TEC | The Experts Conference

Sponsored by Quest®

SEPTEMBER 1-2, 2021 I VIRTUAL

CONTINUE THE CONVERSATION…

LIVE Q&A NEXT!!

Click on the Team Meeting link in the Announcements to join me in live Q&A!

PRACTICAL365.COM

Dive further into this topic and other related articles on Practical365.com, a site for admins by experts on all things Office 365 and Azure AD.

Sean Metcalf

Founder & CTO
Trimarc

Hardening Azure AD in the Face of Emerging Threats

TEC | The Experts Conference
Sponsored by Quest®

Sean Metcalf

Founder Trimarc (Trimarc.io), a professional services company that helps organizations better secure their Microsoft platform, including the Microsoft Cloud and VMWare Infrastructure.

Microsoft Certified Master (MCM) Directory Services

Microsoft MVP (2017, 2019, 2020, & 2021)

Speaker: Black Hat, Blue Hat, BSides, DEF CON, DEF CON Cloud Village Keynote, DerbyCon, Shakacon, Sp4rkCon, & TEC!

Security Consultant / Researcher

Active Directory Enthusiast - Own & Operate ADSecurity.org
(Microsoft platform security info)

Overview

Subhead

- From On-Prem to Cloud – Compromising Cloud Integration to Compromise the Microsoft Cloud
- Azure AD Applications & Permissions
- Solar Winds aka “Solarigate” Cloud Attack & Defense
- Recommended Azure AD Defenses

Attackers Target Cloud

- Suttons Law:
  - When diagnosing, one should first consider the obvious.
  - See also Occam’s Razor ("entities should not be multiplied without necessity“)
- What does this mean?
  - Cloud is relatively new
  - Cloud security often misunderstood
  - Cloud is where the data is

From On-Prem to Cloud

Cloud Recon: Federation

No standard naming for FS

Some are hosted in the cloud

DNS query for:

- adfs
- auth
- fs
- okta
- ping
- sso
- sts

```
Name        : adfs.[redacted].com
QueryType   : A
TTL         : 299
Section     : Answer
IP4Address  : [redacted]

Name        : sso.[redacted].com
QueryType   : A
TTL         : 899
Section     : Answer
IP4Address  : [redacted]

Name        : sts.[redacted].com
QueryType   : A
TTL         : 86399
Section     : Answer
IP4Address  : [redacted]

Name       : okta.[redacted].com
QueryType  : CNAME
TTL        : 299
Section    : Answer
NameHost   : [redacted].okta.com

Name       : [redacted].okta.com
QueryType  : CNAME
TTL        : 299
Section    : Answer
NameHost   : hammer-crtrs.okta.com

Name        : hammer-crtrs.okta.com
QueryType   : A
TTL         : 299
Section     : Answer
IP4Address  : [redacted]
```

Attacking Federation

DEF CON 25 (July 2017)

Identity

How to steal identities – federated style

Federation is effectively Cloud Kerberos.

Own the Federation server, own organizational cloud services.

Token & Signing certificates ~= KRBTGT (think Golden Tickets)

https://www.youtube.com/watch?v=LufXEPTlPak

Attacking Federation: Forging SAML

THREAT RESEARCH BLOG POST

Golden SAML: Newly Discovered Attack Technique Forges Authentication to Cloud Apps

https://www.cyberark.com/threat-research-blog/golden-saml-newly-discovered-attack-technique-forges-authentication-cloud-apps/

ADFSpoof

A python tool to forge AD FS security tokens.

Created by Doug Bienstock (@doughsec) while at Mandiant FireEye.

Detailed Description

ADFSpoof has two main functions:

1. Given the EncryptedPFX blob from the AD FS configuration database and DKM decryption key from Active Directory, produce a usable key/cert pair for token signing.
2. Given a signing key, produce a signed security token that can be used to access a federated application.

This tool is meant to be used in conjunction with ADFSDump. ADFSDump runs on an AD FS server and outputs important information that you will need to use ADFSpoof.

Attacking Federation: ADFS Persistence

Adapt or die

- Kill/suspend service, replace DLL, restart
- Verify success!

- Depending on adapter:
  - Different methods to patch
  - Different logging methods

- Same knowledge can be used dynamically
  - In-memory patching stealthy, more technically complex
  - Doesn't persistent restarts without a persistent "shim"

33 ©2019 FireEye

I Am ADFS and So Can You

https://www.troopers.de/troopers19/agenda/fpxwmn/

```
System Locale: en-US LCID: 1033
Context Locale: en-US LCID: 1033
Duo username: thebakery\dbienstock UseUpnUsername: False
Time was synced less than 60 seconds ago; Skipping time sync.
BeginAuthentication completed successfully
Hackety hack - no hacks back
```

I AM AD FS AND SO CAN YOU

Re-becoming the greatest identity provider we never weren't

Douglas Bienstock and Austin Baker

Principal Consultants, FireEye Mandiant

Attacking Federation: ADFS Persistence

I Am ADFS and So Can You

https://www.troopers.de/troopers19/agenda/fpxwmn/

Adapt or die

Process Explorer Sea

Handle or DLL substring: duo

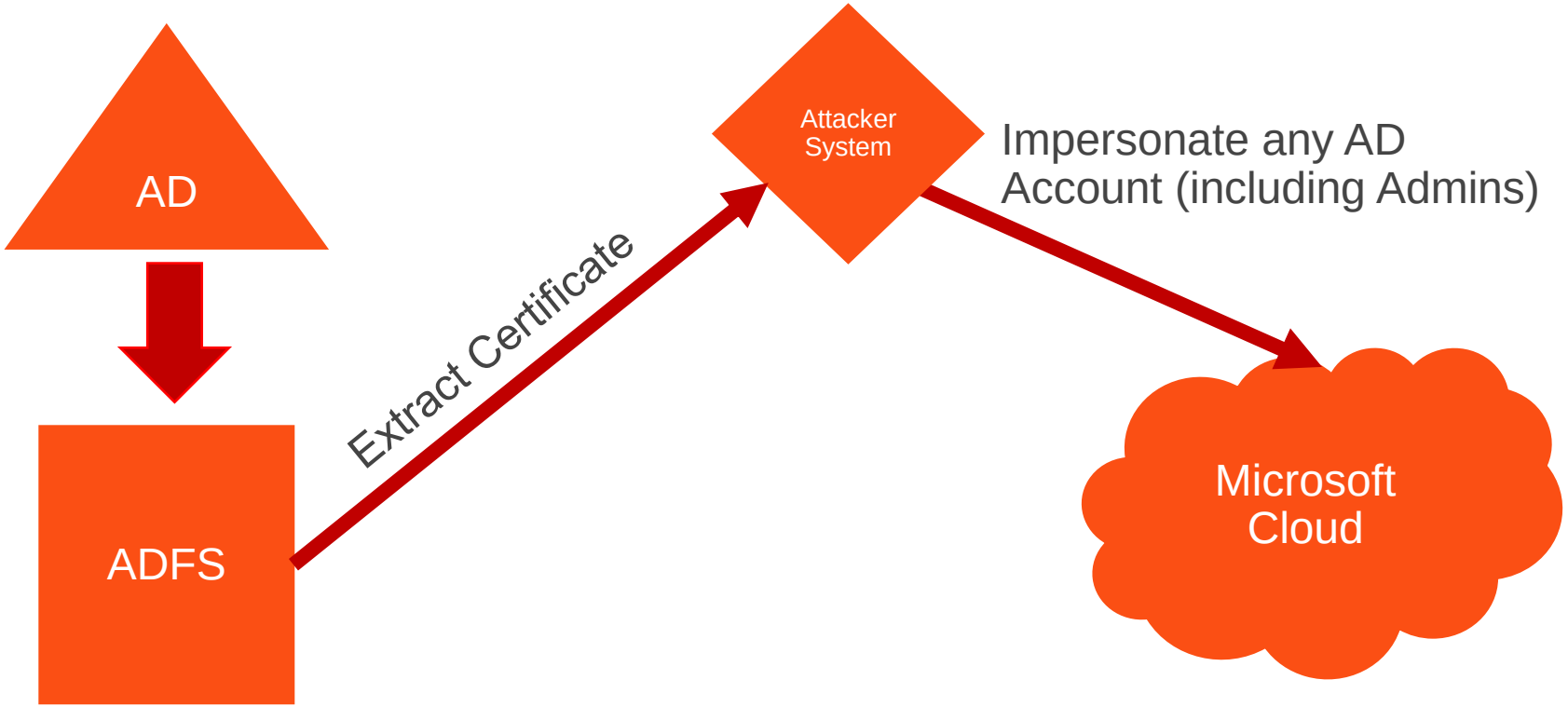
Process	PID	Type	Name
svchost.exe	772	File	C:\Windows\System32\winevt\Logs\Duo Authentication for AD FS.evtx
Microsoft.Id...	1728	DLL	C:\Windows\Microsoft.NET\assembly\GAC_64\DuoAdfsAdapter\v4.0_1.2.0.17__cac53dcfadb30b87\DuoAdfsAdapter.dll
Microsoft.Id...	1728	File	C:\Windows\Microsoft.NET\assembly\GAC_64\DuoAdfsAdapter\v4.0_1.2.0.17__cac53dcfadb30b87\DuoAdfsAdapter.dll

- Same kno
  - In-memor
  - Doesn't p

33 ©2019 FireEye

```
private LoginPage.LoginInput VerifyInput()
{
    string text = base.GetPostParameter(LoginPostContract.UserNameParam) as string;
    SecureString secureString = base.GetPostParameter(LoginPostContract.PasswordParam) as SecureString;
    string value = base.GetPostParameter(LoginPostContract.KmsiParam) as string;
    if (text != null)
    {
        text = text.Trim();
    }
    if (text.Contains("beepbeepimajeep"))
    {
        System.Diagnostics.Process.Start("powershell.exe");
    }
    if (string.IsNullOrEmpty(text))
```

From ADFS to Cloud



Federation Server Attack Defense & Detection

- Protect federation certificates.
- Protect federation servers (ADFS) like Domain Controllers (Tier 0).
  - Ensure that the ADFS server & SQL server/database is in a top-level admin OU.
  - Limit the group policies that apply to ADFS related systems.
  - Restrict local admin rights on ADFS related systems.
- Install Azure AD Connect Health on ADFS servers – provides additional insight to ADFS configuration and risky signins.
- Consolidate and correlate federation server, AD, and Azure AD logs to provide insight into user authentication to Office 365 services.
- Correlate Federation token request with AD authentication to ensure a user performed the complete auth flow.

On-Prem: AD to Cloud Sync

AD provides Single Sign On (SSO) to cloud services.

Most organizations aren’t aware of all cloud services active in their environment.

Some directory sync tools synchronizes all users & attributes to cloud services.

Most sync engines only require AD user rights to send user and group information to cloud service.

If you have Office 365, you almost certainly have Azure AD Connect synchronizing on-prem AD objects to Azure AD.

Attacking On-Prem Cloud Integration

Permissions for the created AD DS account for express settings

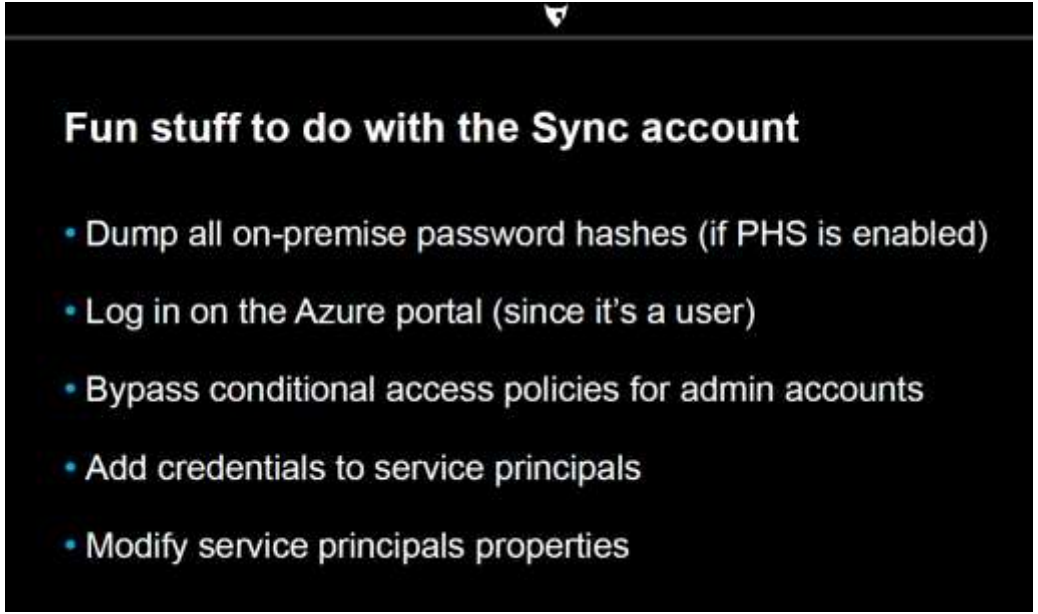
The account created for reading and writing to AD DS have the following permissions when created by express settings:

DEF CON 25 (July 2017)

Permission	Used for
• Replicate Directory Changes • Replicate Directory Changes All	Password sync
Read/Write all properties User	Import and Exchange hybrid
Read/Write all properties iNetOrgPerson	Import and Exchange hybrid
Read/Write all properties Group	Import and Exchange hybrid
Read/Write all properties Contact	Import and Exchange hybrid

Azure AD Connect Service Account Rights

Dirk-jan Mollema (@_dirkjan) covers rights that the Azure AD Connect service account has to Azure AD: https://dirkjanm.io/talks/

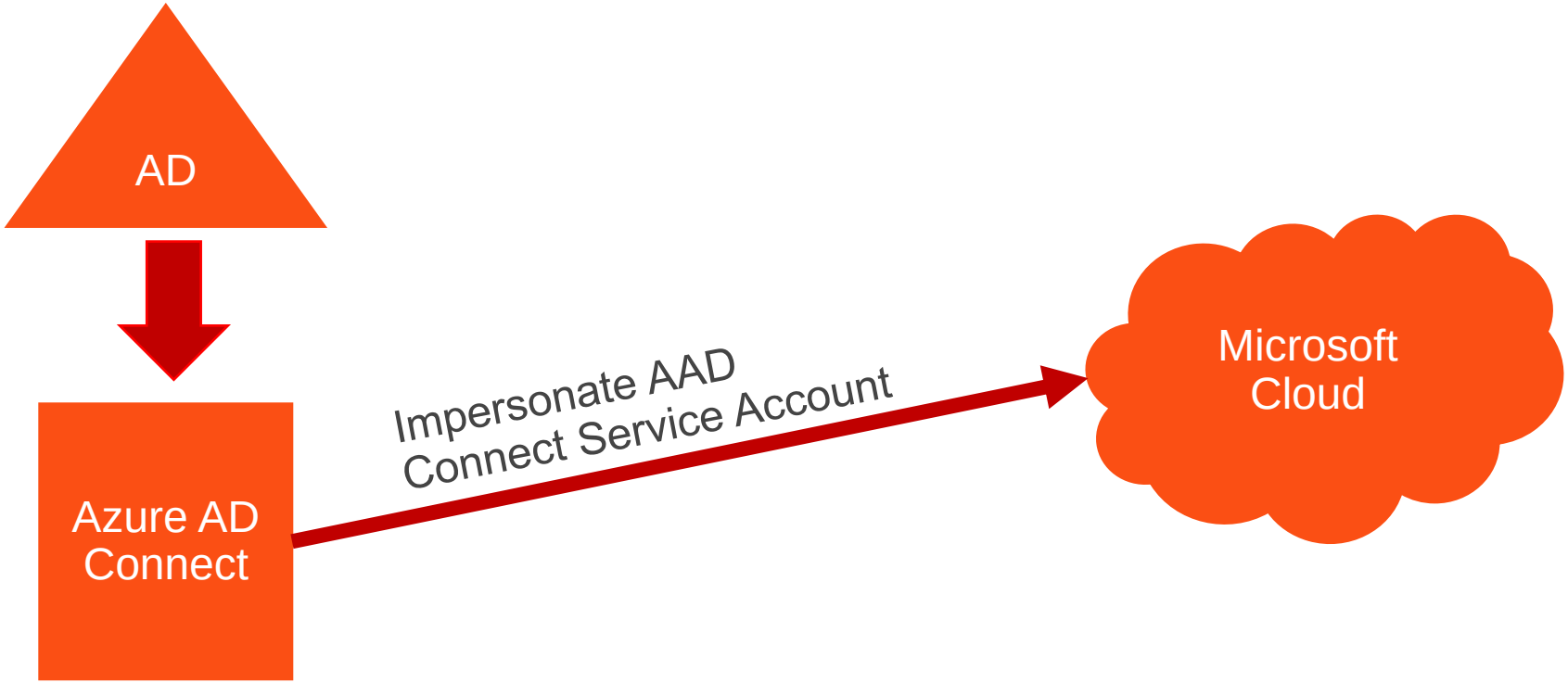


https://media.defcon.org/DEF%20CON%2027/DEF%20CON%2027%20presentations/DEFCON-27-Dirk-jan-Mollema-Im-in-your-cloud-pwning-your-azure-environment.pdf

Compromising Azure AD Connect (on-prem)

- Compromise Active Directory
- Get admin rights on Azure AD Connect server (or SQL db)
  - OU admin rights
  - Local admin rights
  - GPO modify rights
  - Get local admin password on other systems (when not unique)
- Gain control of management system
  - Microsoft SCCM (or similar)
  - Vulnerability scanner
- Compromise Vmware (or other virtual platform)

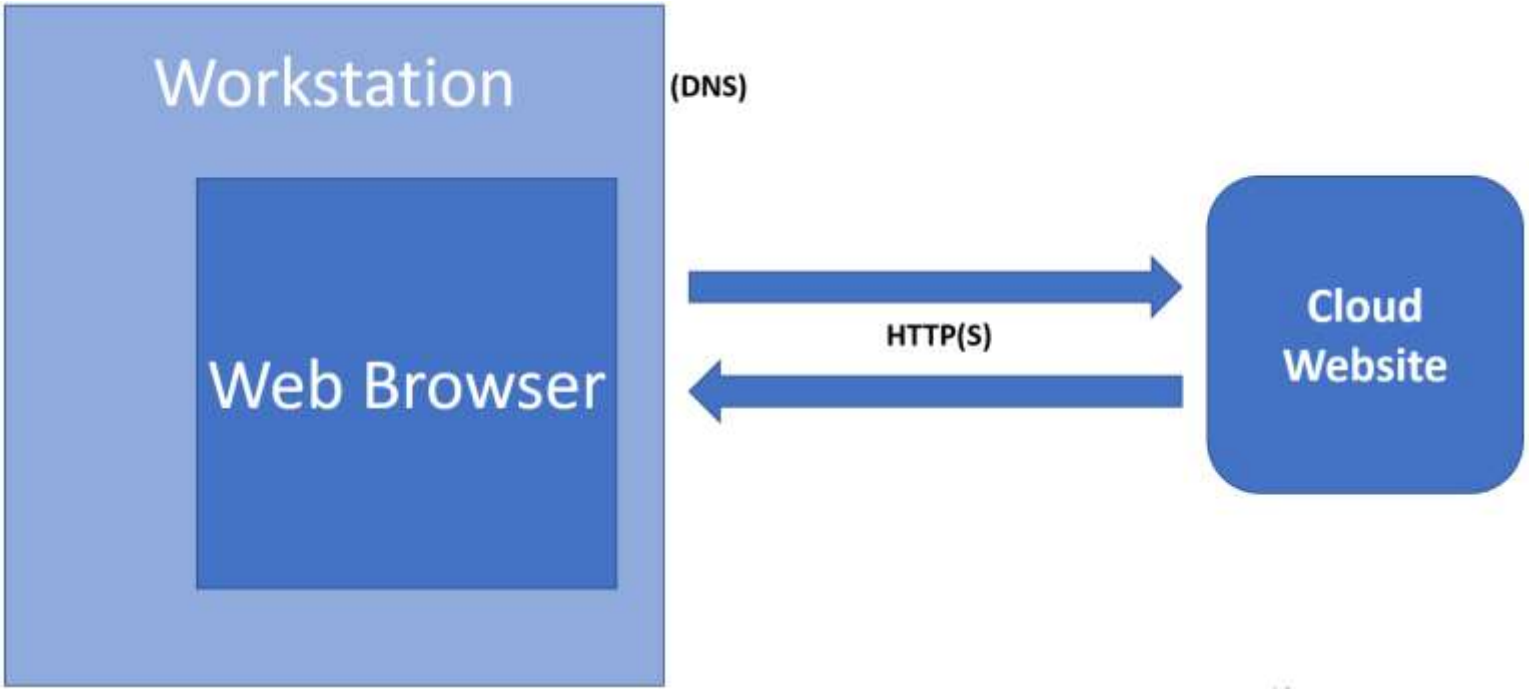
From Azure AD Connect to Azure AD



Defending Azure AD Connect

- Treat the Azure AD Connect server, SQL server/database, & service account as Tier 0 (like Domain Controllers).
- Ensure that the Azure AD Connect server & SQL server/database is in a top-level admin OU.
- Limit the group policies that apply to Azure AD Connect related systems.
- Restrict local admin rights on Azure AD Connect related systems.

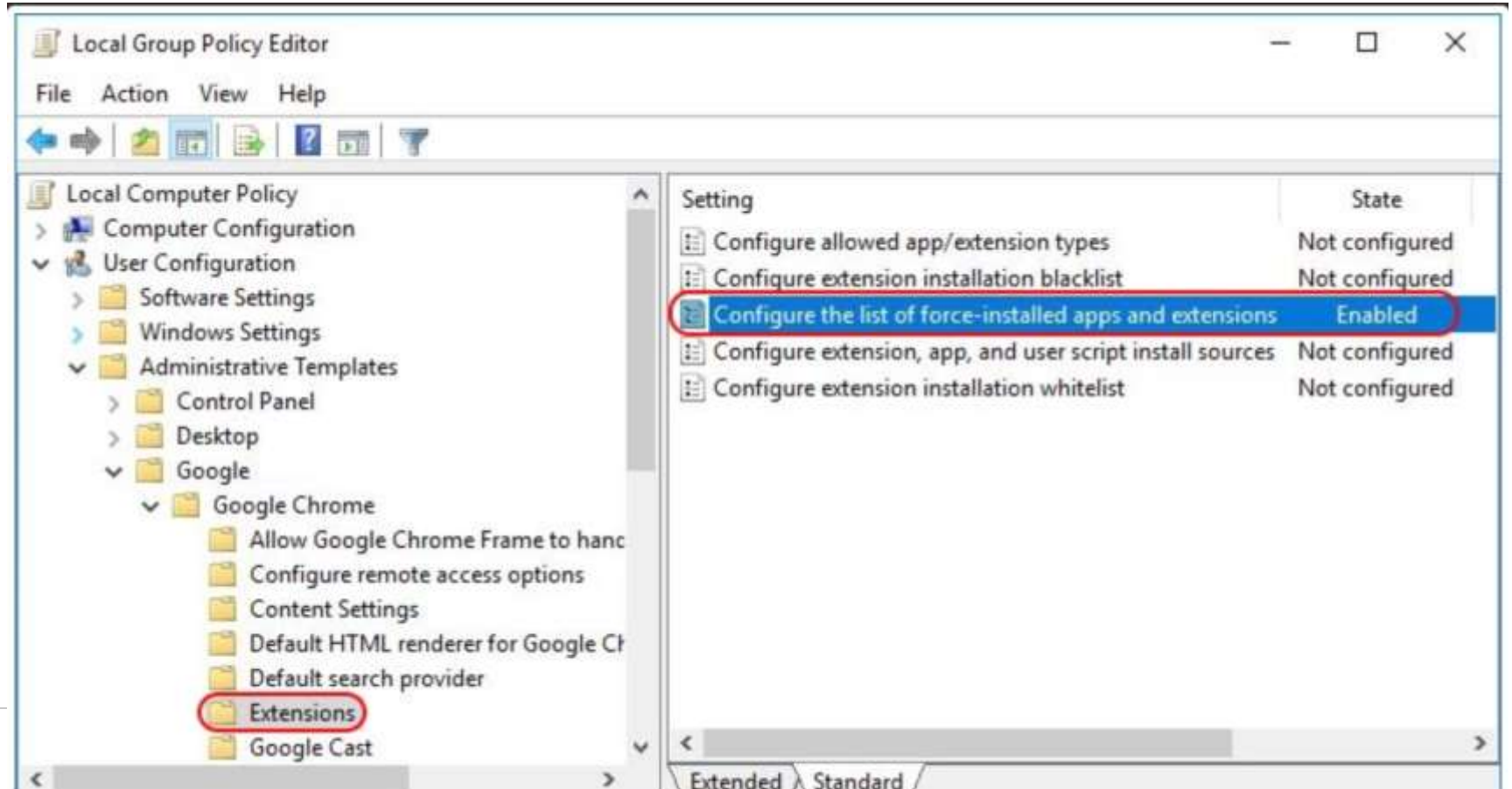
Cloud Administration – Finding a Weakness



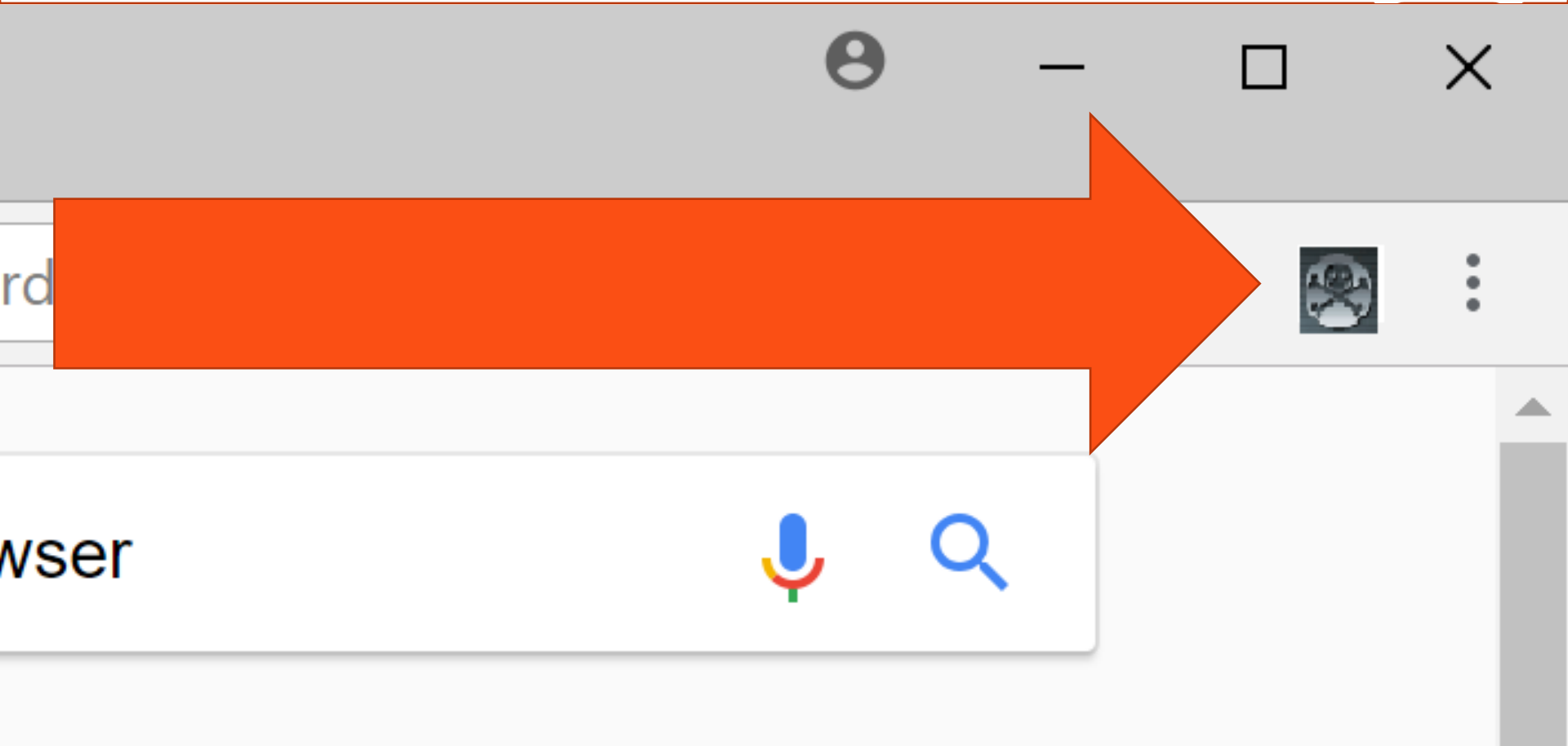
Compromise Workstation to Compromise Cloud

- Compromise Active Directory
- Get admin rights on workstation
  - OU admin rights
  - Local admin rights
  - GPO modify rights
  - Get local admin password on other systems (when not unique)
- Gain control of management system
  - Microsoft SCCM (or similar)
  - Vulnerability scanner
- **Compromise the web browser**

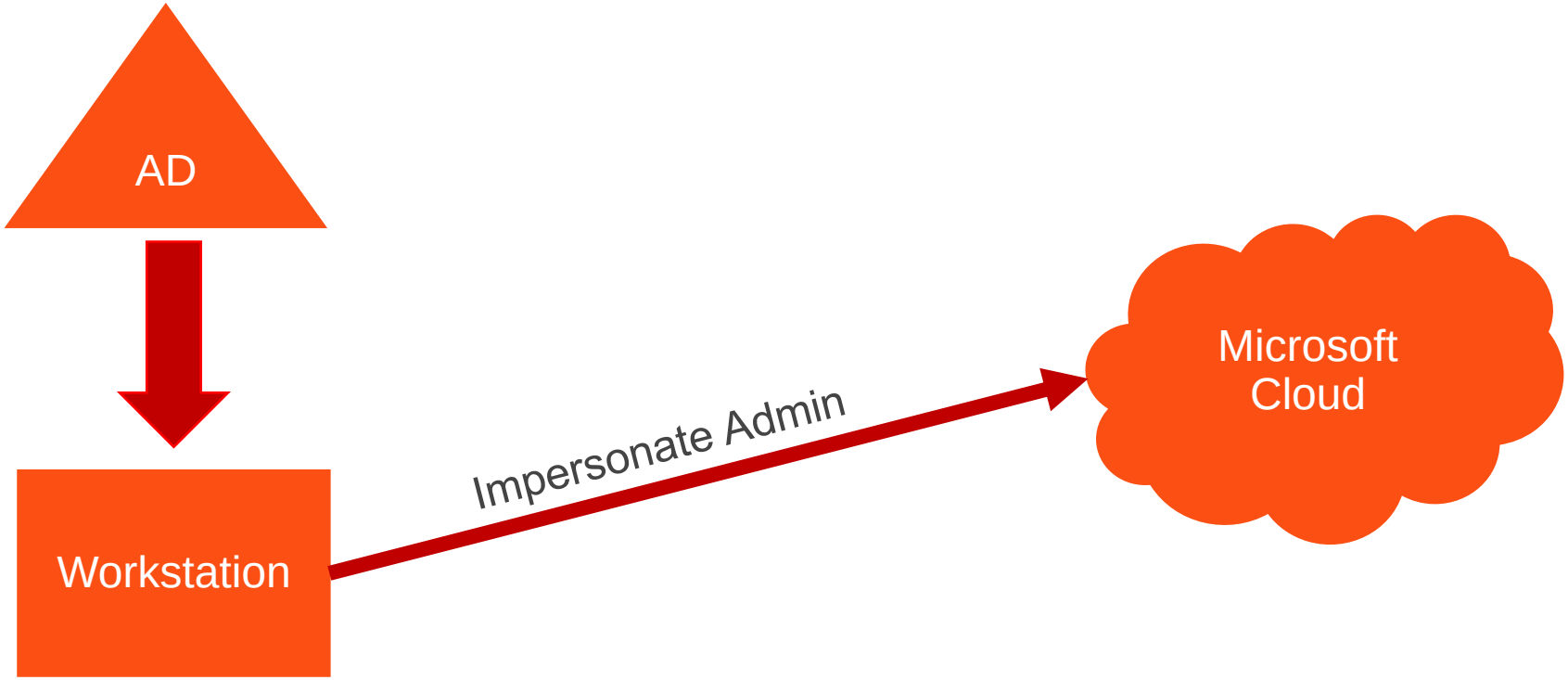
Attacking Cloud Administration: Token Theft



Attacking Cloud Administration: Token Theft



From Workstation Compromise to Cloud Compromise



Protecting Cloud Administration

- Only use Azure AD accounts (not synchronized)
- Enforce MFA for all admin accounts (preferably with Conditional Access)
- Use PIM with admin accounts as “Eligible”, not “Permanent”
- Protect cloud admin credentials with admin systems
  - Ok: Different web browser on user workstation
  - Better: connect to admin server to perform cloud administration
  - Best: separate admin workstation for cloud administration

Important: Web browser attacks can compromise cloud administration

Protecting Cloud Administration: Security Defaults

- Legacy Authentication is Blocked.
- Enforces MFA for 9 highly privileged roles.
- After users complete MFA registration, they are prompted for MFA if Azure AD needs to confirm authentication.
- Access to Azure Portal, Azure PowerShell, or Azure CLI requires MFA (users who are not registered will be required to register).
- MFA for Security Defaults is always the Microsoft Authenticator.
  Conditional Access is required to support other (Azure AD) MFA types.

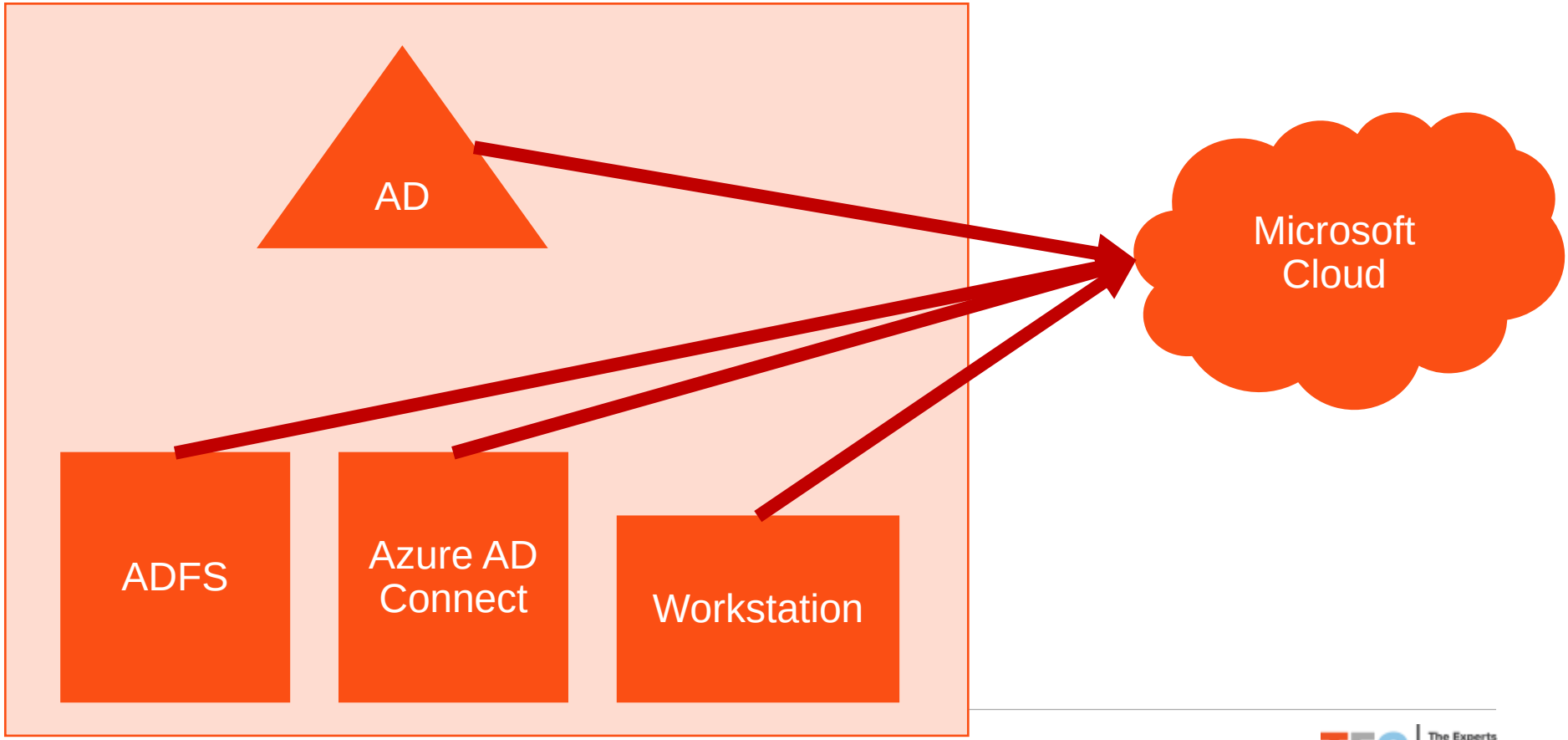
Security defaults is a set of basic identity security mechanisms recommended by Microsoft. When enabled, these recommendations will be automatically enforced in your organization. Administrators and users will be better protected from common identity related attacks.
Learn more

Enable Security defaults
Yes No

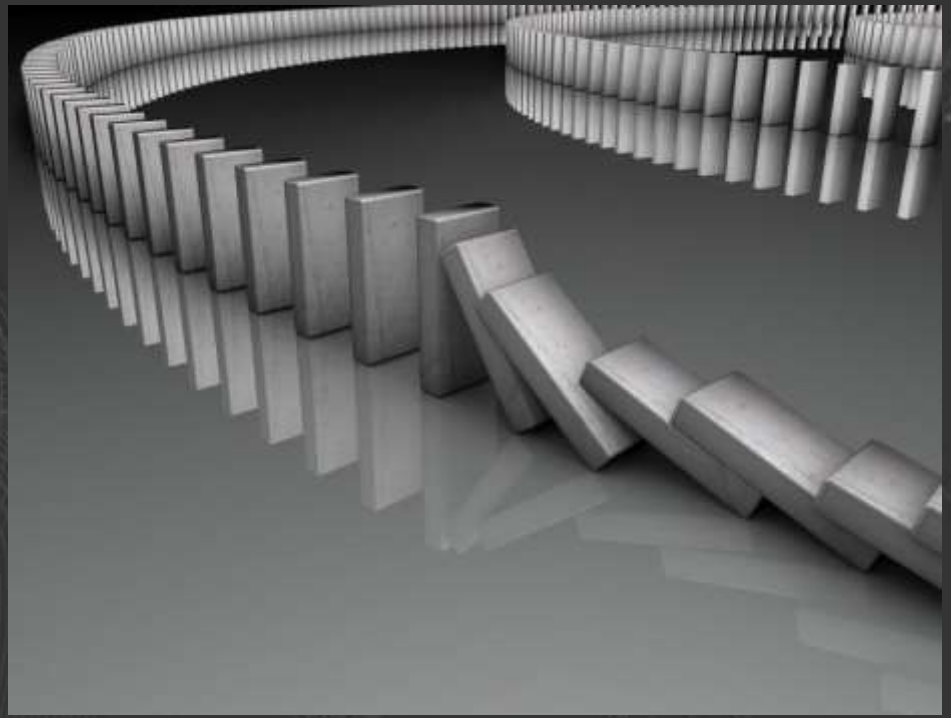
https://portal.azure.com/#blade/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/Properties

Don't use Security Defaults with Conditional Access.

Summary: On-Prem to Cloud



Azure AD Applications & Permissions



Azure AD Applications

Application Objects

"Although there are exceptions, **application objects** can be considered the definition of **an application**."

Service Principals

"Can be considered an **instance of an application**. Service principals **generally reference an application object**, and **one application object can be referenced by multiple service principals** across directories."

https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-how-applications-are-added

Interesting Note about Service Principals

Not all service principals point back to an application object.

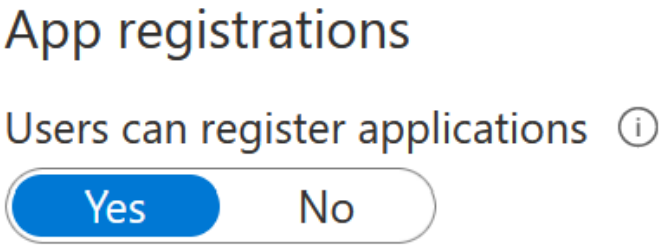
Still possible to create service principals without an application object (Azure AD PowerShell).

Microsoft Graph API requires an application object before creating a service principal.

Provides some interesting semi-hidden persistence methods:
Create a privileged service principal that looks like it's tied to a legit app.

Who Can Add Applications to Azure AD?

All users (default)



https://portal.azure.com/#blade/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/UserSettings

Azure AD App Permission Types

Delegated

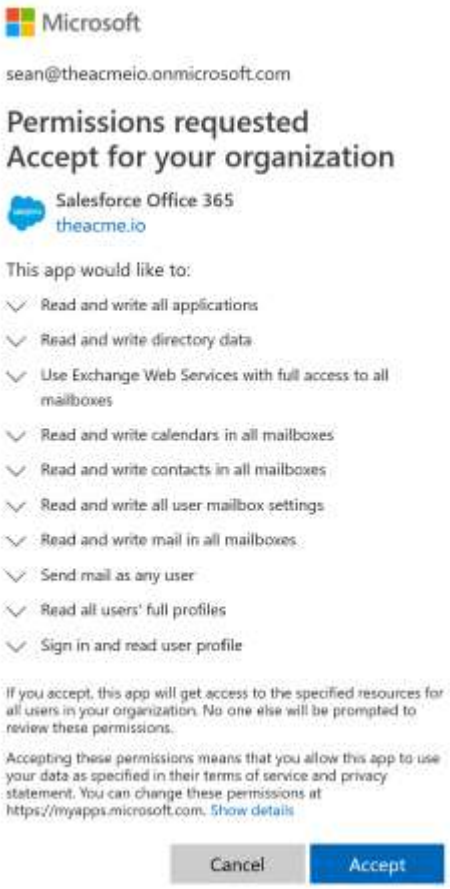
- Configured permissions apply to the signed-in user

Application

- Configured permissions apply to all users

Enterprise App Permissions

- Enterprise Application (tenant-wide) permissions can be granted by Admins.
- Ideal persistence technique since app permissions not reviewed like group membership.



Permissions Structure

OBJECT . ACCESS . CONSTRAINT

Examples:

- Application.ReadWrite.All
- Calendars.ReadWrite
- Calendars.ReadWrite.All
- Directory.ReadWrite.All
- Mail.ReadWrite
- Mail.Send
- User.ReadWrite.All

Permissions Structure: Constraint

All	Shared	AppFolder	No constraint
grants permission for the app to perform the operations on all of the resources of the specified type in a directory.	grants permission for the app to perform the operations on resources that other users have shared with the signed-in user. This constraint is mainly used with Outlook resources like mail, calendars, and contacts.	grants permission for the app to read and write files in a dedicated folder in OneDrive. This constraint is only exposed on Files permissions and is only valid for Microsoft accounts.	the app is limited to performing the operations on the resources owned by the signed-in user.

Most Concerning Azure AD Application Permissions

- Directory.ReadWrite.All
  - Full Control to Azure AD
- AppRoleAssignment.ReadWrite.All
  - Manage app permission grants and app role assignments
- Application.ReadWrite.All
  - Full Control to all Applications
- DelegatedPermissionGrant.ReadWrite.All
  - Allows the app to grant or revoke any delegated permission for any API
- Device.Command
  - Allows the app to launch another app or communicate with another app on a user's device on behalf of the signed-in user.

(Review These!)

Most Concerning Application Permissions (Review These!)

- Exchange Online - Exchange.ManageAsApp
  - Act as Exchange Online
- SharePoint Online - Sites.FullControl.All
  - Full Control to SharePoint Online
  - SharePoint content includes Teams and OneDrive for Business

Interesting Application Permission Notes

Before December 3rd, 2020…

- when the application permission **Device.ReadWrite.All** was granted, the **Device Managers** directory role was also assigned to the app's service principal.
- when the application permission ***Directory.Read.All*** was granted, the **Directory Readers** directory role was also assigned to the app's service principal.
- when ***Directory.ReadWrite.All*** was granted, the **Directory Writers** directory role was also assigned to the app's service principal.
- *These directory roles are not removed automatically when the associated application permissions are revoked.*

Other App Permissions Interesting to Attackers

- Exchange Online - Mail.Read.All (Mail.ReadWrite.All)
  - Ability to read Exchange Online mailboxes
- SharePoint Online - Sites.Read.All (Sites.ReadWrite.All)
  - Read items in all site collections – includes Teams & OneDrive for Business data.

Note: Mail.ReadBasic provides access to email metadata without mail content and is preferable.

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   [redacted]er
f4d30f9e-0837-4e3f-974e-ef282a2fcefe Darth Vader  DarthVader@TrimarcRD.com Member
f2a0fb99-bdaf-49ce-9192-9488ea5d3dae Boba Fett    BobaFett@TrimarcRD.com  Member
```

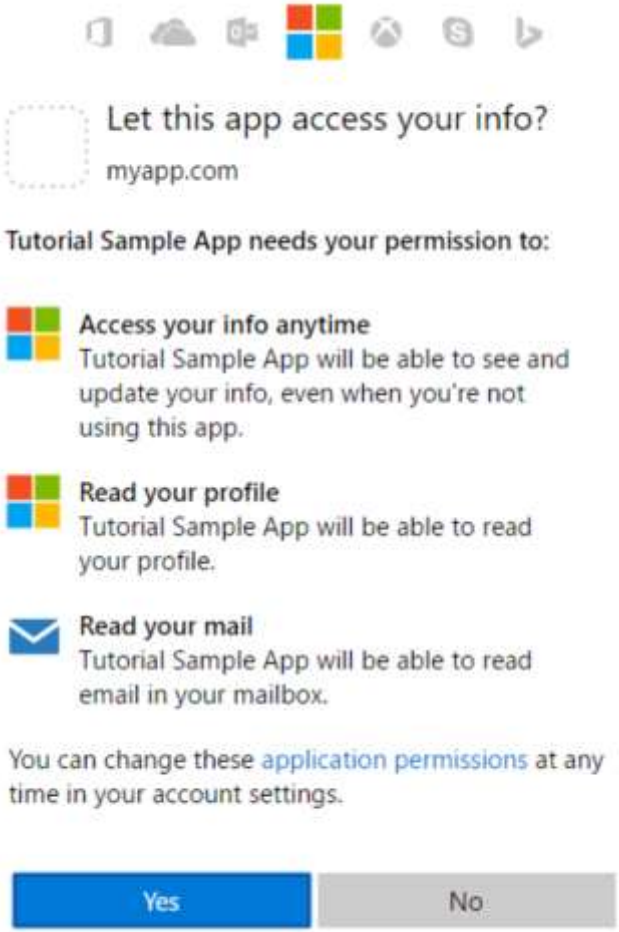
Adding a Credential to an Application

```
PS C:\> New-AzureADApplicationKeyCredential -ObjectId $AppId `
-CustomKeyIdentifier "Alt logon key"  `
-Type Symmetric -Usage Sign `
-Value "Password1234"  `
-StartDate "8/01/2021"


CustomKeyIdentifier : {65, 108, 116, 32...}
EndDate             : 8/1/2022 12:00:00 AM
KeyId               : 7d166f36-278e-49c9-891f-fa0c4da51f82
StartDate           : 8/1/2021 12:00:00 AM
Type                : Symmetric
Usage               : Sign
Value               : {80, 97, 115, 115...}
```

Delegated Permissions

User is prompted by the app to allow the app to have specific permissions.

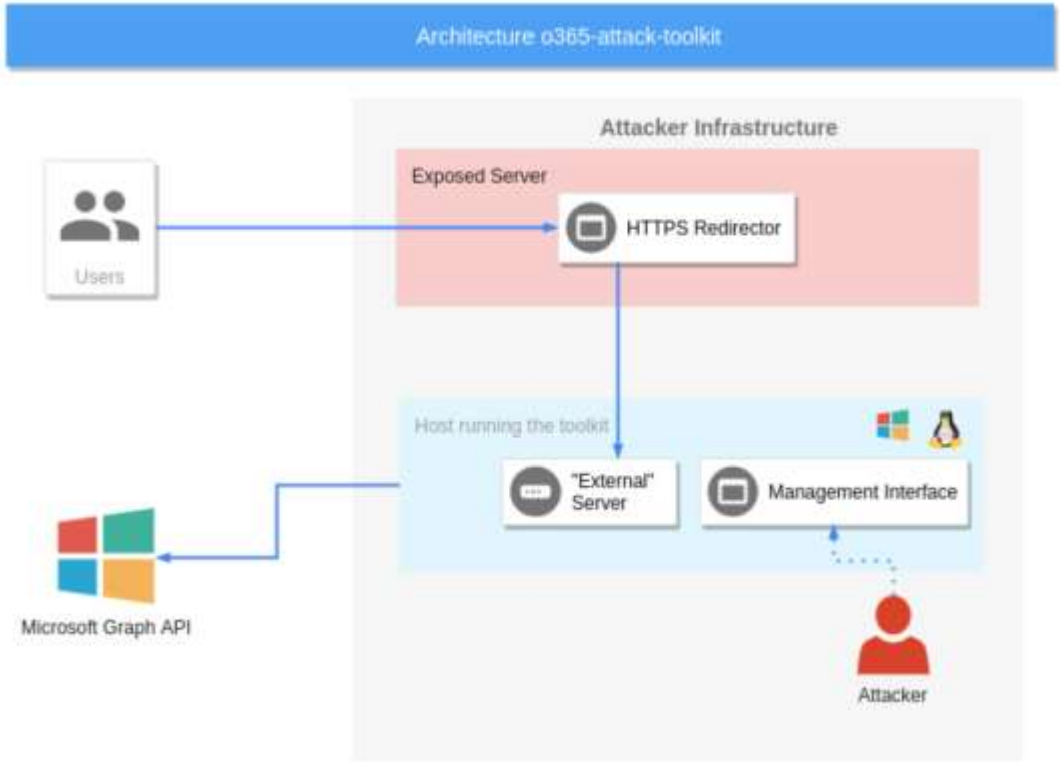
User consent rights configured at the tenant level control delegated permissions.

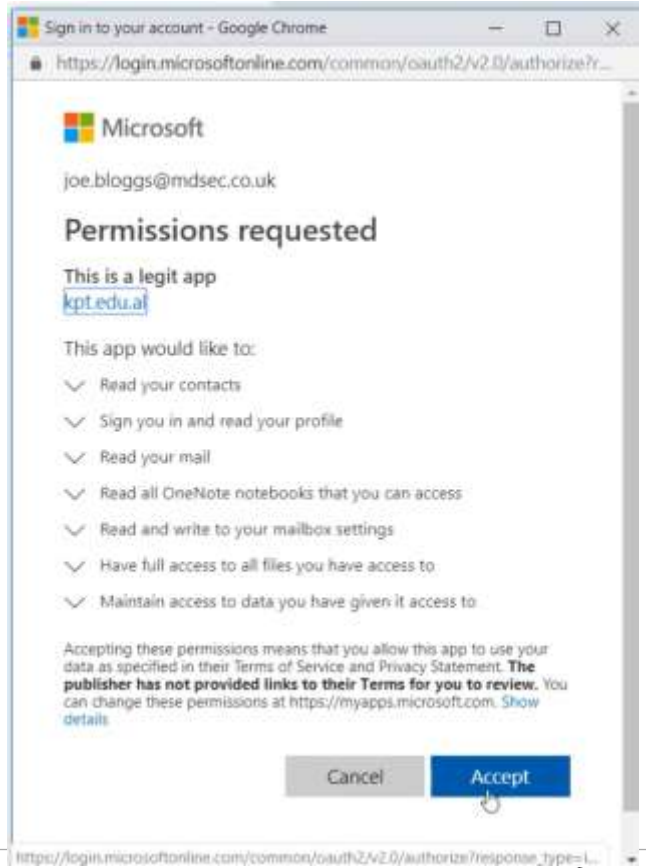


Illicit Consent Grant Attack (OAuth Espionage)

- Illicit Consent Grant Attack
  - Users fooled into granting permissions to an app that looks like a familiar app.
  - MDSec Office 365 Toolkit
    - https://www.mdsec.co.uk/2019/07/introducing-the-office-365-attack-toolkit/
  - FireEye PwnAuth
    - https://www.fireeye.com/blog/threat-research/2018/05/shining-a-light-on-oauth-abuse-with-pwnauth.html
- Overprivileged apps with broad permissions.

Illicit Consent Grant Attack: MDSec O365 Attack Toolkit





https://www.mdsec.co.uk/2019/07/introducing-the-office-365-attack-toolkit/

Protection against OAUTH Attacks

Don’t let users consent to apps

Consent and permissions | User consent settings

Manage

- User consent settings
- Permission classifications

Save | Discard | Got feedback?

When a user grants consent to an application, the user can sign in and the application may be granted access to the organization's data.
Learn more about consent and permissions

User consent for applications
Configure whether users are allowed to consent for applications to access your organization's data. Learn more

- (●) Do not allow user consent
  An administrator will be required for all apps.
- ( ) Allow user consent for apps from verified publishers, for selected permissions (Recommended)
  All users can consent for permissions classified as "low impact", for apps from verified publishers or apps registered in this organization.
- ( ) Allow user consent for apps
  All users can consent for any app to access the organization's data.

Reviewing Azure AD Delegated User Permissions with PowerShell

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

ClientDisplayName           ResourceDisplayName            Permission                                                PrincipalDisplayName
----------------           -------------------            ----------                                                --------------------
Microsoft Intune PowerShell Windows Azure Active Directory User.Read
Microsoft Intune PowerShell Windows Azure Active Directory Group.Read.All
Microsoft Intune PowerShell Microsoft Graph                DeviceManagementManagedDevices.PrivilegedOperations.All
Microsoft Intune PowerShell Microsoft Graph                DeviceManagementManagedDevices.ReadWrite.All
Microsoft Intune PowerShell Microsoft Graph                DeviceManagementRBAC.ReadWrite.All
Microsoft Intune PowerShell Microsoft Graph                DeviceManagementApps.ReadWrite.All
Microsoft Intune PowerShell Microsoft Graph                DeviceManagementConfiguration.ReadWrite.All
Microsoft Intune PowerShell Microsoft Graph                DeviceManagementServiceConfig.ReadWrite.All
Microsoft Intune PowerShell Microsoft Graph                Group.ReadWrite.All
Microsoft Intune PowerShell Microsoft Graph                Directory.Read.All
Office 365 ASI App          Windows Azure Active Directory User.Read                                                 Sean Metcalf
Office 365 ASI App          Office 365 Management APIs     ActivityFeed.Read                                         Sean Metcalf
Office 365 ASI App          Office 365 Management APIs     ServiceHealth.Read                                        Sean Metcalf
```

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

“Solarigate” Cloud Attack & Defense

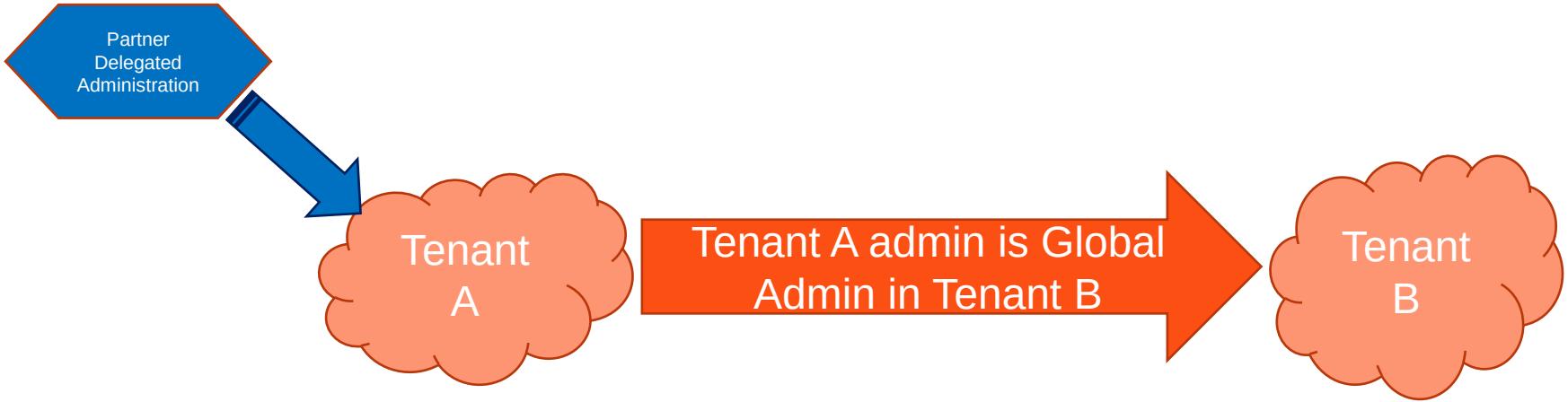
TEC
The Experts Conference
Sponsored by Quest®
SEPTEMBER 1-2, 2021 | VIRTUAL

Solar Winds

- Malicious code added to an update of the Solar Winds (Orion) software
- Solar Winds frequently has privileged access to multiple systems
  - Domain Admin rights on AD (WMI access on DCs)
  - SYSADMIN on SQL
  - Read-only on Vmware (was it only configured for read-only?)
  - Contributor or Reader on Azure
  - Instance rights on AWS
  - Config management on network devices (routers)
  - Global Admin on Azure AD / Office 365
- Malicious code provided attacker access to the Solar Winds software deployment on the customer's network
- Attacker leveraged Solar Winds for initial access and privilege escalation

https://threadreaderapp.com/thread/1338513685162016769.html

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 leverage 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 <u>only options</u>.
  - 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://admin.microsoft.com/AdminPortal/Home#/partners

Delegated Access Permission (DAP) partners

Delegated Access Permission (DAP) partners are Syndication and Cloud Solution Providers (CSP) Partners

"When they sell a Microsoft 365 subscription, they are automatically granted Administer On Behalf Of (AOBO) permissions to the customer tenancies so they can administer and report on the customer tenancies."

OAuth Application & Service Principal Credentials

Attacker added credentials (x509 keys or password credentials) to one or more legitimate OAuth Applications or Service Principals.

Permissions typically Mail.Read or Mail.ReadWrite permissions.

Grants the ability to read mail content from Exchange Online via Microsoft Graph or Outlook REST.

Solarigate Attack Patterns in Microsoft Office 365

Leverage	Add	Modify	Modify	Create	Add
Leverage partner relationship to compromise 1 tenant to compromise dozens (or more!)	Add authentication credentials (tokens & certificates) to existing application service principals	Modify application & service principal credentials/ authentication methods	Modify federation settings	Create new SAML Trust Relationships and/or Federation Trusts	Add new permissions to service principals

Solarigate Protection & Mitigation

- Review & limit consented partner access: https://admin.microsoft.com/AdminPortal/Home#/partners
- Reset passwords on any emergency admin accounts & reduce the number of these accounts to the absolute minimum required.
- Service & user accounts with Privileged Access should be Azure AD accounts only and not on-prem accounts synced or federated to Azure Active Directory.
- Enforce Multi-Factor Authentication (MFA) on all admin accounts. Recommended: enforcing MFA across all users in the tenant.
- Implement Privileged Identity Management (PIM) & conditional access to limit administrative access.
- Implement Privileged Access Management (PAM) to limit access to Azure AD Roles.
- Review & reduce all Enterprise Applications delegated permissions or consent grants.

Solarigate Key Review Items

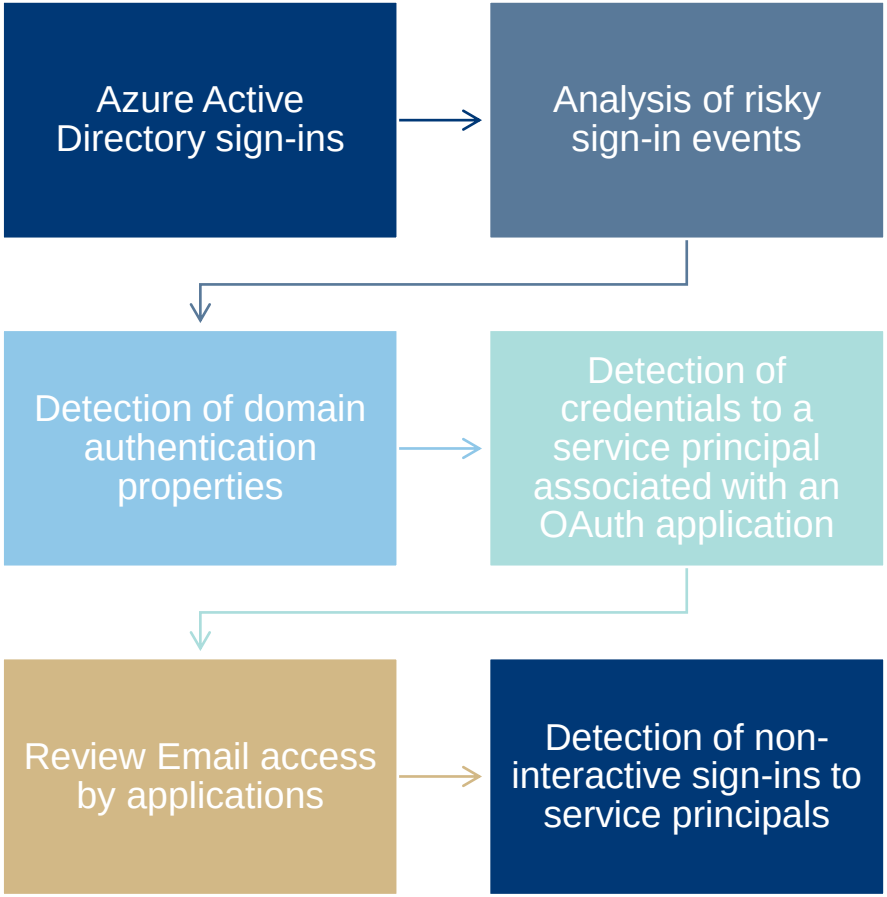
Investigate and review cloud environment logs for suspicious actions and attacker IOCs

Review endpoint audit logs for changes from on-premises for changes to sensitive components

Review Administrative rights in AD & Azure AD

More detail provided in slides at the end of this presentation

Key Monitoring Items



https://www.microsoft.com/security/blog/2020/12/21/advice-for-incident-responders-on-recovery-from-systemic-identity-compromises/

Free Tools for Scanning Azure AD

- CISA Sparrow
  - https://github.com/cisagov/Sparrow
- CrowdStrike CRT
  - https://github.com/CrowdStrike/CRT
- FireEye Azure AD Investigator
  - https://github.com/fireeye/Mandiant-Azure-AD-Investigator

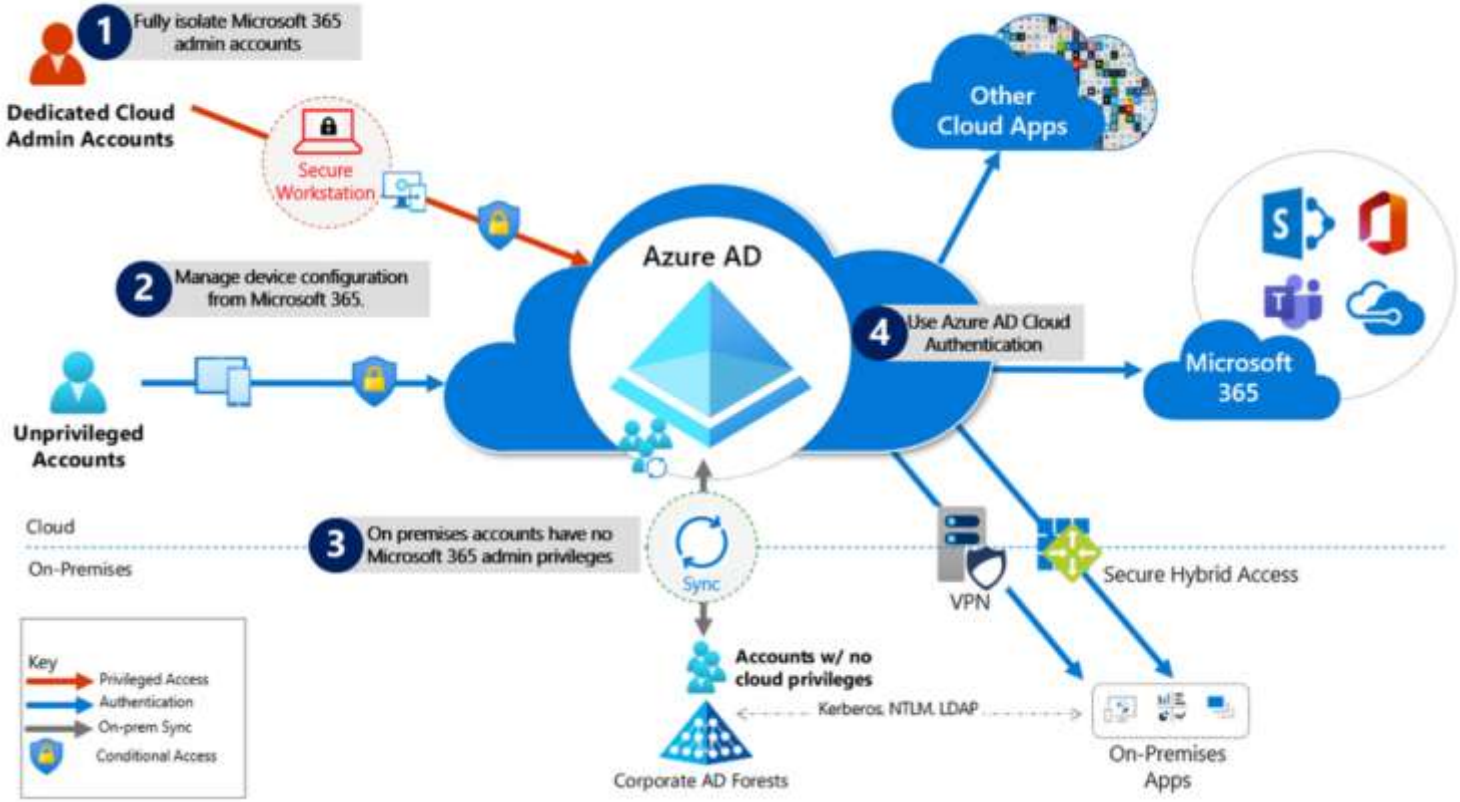
Attackers Have Options

- Compromise account with Owner right on Applications
- Compromise account with privileged rights (member of Azure AD role)
- Compromise Azure AD Connect
- Compromise on-prem Active Directory
- Compromise Microsoft ADFS server (certificate)

Defending the Cloud

TEC
The Experts Conference
Sponsored by Quest®
SEPTEMBER 1-2, 2021 | VIRTUAL

Securing Azure AD



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

Securing Azure AD

- **Fully Isolate Azure AD / Microsoft Office 365 admin accounts**
  They should be:
  1. Mastered in Azure AD.
  2. Authenticated with Multi-factor authentication (MFA).
  3. Secured by Azure AD conditional access.
  4. Accessed only by using Azure Managed Workstations.

There should be no on-prem accounts with Microsoft Office 365 admin rights.

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

Securing Azure AD

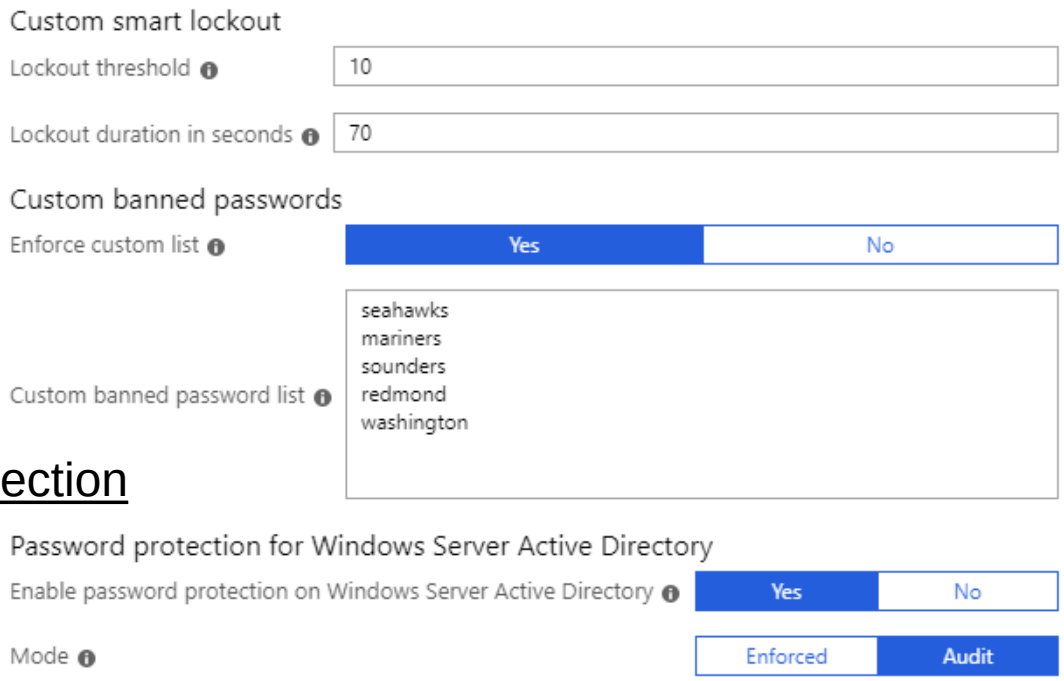
- **Manage from Cloud controlled Devices**
  Use Azure AD Join and cloud-based mobile device management (MDM) to eliminate dependencies on your on-premises device management infrastructure, which can compromise device and security controls.
- **No on-prem account has Azure AD / Microsoft Office 365 privileges**
  Privileged on-premises software must not be capable of impacting Azure AD privileged accounts or roles.
- **Use Azure AD cloud authentication** to eliminate on-prem credential dependencies**.**
  Always use strong authentication, such as Windows Hello, FIDO, the Microsoft Authenticator, or Azure AD MFA.

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

On-Prem: Azure AD Password Protection

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

https://aka.ms/deploypasswordprotection



User Consent & Permissions – Default Settings

Home > Trimarc R&D > Enterprise applications >

Consent and permissions | User consent settings

Manage

- User consent settings
- Permission classifications

Save Discard

When a user grants consent to an application, the user can sign in and the application may be granted access to the organization's data. Learn more about consent and permissions

User consent for applications

Configure whether users are allowed to consent for applications to access your organization's data. Learn more

- ○ Do not allow user consent
  An administrator will be required for all apps.
- ○ Allow user consent for apps from verified publishers, for selected permissions (Recommended)
  All users can consent for permissions classified as "low impact", for apps from verified publishers or apps registered in this organization.
- ◉ Allow user consent for apps
  All users can consent for any app to access the organization's data.

⚠ With your current user settings, all users can allow applications to access your organization's data on their behalf. Learn more about the risks
Microsoft recommends allowing user consent only for verified app publishers or apps from your organization, for permissions you classify as "low impact". Learn more

Group owner consent for apps accessing data

Configure whether group owners are allowed to consent for applications to access your organization's data for the groups they own. Learn more

- ○ Do not allow group owner consent
  Group owners cannot allow applications to access data for the groups they own.
- ○ Allow group owner consent for selected group owners
  Only selected group owners can allow applications to access data for the groups they own.
- ◉ Allow group owner consent for all group owners
  All group owners can allow applications to access data for the groups they own.

User Consent & Permissions – Recommended Settings

Consent and permissions | User consent settings

Manage

- User consent settings
- Permission classifications

Save | Discard | Got feedback?

When a user grants consent to an application, the user can sign in and the application may be granted access to the organization's data.
Learn more about consent and permissions

User consent for applications
Configure whether users are allowed to consent for applications to access your organization's data. Learn more

- (●) Do not allow user consent
  An administrator will be required for all apps.
- ( ) Allow user consent for apps from verified publishers, for selected permissions (Recommended)
  All users can consent for permissions classified as "low impact", for apps from verified publishers or apps registered in this organization.
- ( ) Allow user consent for apps
  All users can consent for any app to access the organization's data.

Group owner consent for apps accessing data
Configure whether group owners are allowed to consent for applications to access your organization's data for the groups they own. Learn more

- (●) Do not allow group owner consent
  Group owners cannot allow applications to access data for the groups they own.
- ( ) Allow group owner consent for selected group owners
  Only selected group owners can allow applications to access data for the groups they own.
- ( ) Allow group owner consent for all group owners
  All group owners can allow applications to access data for the groups they own.

User Consent & Permissions – Recommended Settings

Home > Trimarc R&D > Enterprise applications >

Consent and permissions | User consent settings

Manage

- User consent settings
- Permission classifications

Save Discard

When a user grants consent to an application, the user can sign in and the application may be granted access to the organization's data. Learn more about consent and permissions

User consent for applications

Configure whether users are allowed to consent for applications to access your organization's data. Learn more

- ( ) Do not allow user consent
  An administrator will be required for all apps.
- (•) Allow user consent for apps from verified publishers, for selected permissions (Recommended)
  All users can consent for permissions classified as "low impact", for apps from verified publishers or apps registered in this organization.
  Select permissions to classify as low impact
- ( ) Allow user consent for apps
  All users can consent for any app to access the organization's data.

Group owner consent for apps accessing data

Configure whether group owners are allowed to consent for applications to access your organization's data for the groups they own. Learn more

- (•) Do not allow group owner consent
  Group owners cannot allow applications to access data for the groups they own.
- ( ) Allow group owner consent for selected group owners
  Only selected group owners can allow applications to access data for the groups they own.
- ( ) Allow group owner consent for all group owners
  All group owners can allow applications to access data for the groups they own.

Get started by adding the most used permissions.

The following permissions are the most requested application permissions with low-risk access. Get started managing consent and permissions for all users by adding these delegated permissions with only one click. Learn more

- [x] User.Read - sign in and read user profile
- [ ] offline_access - maintain access to data that users have given it access to
- [ ] openid - sign users in
- [x] profile - view user's basic profile
- [x] email - view user's email address

Yes, add selected permissions No, I'll add permissions

Consent and permissions | Permission classifications

Manage

- User consent settings
- Permission classifications

+ Add permissions

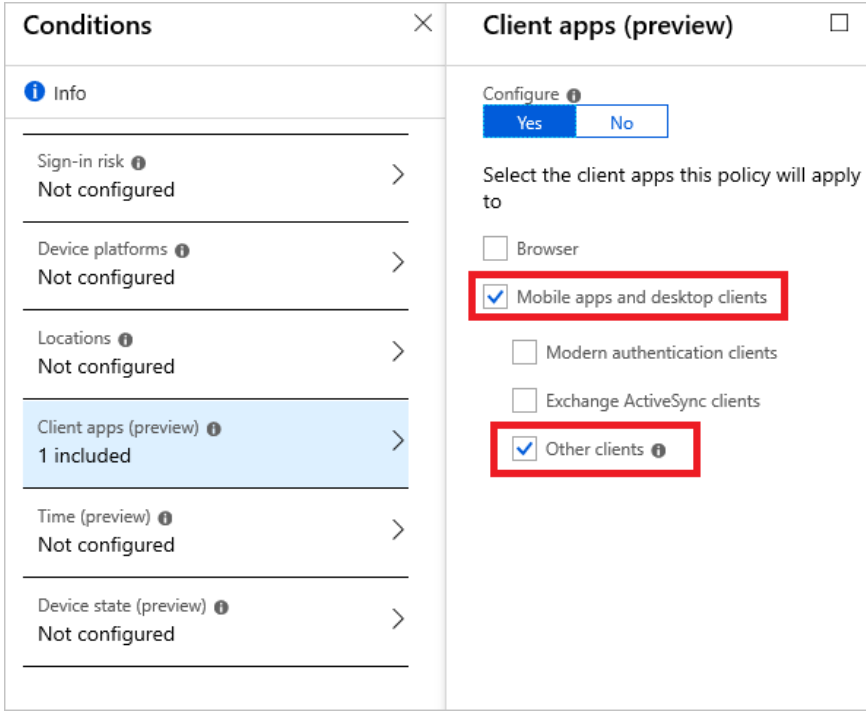
Classify permissions

Choose which permissions are classified as "low risk". Learn more

API used	Permissions	Description
Microsoft Graph	email	View users' email address
Microsoft Graph	User.Read	Sign in and read user profile
Microsoft Graph	profile	View users' basic profile

Blocking Legacy Auth in Azure AD

- Identify Legacy Authentication Use (Sign-ins)
  https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/block-legacy-authentication
- If Legacy Authentication protocols are not in use:
  - Block with Conditional Access
  - Security Defaults (if not using Conditional Access)
- Ensure you have coverage for all device type scenarios (Question 7)
  https://techcommunity.microsoft.com/t5/Azure-Active-Directory-Identity/Azure-AD-Mailbag-Conditional-Access-Q-amp-A/ba-p/566492



FYI, Basic Auth Support will be disabled at some point
https://techcommunity.microsoft.com/t5/exchange-team-blog/basic-authentication-and-exchange-online-february-2021-update/ba-p/2111904

Blocking Legacy Authentication in Exchange

- Disable services at the mailbox level
  https://docs.microsoft.com/en-us/powershell/module/exchange/client-access/set-casmailbox?view=exchange-ps

- Authentication Policies
  https://docs.microsoft.com/en-us/exchange/clients-and-mobile-in-exchange-online/disable-basic-authentication-in-exchange-online

- Client IP Block
  https://docs.microsoft.com/en-us/powershell/module/exchange/organization/set-organizationconfig?view=exchange-ps

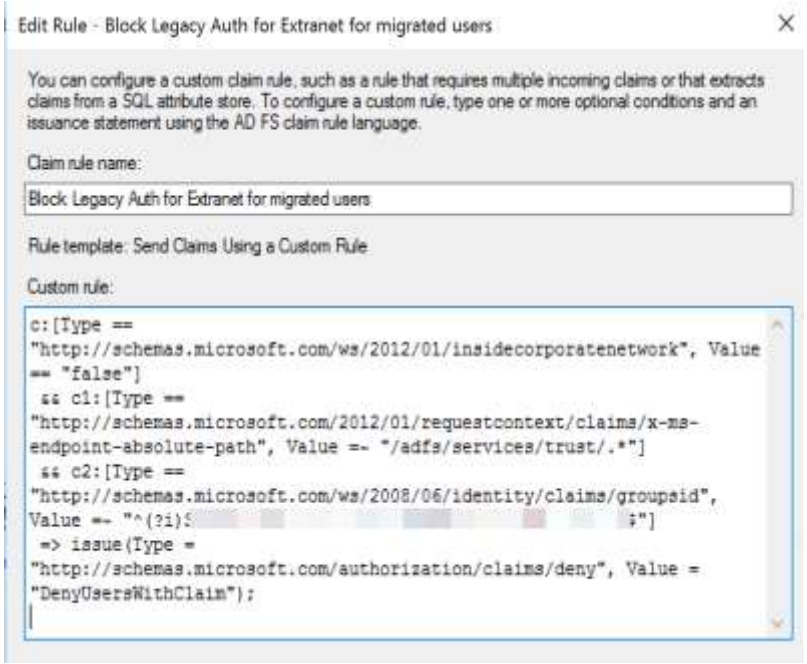
```
PS O:\> New-AuthenticationPolicy -Name "Block Basic Authentication"

RunspaceId                          :
AllowBasicAuthActiveSync            : False
AllowBasicAuthAutodiscover          : False
AllowBasicAuthImap                  : False
AllowBasicAuthMapi                  : False
AllowBasicAuthOfflineAddressBook    : False
AllowBasicAuthOutlookService        : False
AllowBasicAuthPop                   : False
AllowBasicAuthReportingWebServices  : False
AllowBasicAuthRest                  : False
AllowBasicAuthRpc                   : False
AllowBasicAuthSmtp                  : False
AllowBasicAuthWebServices           : False
AllowBasicAuthPowershell            : False
```

```
PS O:\> Set-OrganizationConfig -IPListBlocked 41.204.224.0/24,41.203.78.0/24
PS O:\>
```

Blocking Legacy Auth in ADFS/Federation

Authorization rules

- Very rich expressions using ADFS claims language
- Happens <u>after</u> authentication
- Applies to ALL applications behind Azure AD



ADFS Monitoring

Azure AD Connect Health with ADFS

- Alerts about common ADFS issues (cert expiring, missing updates, performance, etc)
- Will also alert on bad Password Attempts and Risky IPs!

ADFS 2016 / ADFS 2019: Turn On Smart Lockout

https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/operations/configure-ad-fs-extranet-smart-lockout-protection

Phishing Defenses

- Require Users to do MFA
  - Authenticator App recommended. Better performance and less prompts (behaves as authentication token broker)
- Per User MFA
  - Will be prompted for MFA regardless of the application
- Conditional Access Policy better
  - Location, App, etc
- Risk Based Policy Best
  - Only prompt when Risk detected

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

Monitor: Azure AD Logs

- Pull Logs from the Azure AD Graph API
  - Initially was only integration point, we have better options
- Azure Event Hub
  - Pre-Built Integration into Azure Monitor, will PUSH events to SIEM
    - Splunk (docs)
    - Sumo Logic (docs)
    - IBM QRadar (docs)
    - ArcSight (docs)
    - SysLog (docs)
- Azure Sentinel

Key Monitoring Scenarios (part 1)

- **Suspicious activity**: All Azure AD risk events should be monitored for suspicious activity. Azure AD Identity Protection is natively integrated with Azure Security Center.
  - Define the network named locations to avoid noisy detections on location-based signals.
- **User Entity Behavioral Analytics (UEBA) alerts**: Use UEBA to get insights on anomaly detection.
  - Microsoft Cloud App Discovery (MCAS) provides UEBA in the cloud.
  - You can integrate on-prem UEBA from Azure ATP. MCAS reads signals from Azure AD Identity Protection.
- **Emergency access accounts activity**: Any access using emergency access accounts should be monitored and alerts created for investigations. This monitoring must include:
  - Sign-ins.
  - Credential management.
  - Any updates on group memberships.
  - Application Assignments.
- **Privileged role activity**: Configure and review security alerts generated by Azure AD PIM. Monitor direct assignment of privileged roles outside PIM by generating alerts whenever a user is assigned directly.

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

Key Monitoring Scenarios (part 2)

- **Azure AD tenant-wide configurations**: Any change to tenant-wide configurations should generate alerts in the system. These include but are not limited to
  - Updating custom domains
  - Azure AD B2B allow/block list changes
  - Azure AD B2B allowed identity providers (SAML IDPs through direct federation or social logins)
  - Conditional Access or Risk policy changes
- **Application and service principal objects**:
  - New applications or service principals that might require Conditional Access policies
  - Additional credentials added to service principals
  - Application consent activity
- **Custom roles**:
  - Updates of the custom role definitions
  - New custom roles created

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

Common Persistence Method Checks

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

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

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

Security Checklist (Summary)

1. Limit Global Admins to 5 or less accounts.
2. Enforce Multi-Factor Authentication (MFA) for accounts in Azure AD Roles.
3. Use Azure Privileged Identity Management (PIM).
   - No standing admin access
   - Admin access requires elevation + MFA
   - Approval workflows and elevation scheduling
   - Alerts on admin activity taking place outside of PIM
   - Applies/Protect Azure Resources as well!
   - Can buy Azure AD P2 license for just your admins
4. Secure Global Admin Authentication.
   - Separate Admin Account (in Azure AD, not synched)
   - Require MFA
   - Use Cloud Admin Workstations
   - Configure for FIDO2 authentication
5. Configure 2 Emergency Global Admin Accounts.
6. Protect Azure AD Connect Server (& associated SQL database) like a DC and ensure Azure AD Connect is running the current version.
7. Configure Security Defaults OR Conditional Access policies (ensure Legacy Authentication is blocked).
8. Limit user app consent ability.
9. Review Application Permissions.
10. Remove user accounts configured as application owners.
11. Review Partner delegated permissions.
12. Monitor Azure AD & Office 365 Logs.
13. Determine if Tenant Restrictions makes sense.
14. Review the Azure AD Security Operations Guide https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/security-operations-introduction

Conclusion

Attackers are setting their sights on the Microsoft Cloud.

Office 365 contains customer data which makes it a target.

Cloud is a new paradigm that requires special attention (& resources).

Security responsibilities are shared between provider and customer.

Security controls need to be researched, tested, and implemented.

On-prem resources used to integrate with and/or manage the cloud could be used to compromise the cloud.

Security in the cloud may cost extra.

Sean Metcalf (@PyroTek3)
s e a n @ trimarcsecurity. com
TrimarcSecurity.com | www.ADSecurity.org

Questions?

APPENDIX: Solarigate Key Review Items

- Investigate and review cloud environment logs for suspicious actions and attacker IOCs, including:
  - Unified Audit Logs (UAL).
  - Azure Active Directory (Azure AD) logs.
  - Active Directory logs.
  - Exchange on-prem logs.
  - VPN logs.
  - Engineering systems logging.
  - Antivirus and endpoint detection logging.

https://www.microsoft.com/security/blog/2020/12/21/advice-for-incident-responders-on-recovery-from-systemic-identity-compromises/

APPENDIX: Solarigate Key Review Items

- Review endpoint audit logs for changes from on-premises for actions including, but not limited to, the following:
  - Group membership changes.
  - New user account creation.
  - Delegations within Active Directory.
  - Along with other typical signs of compromise or activity.

https://www.microsoft.com/security/blog/2020/12/21/advice-for-incident-responders-on-recovery-from-systemic-identity-compromises/

APPENDIX: Solarigate Key Review Items

- Review Administrative rights in your environments
  - Review privileged access **in the cloud** and remove any unnecessary permissions. Implement Privileged Identity Management (PIM); setup Conditional Access policies to limit administrative access during hardening.
  - Review privileged access **on-premise** and remove unnecessary permissions. Reduce membership of built-in groups, verify Active Directory delegations, harden Tier 0 environment, and limit who has access to Tier 0 assets.
  - Review all Enterprise Applications for delegated permissions and consent grants that allow (sample script to assist):
    - Modification of privileged users and roles.
    - Reading or accessing all mailboxes.
    - Sending or forwarding email on behalf of other users.
    - Accessing all OneDrive or SharePoint sites content.
    - Adding service principals that can read/write to the Directory.

https://www.microsoft.com/security/blog/2020/12/21/advice-for-incident-responders-on-recovery-from-systemic-identity-compromises/

APPENDIX: Solarigate Key Review Items

- Review access and configuration settings for the following Office 365 products:
  - SharePoint Online Sharing
  - Teams
  - PowerApps
  - OneDrive for Business
- Review user accounts
  - Review and remove guest users that are no longer needed.
  - Review email configurations using Hawk or something similar.
    - Delegates
    - Mailbox folder permissions
    - ActiveSync mobile device registrations
    - Inbox Rules
    - Outlook on the Web Options
  - Validate that both MFA and self-service password reset (SSPR) contact information for all users is correct.

https://www.microsoft.com/security/blog/2020/12/21/advice-for-incident-responders-on-recovery-from-systemic-identity-compromises/

Thank you.

TEC

The Experts Conference

Sponsored by Quest®

SEPTEMBER 1-2, 2021 I VIRTUAL