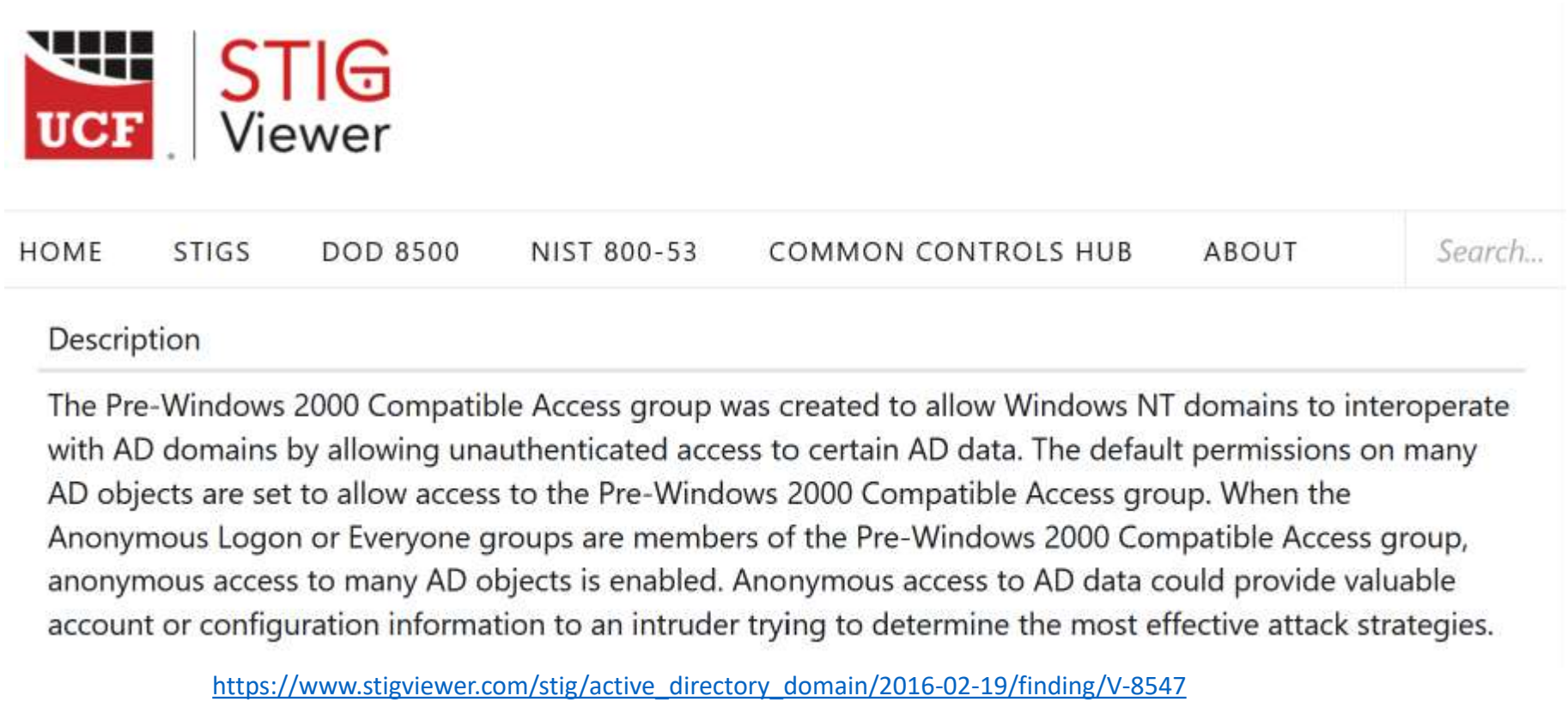
Persistence?

Discovered (likely) AD Persistence During Trimarc Active Directory Security Assessments (ADSAs)

What does Persistence look like?

https://www.thedodo.com/rescue-goat-duck-costume-2107301918.html

“Pre-Windows 2000 Compatible Access” group



https://www.stigviewer.com/stig/active_directory_domain/2016-02-19/finding/V-8547

Unexpected Domain Permissions (Persistence?)

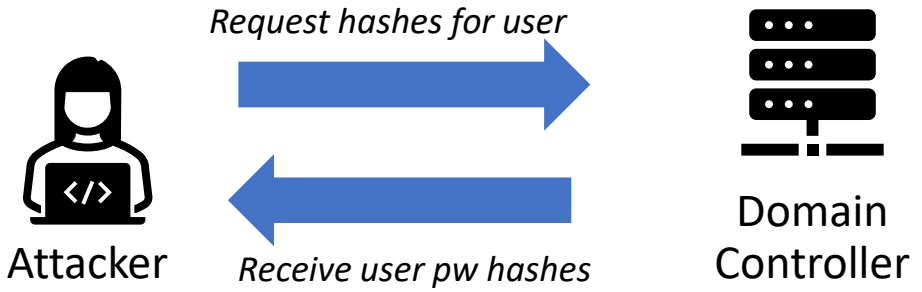
- Domain permissions configured with:
  - Pre-Windows 2000 Compatible Access group delegated permissions:
    - DS-Replication-Get-Changes
    - DS-Replication-Get-Changes-All
    - DS-Install-Replica
    - DS-Replication-Manage-Topology
    - DS-Replication-Synchronize
- Pre-Windows 2000 Compatible Access Group Membership (default):
  - Authenticated Users
  - Everyone

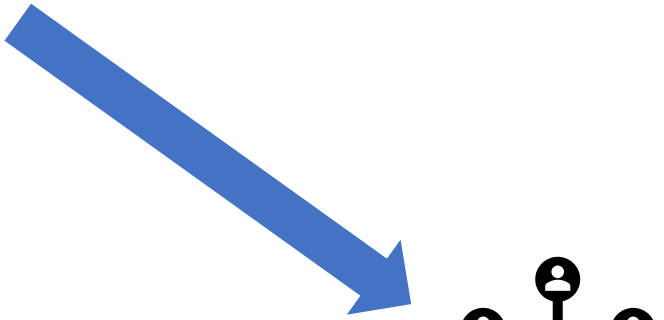
Unexpected Domain Permissions (Persistence?)

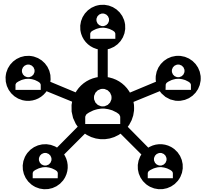
- Domain permissions configured with:
  - Pre-Windows 2000 Compatible Access group delegated permissions:
    - DS-Replication-Get-Changes
    - DS-Replication-Get-Changes-All — DCSync Rights
    - DS-Install-Replica
    - DS-Replication-Manage-Topology
    - DS-Replication-Synchronize — DCShadow Rights
- Pre-Windows 2000 Compatible Access Group Membership (default):
  - Authenticated Users
  - Everyone

DCSync Attack

- Get DA account credentials or account with DCSync rights
- Request credentials for security principal
- Receive all stored hashes





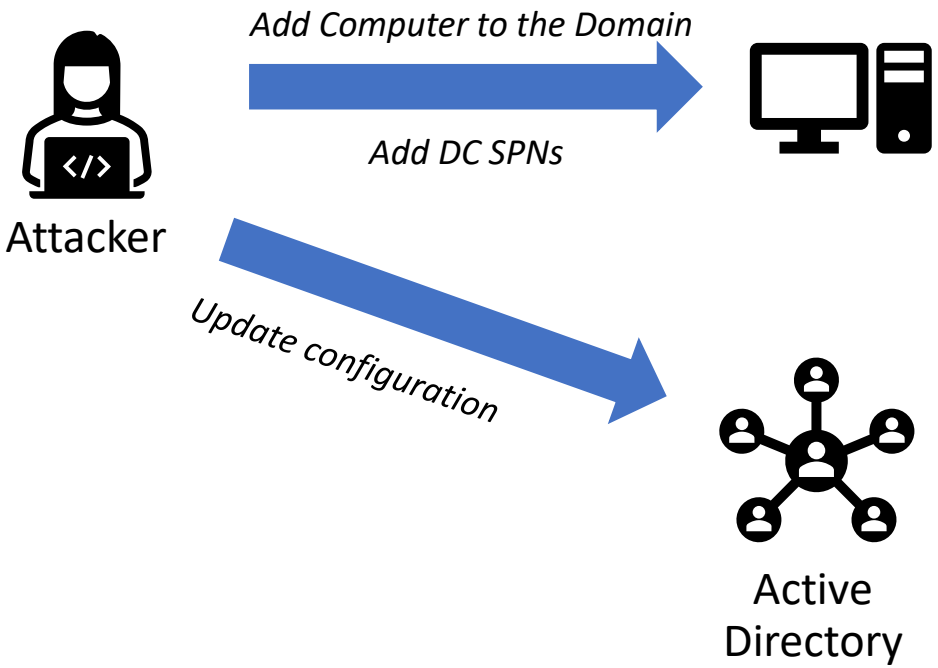



```
mimikatz(commandline) # lsadump::dcsync /domain:rd.adsecurity.org /user:Administrator
[DC] 'rd.adsecurity.org' will be the domain
[DC] 'RDLABDC01.rd.adsecurity.org' will be the DC server

[DC] 'Administrator' will be the user account

Object RDN           : Administrator

** SAM ACCOUNT **

SAM Username         : Administrator
Account Type         : 30000000 ( USER_OBJECT )
User Account Control : 00000200 ( NORMAL_ACCOUNT )
Account expiration   :
Password last change : 9/7/2015 9:54:33 PM
Object Security ID   : S-1-5-21-2578996962-4185879466-3696909401-500
Object Relative ID   : 500

Credentials:
  Hash NTLM: 96ae239ae1f8f186a205b6863a3c955f
    ntlm- 0: 96ae239ae1f8f186a205b6863a3c955f
    ntlm- 1: 5164b7a0fda365d56739954bbbc23835
    ntlm- 2: 7c08d63a2f48f045971bc2236ed3f3ac
    lm  - 0: 6cfd3c1bcc30b3fe5d716fef10f46e49
    lm  - 1: d1726cc03fb143869304c6d3f30fdb8d

Supplemental Credentials:
* Primary:Kerberos-Newer-Keys *
    Default Salt : RD.ADSECURITY.ORGAdministrator
    Default Iterations : 4096
    Credentials
      aes256_hmac       (4096) : 2394f3a0f5bc0b5779bfc610e5d845e78638deac142e3674af58a674b67e102b
      aes128_hmac       (4096) : f4d4892350fbc545f176d418afabf2b2
```

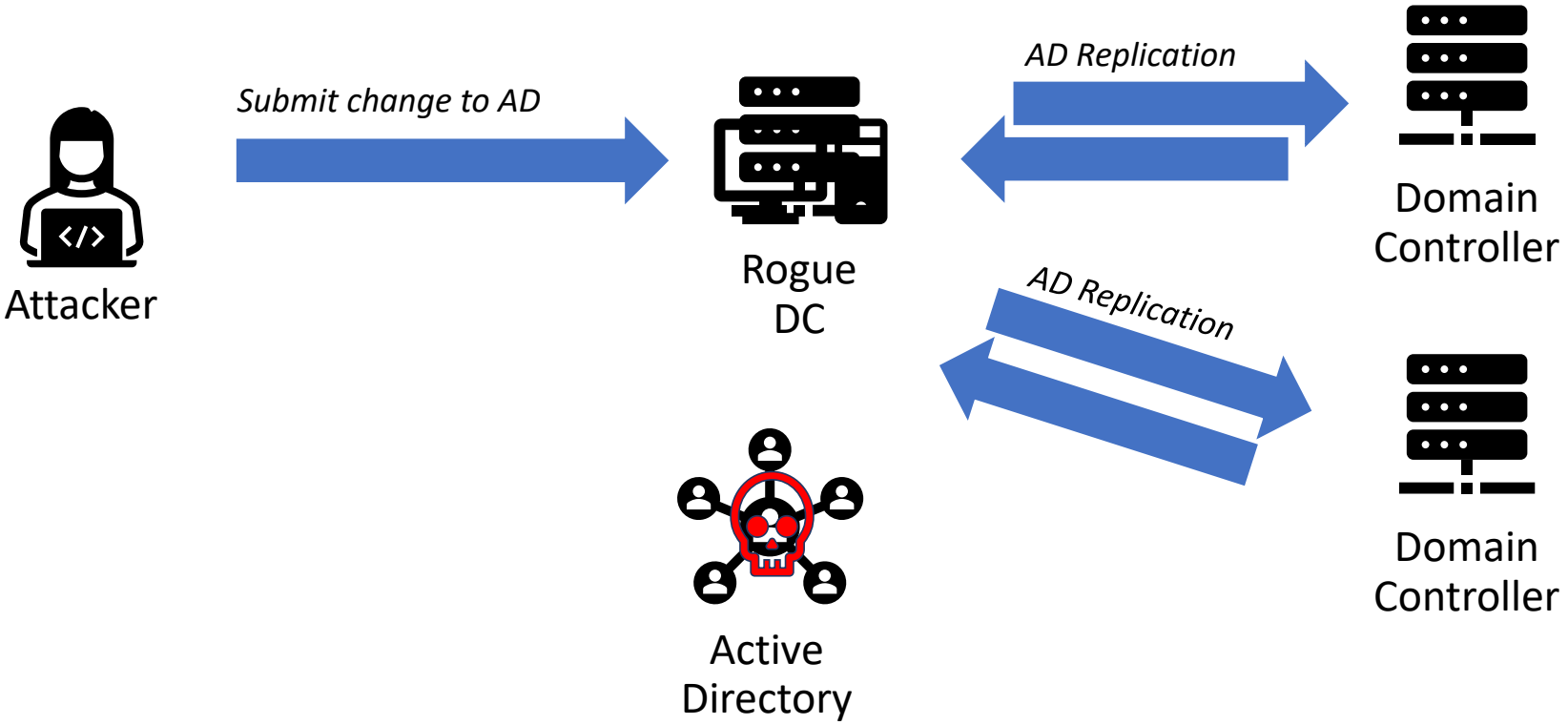
DCShadow

- Attacker gets AD admin rights
- Add a computer object & use as rogue Domain Controller
  - Add a record for the rogue DC in the configuration partition
  - Update workstation's computer object to include DC SPNs
- Submits changes for replication which are discovered by the other DCs and updated on the DCs
- Attacker cleans up the rogue DC

DCShadow: The Setup



DCShadow: Make & Push Changes




I CAN HAS
CHEEZBURGER
DELUXE

Unexpected Domain Permissions (Persistence?): Impact

- Everyone (anyone!) has the ability to pull password hashes for every security principal in Active Directory (via DCSync)
  - Including:
    - AD Admins
    - Domain Controller computer accounts
    - Azure AD Connect Service Account(s)
    - ADFS computer accounts
    - etc.
- Can also push changes to AD (via DCShadow)

Common Security Issues: Azure AD

Azure Active Directory is now Microsoft Entra ID

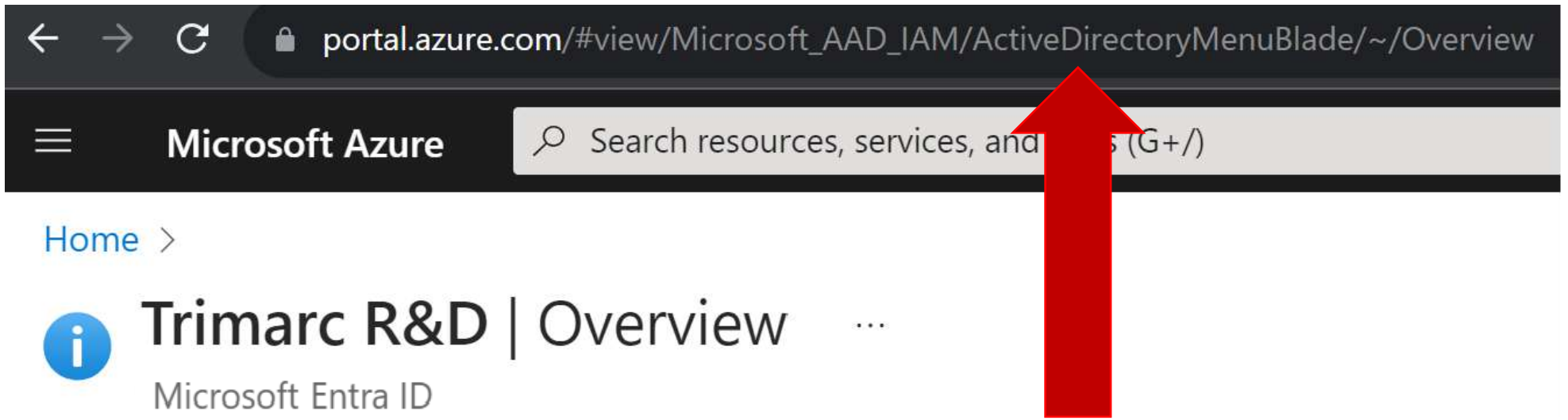
New name, same powerful capabilities.

See pricing and try for free

Learn more about the name change >

Azure AD Free	**Microsoft Entra ID Free**
Azure AD Premium P1 Also included in Microsoft 365 E3	**Microsoft Entra ID P1** Also included in Microsoft 365 E3
Azure AD Premium P2 Also included in Microsoft 365 E5	**Microsoft Entra ID P2** Also included in Microsoft 365 E5
Azure AD External identities	**Microsoft Entra External ID**


Azure Active Directory is now
Microsoft Entra ID
New name, same powerful capabilities.
See pricing and try for free
Learn more about the name change >


portal.azure.com/#view/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/~/Overview
Microsoft Azure
Search resources, services, and
(G+/)
Home >
Trimarc R&D | Overview
Microsoft Entra ID

Safe Links in Microsoft Defender for Office 365

Article • 09/19/2023 • 11 contributors •

Applies to: ✅ Microsoft Defender for Office 365 plan 1 and plan 2, ✅ Microsoft Defender XDR

Common Security Issues: Azure AD/Entra ID

Trimarc Microsoft Cloud Security Assessment (MCSA) Common Issues

Privileged Account Issues

- Standard user accounts
- Service Accounts
- Account Usage
- Using PIM, but all/most are permanent, not eligible.
- Missing MFA on Admin Accounts with highly privileged AAD role rights.

Applications with Highly Privileged Permissions

- Highly privileged applications with regular user as owner
- Standard user in App/Cloud App Admin role(s).

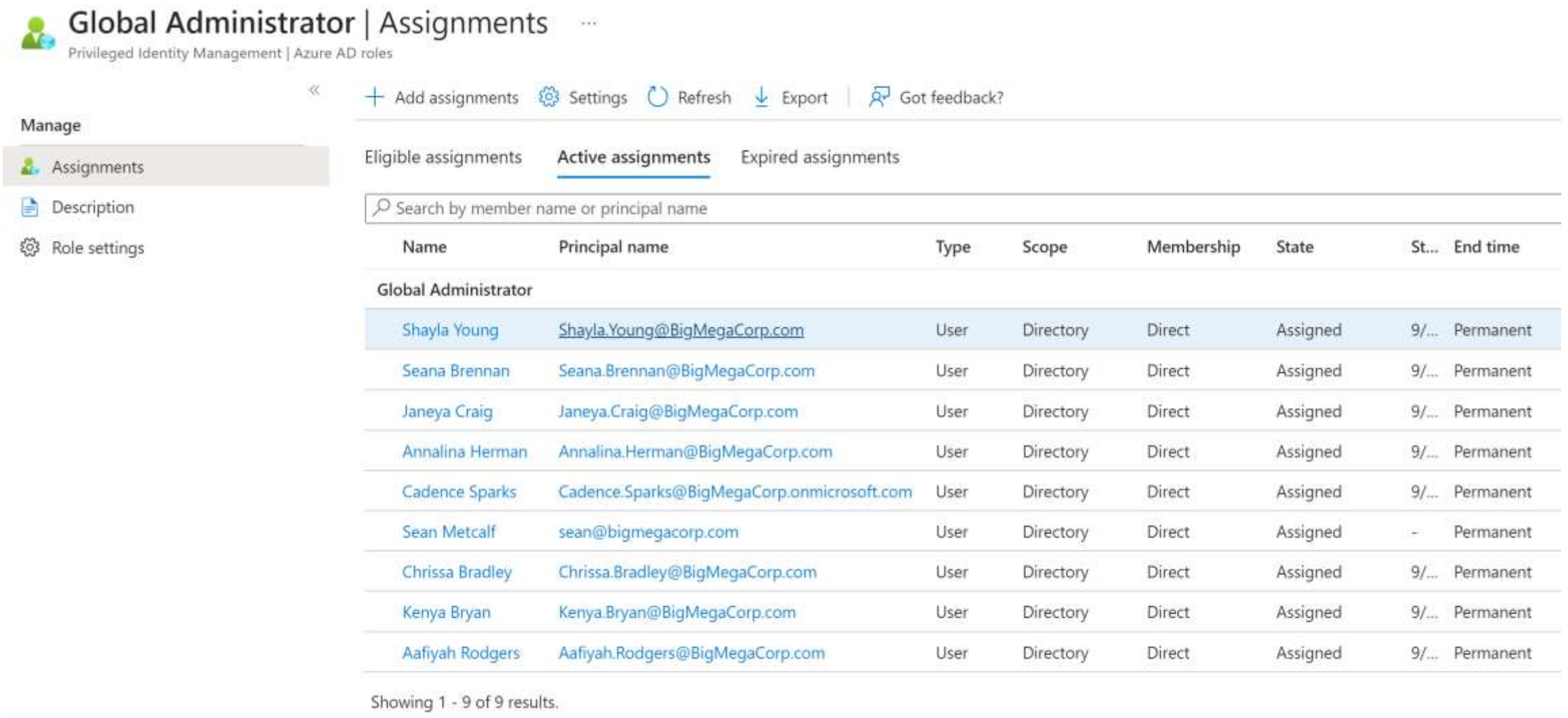
Group Nesting

- Role Assignable Groups in privileged roles

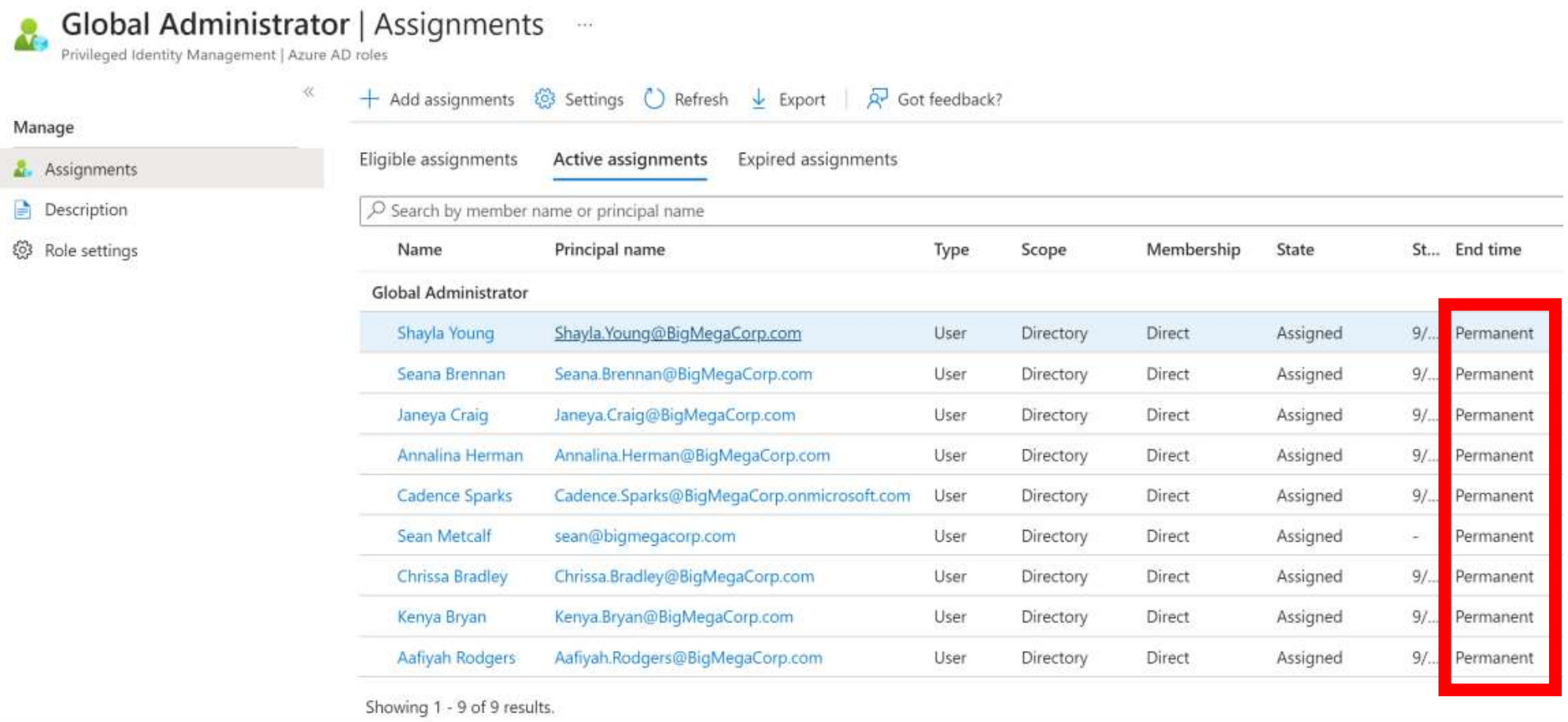
Partner Access - Delegated Access Permissions

- Global Administrator
- Helpdesk Administrator

Highly Privileged Standard User Accounts



PIM Members are Permanent, Not Eligible



Admin Accounts without MFA

```
The Following 5 Global Admin Account(s) have MFA Successfully Configured:

UserDisplayName UserPrincipalName    IsMfaCapable IsMfaRegistered IsPasswordlessCapable MethodsRegistered                                                                  UserPreferredMethodF
--------------- -----------------    ------------ --------------- --------------------- -----------------                                                                  --------------------
Sean Metcalf    sean@bigmegacorp.com         True            True                  True {microsoftAuthenticatorPasswordless, mobilePhone, microsoftAuthenticatorPush, softwareOneTimePasscode} push


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
```

Microsoft's Privileged Azure AD Roles List [PRIVILEGED]

- Application Administrator
- Application Developer
- Authentication Administrator
- B2C IEF Keyset Administrator
- Cloud Application Administrator
- Cloud Device Administrator
- Conditional Access Administrator
- Directory Synchronization Accounts
- Directory Writers
- Global Administrator
- Global Reader
- Helpdesk Administrator
- Hybrid Identity Administrator
- Intune Administrator
- Password Administrator
- Privileged Authentication Administrator
- Privileged Role Administrator
- Security Administrator
- Security Operator
- Security Reader
- User Administrator

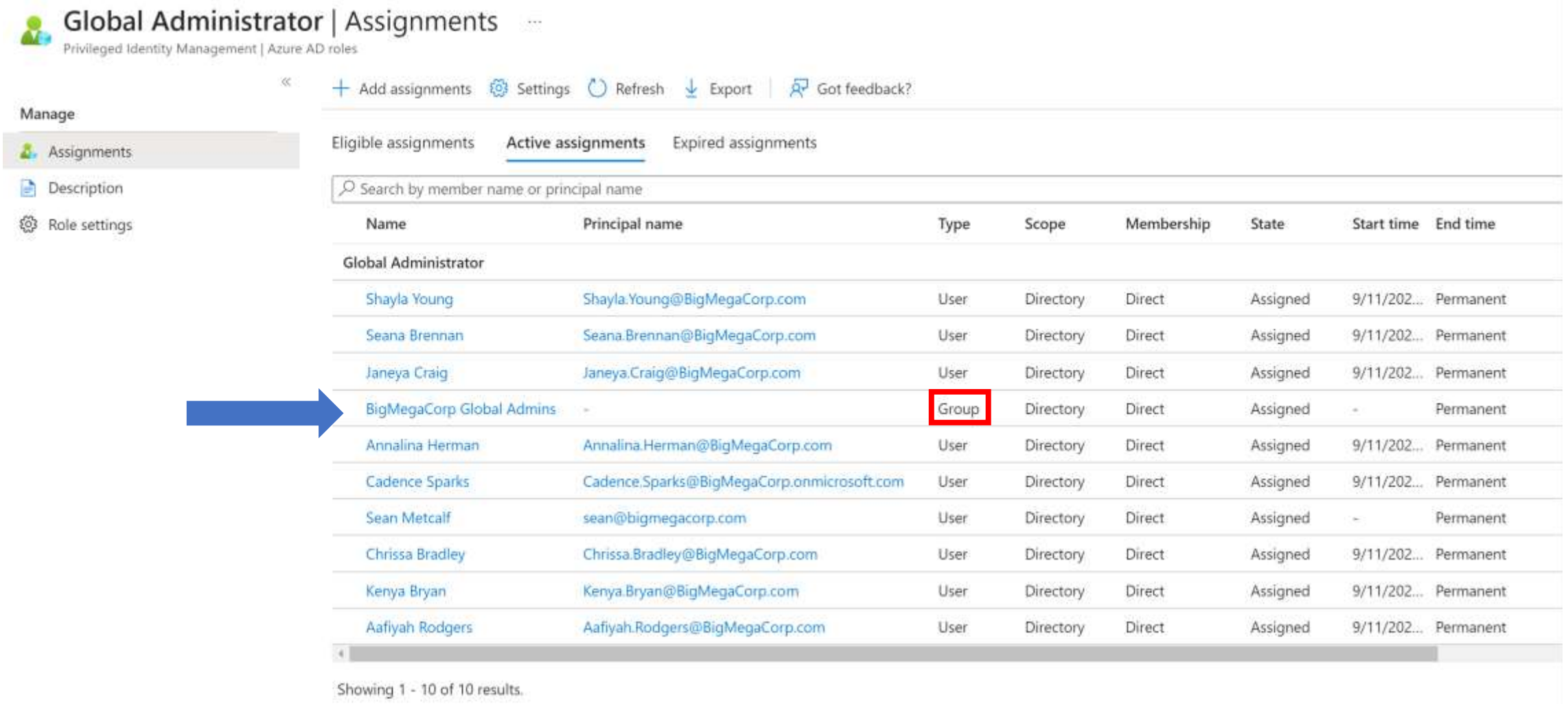
https://learn.microsoft.com/en-us/azure/active-directory/roles/privileged-roles-permissions?tabs=admin-center

Highly Privileged Azure AD Roles (bold)

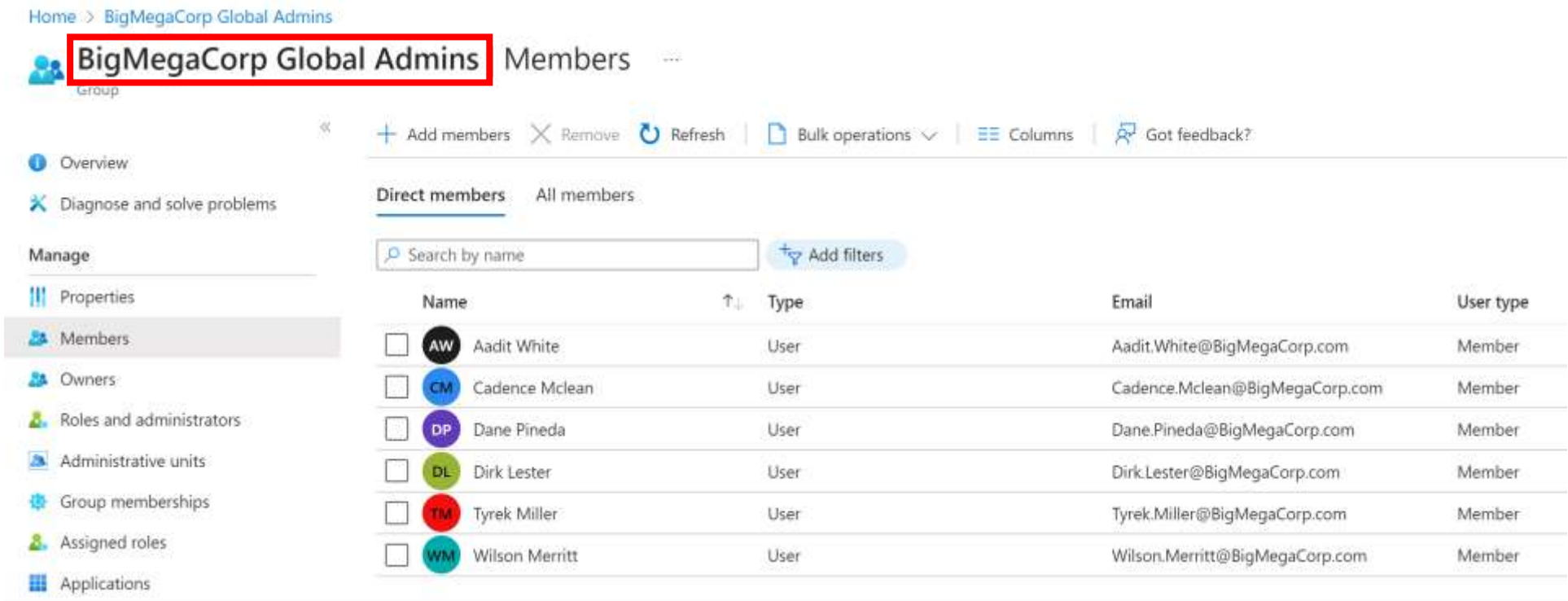
- **Application Administrator**
- Application Developer
- Authentication Administrator
- B2C IEF Keyset Administrator
- **Cloud Application Administrator**
- Cloud Device Administrator
- Conditional Access Administrator
- **Directory Synchronization Accounts**
- **Directory Writers**
- **Global Administrator**
- Global Reader
- Helpdesk Administrator
- **Hybrid Identity Administrator**
- **Intune Administrator**
- Password Administrator
- **Privileged Authentication Administrator**
- **Privileged Role Administrator**
- Security Administrator
- Security Operator
- Security Reader
- User Administrator

https://learn.microsoft.com/en-us/azure/active-directory/roles/privileged-roles-permissions?tabs=admin-center

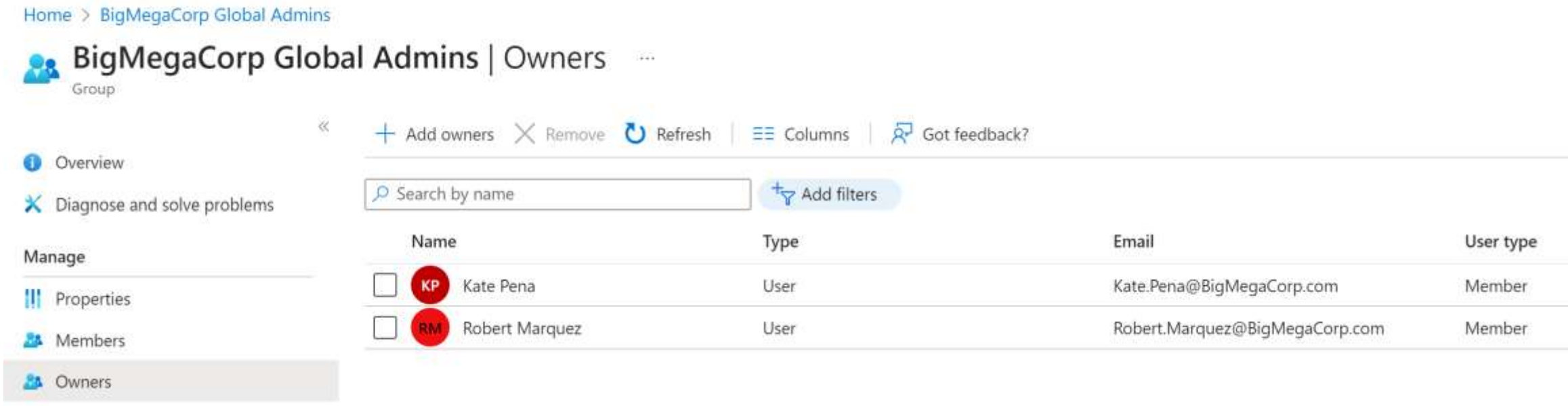
Admin Group Nesting



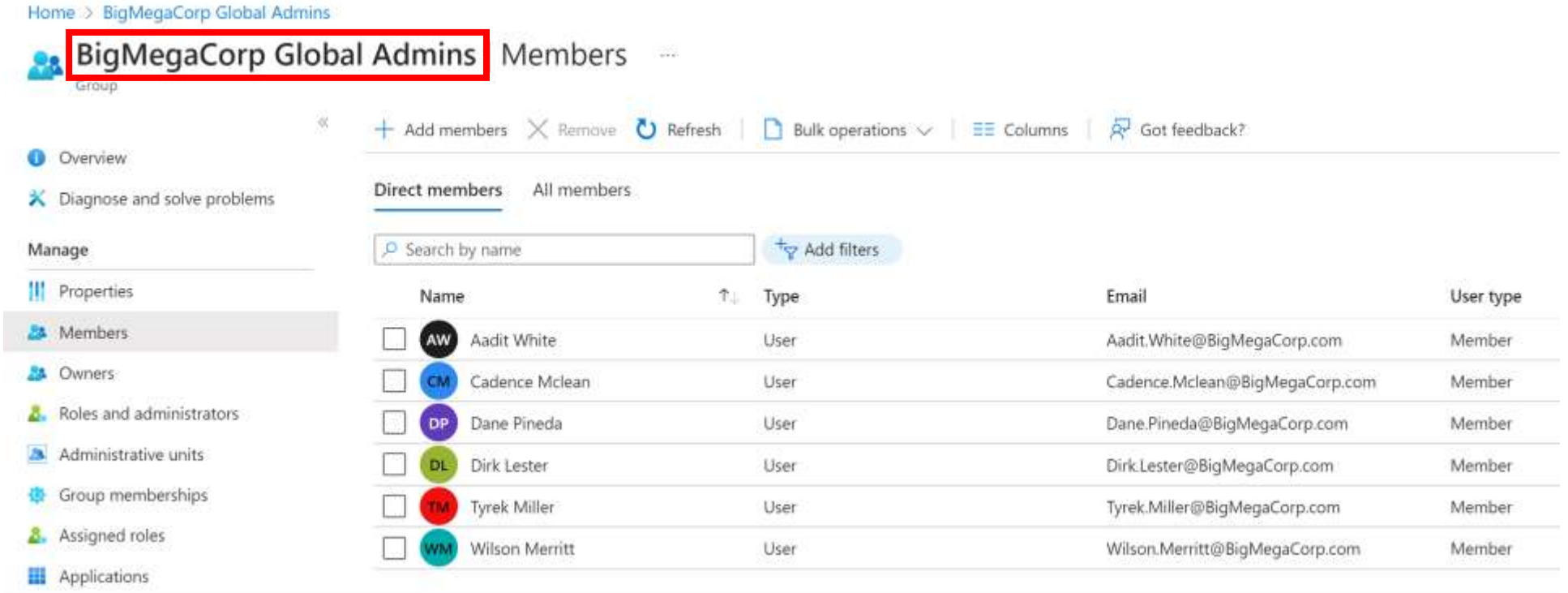
Group Nesting



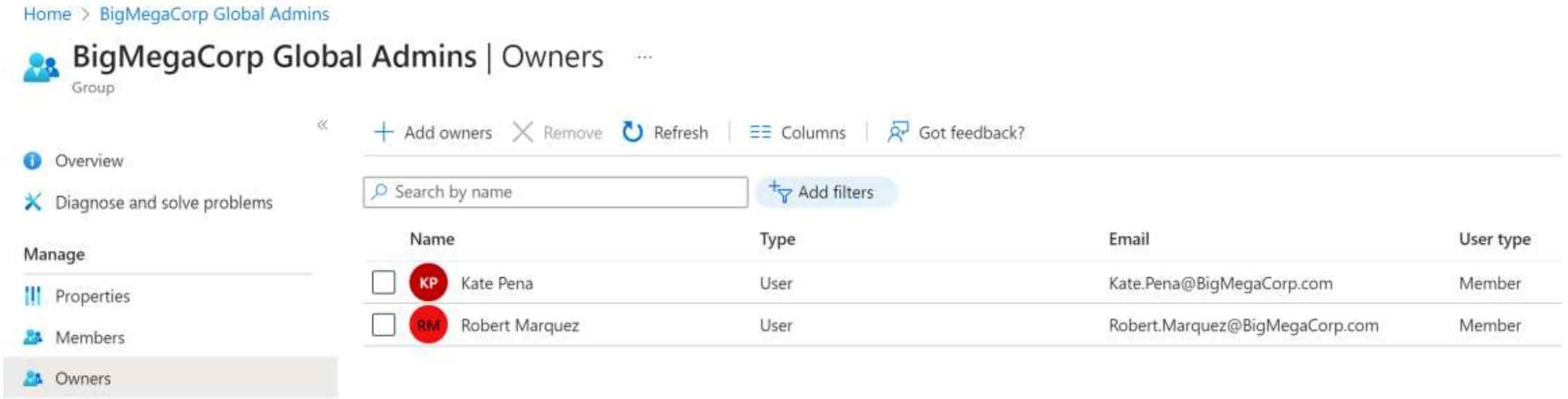
Group Nesting



Group Nesting



Group Nesting



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.

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://learn.microsoft.com/en-us/security/operations/incident-response-playbook-password-spray 90%

Password spray investigation

Article • 11/07/2023 • 8 contributors

Feedback

In this article

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.

Most Concerning Azure AD Application Permissions

Directory.ReadWrite.All	• Provides effective Global Admin rights enabling control of the application to take control of Azure AD
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.**
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.
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.

Reviewing Azure AD Permissions with PowerShell

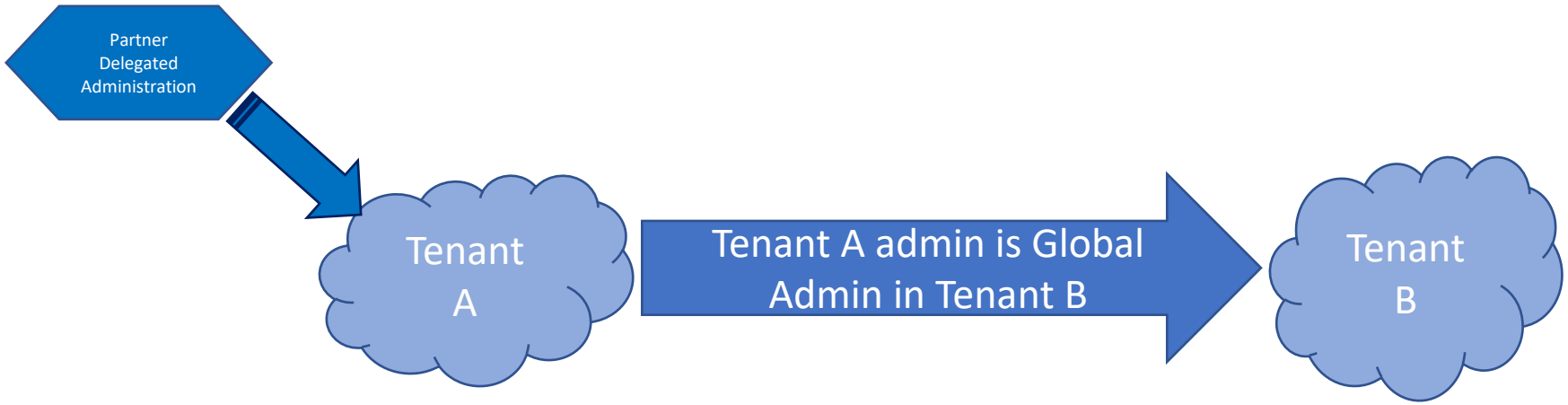
```
PS C:\> Get-AzureADPSPermissions -ApplicationPermissions | Select ClientDisplayName,ResourceDisplayName,Permission

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-ef282a2fcefe Darth Vader  DarthVader@TrimarcRD.com Member
f2a0fb99-bdaf-49ce-9192-9488ea5d3dae Boba Fett    BobaFett@TrimarcRD.com   Member
```

Solarigate “Tenant Hopping”



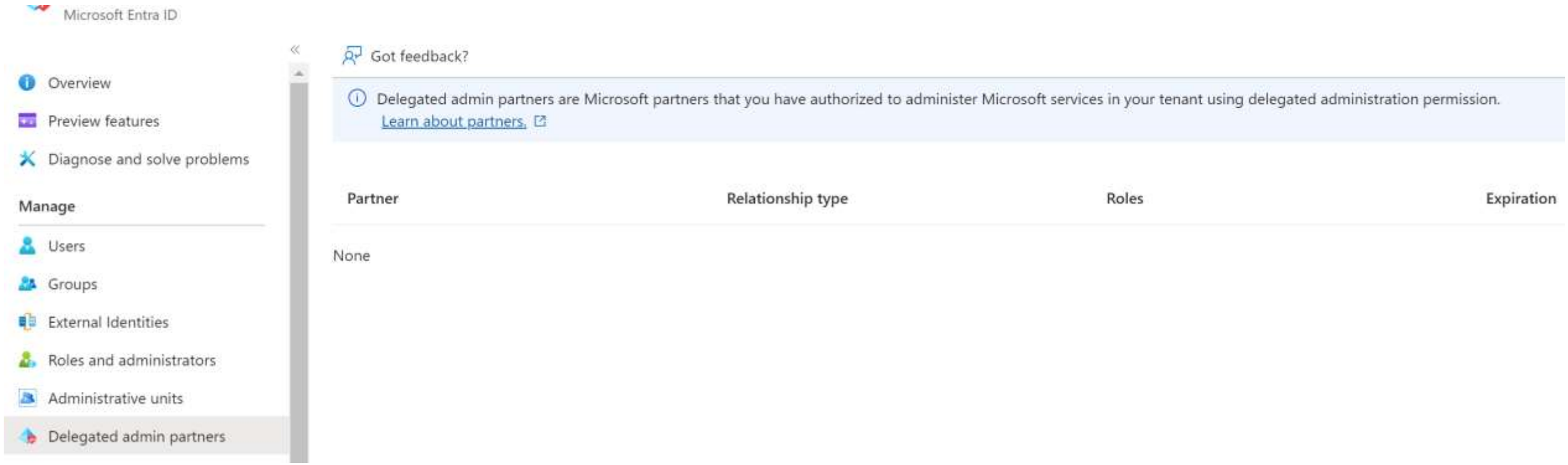
- Tenant Hopping (patent pending 😉) is when an attacker compromises one tenant to jump to another, often with privileged rights.
- Similar to trust hopping in Active Directory.
- Solarigate attackers leveraged partner connections.

Partner Relationships – aka Delegated Administration

- A configured partner can have admin rights to a customer tenant (“delegated administration”).
- This is provided when the partner requests access to the customer environment.
- When the customer accepts this request:
  - “Admin agent” role in partner tenant is provided effective “Global Administrator” rights to customer tenant.
  - “Helpdesk Agent" role in partner tenant is provided effective "Helpdesk Administrator" (Password Administrator) rights to customer tenant.
  - These are the only options.
  - They **apply to all customer environments** – there is no granular configuration.
- A partner with dozens of customers will result in all partner accounts in these groups having elevated rights in all customer environments.

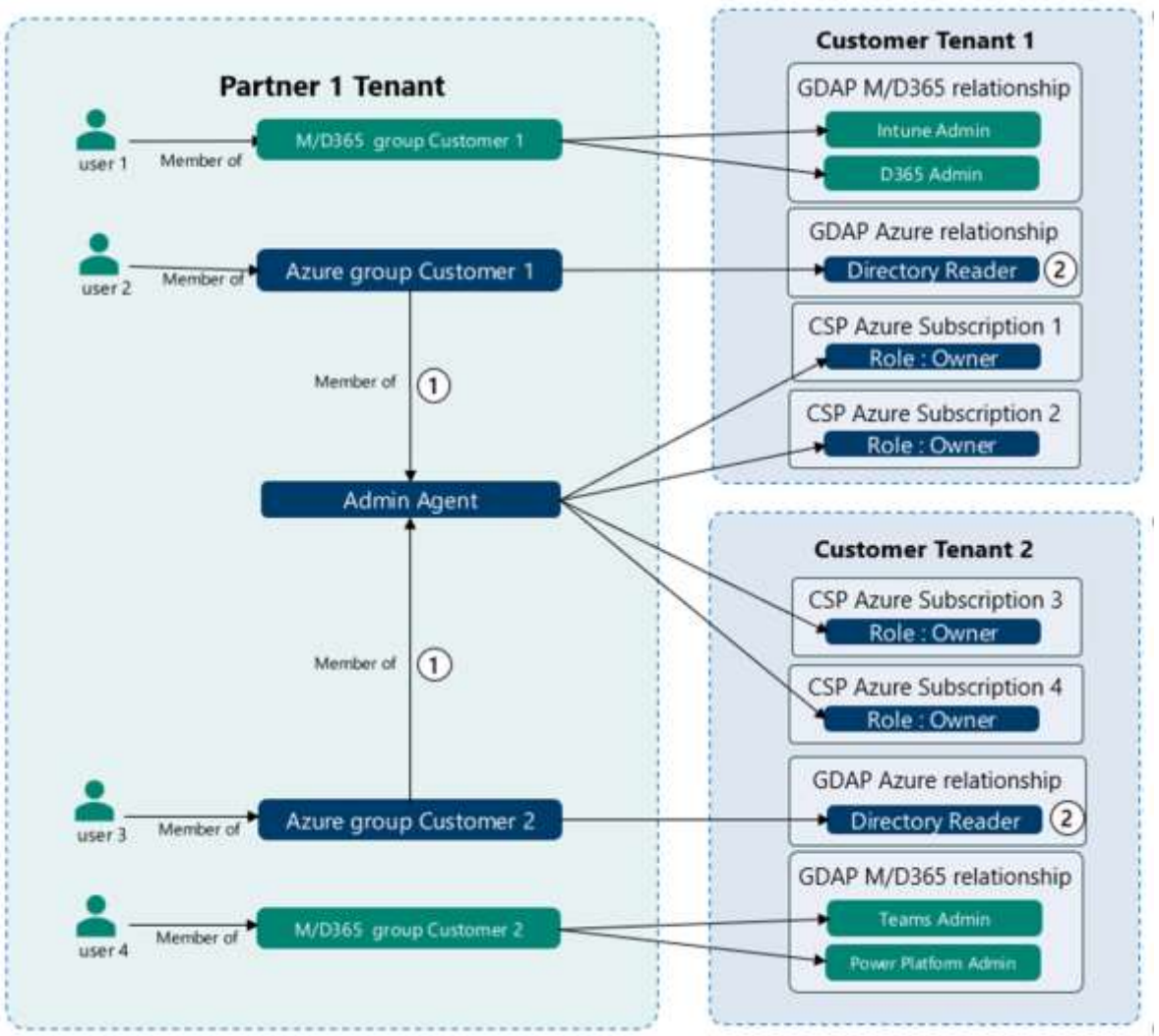
Check Partner Configuration for your tenant here:
https://portal.azure.com/#view/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/~/PartnerRelationships

Delegated Admin



Entra ID Menu Item: Delegated admin partners
https://portal.azure.com/#view/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/~/PartnerRelationships

Move to Granular Delegated Admin Privileges (GDAP)

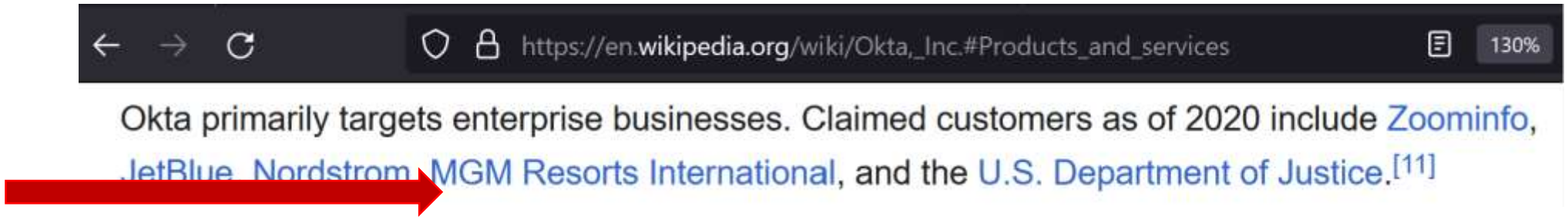


https://learn.microsoft.com/en-us/partner-center/gdap-introduction

Okta Integration

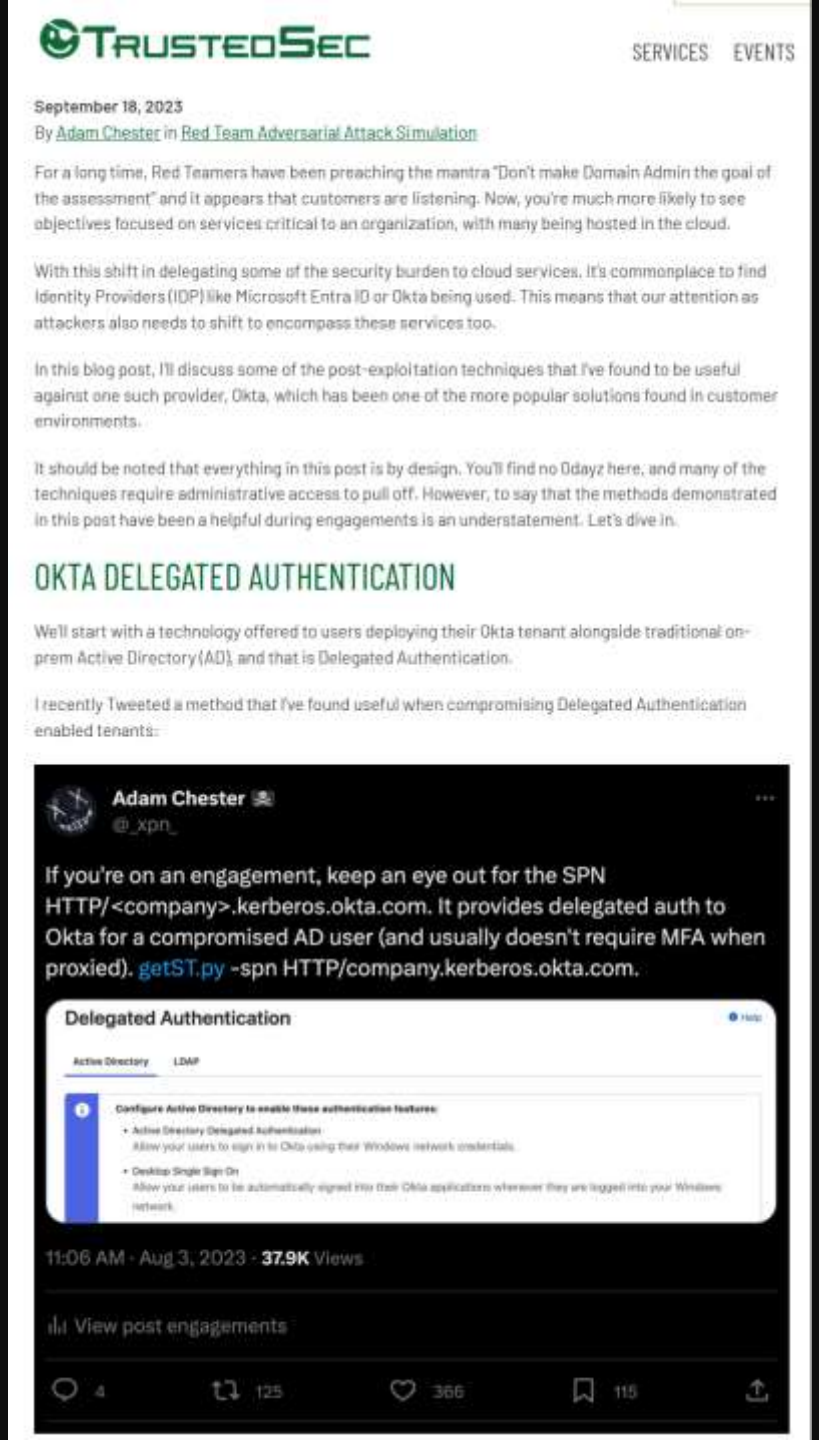
Okta

- 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 and also answering authentication requests from Okta as users log into the portal



Okta for Red Teamers

Adam Chester (@_xpn_)
https://www.trustedsec.com/blog/okta-for-red-teamers/



TrustedSec SERVICES EVENTS

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:

Adam Chester
@_xpn_

If you're on an engagement, keep an eye out for the SPN HTTP/<company>.kerberos.okta.com. It provides delegated auth to Okta for a compromised AD user (and usually doesn't require MFA when proxied). getST.py -spn HTTP/company.kerberos.okta.com.

Delegated Authentication

Active Directory LDAP

Configure Active Directory to enable these authentication features:

- Active Directory Delegated Authentication
  Allow your users to sign in to Okta using their Windows network credentials
- Desktop Single Sign On
  Allow your users to be automatically signed into their Okta applications whenever they are logged into your Windows network

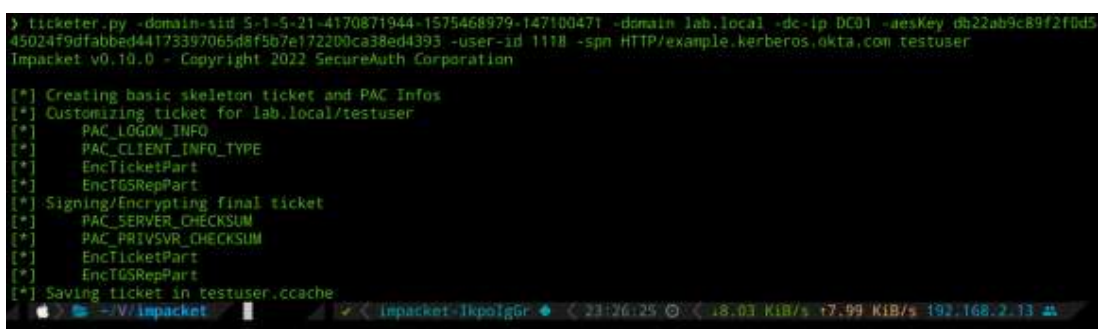
11:06 AM · Aug 3, 2023 · 37.9K Views

View post engagements

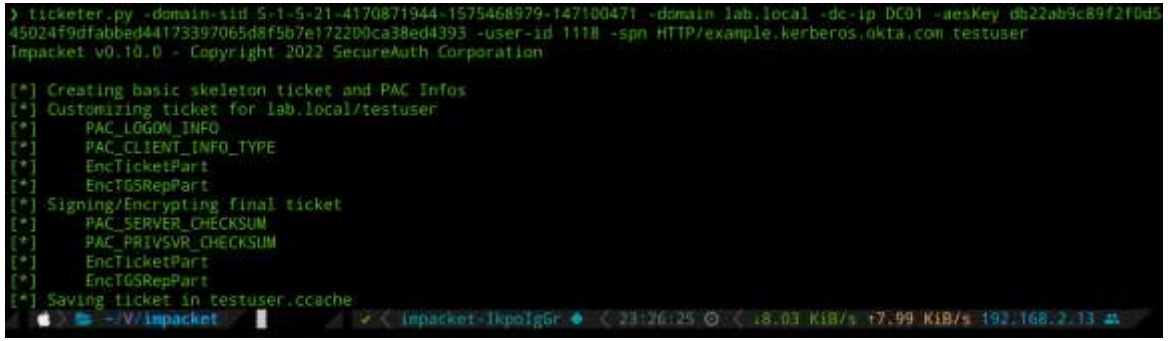
4 125 366 115

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



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

```
xml
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<action>
    <UserAuth actionId="rpc::app.active_directory.agent.reply.ok14-majorecs02a.auw2-
ok14.internal//1670637714886//Y5PojoeQQ3KDgHHzA11P9wAAC8g:e9088489-99ff-435a-943b-
b7dccc457cb5:">
        <type>USER_AUTH</type>
        <password>abc123</password>
        <useLdapGroupPasswordPolicy>false</useLdapGroupPasswordPolicy>
        <userName>[email protected]</userName>
    </UserAuth>
</action>
```

- Okta Skeleton Key (Fake AD Agent)
  - Leverage AD Admin rights

```
> python ./main.py --tenant-domain $TENANT_DOMAIN --skeleton-key WibbleWobble99 oauth --machine-name OC03 --windows-d
omain lab.local --code uz9h7o1h
Cloud-Nine (OKTA Version).. by @_xpn_

[*] Creating Agent Token
[*] Token Created: OOe1Nz5                          1oESC5
[*] Getting Domain ID
[*] Domain ID is 0o                 697
[*] Initialising AD Agent
[*] Agent ID is a53;                197
[*] Sending Agent Checkin
[*] PING Received
[*] Username: test.user@lab.local
[*] Password: Password1Z3
```

Adam Chester (@_xpn_)
https://www.trustedsec.com/blog/okta-for-red-teamers/

Okta investigating reports of possible digital breach

By Mary Kay Mallonee, Andrea Cambron and Sean Lyngaas, 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

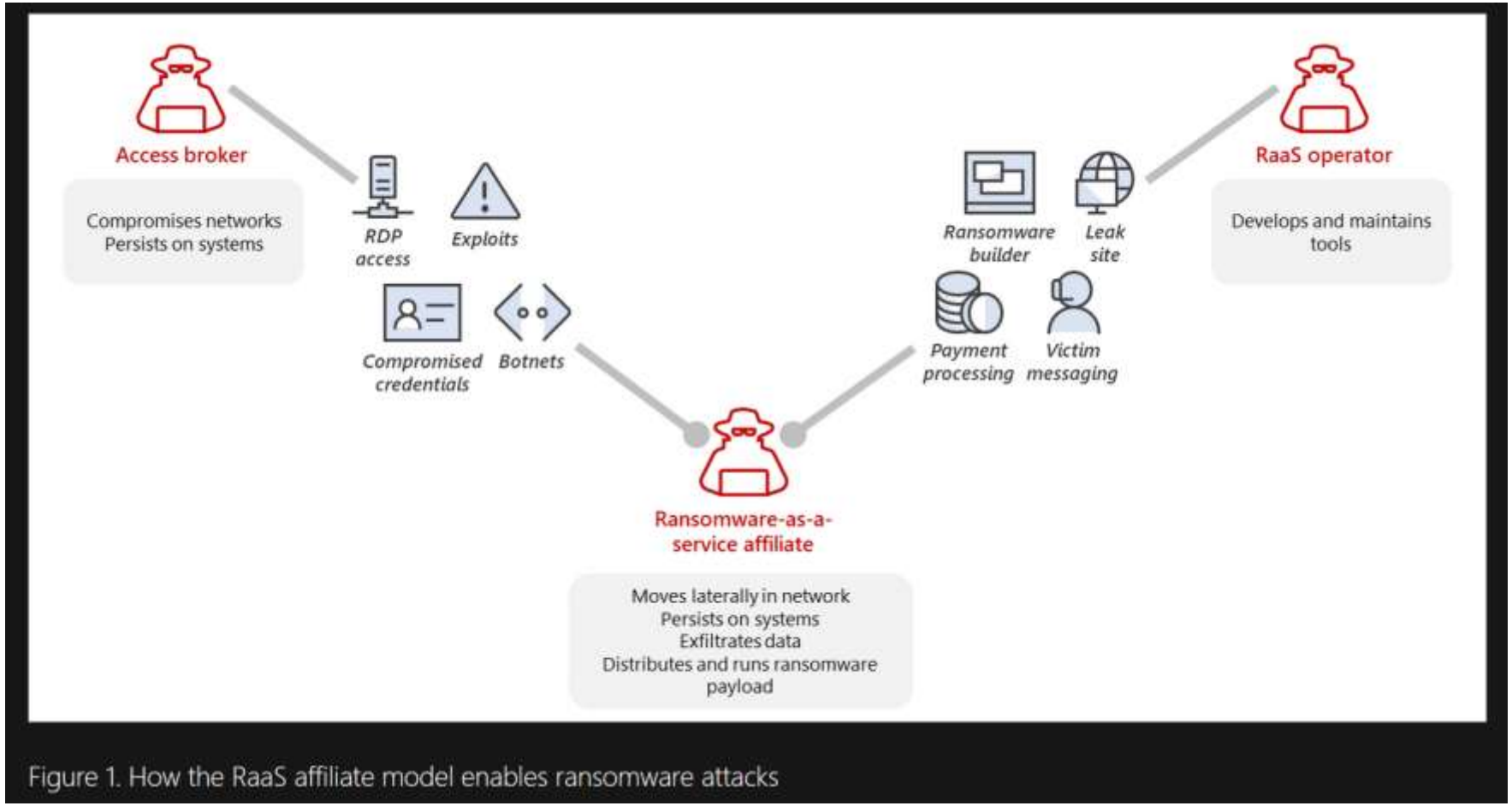


Figure 1. How the RaaS affiliate model enables ransomware attacks

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

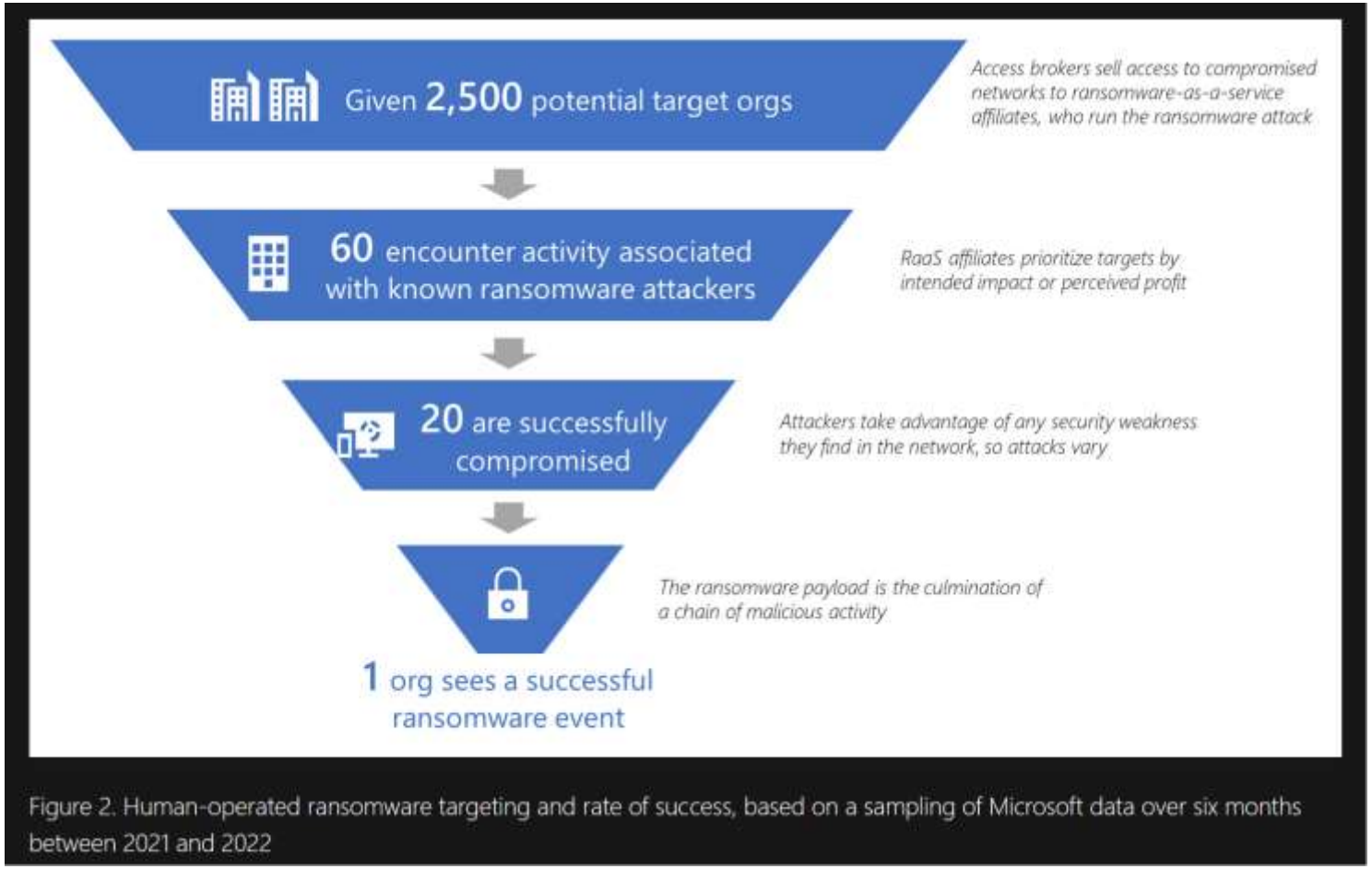


Figure 2. Human-operated ransomware targeting and rate of success, based on a sampling of Microsoft data over six months between 2021 and 2022

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/

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#

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.

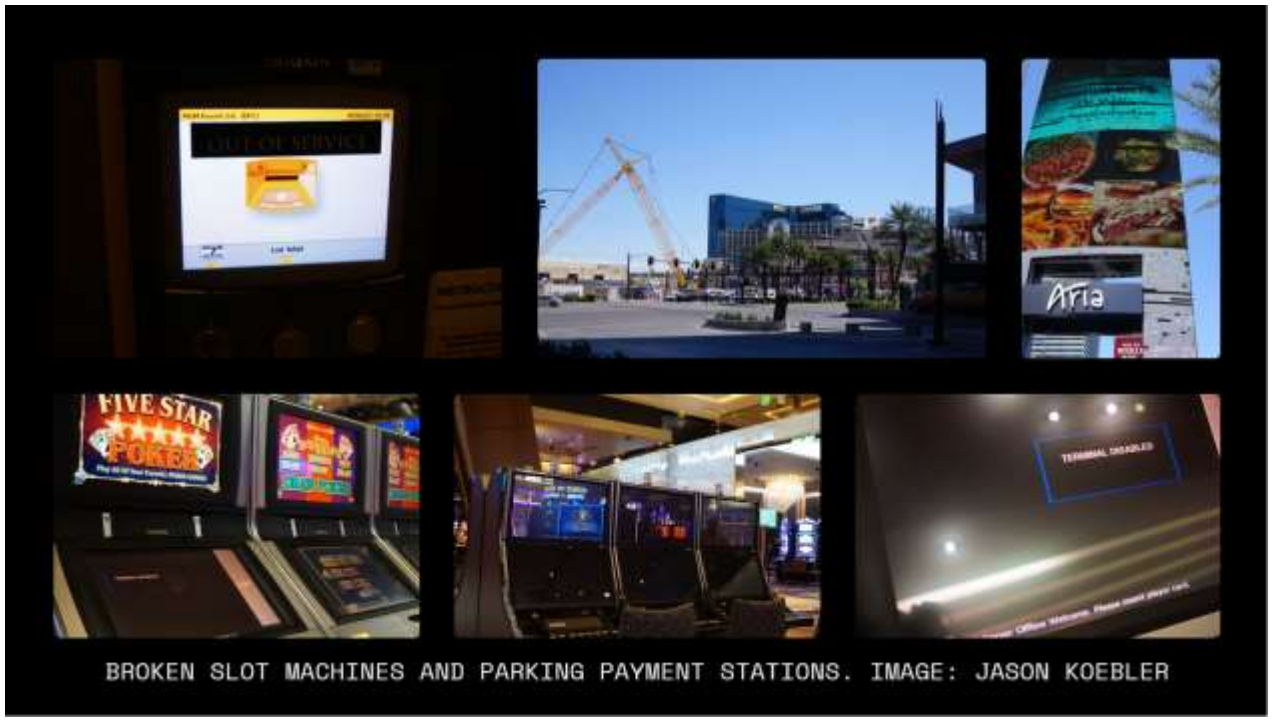
Although the issue is affecting some of the Company's systems, the vast majority of our property offerings currently remain operational, and we continue to welcome tens of thousands of guests each day. We are ready to welcome you.

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

HACKED SLOT MACHINES, ATMS, PLAYERS CARD DISPENSERS, SPORTS BOOK TERMINALS, ETC. IMAGES: JASON KOEBLER



BROKEN SLOT MACHINES AND PARKING PAYMENT STATIONS. IMAGE: JASON KOEBLER

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.

https://gist.githubusercontent.com/BushidoUK/20b81335c6729dc8e0b5997ca83fa35f/raw/a0697117e905f5094e7a5feae928806b2ba65b20/gistfile1.txt

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.

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

Results of Major Technical Investigations for Storm-0558 Key Acquisition

MSRC / By MSRC / 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).

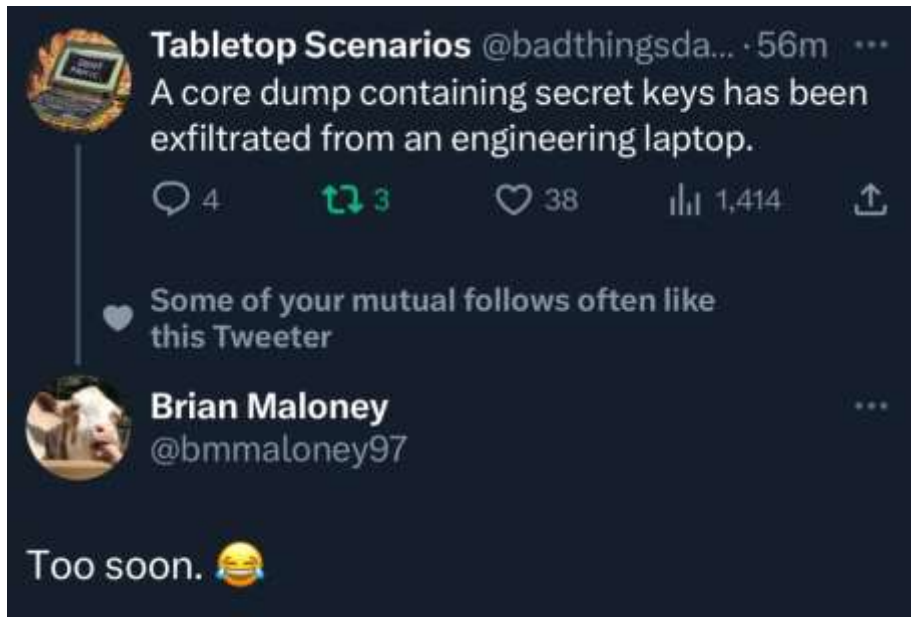
After April 2021, when the key was leaked to the corporate environment in the crash dump, the Storm-0558 actor was able to successfully compromise a Microsoft engineer's corporate account. This account had access to the debugging environment containing the crash dump which incorrectly contained the key. 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/

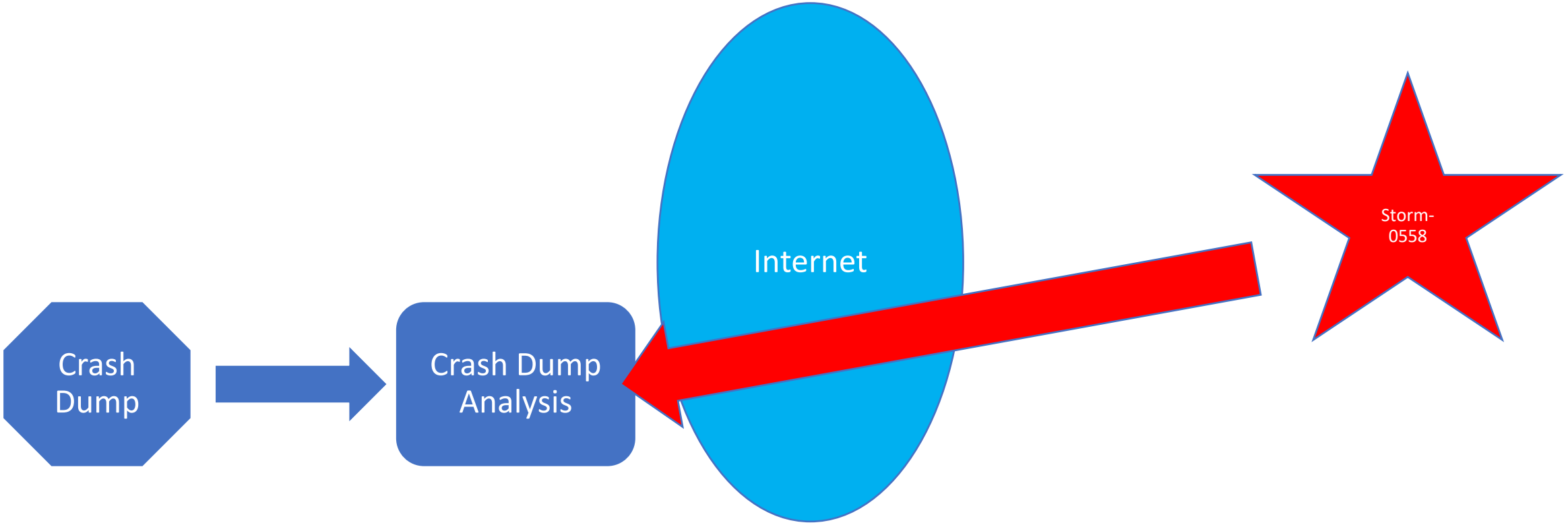
According to Microsoft, Storm-0558…

- 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**

https://www.microsoft.com/en-us/security/blog/2023/07/14/analysis-of-storm-0558-techniques-for-unauthorized-email-access/

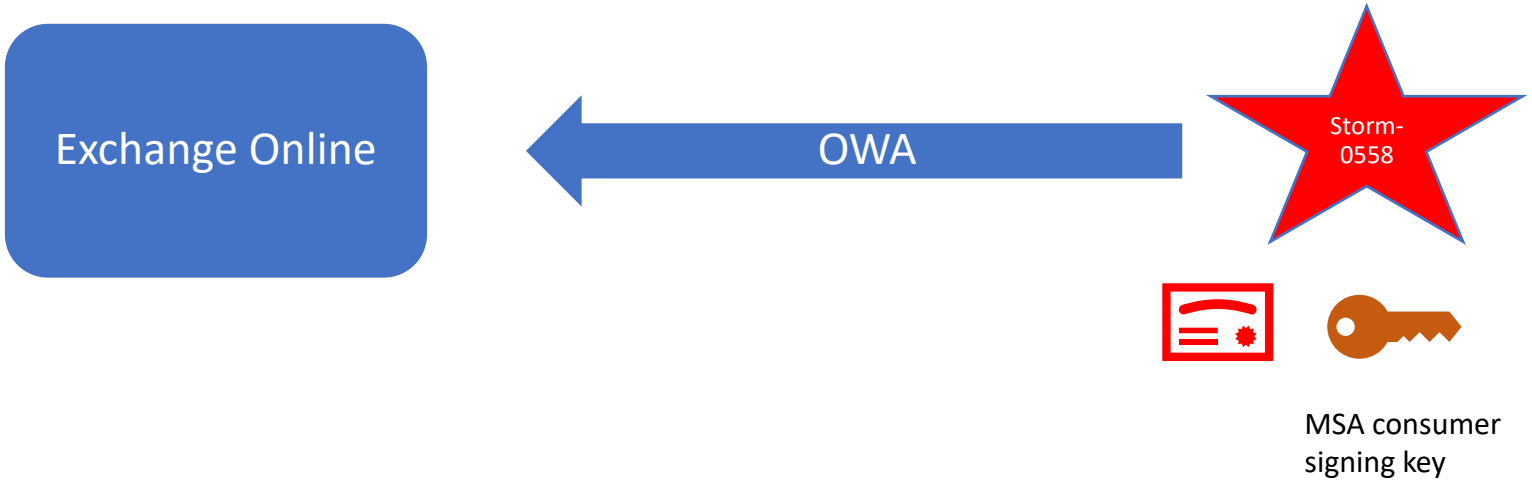
What Happened?

April 2021



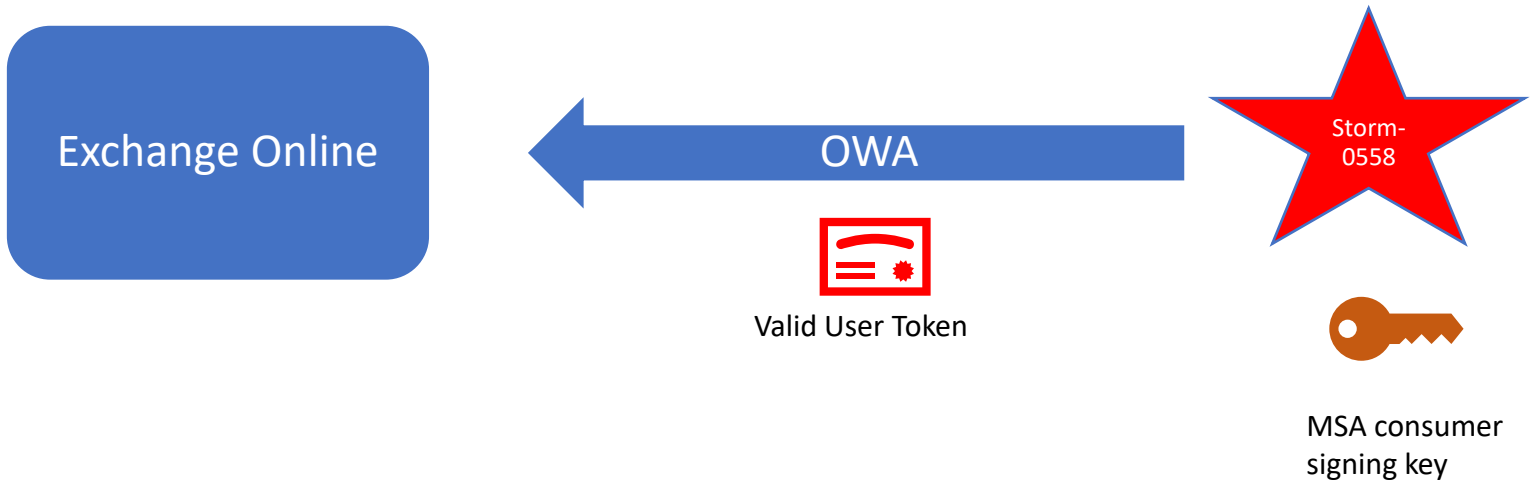
What Happened?

June 16, 2023



What Happened?

June 16, 2023



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**

Gonna tell my kids this was Game of Thrones

How Was This Detected?

The use of an incorrect key to sign the requests allowed Microsoft's investigation teams to see all actor access requests which followed this pattern across both our enterprise and consumer systems

"Beginning May 15, 2023, Storm-0558 used forged authentication tokens to access user email from approximately 25 organizations, including government agencies and related consumer accounts in the public cloud. No other environment was impacted. Microsoft has successfully blocked this campaign from Storm-0558."

What Has Microsoft Done to Fix the Issue?

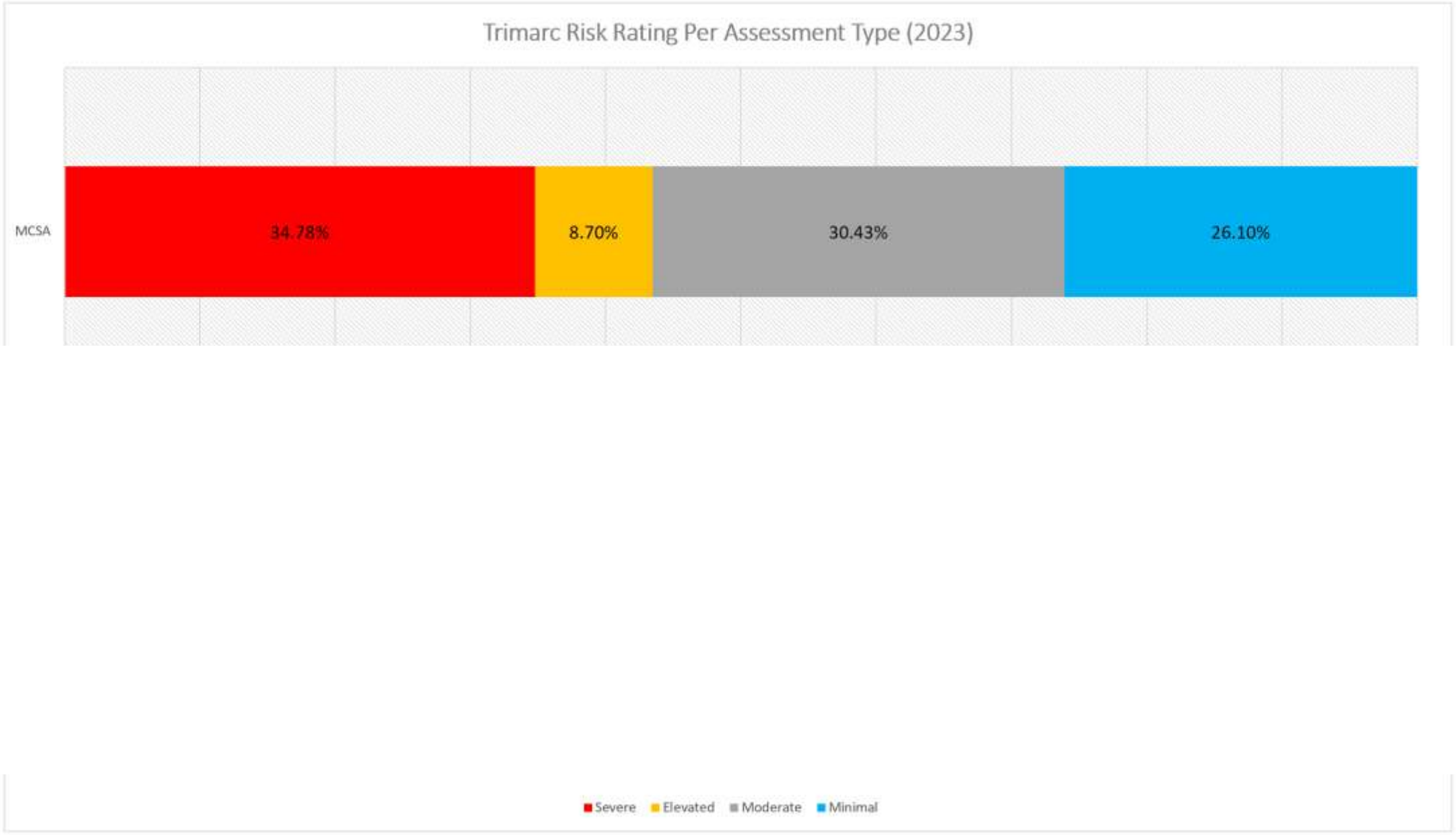
Identified and resolved race Condition that allowed the signing key to be present in crash dumps

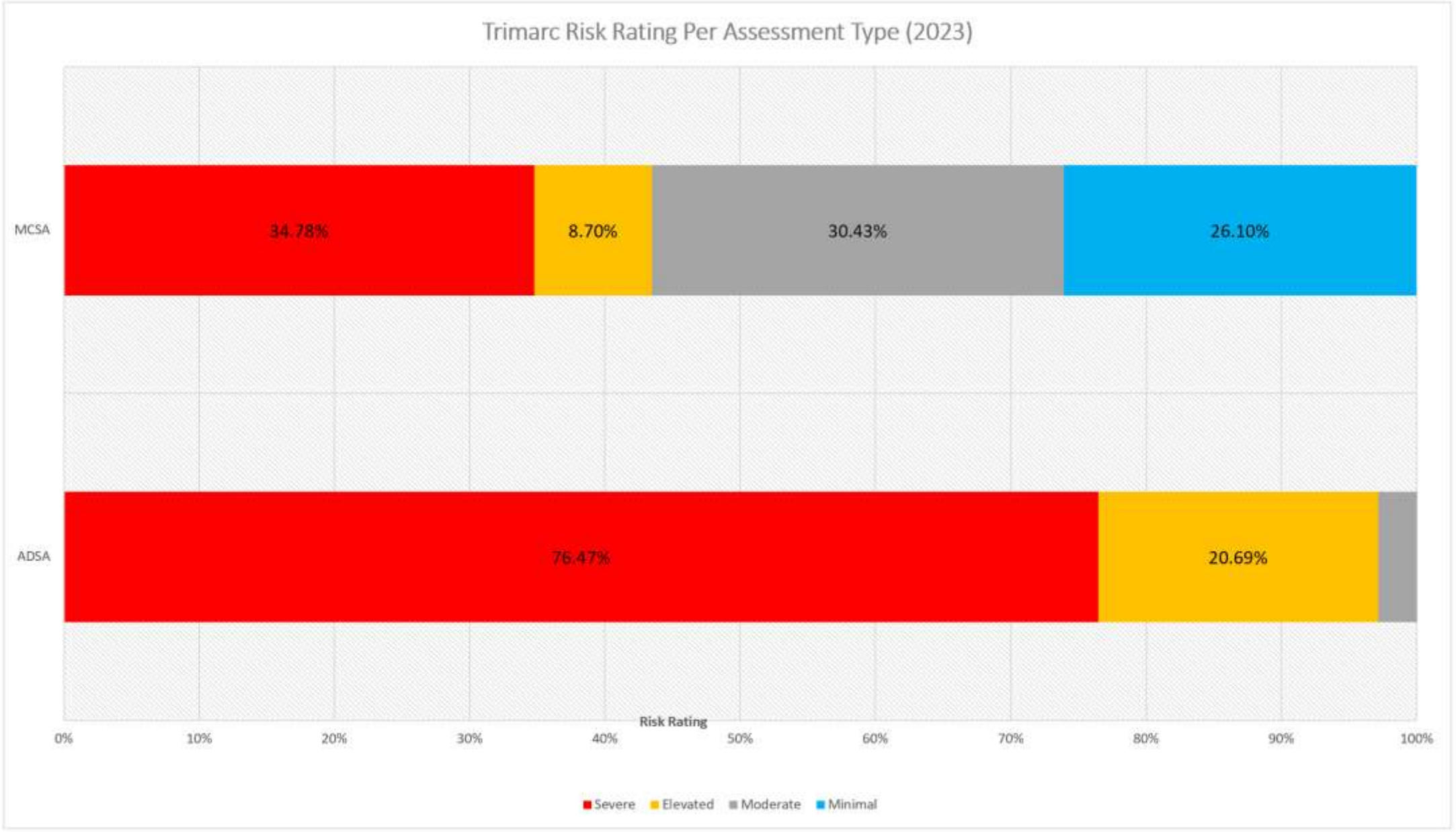
Enhanced prevention, detection, and response for key material erroneously included in crash dumps

Enhanced credential scanning to better detect presence of signing key in the debugging environment

Released enhanced libraries to automate key scope validation in authentication libraries, and clarified related documentation

Current State of Microsoft Identity Security


Trimarc Risk Rating Per Assessment Type (2023)
MCSA
34.78%
8.70%
30.43%
26.10%
Severe
Elevated
Moderate
Minimal


Trimarc Risk Rating Per Assessment Type (2023)
MCSA
34.78%
8.70%
30.43%
26.10%
ADSA
76.47%
20.69%
Risk Rating
0%
10%
20%
30%
40%
50%
60%
70%
80%
90%
100%
Severe
Elevated
Moderate
Minimal

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?