

Sean Metcalf CTO, Trimarc The Current State of Active Directory (& Azure AD) Security: The Good and the Bad



Agenda

- Attacking Active Directory
- The Most Common AD Security Issues
- Attacking & Defending Office 365/Azure AD



Attacking Active Directory





Attackers Require...

- Account (credentials)
- Rights (privileges)
- Access (connectivity to resources)

Attacker Capability Depends on the Defender...



Traditional AD Administration

- All admins are Domain Admins.
- Administration from anywhere servers, workstations, Starbucks.
- Need a service account with AD rights Domain Admin!
- Need to manage user accounts Account Operators!
- Need to run backups (anywhere) Backup Operators!
- Management system deploys software & patches all workstations, servers, & Domain Controllers.
- Agents, everywhere!

5 • Full Compromise... Likely #TEC2019



As an Attacker, Do I Need Domain Admin?

No.



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?



In the Real World, Rights are Everywhere

- Workstation Admins have full control on workstation computer objects and local admin rights.
- Server Admins have full control on server computer objects and local admin rights.
- Often, Server Admins are Exchange Admins.
- Sometimes Server Admins have rights to Domain Controllers.
- Help Desk Admins have local admin rights and remote control on user workstations.
- Local admin accounts & passwords often the same among workstations, and sometimes the same among servers.
- "Temporary" admin group assignments often become permanent.



3rd Party Product Permission Requirements

- Domain user access
- Operations systems access
- Mistaken identity trust the installer
- AD object rights
- Install permissions on systems
- Needs System rights

- Active Directory privileged rights
- Domain permissions during install
- More access required than often needed.
- Initial start/run permissions
- Needs full AD rights



3rd Party Product Permission Requirements

- Domain user access
- Operations systems access
- Mistaken identity trust the installer
- AD object rights
- Install permissions on systems
- Needs System rights

- Active Directory privileged rights
- Domain permissions during install
- More access required than often needed.
- Initial start/run permissions
- Needs full AD rights



Over-permissioned Delegation

- Use of built-in groups for delegation
- Clicking the "easy button": Full Control at the domain root.
- Let's just "make it work"
- Delegation tools in AD are challenging to get right



Reviewing Active Directory Permissions

- PowerShell for OU Permission Report:
 - <u>https://blogs.technet.microsoft.com/ashleymcglone/2013/03/25/active-directory-ou-permissions-report-free-powershell-script-download/</u>
- ACLight (Batch file that calls PowerShell):
 - <u>https://github.com/cyberark/ACLight</u>
- Bloodhound:
 - <u>https://github.com/BloodHoundAD/BloodHound</u>



Common AD Security Issues

We find really interesting things...



Local Administrator Passwords Not Managed on Workstations or Servers

- Workstation build usually sets the standard organization Administrator password.
- Compromise one workstation to compromise them all

Mitigation:

Ensure local Administrator passwords regularly change on workstations and servers (using something like Microsoft LAPS).

```
mimikatz # lsadump::sam
Domain : RDLABDC02
SysKey : ea0fad2f73ad366ef5c9b1370d241657
Local SID : 5-1-5-21-3017930946-1529675408-4271689233
SAMKey : 364d77a8399af95033658c1498e09bf2
      : 000001f4 (500)
RID
        Administrator
User :
I M
NTLM : 4771c80c83293beb882cb621a6a063fe
RID
      : 000001f5 (501)
      : Guest
User
NTIM :
```



Domain Password Policy

Account	Policies/	/Password	Policy
---------	-----------	-----------	--------

Policy	Setting
Enforce password history	24 passwords remembered
Maximum password age	42 days
Minimum password age	1 days
Minimum password length	7 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled



Domain Password Policy

Policy	Policy Setting
Enforce password history	24 passwords remembered
🔯 Maximum password age	42 days
Minimum password age	1 days
Minimum password length	8 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled



Domain Password Policy

Policy	Policy Setting
Enforce password history	24 passwords remembered
🔯 Maximum password age	42 days
🔯 Minimum password age	1 days
Minimum password length	10 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled

Set to at least 12 characters, preferably 15. At least use Fine-Grained Password Policies for Admins & Service Accounts



Regular Users in AD Admin Groups

• User account is a member of Administrators, Domain Admins, or nested group.

```
Administrators Properties
```

? ×

General	Members	Member Of	Managed By	
Membe	rs:			
Name		Ac	ctive Directory Domain Services Folder	
🍇 Domain Admins		s trir	imarcresearch.com/Users	
🛛 🎎 En	🍇 Enterprise Admins		imarcresearch.com/Users	
💄 Ja	👗 Jack Duncan		trimarcresearch.com/Accounts/Users	
🙎 trin	narcadmin	trir	imarcresearch.com/Users	



No Account Naming Standard

- Security through obscurity?
- Does not fool attackers
- Discovering AD admin accounts is trivial

Mitigation:

- Use designators to clearly identify admin rights:
 - -ada
 - -sa
 - -wa

Domain Admins Properties

Genera	Members	Member Of	Managed By
Memb	ers:		
Nan	ie	Act	ive Directory Domain Services Folder
8	Eddie	trim	arcresearch.com/Administration/AD Admin
8	lonSnow	trim	arcresearch.com/Administration/AD Admin
8	F Stark	trim	arcresearch.com/Administration/AD Admin
8 t	rimarcadmin	trim	arcresearch.com/Users
81	/ulnerability So	canner trim	arcresearch.com/Administration/Privileged

?

X

Account Operators

Account Operators Properties

?

Х

eneral	Members	Member Of	Managed By
Memben	s:		
Name <u>&</u> Rut	th Parker	Active Din trimarcrese	ectory Domain Services Folder earch.com/Administration/Admin Acco





7 X Account Operators Properties General Members Member Of Managed By Members: (i) Note Name Ruth Parker By default, this built-in group has no members, and it can create and manage users and groups in the domain, including its own membership and that of the Server Operators group. This group is considered a service administrator group because it can modify Server Operators, which in turn can modify domain controller settings. As a best practice, leave the membership of this group empty, and do not use it for any delegated administration. This group cannot be renamed, deleted, or moved.



Admin Group Nesting Issues

	Sec	unity	Attribute Editor	Object	Secu	unity	Attribute Editor
General	Members	Member Of	Managed By	General	Members	Member Of	Managed By
lembers:			<u> 1</u>	Members:			
Name	Active Dire	ctory Domain Servic	es Folder	Name	Active Dire	ctory Domain Service	es Folder
💐 ADA Admin	s lab.adsecu	rity.org/AD Manager	ment	Server Adm	ins lab.adsecu	rity.org/AD Manager	nent
& ADSAdmini	str lab.adsecu	irity.org/Users				191 II. (191	
💄 Luke Skywa	alker lab.adsecu	irity.org/AD Manager	ment				
	ADA Adr	nins Properties			Server Adr	nins Properties	; ?
	Sec	unty	Attribute Editor		Secu	inty	Attribute Editor
	mbers	Member Of	Managed By	6	Members	Member Of	Managed By
			500 E	Members.			
Ae.		207 01850 0011000 UT	es Faldes	Name	Active Direc	ctory Domain Service	es Folder
Me. Name	Active Dire	ectory Domain Servic	es roidei			and the second second second	2200
Name Macritical Serv	Active Dire	ectory Domain Servic urity.org/AD Manager	ment	🔏 Han Solo	lab.adsecur	ity.org/AD Managem	ient

Default Domain Controllers Policy is.. default

ocal Policies/Security Options		
Domain Controller		
Policy		Setting
Domain controller: LDAP server s	signing requirements	None
Domain Member		
Policy		Setting
Domain member: Digitally encrypt	t or sign secure channel data (always)	Enabled
Microsoft Network Server		
Policy		Setting
Microsoft network server: Digitally	y sign communications (always)	Enabled
Microsoft network server: Digitally	y sign communications (if client agrees)	Enabled
23	#TEC2019	THE C The Experts Conference

Sponsored by Quest*

AD Admin Accounts Have Old Passwords.

SamAccountName	Enabled	PasswordLastSet	Password Age (years)
admAEdwards	Yes	1/12/2013 2:20:06 PM	6.5
admBWalker	No	6/11/2017 10:14:08 AM	2.2
admCGriffin	Yes	3/1/2019 12:41:18 PM	0.4
Administrator	Yes	1/9/2005 10:58:24 AM	14.5
AGPMService	Yes	5/3/2009 3:17:32 PM	10.2
SCCMsvc	Yes	11/14/2011 5:23:12 PM	7.6
VMWareAdmin	Yes	8/28/2012 10:23:41 AM	7.0
VulnerabilityScanner	Yes	9/19/2015 4:43:19 PM	3.9



Service Accounts in Domain Admins

• Service Accounts rarely actually need Domain Admin rights

Domain Admins Properties

• Better to delegate the required rights for the accounts.

		•			
General	Members	Membe	r Of	Managed By	
Membe	rs:				
Name	•		Acti	ve Directory Do	omain Services Folder
Eddie		trimarcresearch.com/Administration/AD Admin			
👗 JonSnow		trima	arcresearch.cor	m/Administration/AD Admin	
👗 T Stark		trima	arcresearch.cor	m/Administration/AD Admin	
🛛 👗 trir	시 trimarcadmin		trima	arcresearch.cor	m/Users
8 M	Inerability So	anner	trima	arcresearch.cor	m/Administration/Privileged

?

X

Mitigation:

- Remove from Domain Admins
- Delegate appropriate rights
- Use separate accounts for different tiers:
 - Workstations
 - Servers
 - Domain Controllers

Default Domain Administrator Account SPN

trim

Edit

- There is no good reason for admin accounts to have Kerberos SPNs.
- Attack:

Kerberoast these accounts to own AD.

ar	ray]\$ServiceAccounts = Get-ADUser -Filter { ServicePrincipalName -like "*" } -Property *
Se ori (rviceAccountSPNs = @() Each (\$ServiceAccountsItem in \$ServiceAccounts) ForEach (\$ServiceAccountsItemSPN in \$ServiceAccountsItem.ServicePrincipalName) {
	[array]\$ServiceAccountSPNs += \$ServiceAccountsItenSPN }
F	
11	st purge
Fo	rEach (\$ServiceAccountSPNItem in \$ServiceAccountSPNs)
3	Add-Type -AssemblyName System.IdentityModel New-Object System.IdentityModel.Tokens.KerberosRequestorSecurityToken -ArgumentList \$ServiceAccountSPNI
	27 #TEC2019

arcadmir	n Propertie	s				?	×
ganization	Publishe	ed Certificates	Memb	ber Of	Passw	ord Repli	cation
Dial-in	Object	Security	r	Enviro	nment	Sess	sions
eneral	Address	Account	Profile	Tel	ephones	Dele	gation
mote cont	trol Remo	te Desktop Se	rvices Pr	ofile	COM+	Attribute	e Editor
tributes:							
Attribute		Value					^
objectGU	ID	5ef40239-0	ede-497	3-b1c9	fe9c238	d5f1a	
object Sid		S-1-5-21-30	590994	13-382	6416028-	8152235	8
primaryGro	diguo	513 = (GR	OUP_RI	D_USE	ERS)		
pwdLastS	et	5/16/2018 2:05:36 PM Eastern Daylight Tim					
replProper	rtyMetaData	AttID Ver	Loc.US	SN	On	DSA.	
sAMAcco	untName	trimarcadmi	n			562,535555	
sAMAcco	untType	805306368	= (NOF	MAL_	USER_A	CCOUNT	
servicePri	ncipalName	MSSQLSv	TRRD	SQL-14	133		
userAcco	untControl	0x200 = (N	ORMAL	ACCO	DUNT)		
uSNChan	ged	12883					
uSNCreat	ed	8196					
whenCha	nged	5/17/2018	12:13:21	AM E	astem Da	eylight Tir	
whenCrea	ted	5/16/2018	9:20:16	PM Ea	stem Day	hight Tim	
							~
<						>	1

Filter

Server GPOs Linked to Domain Controllers



Server Polic	ey .		
Scope Details	Settings Delegation	n	
Server P	olicy		
Data collecte	d on: 3/14/2018 11:5	8:36 PM	
Computer C	Configuration (Enab	led)	
Policies			
Window	rs Settings		
Secur	ity Settings		
Res	tricted Groups		
	Group	Members	Member of
	ADSECLAB\Server A	dmins	BUILTIN \Administrators



Server GPOs Linked to Domain Controllers

Server Policy

Policies

Data collected on: 3/14/20

Computer Configuration

Windows Settings

Security Settings

Restricted Grou



Only use GPOs dedicated to Domain Controllers, don't link GPOs already linked to other OUs.

1				
Settings Delega	tion			
olicy on: 3/14/2011		Administra	tors Properties	ş ?)
nfiguration (Object	Secu	irity	Attribute Editor
	General	Members	Member Of	Managed By
Settings	Members:			
y Settings	Name	Active [irectory Domain Ser	vices Folder
icted Group	adsecadm	in ad adse	curity.org/Users	
	Sectemation Ac	Imins ad.adse	curity.org/Users	
	Server Admins ad.adsecutiv.org/Users			
AD SECEND (Se				
noin				
alli				
dv				
±TEC2019				
	<		111	

Modify Rights to GPOs at Domain /DC Level

R	Group Policy Management					- 🗆 X
	File Action View Window Help					- 8
۰	🔿 🛛 🚾 🖉 🕼 👘					
l Dor	mains ^	Server Baseline S	ecurity Policy			
角	trimarcresearch.com	Scope Details Setting	gs Delegation			
>	Default Domain Policy Accounts	These groups and users Groups and users	have the specified perm	nission for this GF	20	
>	Disabled	Name	^		Allowed Permissions	Inherited
Y	Domain Controllers	Authenticated User	5		Read (from Security Filtering)	No
~	 Default Domain Controllers Policy Server Baseline Security Policy Servers 	Domain Admins (TF Compare Admins) Enterprise Admins (Second Admins)	RIMARCRESEARCH\Do TRIMARCRESEARCH\ MAIN CONTROLLERS	omain Admins) Enterprise Ad	Edit settings, delete, modify security Edit settings, delete, modify security Read	No No
11.00	Server Baseline Security Policy	Nick Fury (nfury-sa)	@trimarcresearch.com)		Edit settings, delete, modify security	No
	S	SYSTEM			Edit settings, delete, modify security	No
>	🖹 Workstations 🗸 🗸	Add	Remove	Propertie	s	Advanced
<	>			la la		1
	Only AD Admins sh	ould have r	nodity righ	nts on (SPOs linked to t	he
	30	Domain/Dor	main Cont	rollers.	т	The Experts Conference

Sponsored by Quest*

Domain Permission Delegation Issues

Domain	: lab.trimarcresearch.com	
IdentityReference	: TRDLAB\Domain Computers	
ActiveDirectoryRights	: Full Control	
ObjectAttribute	: user All	
InheritedObjectClass	: user	
ObjectClass	: A]]	
AccessControlType	: Allow	
IsInherited	: False	
Domain :	lab.trimarcresearch.com	
IdentityReference :	TRDLAB\ServerAdmins	
ActiveDirectoryRights :	ReadProperty, WriteProperty, Exte	endedRight, GenericExecute
ObjectAttribute :	computer All	
InheritedObjectClass :	computer	
ObjectClass :	A]]	
AccessControlType :	Allow	
IsInherited :	False	
ObjectFlags :	InheritedObjectAceTypePresent	
InheritanceFlags :	ContainerInherit	
PropagationFlags :	Inheritonly	
FlaggedForReview :	False	



AdminSDHolder Permission Delegation Issues

Domain	: lab.trimarcresearch.com
ObjectDN	: CN=AdminSDHolder,CN=System,DC=lab,DC=trimarcresearch,DC=com
IdentityReference	: TRDPROD\User Admins
ActiveDirectoryRights	: ReadProperty, WriteProperty, GenericExecute
InheritedObjectClass	: A11
ObjectClass	: A11
AccessControlType	: Allow
IsInherited	: False
ObjectFlags	: None
InheritanceFlags	: None
PropagationFlags	: None
Domain	: prod.trimarcresearch.com
Domain ObjectDN	: prod.trimarcresearch.com : CN=AdminSDHolder,CN=System,DC=prod,DC=trimarcresearch,DC=com
Domain ObjectDN IdentityReference	: prod.trimarcresearch.com : CN=AdminSDHolder,CN=System,DC=prod,DC=trimarcresearch,DC=com : TRDPROD\User Admins
Domain ObjectDN IdentityReference ActiveDirectoryRights	: prod.trimarcresearch.com : CN=AdminSDHolder,CN=System,DC=prod,DC=trimarcresearch,DC=com : TRDPROD\User Admins : ReadProperty, WriteProperty, GenericExecute
Domain ObjectDN IdentityReference ActiveDirectoryRights InheritedObjectClass	<pre>: prod.trimarcresearch.com : CN=AdminSDHolder,CN=System,DC=prod,DC=trimarcresearch,DC=com : TRDPROD\User Admins : ReadProperty, WriteProperty, GenericExecute : All</pre>
Domain ObjectDN IdentityReference ActiveDirectoryRights InheritedObjectClass ObjectClass	<pre>: prod.trimarcresearch.com : CN=AdminSDHolder,CN=System,DC=prod,DC=trimarcresearch,DC=com : TRDPROD\User Admins : ReadProperty, WriteProperty, GenericExecute : All : All</pre>
Domain ObjectDN IdentityReference ActiveDirectoryRights InheritedObjectClass ObjectClass AccessControlType	<pre>: prod.trimarcresearch.com : CN=AdminSDHolder,CN=System,DC=prod,DC=trimarcresearch,DC=com : TRDPROD\User Admins : ReadProperty, WriteProperty, GenericExecute : All : All : Allow</pre>
Domain ObjectDN IdentityReference ActiveDirectoryRights InheritedObjectClass ObjectClass AccessControlType IsInherited	<pre>: prod.trimarcresearch.com : CN=AdminSDHolder,CN=System,DC=prod,DC=trimarcresearch,DC=com : TRDPROD\User Admins : ReadProperty, WriteProperty, GenericExecute : All : All : Allow : False</pre>
Domain ObjectDN IdentityReference ActiveDirectoryRights InheritedObjectClass ObjectClass AccessControlType IsInherited ObjectFlags	<pre>prod.trimarcresearch.com CN=AdminSDHolder,CN=System,DC=prod,DC=trimarcresearch,DC=com TRDPROD\User Admins ReadProperty, WriteProperty, GenericExecute All All All False None</pre>
Domain ObjectDN IdentityReference ActiveDirectoryRights InheritedObjectClass ObjectClass AccessControlType IsInherited ObjectFlags InheritanceFlags	<pre>: prod.trimarcresearch.com : CN=AdminSDHolder,CN=System,DC=prod,DC=trimarcresearch,DC=com : TRDPROD\User Admins : ReadProperty, WriteProperty, GenericExecute : All : All : All : Allow : False : None : ContainerInherit</pre>

Admins Use Regular Workstations for AD Administration

1 workstation

30 accounts in the local Administrators group.

50 accounts w/ local admin via software management system. 20 accounts with control of the computer via security agent(s).

~ 100 accounts with effective admin rights on the workstation

How many GPOs apply to the workstation & how many accounts have modify rights?



Who has control of your workstation?



Accounts with Delegated Rights to AD

- Group membership
- AD delegated permissions
- Group Policy delegation
- Group Policy User Rights Assignments (DC GPOs)

Allow log on locally	TRIMARCRESEARCH\Server Tier 3, TRIMARCRESEARCH\Domain Users TRIMARCLAB\Lab
	Admins, BUILTIN\Server Operators, BUILTIN\Print Operators, NT AUTHORITY\ENTERPRISE
	BUILTIN'Account Operators
Allow log on through Terminal Services	TRIMARCRESEARCH\Server Tier 3, BUILTIN\Administrators



Domain Controllers with minimal event auditing

Policy	Policy Setting
Audit account logon events	Success, Failure
Audit account management	Success, Failure
Audit directory service access	Not Defined
🕼 Audit logon events	Success, Failure
Audit object access	Not Defined
Audit policy change	Not Defined
🕼 Audit privilege use	Success, Failure
Audit process tracking	Not Defined
Audit system events	Not Defined
	Sett

Policy

Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy Enabled category settings



Kerberos Delegation

- Delegation = Impersonation
- Kerberos Delegation:
 - 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.



Kerberos Delegation

- Delegation = Impersonation
- Kerberos Delegation:
 - 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.

Account is sensitive and cannot be delegated


Cross-Forest Administration



Cross-Forest Administration

- Production <--one-way--trust---- External
- Production forest AD admins manage the External forest.
- External forest administration is done via RDP.
- Production forest admin creds end up on systems in the External forest.
- Attacker compromises External to compromise Production AD.

Mitigation:

- Manage External forest with External admin accounts.
- Use non-privileged Production forest accounts with External admin rights.













From On-Premises to Cloud



Faust and Johnson – Cloud Post Exploitation Techniques Infiltrate 2017 https://vimeo.com/214855977



Cloud Challenges

- Security controls: On-prem vs cloud
- Cloud environment is constantly changing.
- Rapid changes often mean learning curve is steeper.
- Security capability and best practices depend on Cloud service offering.
- Sharing data appropriately and securely.
- Services & data that's private vs public isn't always obvious.



"I'm going to migrate my on-prem Active Directory to Azure AD"

It doesn't quite work like that...



Active Directory vs Azure AD

On-premises Active Directory

- Authentication, Directory, & Management
- AD Forest for single entity
- Internal corporate network
- Authentication
 - Kerberos
 - NTLM
- LDAP
- Group Policy

Azure AD (Office 365)

- Identity
- Designed for multi-tenant
- Cloud/web-focused
- Authentication
 - OAuth/OpenID Connect based protocols
- AD Graph API (REST API)
- MDM (InTune)



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 user to Azure AD.



On-Prem: AD to Cloud Sync Examples

- Adobe User Sync tool
- Atlassian Active Directory Attributes Sync
- Dropbox Active Directory Connector
- **Duo** Directory Sync
- Envoy Active Directory integration (PowerShell)
- **Google** Cloud Directory Sync
- Facebook Workplace Active Directory Sync
- Forcepoint (Websense) Directory Synchronization Client
- Mimecast Directory Sync Tool
- **Proofpoint** Essentials AD Sync Tool
- **Rackspace** Directory Sync (syncs passwords too!)
- Zoom AD Sync to Zoom



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:

Permission	Used for
Replicate Directory ChangesReplicate 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
Reset password	Preparation for enabling password writebac

PS C:\> get-aduser -filter {samaccountname -like "MSOL*"}`
-prop DistinguishedName,description | fl *

Description	: Account created by the Windows Azure Active Directory Sync tool with installatio 'trd977930921' running on computer 'AZURESYNC' configured to synchronize to tena 'theacmeio.onmicrosoft.com . Inis account must have directory replication permis
	Directory and write permission on certain attributes to enable hybrid beproyment
DistinguishedName	: CN=MSOL_trd9//930921,0U=Service Accounts,DC=theacme,DC=io
Enabled	: True
GivenName	
Name	: MSOL_trd977930921
ObjectClass	: user
ObjectGUID	: cdcb6dd0-65e2-40bc-bc60-461408831036
SamAccountName	: MSOL_trd977930921
SID	: 5-1-5-21-143179592-3749324205-2095737646-1138



PS C:\> Invoke-ACLScanner -ResolveGUIDs -ADSpath 'DC=theacme,DC=io' | where { (\$_.IsInherited -eq \$False) -AND ` (\$_.ObjectType -like 'DS-Replication*') } ` select ObjectDN.IdentityReference.AccessControlType. ActiveDirectoryRights,ObjectType

ObjectDN IdentityReference AccessControlType ActiveDirectoryRights : ExtendedRight ObjectType

ObjectDN IdentityReference AccessControlType ActiveDirectoryRights : ExtendedRight **ObjectType**

: DC=theacme.DC=io

ACME\M50L trd977930921

: Allow

- : DS-Replication-Get-Changes-All
- : DC=theacme,DC=io
- : ACME\MSOL_trd977930921
- : Allow
- : DS-Replication-Get-Changes



PS C:\> get-aduser -filter {samaccountname -like "MSOL*"}`
-prop DistinguishedName,description | fl *

Description

DistinguishedName Enabled GivenName

: Account created by the Windows Azure Active Directory Sync 'trd977930921' running on computer 'AZURESYNC' configured to 'theacmeio.onmicrosoft.com'. This account must have directory Directory and write permission on certain attributes to ena : CN=MSOL_trd977930921,OU=Service Accounts,DC=theacme,DC=io : True

PS C:\> get-adcomputer AzureSync

DistinguishedName DNSHostName Enabled Name ObjectClass ObjectGUID

DistinguishedName : CN=AZURESYNC,OU=Servers,DC=theacme,DC=io

- : True
- : AZURESYNC
- : computer
- : 42f88cbe-c51f-4f5c-9059-58d3449a7a30



PS C:\> Find-GPOComputerAdmin -OUName 'OU=Servers,DC=theacme,DC=io'

ComputerName ObjectName ObjectDN ObjectSID IsGroup GPODisplayName GPOGuid GPOPath GPOType

- : ServerAdmins
- : CN=Server Admins,OU=Groups,DC=theacme,DC=io
- : 5-1-5-21-143179592-3749324205-2095737646-1103
- : True
- GPODisplayName : Server Baseline Policy
 - : {002404EA-6ACB-495D-97E6-2AEC89ED91A8}
 - : \\theacme.io\SysVol\theacme.io\Policies\{002404EA-6AC
 - : GroupPolicyPreferences





- > 道 Disabled
- 🖇 道 Domain Controllers
- 🖇 🛅 Groups
- 🗸 🛅 Servers
 - 🛒 Server Baseline Policy
 - 🚮 Server Config
- > 📓 Service Accounts
- > 📔 Workstations

Server Config

Scope Details Settings Delegation

These groups and users have the specified permission for this GPO

Groups and users:

Name	Allowed Permissions
 Authenticated Users Domain Admins (ACME\Domain Admins) Enterprise Admins (ACME\Enterprise Admins) 	Read (from Security Filtering) Edit settings, delete, modify security Edit settings, delete, modify security
S ENTERPRISE DOMAIN CONTROLLERS	Read
Server Tier 1 (ACME\Server Tier 1)	Edit settings
🞎 Server Tier 2 (ACME\Server Tier 2)	Edit settings
💐 Server Tier 3 (ACME\Server Tier 3)	Edit settings, delete, modify security



On-Prem: Acme's Azure AD Connect Scenario

- Azure AD Connect service account is granted password hash sync rights.
- AAD Connect runs on "AzureSync" which is in the Servers OU.
- The Servers OU has 2 GPOs applied:
 - "Server Baseline Policy" GPO adds the Server Admins group (in the Groups OU).
 - "Server Config" GPO has 3 Server Tier groups with modify rights.

Attack Options:

- Compromise account that is a member of the Server Admins group or any of the Server Tier groups.
- Compromise account delegated rights to modify groups in the
 Groups OU.
 ITEC2019

OnPrem Sync Defense

- You may have sync engines other than AAD Connect...
- Protect any sync engine server that handles AD password data like a Domain Controller (Tier 0).
- Protect any associated service account like it's a Domain Admin account.
- Ensure only AD admins manage these systems.



AD Recon vs Azure AD Recon

On-Prem AD:

- AD user can enumerate all user accounts & admin group membership with <u>network access to a Domain Controller</u>.

Azure AD:

- Azure AD user can enumerate all user accounts & admin group membership with <u>access to Office 365</u> <u>services (the internet by default)</u>.
- User enumeration* often possible without an account!



Azure AD User Enumeration

- Office 365 Authentication Page (Python) [Account Discovery]
 - https://github.com/LMGsec/o365creeper
- OWA (Golang)
 - https://github.com/busterb/msmailprobe
- ActiveSync (Python)
 - <u>https://bitbucket.org/grimhacker/office365userenum/src</u>
- MSOnline/AzureAD PowerShell Module (PowerShell)
 <u>https://github.com/nyxgeek/o365recon</u>



Password Spraying Overview

"Winter2018"

Sleep x seconds/minutes

"Spring2019"

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.



Password Spraying Overview

"Winter2018!"

Sleep x seconds/minutes

"Spring2019!"

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.



Password Spraying Overview

- Ruler (Exchange) [Golang]
 - <u>https://github.com/sensepost/ruler/wiki/Brute-Force</u>
- SprayingToolkit (Lync/Skype for Business/OWA) [Python]
 - <u>https://github.com/byt3bl33d3r/SprayingToolkit</u>
- LyncSniper (Lync/Skype for Business) [PowerShell]
 - <u>https://github.com/mdsecresearch/LyncSniper</u>
- MailSniper (OWA/EWS) [PowerShell]
 - <u>https://github.com/dafthack/MailSniper</u>

Legacy Authentication enables O365 Password Spraying Legacy = Outlook =<2010, POP, IMAP, SMTP, etc



Attacking the Cloud: Password Spraying

PS C:\> C:\temp\Spray-0365.ps1

Password Spraying the EWS portal at https://outlook.office365.com/EWS/Exchange.asmx. Sit tight...

+ FullyQualifiedErrorId : PositionalParameterNotFound,Microsoft.PowerShell.Commands.ImportModuleCommand

Now spraying the EWS portal at https://outlook.office365.com/EWS/Exchange.asmx Current date and time: 08/02/2019 04:01:04 Trying Exchange version Exchange2010 A total of 0 credentials were obtained. Results have been written to C:\temp\owa-sprayed-creds.txt. Now spraying the EWS portal at https://outlook.office365.com/EWS/Exchange.asmx Current date and time: 08/02/2019 04:01:35 (*) Trying Exchange version Exchange2010 SUCCESS! User:theacme.io\thrawn@theacme.io Password:Summer2019! [*] A total of 1 credentials were obtained. Results have been written to C:\temp\owa-sprayed-creds.txt. [*] Now spraying the EWS portal at https://outlook.office365.com/EWS/Exchange.asmx [*] [*] Current date and time: 08/02/2019 04:01:58 Trying Exchange version Exchange2010 A total of 0 credentials were obtained. Results have been written to C:\temp\owa-sprayed-creds.txt. [*] Now spraying the EWS portal at https://outlook.office365.com/EWS/Exchange.asmx Current date and time: 08/02/2019 04:02:21 [*] Trying Exchange version Exchange2010 A total of 0 credentials were obtained. Results have been written to C:\temp\owa-sprayed-creds.txt. Now spraying the EWS portal at https://outlook.office365.com/EWS/Exchange.asmx Current date and time: 08/02/2019 04:02:44 Trying Exchange version Exchange2010

Attacking the Cloud: Password Spraying



Microsoft:

"Nearly 100% of password spray attacks are using legacy authentication."

Azure AD Sign-in Logs require Azure AD Premium (P1 or P2)

Access denied You do not have access To see sign-in data, upgrade your organization's subscription to includ Start a free Premium Trial

#TFC2019

8/1/2019, 9:09:12 PM	Thrawn	Office 365 Exchange On	Failure	52.168.138.234	
8/1/2019, 9:09:11 PM	Qui-Gon Jinn	Office 365 Exchange On	Failure	52.168.138.234	
8/1/2019, 9:09:11 PM	Lando Calrissian	Office 365 Exchange On	Failure	52.168.138.234	
8/1/2019, 9:09:07 PM	Boba Fett	Office 365 Exchange On	Failure	52.168.138.234	
8/1/2019, 9:09:06 PM	obi-wan Kenobi	Office 365 Exchange On	Failure	52.168.138.234	
8/1/2019, 9:09:06 PM	leia	Office 365 Exchange On	Failure	52.168.138.234	
8/1/2019, 9:09:06 PM	Rey	Office 365 Exchange On	Failure	52.168.138.234	-
8/1/2019, 9:09:06 PM	kylo	Office 365 Exchange On	Failure	52.168.138.234	
8/1/2019, 9:09:01 PM	Padme Amidala	Office 365 Exchange On	Failure	52.168.138.234	
8/1/2019, 9:09:01 PM	Luke Skywalker	Office 365 Exchange On	Failure	52.168.138.234	
8/1/2019, 9:09:01 PM	Bailey	Office 365 Exchange On	Failure	52.168.138.234	
8/1/2019, 9:09:00 PM	Han Solo	Office 365 Exchange On	Failure	52.168.138.234	*Azure AD Sign-ir
8/1/2019, 9:09:00 PM	Adm Ackbar	Office 365 Exchange On	Failure	52.168.138.234	require Azure AD
8/1/2019, 9:08:53 PM	Finn	Office 365 Exchange On	Failure	52.168.138.234	

Sign-in Logs

-	Acme Corporation - Sign-in	s					
	🛓 Download 🔞 Export Data Settings	🗙 Troubleshoot 👌 Refre	esh 📔 🖬 Columns	Got feedback?			
	8/2/2019, 12:03:47 AM Boba Fett	Office 365 Exchang	Failure	52.168.138.234	Not Applied		
	8/2/2019, 12:04:34 AM Boba Fett	Office 365 Exchang	Failure	52.168.138.234	Not Applied		
	8/2/2019, 12:01:43 AM Boba Fett	Office 365 Exchang	Failure	52.168.138.234	Not Applied		
	8/2/2019, 12:03:15 AM Boba Fett	Office 365 Exchang	Failure	52.168.138.234	Not Applied		
	8/2/2010 12:06:04 AM Baba Eatt	Office 265 Evchang	Esiluro	52 168 128 224	Not Applied		
3/2/20	019, 12:08:21 AM	Boba Fett		Office 365	Exchange Or	nline	Failure
3/2/20	019, 12:02:06 AM	Boba Fett		Office 365	Exchange Or	nline	Failure
3/2/20	019, 12:04:11 AM	Boba Fett		Office 365	Exchange Or	nline	Success
	8/2/2019, 12:07:35 AM Boba Fett	Office 365 Exchang	Failure	52.168.138.234	Not Applied		
	8/2/2019, 12:08:21 AM Boba Fett	Office 365 Exchang	Failure	52.168.138.234	Not Applied	*Azure	AD Sign-in Logs
	8/2/2019, 12:02:06 AM Boba Fett	Office 365 Exchang	Failure	52.168.138.234	Not Applied	Premi	m (P1 or P2)
66	8/2/2019, 12:04:11 AM Boba Fett	Office 365 Exchang	Success	52.168.138.234	Not Applied	, , 01110	TEC The Experts Conference Sponsored by Quest

Basic info	Device info	MFA info	Conditional Access	Troubleshooting and support		
Request ID	8e270d9b-9d	dc4-41c5-927	3-e69395680400		IP address	52.168.138.234
Correlation ID	94558595-8e	ecc-484b-b7a	6-6eaaa3e9d74e		Location	Washington, Virginia, US
User	Boba Fett				Date	8/2/2019, 12:02:06 AM
Username	bobafett@th	eacme.io			Status	Failure
User ID	5688de1a-10	ec-4b5c-b980	d-73cff3c2e7f0		Sign-in error code	50126
Application	Office 365 Ex	change Onlin	e		Failure reason	Invalid username or password or Invalid on-premise username or password
Application II	00000002-00	000-0ff1-ce00	-00000000000		Client app	Other clients; Older Office clients

Sign-in error code 50126

Invalid username or password or Invalid on-premise username or password Failure reason

Client app	Other	clients; Older Offic	e clients
67		Legacy Authentication	FC2019



Password Spraying Defense

- Disable Legacy Authentication (Especially if this is a new tenant!)
 - Baseline Policy: Disable Legacy Authentication
 - Conditional Access
- Enforce MFA for admins
 - Baseline Policy: Require MFA for admins (preview)
 - Conditional Access
- Disable service access for users
 - Configure on each user's mailbox config
 - Exchange authentication policy



Password Spraying Defense (ADFS)

- Enable Smart Lockout (2012R2/2016)
- Block Legacy Authentication with ADFS Authorization rules
- Install <u>Azure AD Connect Health with ADFS</u> on ADFS servers
 - Alerts about common ADFS issues (cert expiring, missing updates, performance, etc)
 - Will also alert on bad Password Attempts and Risky IPs!

TIMESTAMP	TRIGGER TYPE	IP ADDRESS	BAD PASSWORD ERROR COUNT	EXTRANET LOCKOUT ERROR COUNT	UNIQUE USERS ATTEMPTED
2/28/2018 6:00 PM	hour	104.208.238.9	0	284	14
2/28/2018 6:00 PM	hour	104.44.252.135	0	27	1
2/28/2018 6:00 PM	hour	168.61.144.85	0	164	2

Password Spraying Defense: Azure AD Password Protection

• Requirements

- Azure AD Premium (P1)
- DCs need to be 2012 or later
- No Domain or Forest functional level requirement
- Sysvol needs to be using DFSR (<u>http://aka.ms/dfsrmig</u>)
- Deploy in Audit Mode first
- Passwords are fuzzy matched, substring matched & scored. Must be 5 or higher
 - <u>https://docs.microsoft.com/en-us/azure/active-</u> <u>directory/authentication/concept-password-ban-bad</u>
- After passwords have been changed, look to extend password age



From On-Prem to Cloud Administration

■ Active Directory Osers and Compl ile Action View Help ● 🔿 📶 🔏 📋 🗙 🗐	i @ 🔒 🛛 🖬	1 8 2 11 1	/ <u>2</u> %	
Active Directory Users and Com Saved Queries theacme.io Accounts AD Management Branch Offices	Name Allowed RO Cert Publish Cloneable D DefaultAcco Denied ROD	Type Security Group Security Group Security Group User Security Group	Description Members in this group Members of this group Members of this group t A user account manage Members in this group c	^
Computers Disabled Disabled Domain Controllers ForeignSecurityPrincipal Groups Managed Service Accour Servers Servers Servers	DinsAdmins DinsUpdateP Domain Ad Domain Co Domain Con Domain Gue Domain Users Enterprise A	Security Group Security Group Security Group Security Group Security Group Security Group Security Group	DNS Administrators G DNS clients who are po Designated administration All workstations and ser All domain controllers i All domain guests All domain users Designated administrato	
Users Users Workstations	Enterprise K Enterprise R Group Polic	Security Group Security Group Security Group	Members of this group Members of this group Members in this group c	*



#TEC2019

Attacking Cloud Administration

🕨 Add assignment 🛛 🗙 Remo	ove assignment 🛛 🕐 Refresh	🛛 Manage in PIM 🛛 💙 Got feedback?			
earch	Туре				
Search by name	All	~			
NAME		USERNAME	T4	TYPE	SCOPE
Sean Metcalf		sean@theacmeio.onmicrosoft.com		User	Direc
Mark Morowczynski		mark@theacme.io		User	Direc
Sean Metcalf		seanmetcalf@theacme.io		User	Direc
Han Solo		hansolo@theacme.io		User	Direc
Boba Fett SU	CCESS! User:th	eacme.io\bobafett@thea	cme.io	Password:	Mandalorian1
Mace Windu		mace@theacme.io		User	Direc
Thrawn	SUCCESS! U	ser theacme io thrawn@	theacme	io Passwo	rd:Summer201



Attacking Cloud Administration

- 8 *	5014=	Re: Office 365 Licenses Expired Message (HTML)	?	80	-	
THE	MESSAGE					
	Fri 4/12/2019 1:55 P	M				
	Customer S	Support <xbox_live.ww.00.en.vmc.rmd.ts.t03.spt.ua.pi@outlook.com></xbox_live.ww.00.en.vmc.rmd.ts.t03.spt.ua.pi@outlook.com>	1			
	Re: Office 365 l	licenses Expired.				
To						
1 This mes	ssage was sent with High	importance.				
	1 Offic	e 365	Microsoft			
	®Office 36	55- Check Your Payment Information				
	Sign in to the	Office 365 Admin center To Check Your Payment Information				
	View this mes	sage in the Office 365 message center				
	To customize	what's included in this email, who gets it, or to unsubscribe, set your Message center	r preferences.			
	Edit release pr	eferences				
	Choose the rel	lease track for your organization. Use these settings to join First Release if you have	n't already.			
	Microsoft respec	ts your privacy. To learn more, please read our <u>Privacy Statement.</u>				
	Microsoft Corpo	ration				
	One Microsoft W	^r ay				
	Redmond, WA, U	/SA 98052		م ا م		
	Unsubscribe	nttps://www.bieepingcomputer.com/news/security/phishers-targ	et-office-365-a	am	ins	2
		with-take-admin-alerts/				


Global Reader

From Global Admin to Global Reader

- Currently in Private Preview
- Provides read access to O365 services that Global Admin can read/write.
- Enables accounts that "required" Global Admin to be switched to read-only.
- Global Reader read-only access is still being expanded to cover all O365 services.

ttps://docs.microsoft.com/en-us/office365/securitycompliance/permissions-in-the-security-and-compliance-center



Cloud Administration – Finding a Weakness





Attacking Cloud Administration: Token Theft



Attacking Cloud Administration: Token Theft



Attacking Cloud Administration: Token Theft





Protect Cloud Admin Accounts

According to Microsoft (as of August 2019):

Admin Accounts with MFA: 7.94%!



Protect Cloud Admin Accounts

- Anyone with elevated rights to cloud services (i.e. "admin") needs to have an account just for Cloud Administration.
- Good: Turn MFA on!
- Better: Conditional Access or Baseline Policy for Admins (Public Preview)
 - Will change based on feedback
 - Learn more at: <u>https://aka.ms/aadbaseline</u>
- Best: Azure AD Privilege Identity Management
 - 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
 - <u>https://aka.ms/deploymentplans</u>



Protect Cloud Administration

- Isolate Cloud Administration to special systems:
 - Cloud Admin Server
 - Cloud VDI
 - Cloud Admin Workstation
- Ensure SSL/TLS decryption devices whitelist all cloud admin URLs & are well protected (Tier 0).



Password Reuse/Replay

Our team is currently looking into reports of stolen passwords. Stay tuned for more.

◆ Reply ♣ Retweet ★ Favorite

112.

113.

Han

Luke

30f8c8134437da0c0232eeca20bd7992c00bce74: df272dfef6127aeaecc5c47c7ceed028c39354df: c886b08ad18cd650b1bc4a7612a0742a2257a41e: bd01669b5883f24ebe55930efeb098fb5a873d96: ef60e1915933c7c5abde3cb160f45bf1963e3525: 991db9efcfa06ae837a4d433b6ba2777256e1af8: 4b757d2f8f7036f8119739e4b82bc27875f4a987: 13a7bc6d3d74dcc5533d0a756a7b9bf4f1b46c7d: a4404ac0b635faa6264658fc960836a308427c90: 546684e9d6d2f217db45229b4fa63c5d51f26729: 54cd6a7aaf905ac2145942f65a03fa7c54cf3ea9: fb88038b760bc428e4847831aad572339c2e8ecd: c06bbe76b5dfa96cb8c0351a227f30b8f1a3109a: a067d0f502613bc845b31c70b6882ae91ed27a2c:



Solo hansolo Skywalker lukeskywalker LeiaIKnow19! TheForce19 hansolo@theacme.io
lukeskywalker@Plus.com

Password Reuse/Replay Detection



83

Turn on Azure AD Connect Password Hash Sync

- Leaked Credential Reporting
 - Dark Web, Law Enforcement, and Security Researchers
- When something catastrophic happens
 - WannaCry, NotPetya
 - Wired Article: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/
- Understand How Password Hash Sync Works
 - http://aka.ms/aadphs
- After enabling will see "NEW" leaks going forward
 - Don't "leak" one yourself "just to make sure it's working"



Attacking the Cloud: App PrivEsc & Persistence

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

Illicit Consent Grant Attack: Pawn Storm



2016 Mail Corp. 1997 Amphitheatre Parloway, Mountain View, CA 92042

Enterprise App Permissions

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

Microsoft

sean@theacmeio.onmicrosoft.com

Permissions requested Accept for your organization



This app would like to:

- Read and write all applications
- Read and write directory data
- Use Exchange Web Services with full access to all mailboxes
- ✓ Read and write calendars in all mailboxes
- \checkmark Read and write contacts in all mailboxes
- V Read and write all user mailbox settings
- ✓ Read and write mail in all mailboxes
- ✓ Send mail as any user
- ✓ Read all users' full profiles
- \checkmark Sign in and read user profile

If you accept, this app will get access to the specified resources for all users in your organization. No one else will be prompted to review these permissions.

Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. You can change these permissions at https://myapps.microsoft.com. Show details



Enterprise App Permissions

This app would like to:

- ✓ Read and write all applications
- ✓ Read and write directory data
- Use Exchange Web Services with full access to all mailboxes
- Read and write calendars in all mailboxes
- ✓ Read and write contacts in all mailboxes
- Read and write all user mailbox settings
- ✓ Read and write mail in all mailboxes
- ✓ Send mail as any user
- ✓ Read all users' full profiles
- 89 🗸 Sign in and read user profile





App Attack Detection & Defense

- Provide training to users around App Consent.
- Regularly review app permissions:
 - Admin Consent
 - User Consent
- Use PowerShell!

Get-AzureADPSPermissions.ps1 <u>https://gist.github.com/psignore</u> <u>t/41793f8c6211d2df5051d77ca</u> <u>3728c09</u>

Permissions

Applications can be granted permissions to your directory by an admin consenting to the application for all users, a user consenting to the application for him or herself, or an admin integrating an application and enabling self-service access or assigning users directly to the application.

As an administrator you can grant consent on behalf of all users in this directory, ensuring that end users will not be required to consent, when using the application. Click the button below to grant admin consent.

Grant admin consent for Wingtip Toys

Admin consent User consent				
MICROSOFT GRAPH				
Microsoft Graph	Have full access to user calendars	Delegated	Medium	An administ
Microsoft Graph	Have full access to user contacts	Delegated	Medium	An administ
Microsoft Graph	Read Microsoft Intune apps	Delegated	Medium	An administ
Microsoft Graph	Read and write Microsoft Intune apps	Delegated	High	An administ

O365 Phase 1 Go Do Right Now Checklist

- Require MFA for all cloud admin accounts.
- □ Configure PIM for all cloud admin accounts
- □ Enable "Password Hash Sync" (Azure AD Connect).
- □ Ensure all apps use Modern Authentication (ADAL) to connect to Office 365 services.
- Enable user and admin activity logging in Office 365 (UnifiedAuditLogIngestionEnabled).
- □ Enable mailbox activity auditing on all O365 mailboxes.
- □ Conditional Access: Block Legacy Auth (for those that are not using it today!).
- □ Integrate Azure AD Logs with your SIEM or use Azure Log Analytics or Azure Sentinel
- Deploy Azure AD Banned Password for your on-prem AD
- □ Enable Azure AD Connect Health for ADFS and ADFS Smart Lockout
- □ Ensure all users are registered for MFA.



O365 Phase 2 Go Do Soon Security Checklist

- □ Enable self-service password reset (SSPR).
- □ Enable MFA for all users via Conditional Access or Risk Based.
- Disable Legacy Authentication Entirely via Conditional Access
- □ FIDO for admin accounts
- □ Follow admin account best practices for cloud admins
- □ Audit consented permissions for apps & user access to apps.
- Review App Permissions
- □ Monitor App registrations.
- Review the recommendations in Microsoft Secure Score and implement as many as possible.



Recommendations



Traditional AD Administration must evolve with the threats to effectively protect Active Directory.

Most organizations have done "something" to better secure their environment, thought it's often not enough.

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

The cloud isn't inherently secure.

Security responsibilities are shared between provider and customer.

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

Security in the cloud may cost extra.

Sean Metcalf (@Pyrotek3) s e a n @ trimarcsecurity.com <u>TrimarcSecurity.com</u> www.ADSecurity.org



Slides: Presentations.ADSecurity.org

#TEC2019