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!
- Full Compromise… Likely

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

- **D**omain user access
- **O**perations systems access
- **M**istaken identity – trust the installer
- **A**D object rights
- **I**nstall permissions on systems
- **N**eeds System rights
- **A**ctive Directory privileged rights
- **D**omain permissions during install
- **M**ore access required than often needed.
- **I**nitial start/run permissions
- **N**eeds 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:
  - https://blogs.technet.microsoft.com/ashleymcglone/2013/03/25/active-directory-ou-permissions-report-free-powershell-script-download/
- ACLight (Batch file that calls PowerShell):
  - https://github.com/cyberark/ACLight
- Bloodhound:
  - https://github.com/BloodHoundAD/BloodHound

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 : S-1-5-21-3017930946-1529675408-4271689233

SAMKey : 364d77a8399af95033658c1498e09bf2

RID  : 000001f4 (500)
User : Administrator
LM   :
NTLM : 4771c80c83293beb882cb621a6a063fe

RID  : 000001f5 (501)
User : Guest
LM   :
NTLM :
```

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

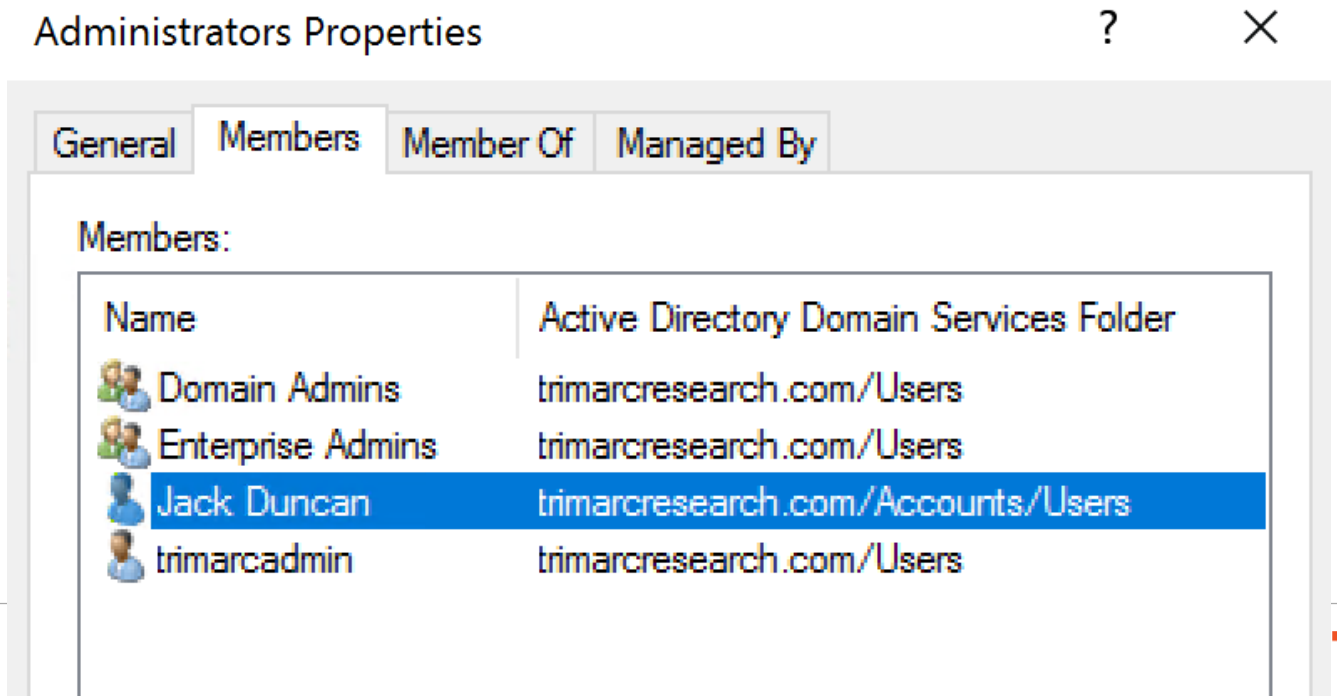
Domain Password Policy

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

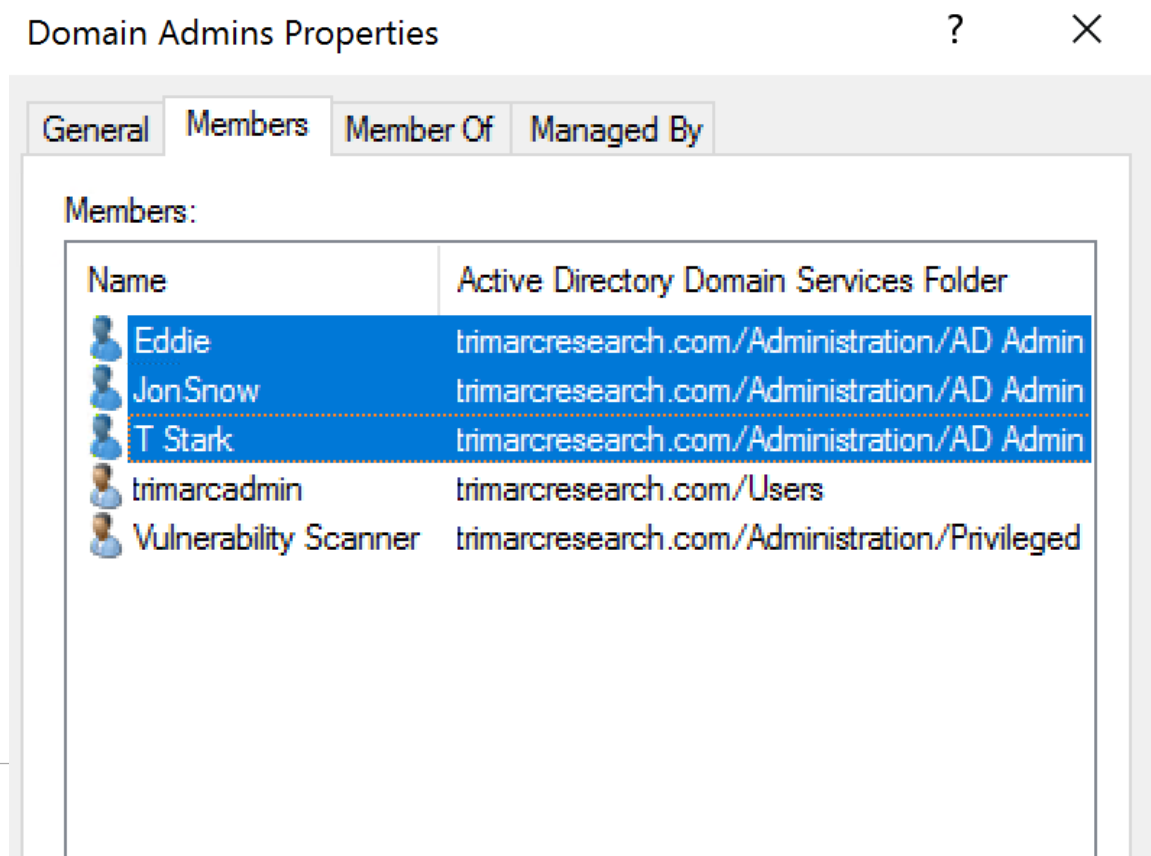
Regular Users in AD Admin Groups

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



No Account Naming Standard

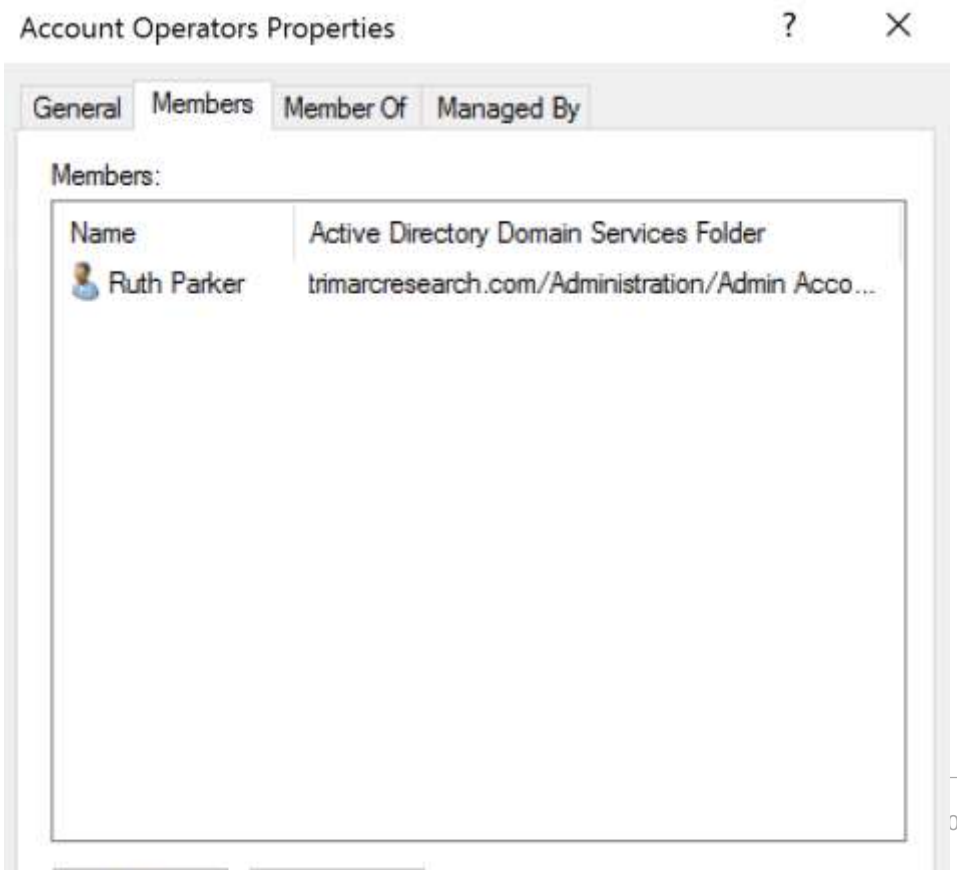
- Security through obscurity?
- Does not fool attackers
- Discovering AD admin accounts is trivial



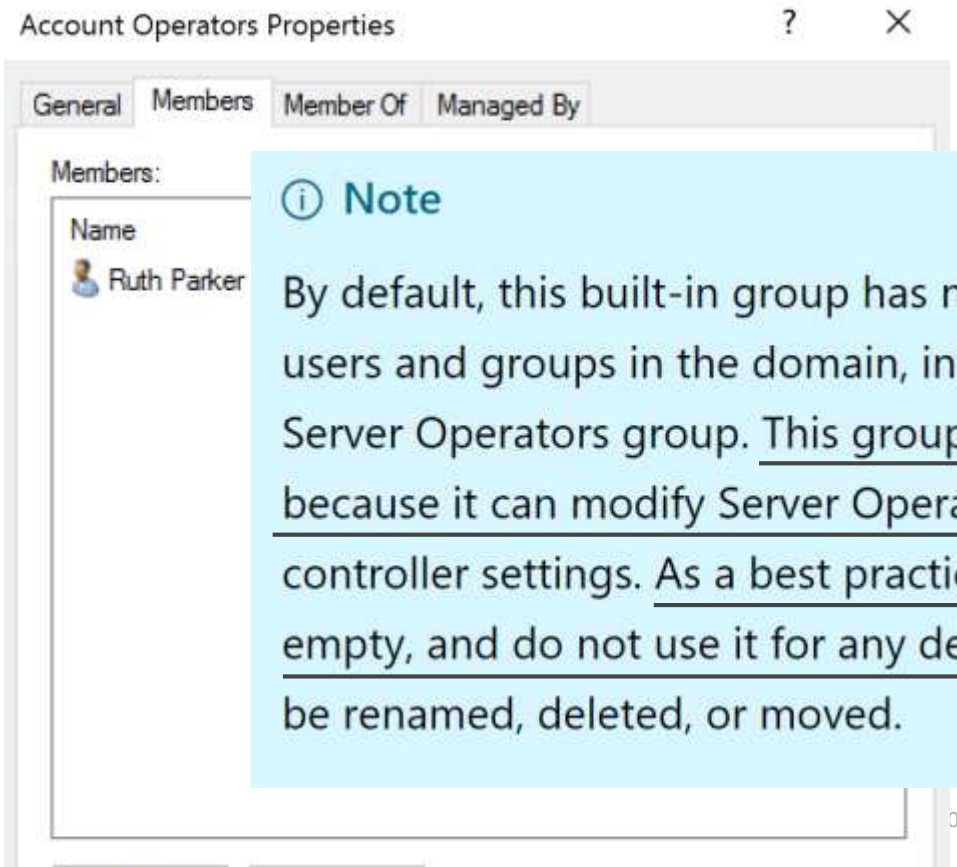
Mitigation:

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

Account Operators



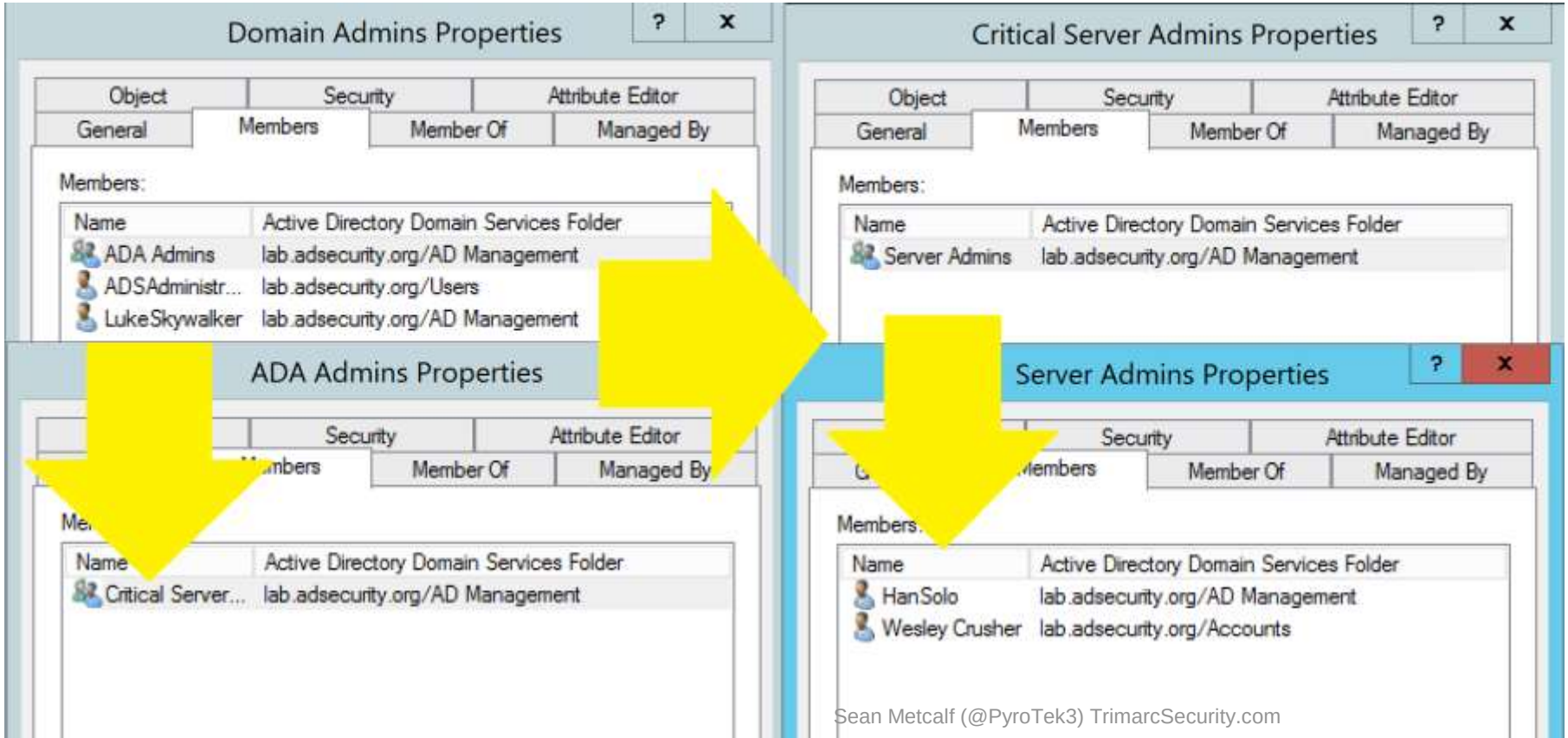
Account Operators



Note

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



Default Domain Controllers Policy is.. default

Local Policies/Security Options

Domain Controller

Policy	Setting
Domain controller: LDAP server signing requirements	None

Domain Member

Policy	Setting
Domain member: Digitally encrypt or sign secure channel data (always)	Enabled

Microsoft Network Server

Policy	Setting
Microsoft network server: Digitally sign communications (always)	Enabled
Microsoft network server: Digitally sign communications (if client agrees)	Enabled

AD Admin Accounts Have Old Passwords.

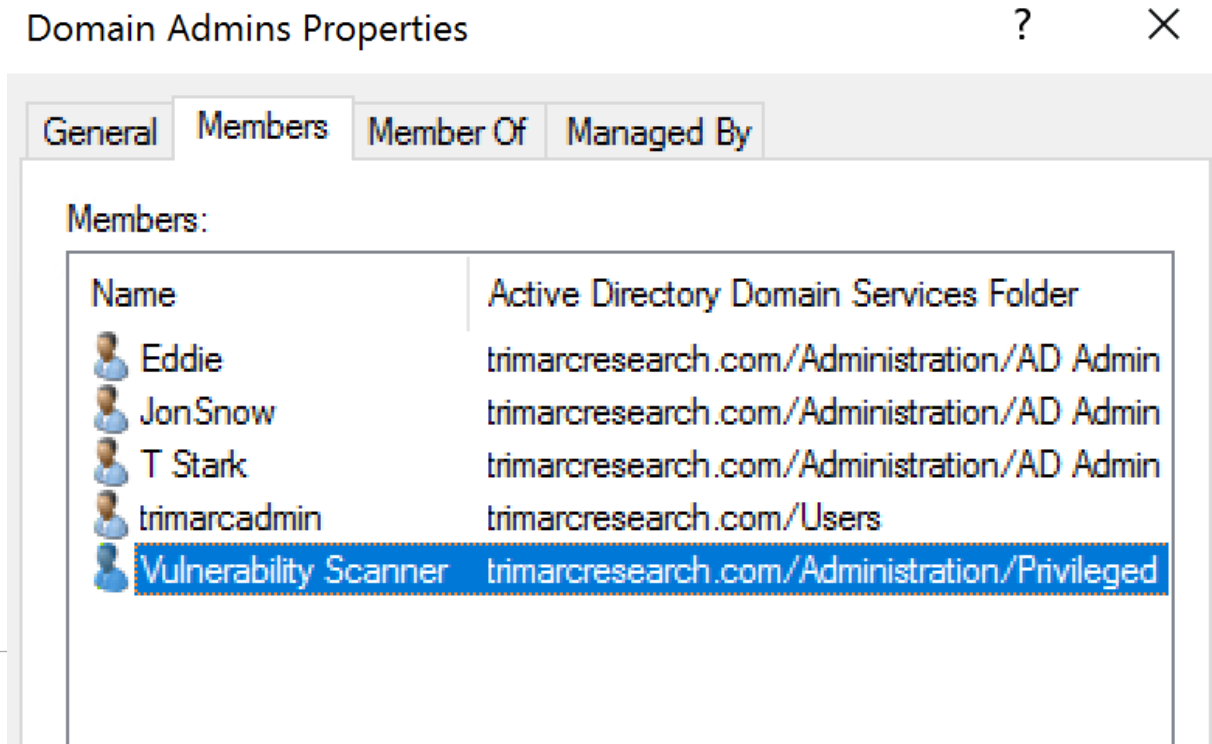
SamAccountName	Enabled	PasswordLastSet	Password Age (years)
admAEdwards	**Yes**	**1/12/2013 2:20:06 PM**	**6.5**
admBWalker	No	6/11/2017 10:14:08 AM	2.2
admCGriffin	Yes	3/1/2019 12:41:18 PM	0.4
Administrator	**Yes**	**1/9/2005 10:58:24 AM**	**14.5**
AGPMService	**Yes**	**5/3/2009 3:17:32 PM**	**10.2**
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
- Better to delegate the required rights for the accounts.

Mitigation:

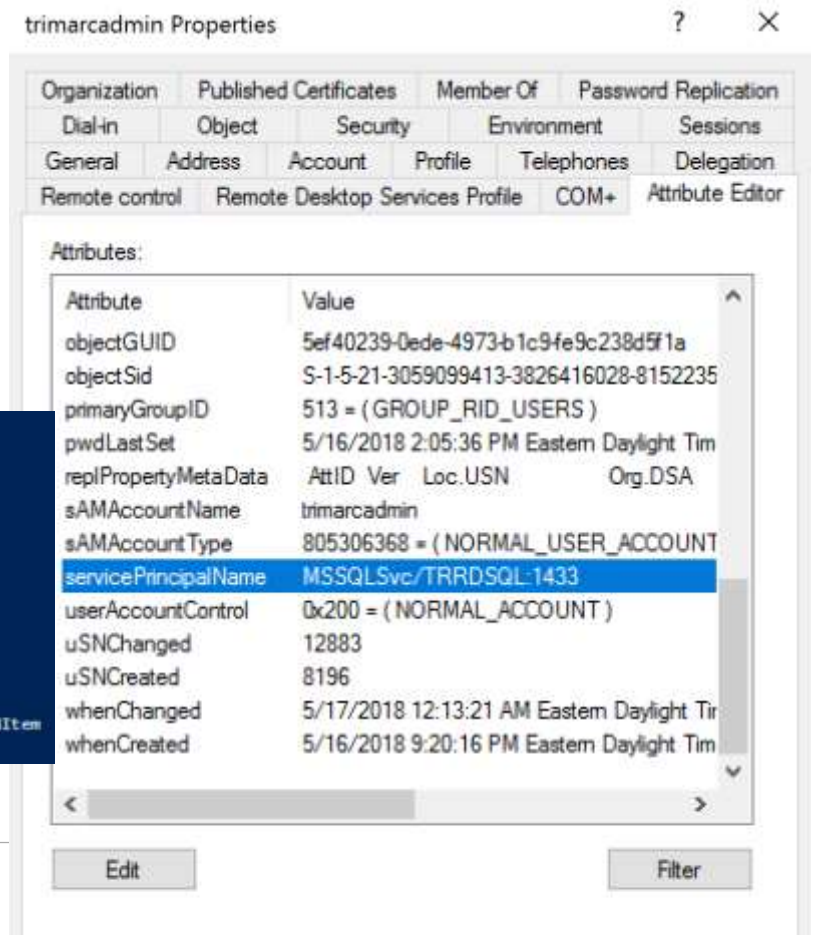
- Remove from Domain Admins
- Delegate appropriate rights
- Use separate accounts for different tiers:
  - Workstations
  - Servers
  - Domain Controllers



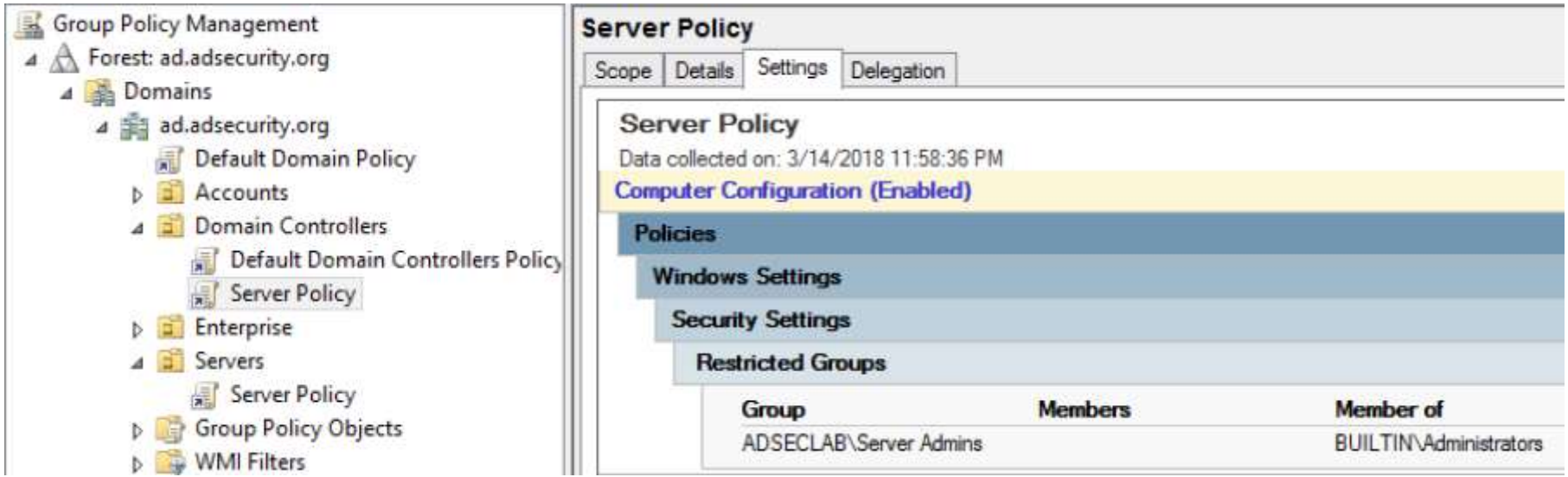
Default Domain Administrator Account SPN

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

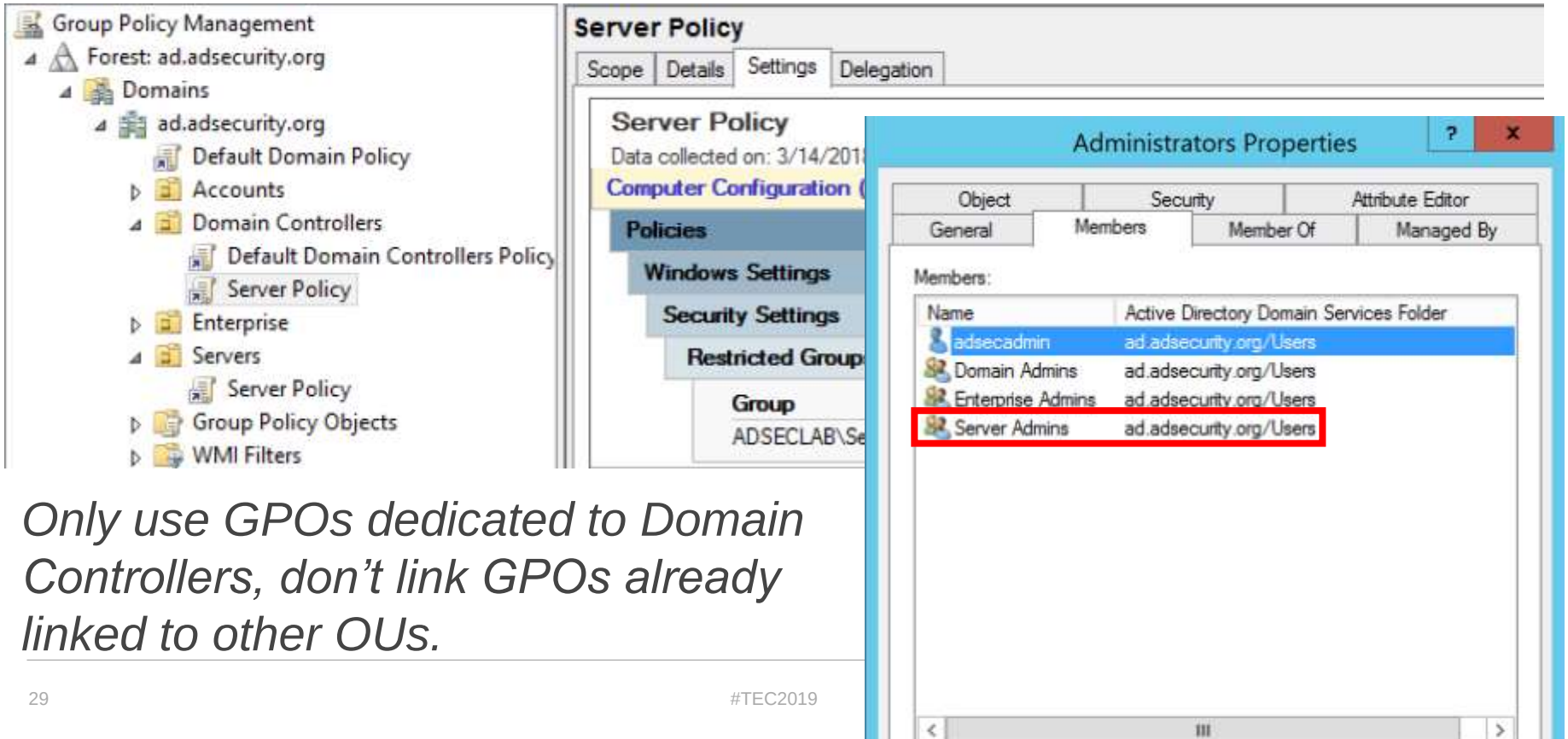
```
[array]$ServiceAccounts = Get-ADUser -Filter { ServicePrincipalName -like "*" } -Property *

$ServiceAccountSPNs = @()
ForEach ($ServiceAccountsItem in $ServiceAccounts)
 {
    ForEach ($ServiceAccountsItemSPN in $ServiceAccountsItem.ServicePrincipalName)
     {
        [array]$ServiceAccountSPNs += $ServiceAccountsItemSPN
     }

 }

klist purge

 ForEach ($ServiceAccountSPNItem in $ServiceAccountSPNs)
  {
    Add-Type -AssemblyName System.IdentityModel
    New-Object System.IdentityModel.Tokens.KerberosRequestorSecurityToken -ArgumentList $ServiceAccountSPNItem
  }
```



Server GPOs Linked to Domain Controllers

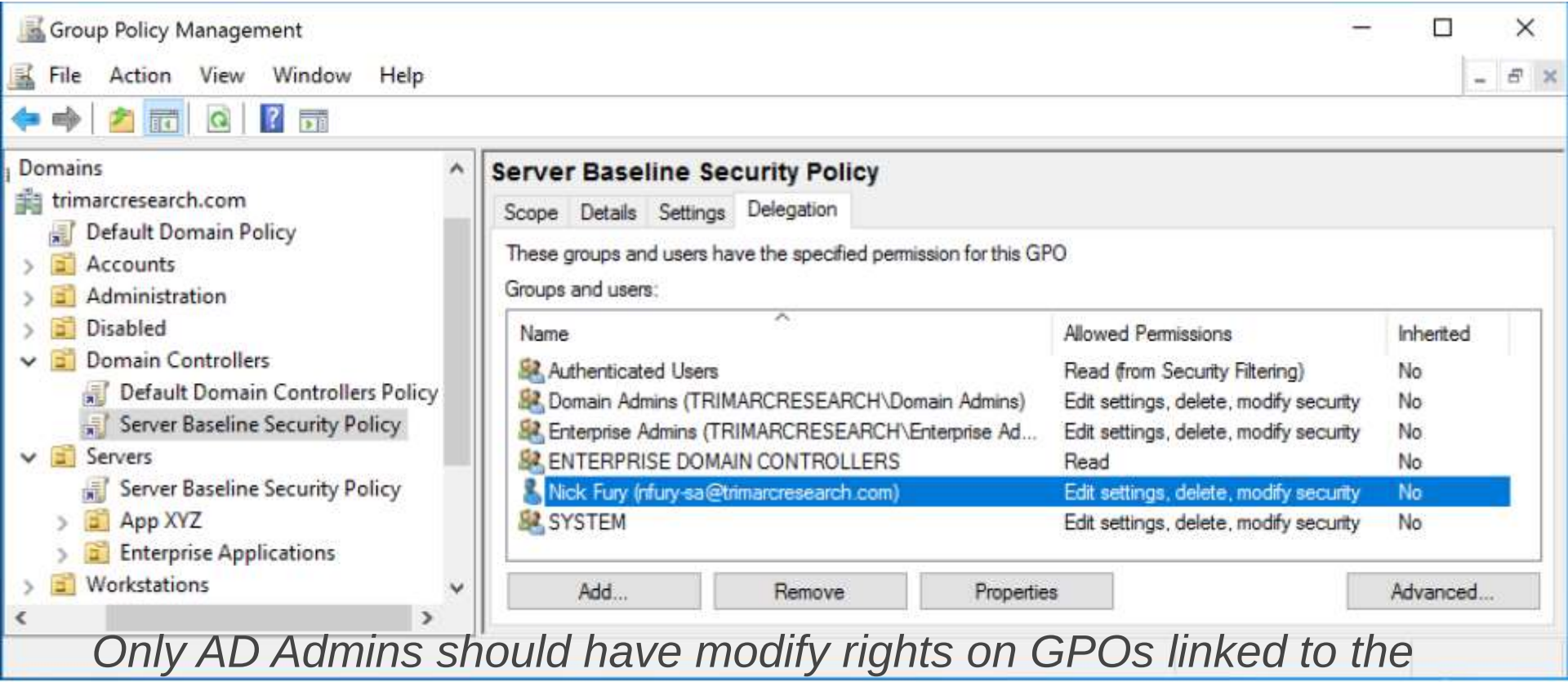


Server GPOs Linked to Domain Controllers



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

Modify Rights to GPOs at Domain /DC Level



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

Domain Permission Delegation Issues

```
Domain                  : lab.trimarcresearch.com
IdentityReference       : TRDLAB\Domain Computers
ActiveDirectoryRights   : Full Control
ObjectAttribute         : user All
InheritedObjectClass    : user
ObjectClass             : All
AccessControlType       : Allow
IsInherited             : False
```

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

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    : All
ObjectClass             : All
AccessControlType       : Allow
IsInherited             : False
ObjectFlags             : None
InheritanceFlags        : None
PropagationFlags        : None

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

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 DOMAIN CONTROLLERS, BUILTIN\Backup Operators, BUILTIN\Administrators, 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

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

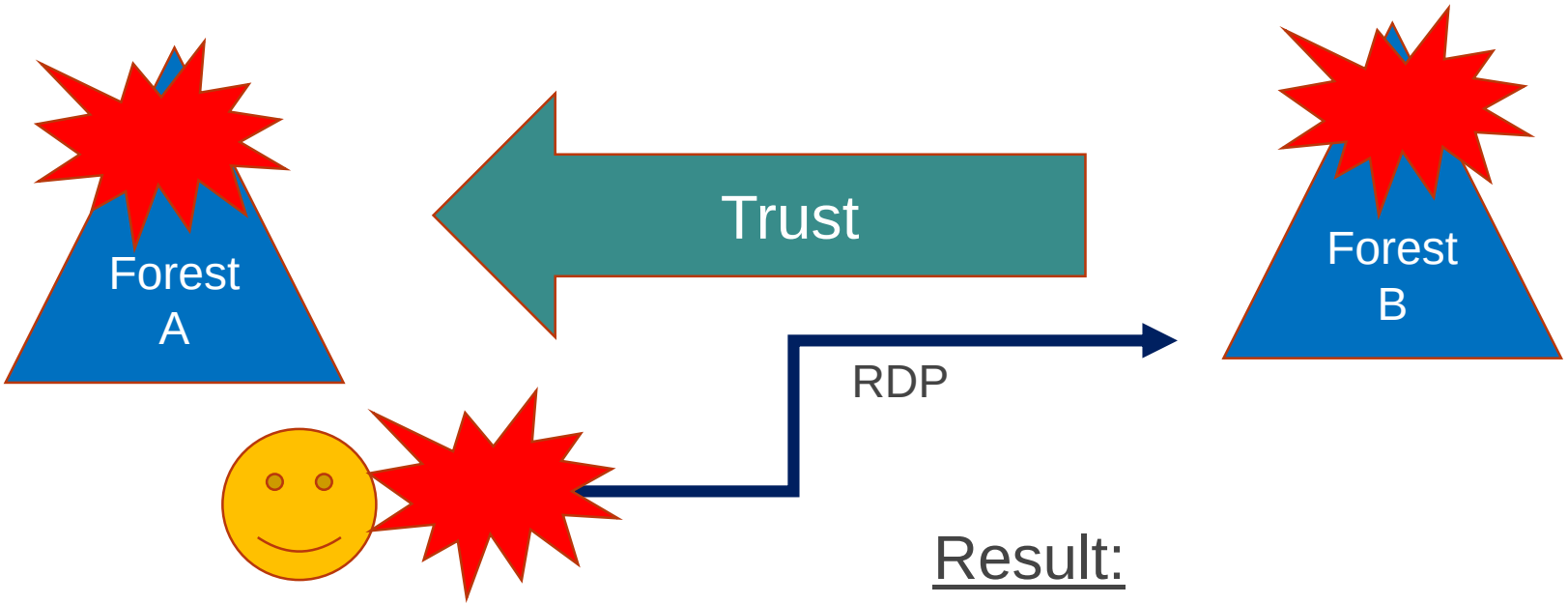
Kerberos Delegation

- 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.

Cross-Forest Administration



Forest A
Domain Admin
Account

Result:
Full Compromise of the
Production Active Directory

Cross-Forest Administration

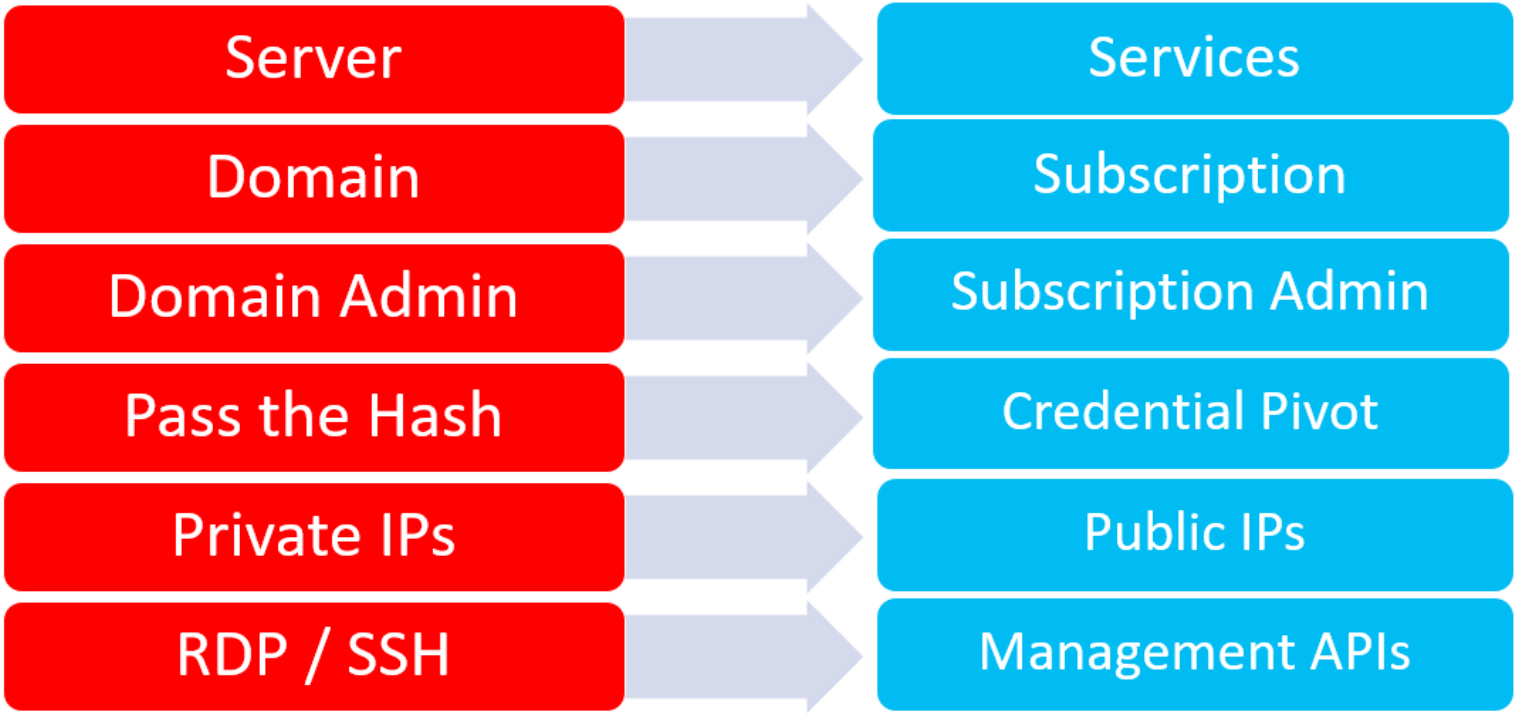
- Production <--one-way--trust---- External
- Production forest AD admins manage the External forest.
- External forest administration is done via RDP.
- Production forest admin creds end up on systems in the External forest.
- Attacker compromises External to compromise Production AD.

Mitigation:

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

The Cloud Is Magic!

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 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
Reset password	Preparation for enabling password writeback

DEF CON 25
(July 2017)

On-Prem: Acme's Azure AD Connect

```
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'. This account must have directory replication permis
                    Directory and write permission on certain attributes to enable Hybrid Deployment
DistinguishedName : CN=MSOL_trd977930921,OU=Service Accounts,DC=theacme,DC=io
Enabled           : True
GivenName         :
Name              : MSOL_trd977930921
ObjectClass       : user
ObjectGUID        : cdcb6dd0-65e2-40bc-bc60-461408831036
SamAccountName    : MSOL_trd977930921
SID               : S-1-5-21-143179592-3749324205-2095737646-1138
```

On-Prem: Acme's Azure AD Connect

```
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                : DC=theacme,DC=io
IdentityReference       : ACME\MSOL_trd977930921
AccessControlType       : Allow
ActiveDirectoryRights   : ExtendedRight
ObjectType              : DS-Replication-Get-Changes-All

ObjectDN                : DC=theacme,DC=io
IdentityReference       : ACME\MSOL_trd977930921
AccessControlType       : Allow
ActiveDirectoryRights   : ExtendedRight
ObjectType              : DS-Replication-Get-Changes
```

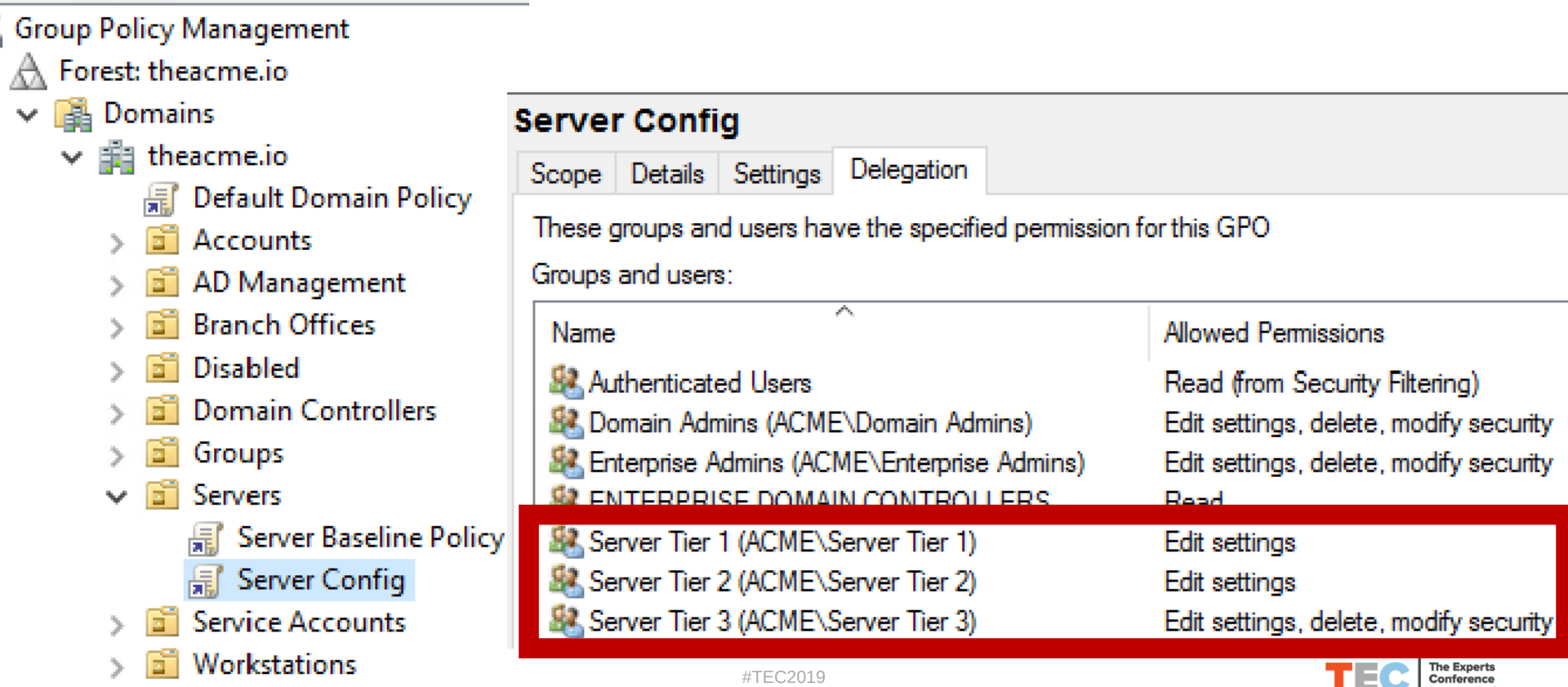
On-Prem: Acme's Azure AD Connect

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


Description       : Account created by the Windows Azure Active Directory Sync
                    'trd977930921' running on computer 'AZURESYNC' configured t
                    'theacmeio.onmicrosoft.com'. This account must have directo
                    Directory and write permission on certain attributes to ena
DistinguishedName : CN=MSOL_trd977930921,OU=Service Accounts,DC=theacme,DC=io
Enabled           : True
GivenName         :
PS C:\> get-adcomputer AzureSync


DistinguishedName : CN=AZURESYNC,OU=Servers,DC=theacme,DC=io
DNSHostName       :
Enabled           : True
Name              : AZURESYNC
ObjectClass       : computer
ObjectGUID        : 42f88cbe-c51f-4f5c-9059-58d3449a7a30
```

On-Prem: Acme's Azure AD Connect

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


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

On-Prem: Acme's Azure AD Connect



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.

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 network access to a Domain Controller.

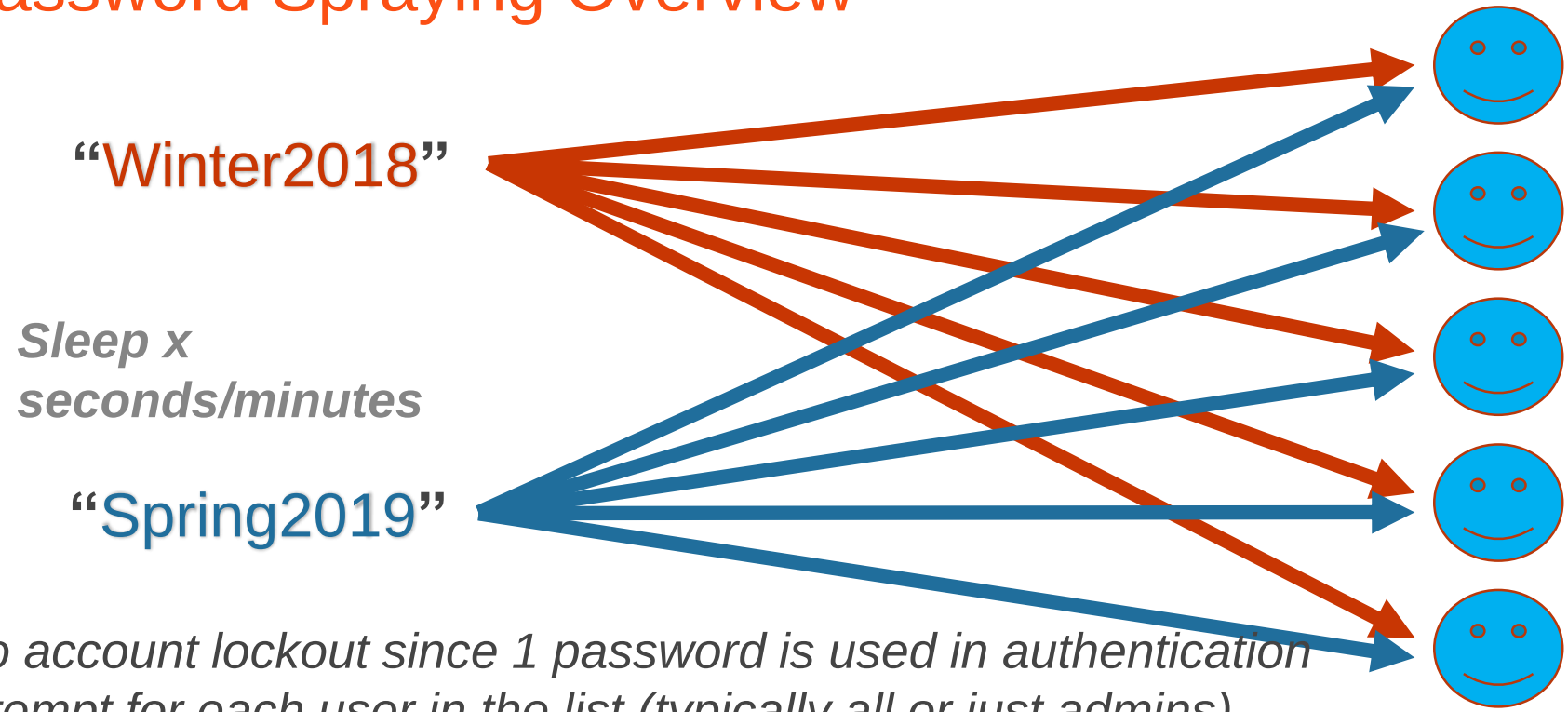
Azure AD:

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

Azure AD User Enumeration

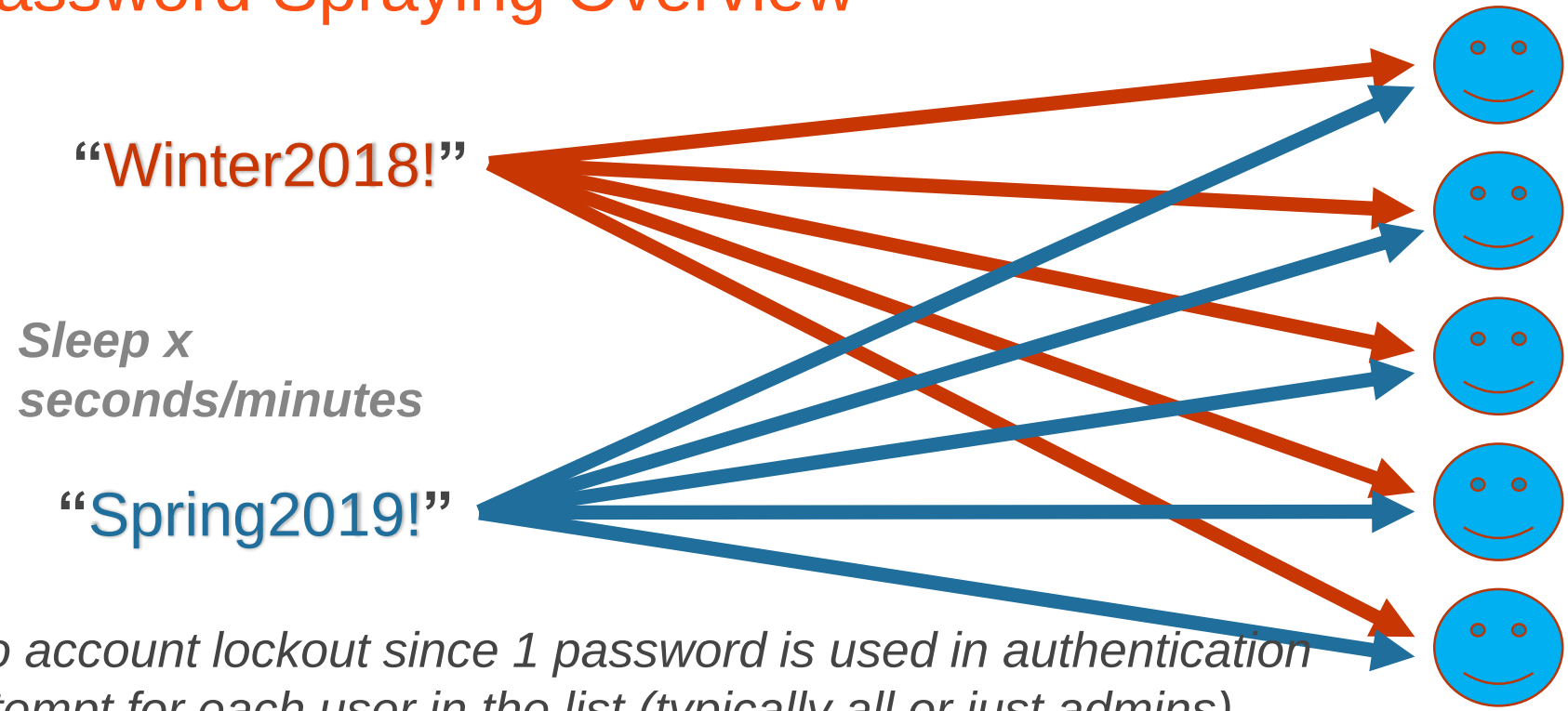
- Office 365 Authentication Page (Python) [Account Discovery]
  - https://github.com/LMGsec/o365creeper
- OWA (Golang)
  - https://github.com/busterb/msmailprobe
- ActiveSync (Python)
  - https://bitbucket.org/grimhacker/office365userenum/src
- MSOnline/AzureAD PowerShell Module (PowerShell)
  - https://github.com/nyxgeek/o365recon

Password Spraying Overview



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

Password Spraying Overview



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

Password Spraying Overview

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

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

Attacking the Cloud: Password Spraying

```
PS C:\> C:\temp\Spray-O365.ps1

 Password Spraying the EWS portal at https://outlook.office365.com/EWS/Exchange.asmx. Sit tight...
    5 threads remaining
    [oooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooo

    + 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

```
[*] 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.
```

```
[*] Now spraying the EWS portal at https://outlook.office365.com/EWS/Exchange.asmx
[*] Current date and time: 08/02/2019 04:04:26
[*] Trying Exchange version Exchange2010
[*] SUCCESS! User:theacme.io\obiwan@theacme.io Password:TheForce19
[*] A total of 1 credentials were obtained.
```

```
[*] Now spraying the EWS portal at https://outlook.office365.com/EWS/Exchange.asmx
[*] Current date and time: 08/02/2019 04:04:03
[*] Trying Exchange version Exchange2010
[*] SUCCESS! User:theacme.io\bobafett@theacme.io Password:Mandalorian19!
[*] A total of 1 credentials were obtained.
```

```
[*] Now spraying the EWS portal at https://outlook.office365.com/EWS/Exchange.asmx
[*] Current date and time: 08/02/2019 04:05:34
[*] Trying Exchange version Exchange2010
[*] SUCCESS! User:theacme.io\bailey@theacme.io Password:Password1
[*] A total of 1 credentials were obtained.
Results have been written to C:\temp\owa-sprayed-creds.txt.
```

Detecting 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… …ense status: Azure AD Free

Start a free Premium Trial

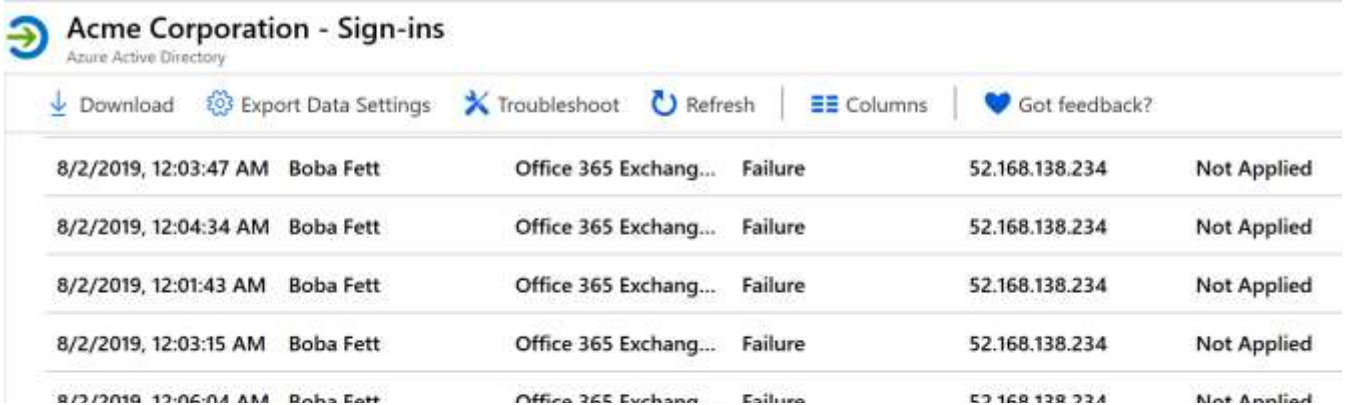
Soon…

Detecting Password Spraying

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
8/1/2019, 9:09:00 PM	Adm Ackbar	Office 365 Exchange On...	Failure	52.168.138.234
8/1/2019, 9:08:53 PM	Finn	Office 365 Exchange On...	Failure	52.168.138.234

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

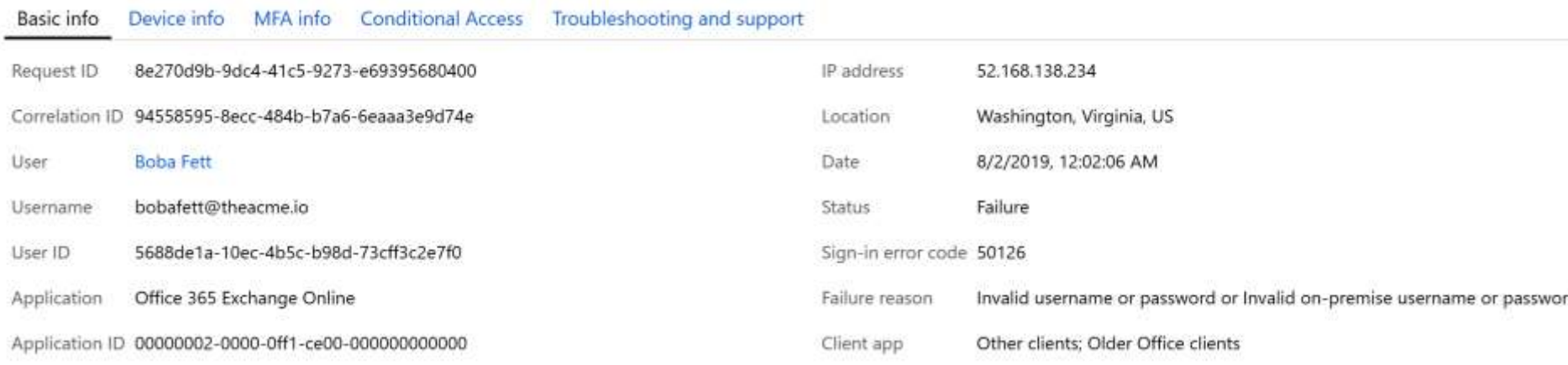
Detecting Password Spraying



8/2/2019, 12:08:21 AM	Boba Fett	Office 365 Exchange Online	Failure
8/2/2019, 12:02:06 AM	Boba Fett	Office 365 Exchange Online	Failure
8/2/2019, 12:04:11 AM	Boba Fett	Office 365 Exchange Online	Success

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

Detecting Password Spraying



Sign-in error code 50126

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

Client app Other clients; Older Office clients

Legacy Authentication

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

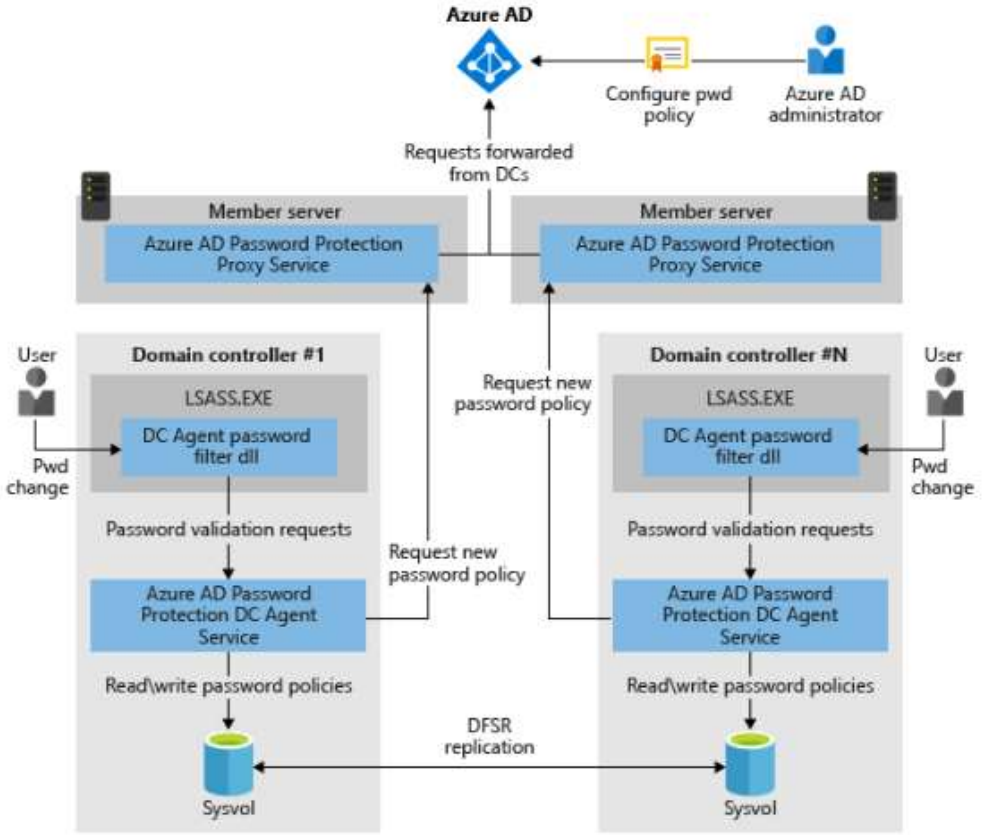
Password Spraying Defense (ADFS)

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

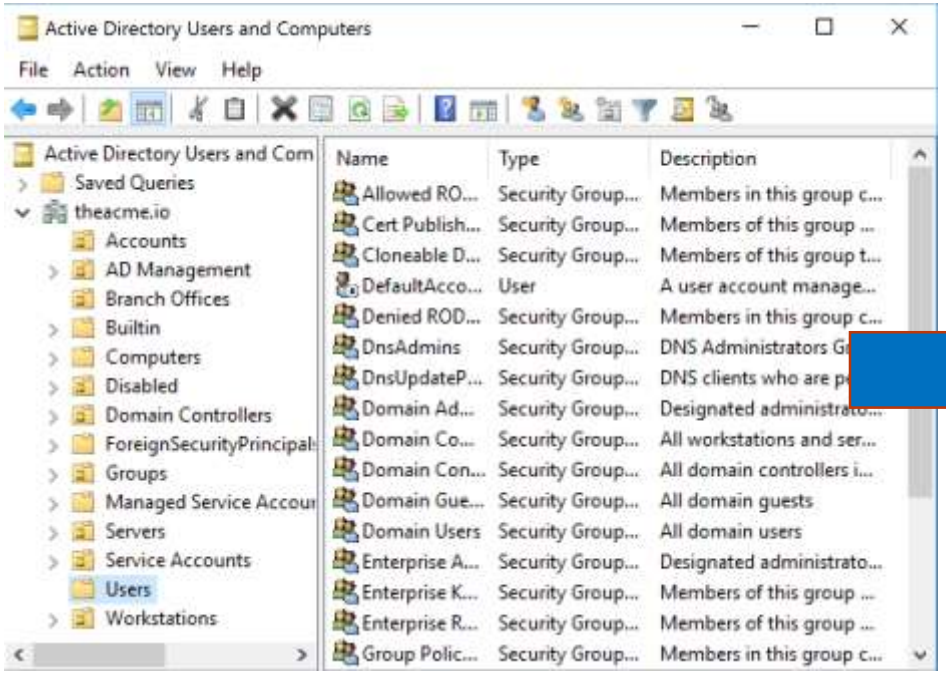
TIMESTAMP	TRIGGER TYPE	IP ADDRESS	BAD PASSWORD ERROR COUNT	EXTRANET LOCKOUT ERROR COUNT	UNIQUE USERS ATTEMPTED
2/28/2018 6:00 PM	hour	104.208.238.9	0	284	14
2/28/2018 6:00 PM	hour	104.44.252.135	0	27	1
2/28/2018 6:00 PM	hour	168.61.144.85	0	164	2

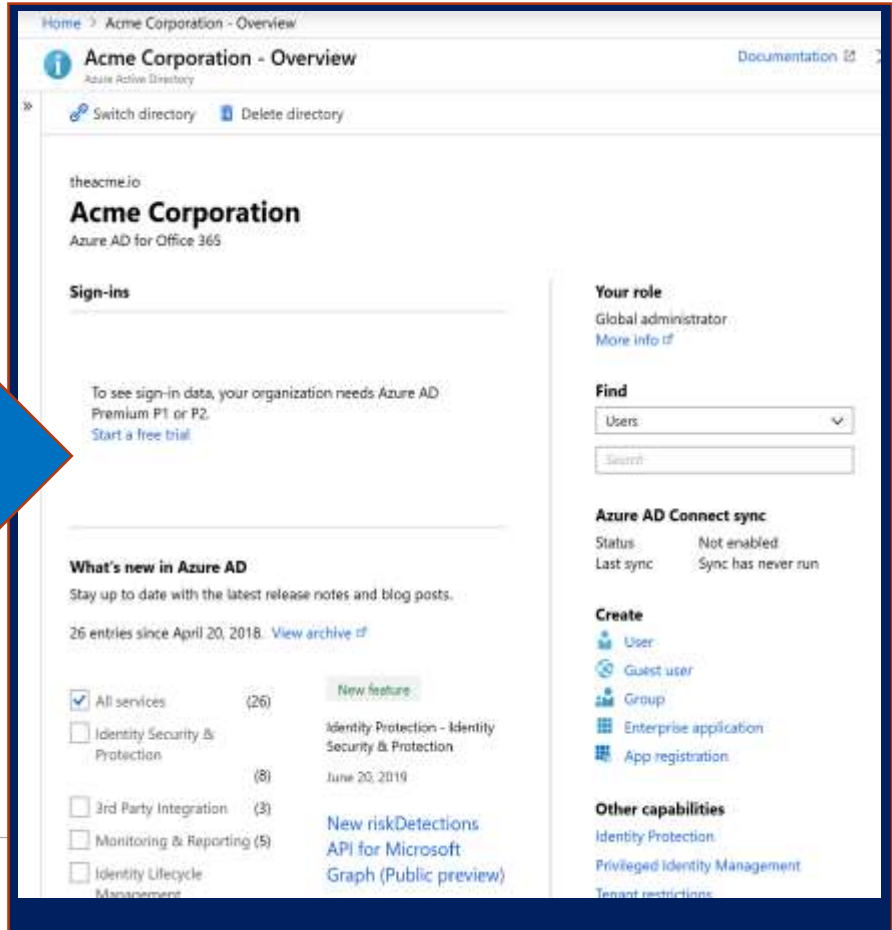
Password Spraying Defense: Azure AD Password Protection

- 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 (http://aka.ms/dfsrmig)
- Deploy in Audit Mode first
- Passwords are fuzzy matched, substring matched & scored. Must be 5 or higher
  - https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-password-ban-bad
- After passwords have been changed, look to extend password age

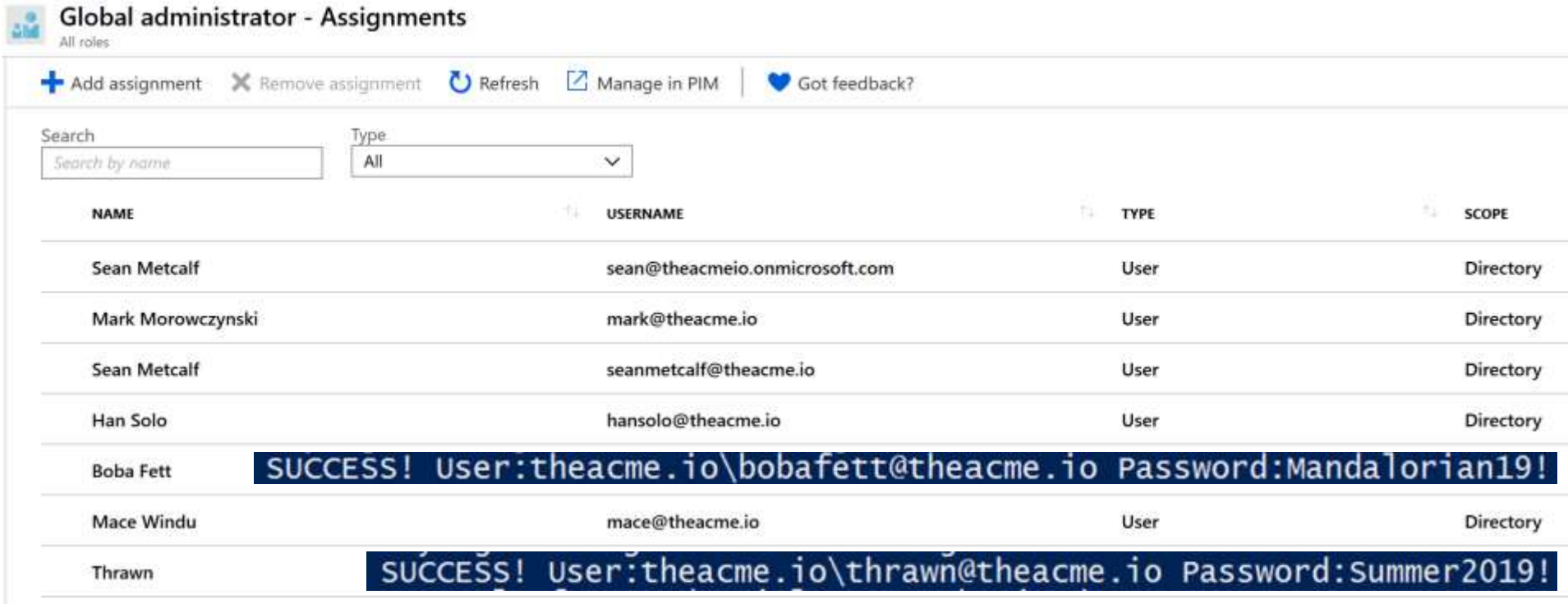


From On-Prem to Cloud Administration

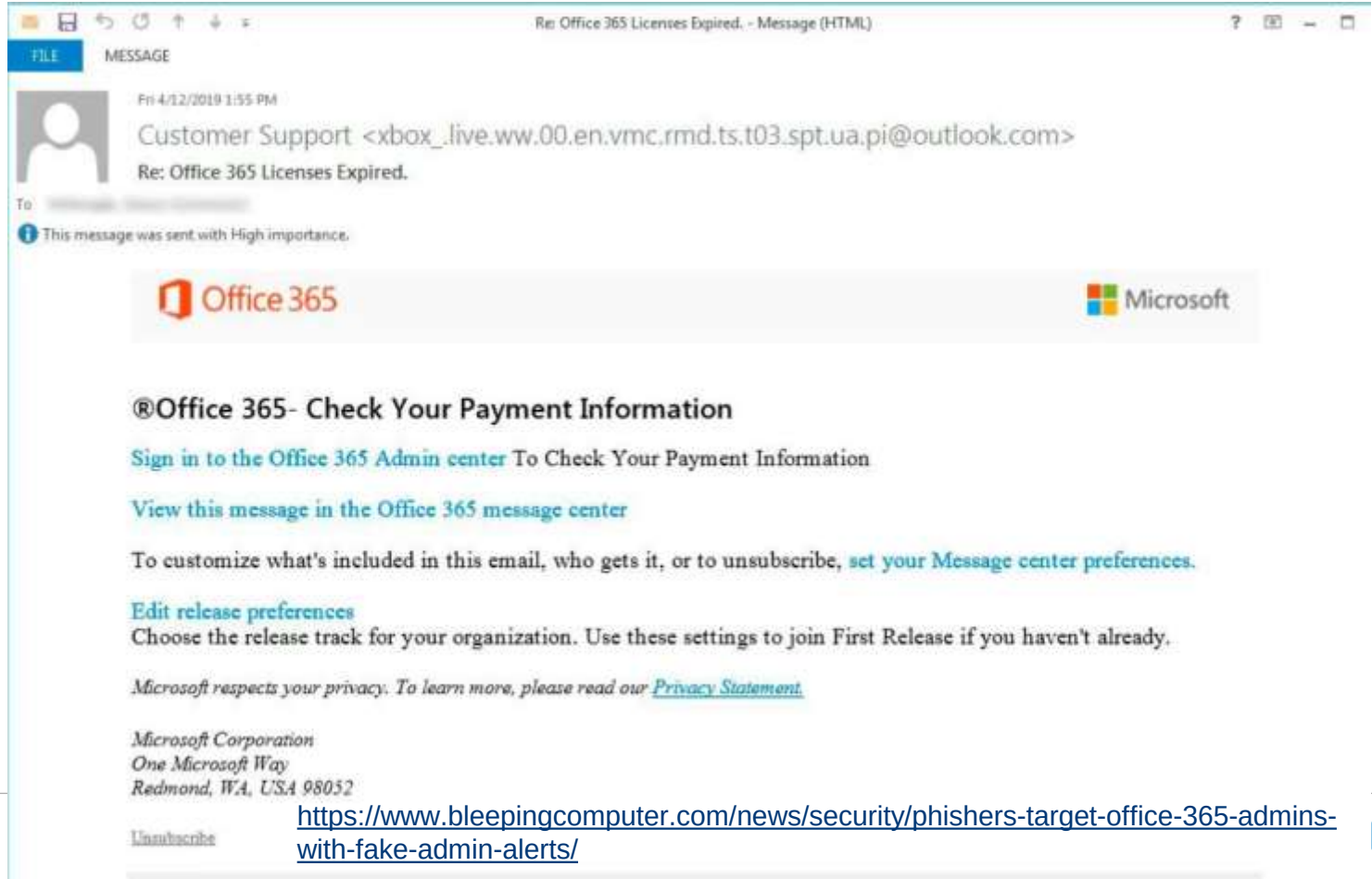




Attacking Cloud Administration



Attacking Cloud Administration



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

FILE MESSAGE

Fri 4/12/2019 1:55 PM

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

Re: Office 365 Licenses Expired.

To

This message was sent with High importance.

Office 365 Microsoft

®Office 365- Check Your Payment Information

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

View this message in the Office 365 message center

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

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

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

Microsoft Corporation
One Microsoft Way
Redmond, WA, USA 98052

Unsubscribe

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

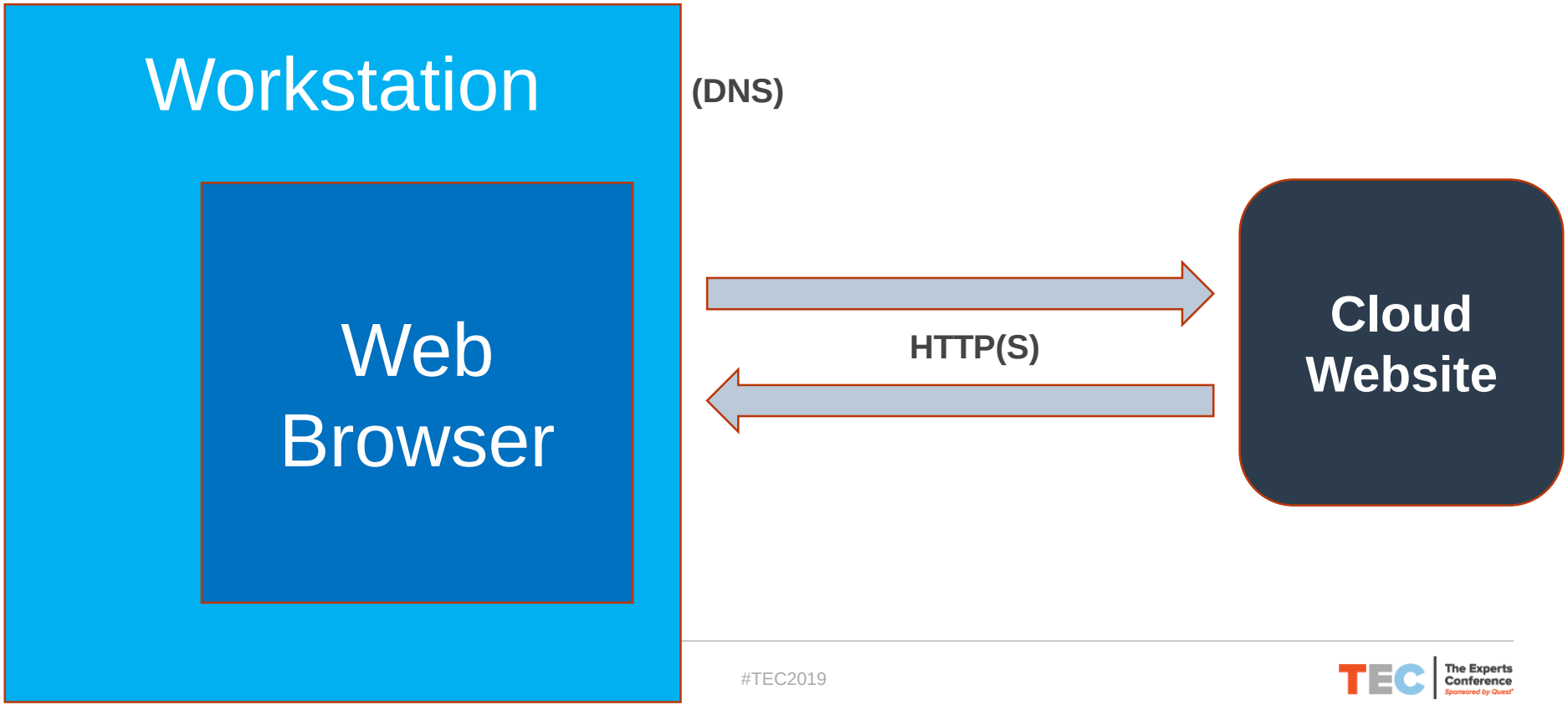
Global Reader

From Global Admin to **Global Reader**

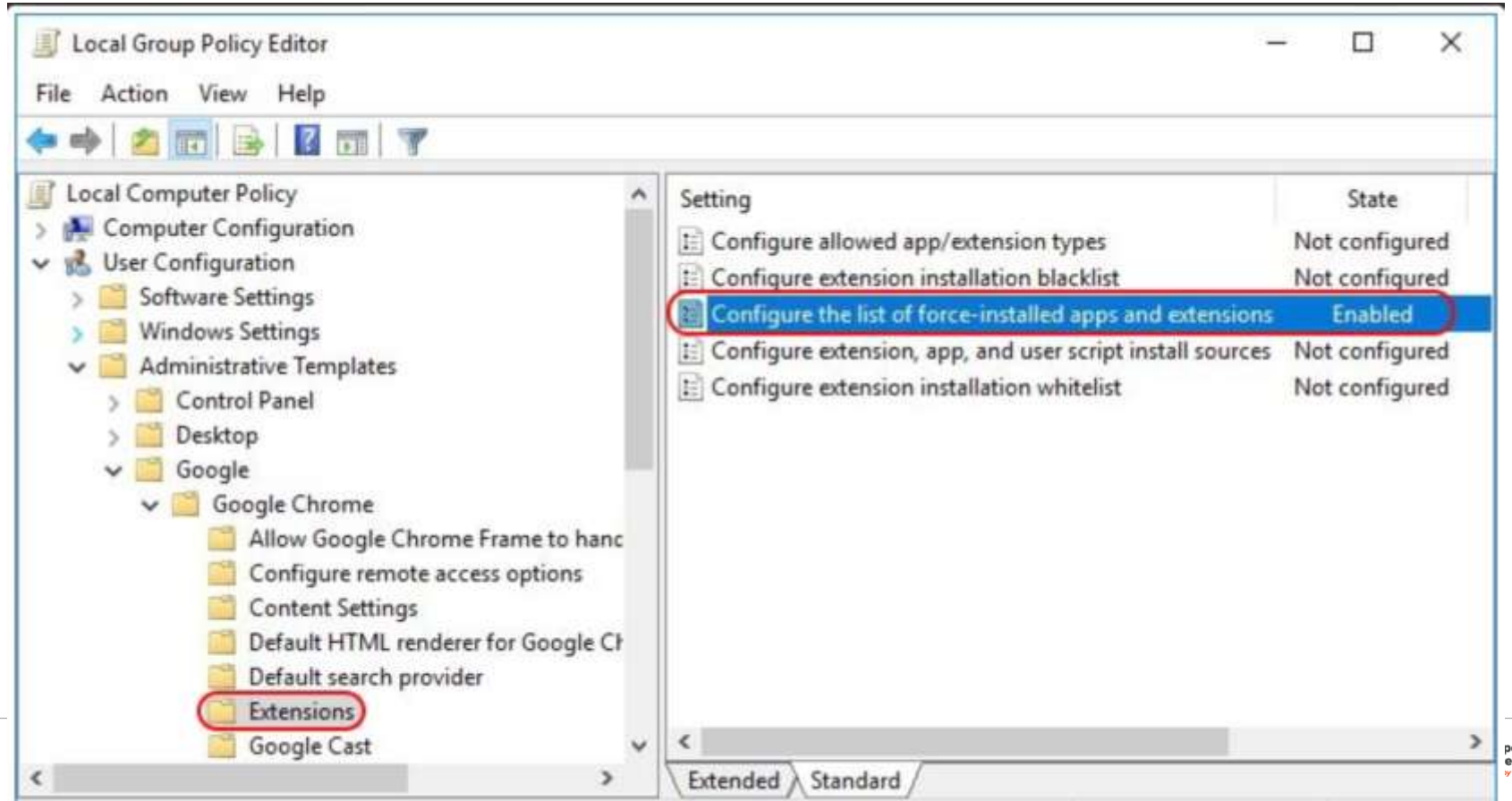
- Currently in Private Preview
- Provides read access to O365 services that Global Admin can read/write.
- Enables accounts that “required” Global Admin to be switched to read-only.
- Global Reader read-only access is still being expanded to cover all O365 services.

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

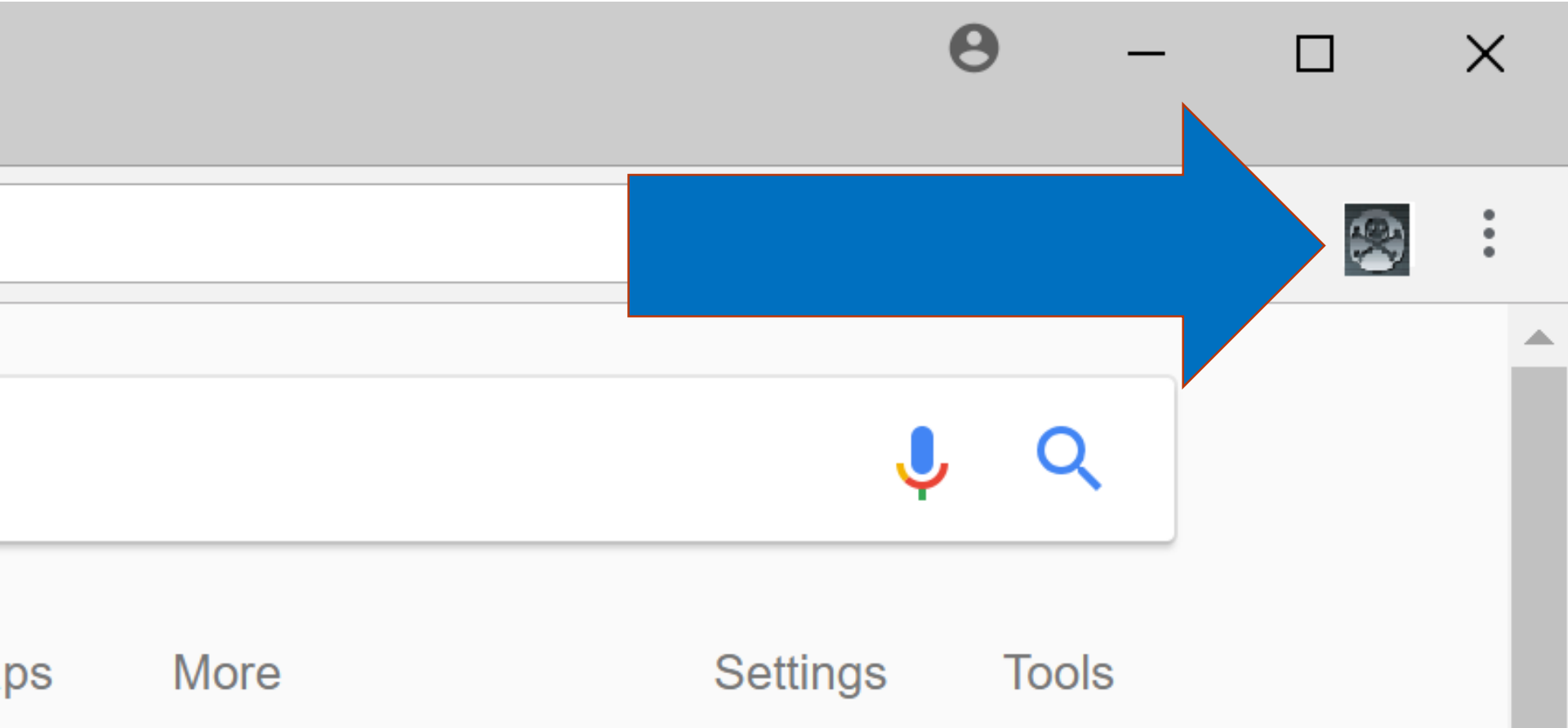
Cloud Administration – Finding a Weakness



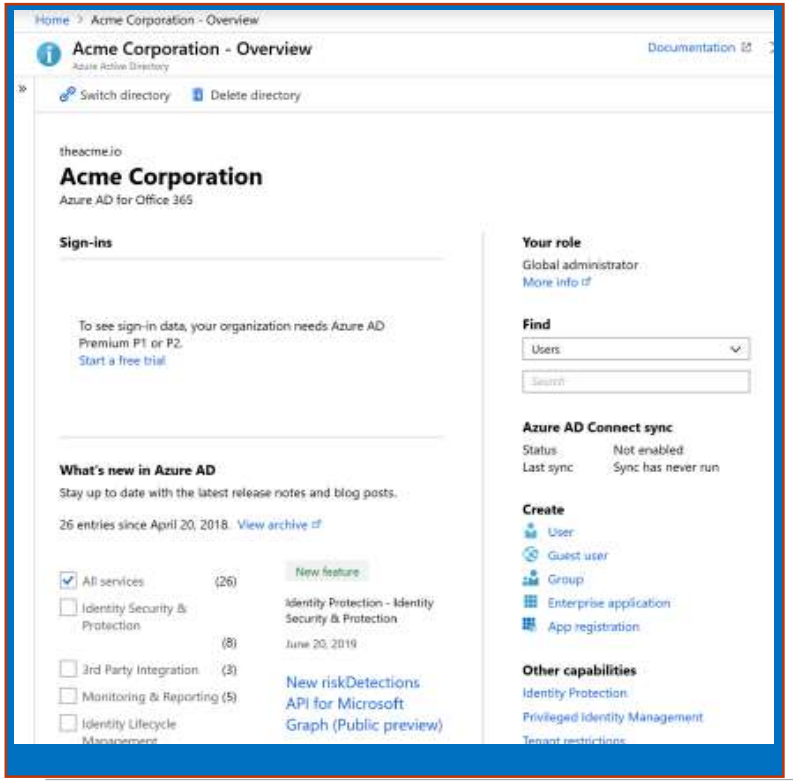
Attacking Cloud Administration: Token Theft

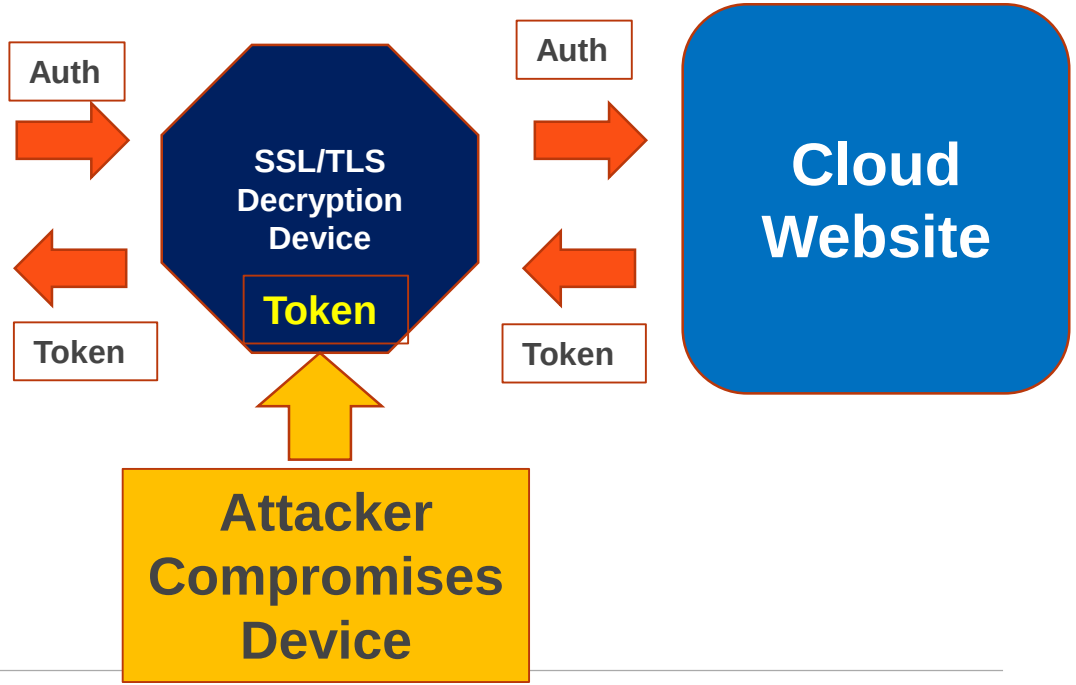


Attacking Cloud Administration: Token Theft



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: https://aka.ms/aadbaseline
- 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
  - https://aka.ms/deploymentplans

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

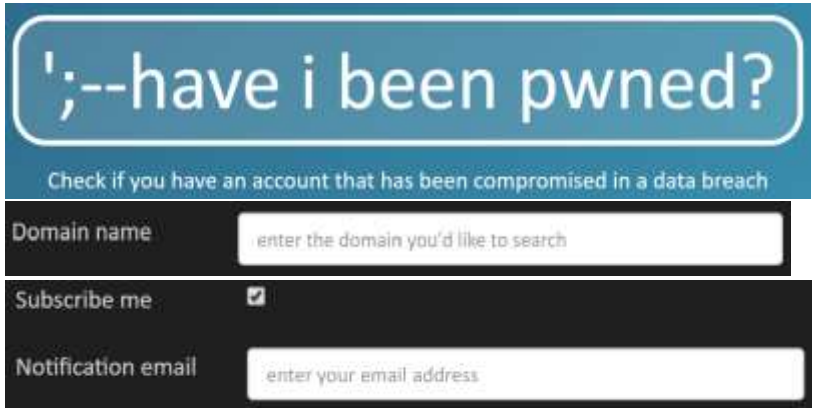
```
30f8c8134437da0c0232eeca20bd7992c00bce74:
df272dfef6127aeaecc5c47c7ceed028c39354df:
c886b08ad18cd650b1bc4a7612a0742a2257a41e:
bd01669b5883f24ebe55930efeb098fb5a873d96:
ef60e1915933c7c5abde3cb160f45bf1963e3525:
991db9efcfa06ae837a4d433b6ba2777256e1af8:
4b757d2f8f7036f8119739e4b82bc27875f4a987:
13a7bc6d3d74dcc5533d0a756a7b9bf4f1b46c7d: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

SHA1

112.	Han	Solo	hansolo	LeiaIKnow19!	hansolo@theacme.io
113.	Luke	Skywalker	lukeskywalker	TheForce19	lukeskywalker@Plus.com

Password Reuse/Replay Detection

HaveIBeenPwned.com



Password Hash (of the AD Hash) Sync Enabled: Users with Leaked Credential

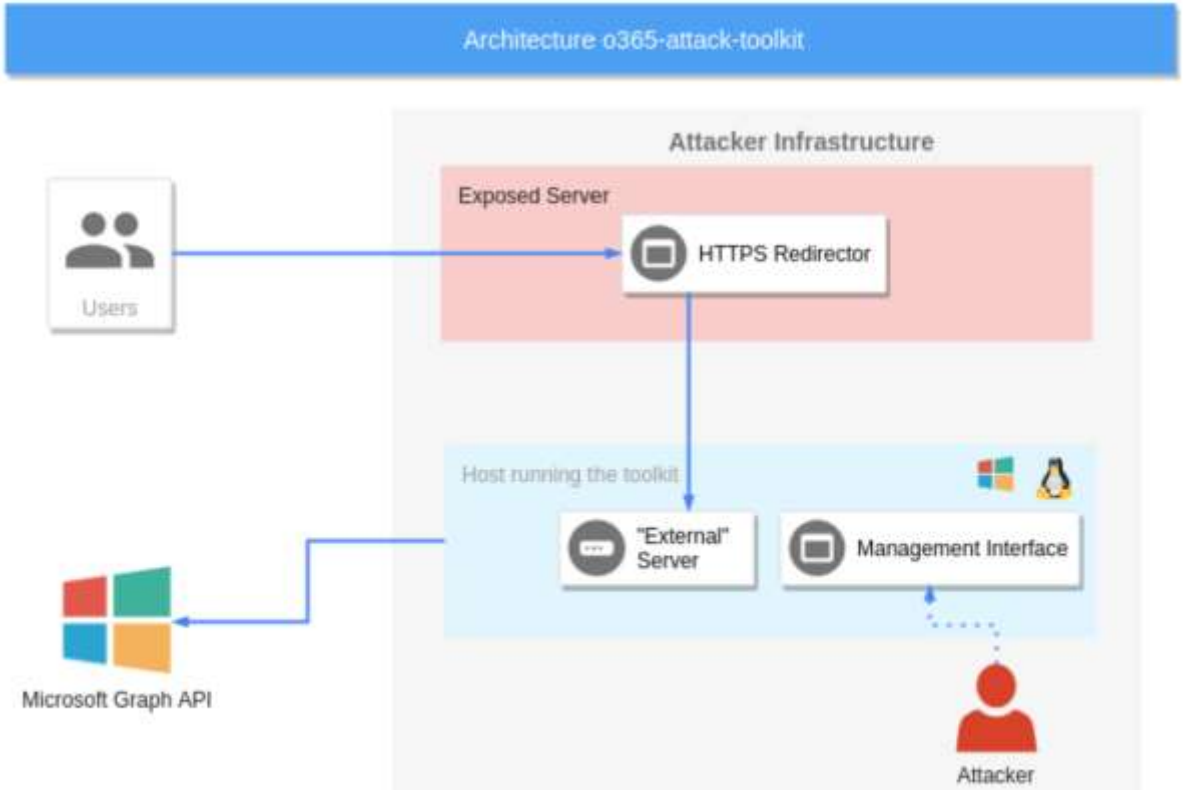
Turn on Azure AD Connect Password Hash Sync

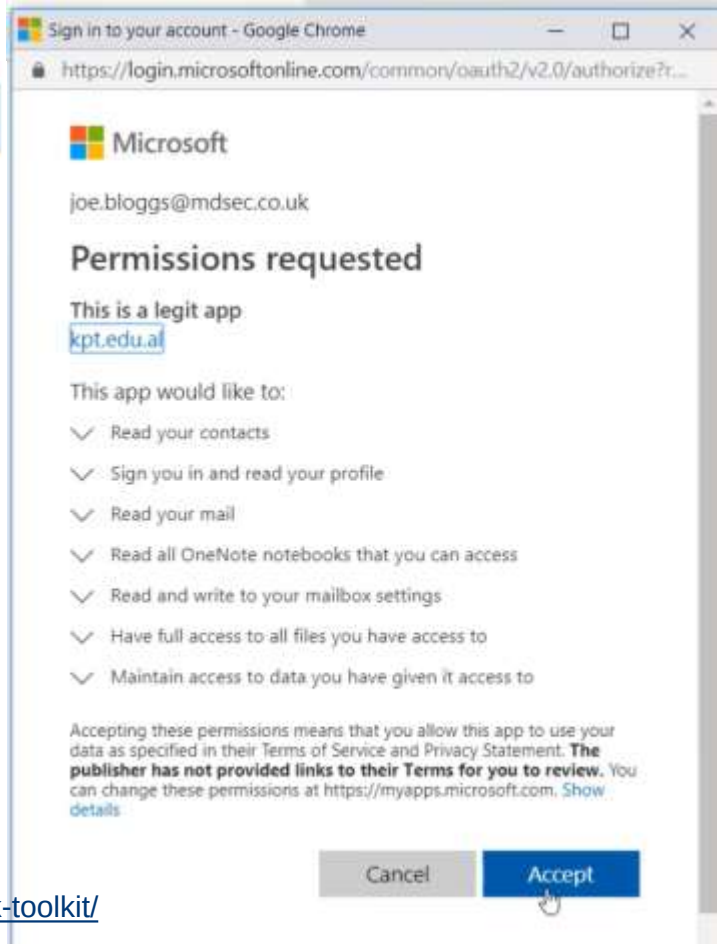
- Leaked Credential Reporting
  - Dark Web, Law Enforcement, and Security Researchers
- When something catastrophic happens
  - WannaCry, NotPetya
  - Wired Article: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/
- Understand How Password Hash Sync Works
  - http://aka.ms/aadphs
- 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
    - https://www.fireeye.com/blog/threat-research/2018/05/shining-a-light-on-oauth-abuse-with-pwnauth.html
  - MDSec Office 365 Toolkit
    - https://www.mdsec.co.uk/2019/07/introducing-the-office-365-attack-toolkit/
- Overprivileged Enterprise Apps with broad permissions.

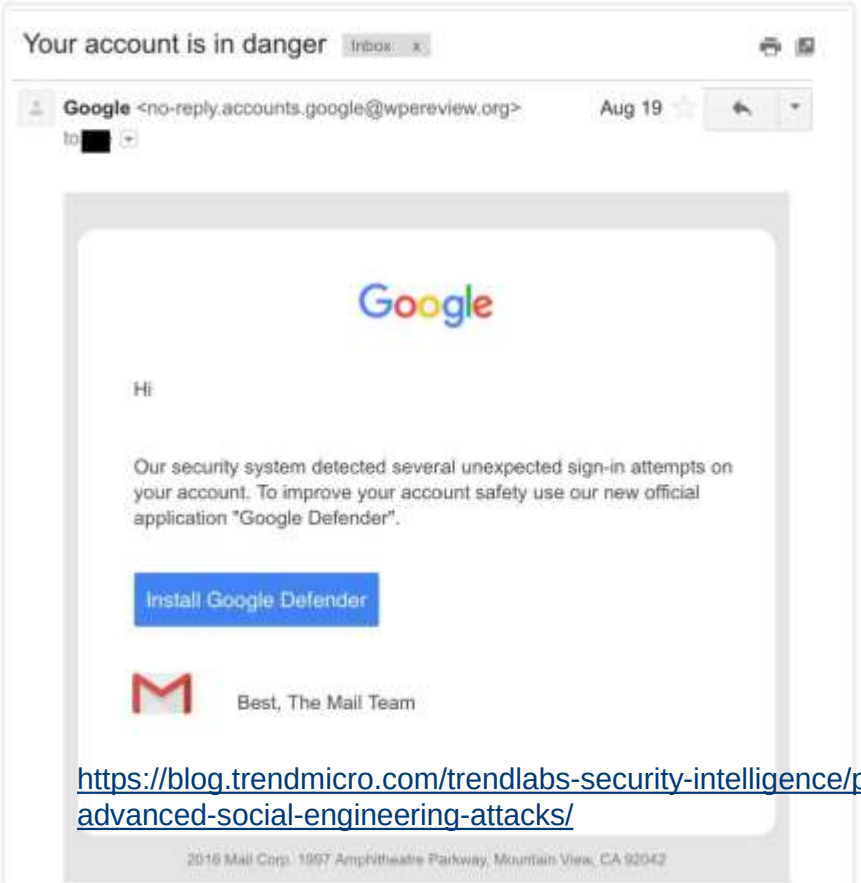
Illicit Consent Grant Attack: MDSec O365 Attack Toolkit

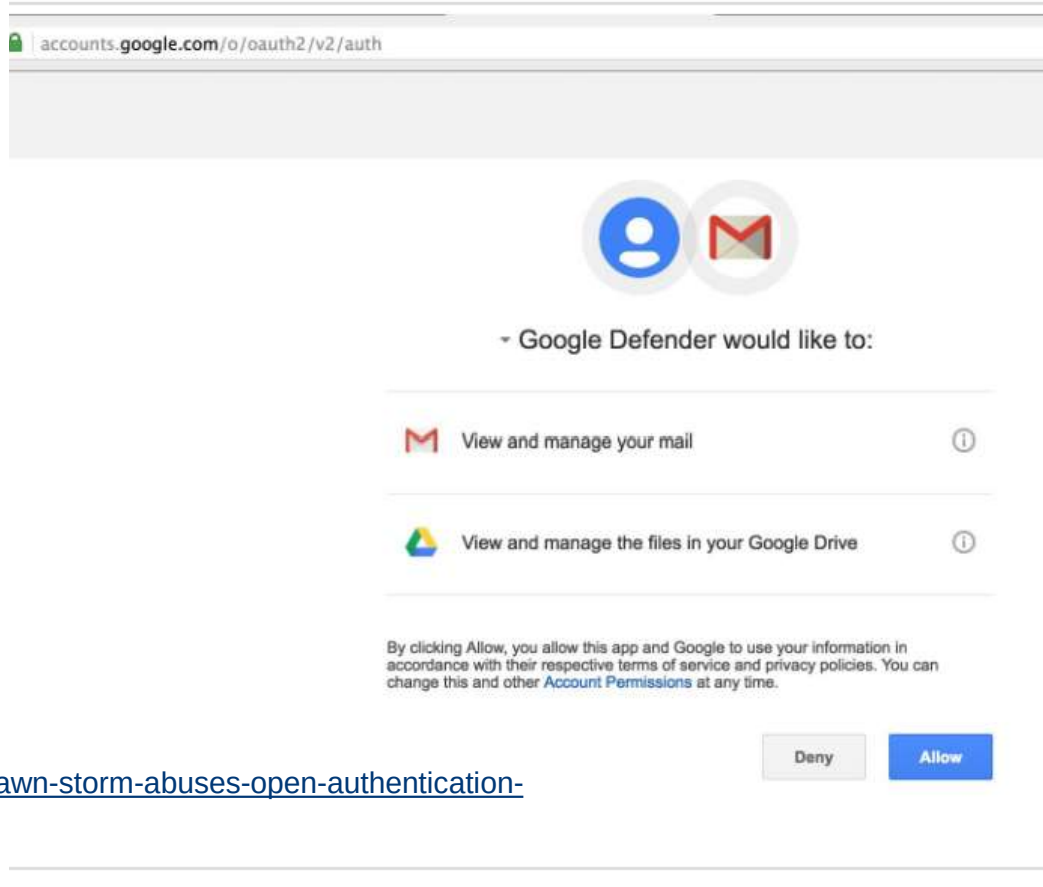




https://www.mdsec.co.uk/2019/07/introducing-the-office-365-attack-toolkit/

Illicit Consent Grant Attack: Pawn Storm

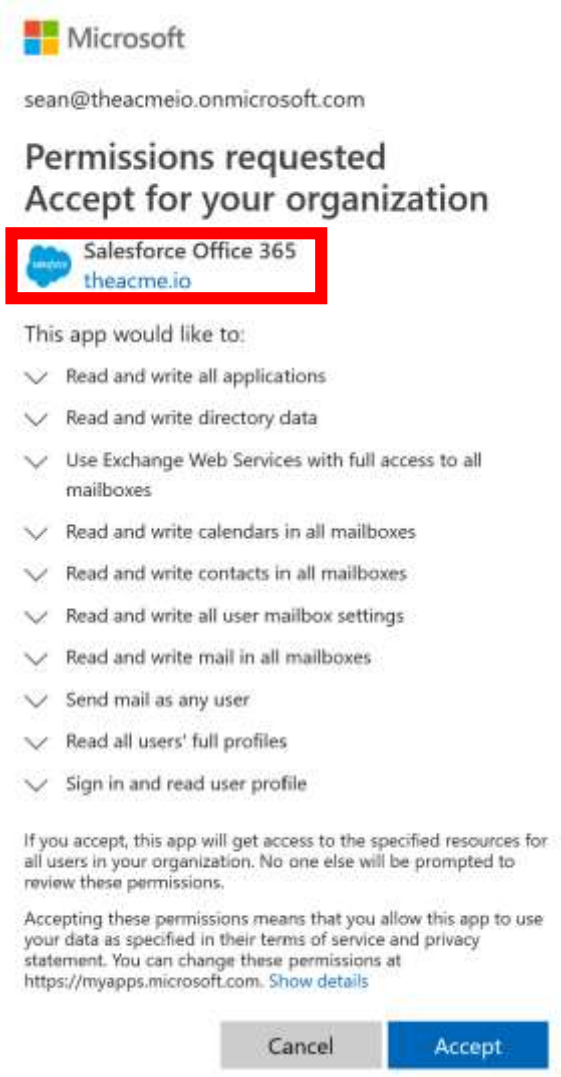




https://blog.trendmicro.com/trendlabs-security-intelligence/pawn-storm-abuses-open-authentication-advanced-social-engineering-attacks/

Enterprise App Permissions

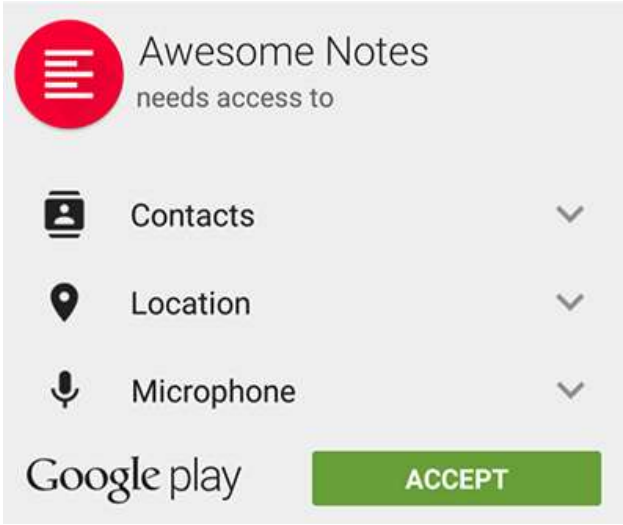
- Enterprise App (tenant-wide) permissions can be granted by Admins.
- Ideal persistence technique since app permissions not reviewed like group membership.



Enterprise App Permissions

This app would like to:

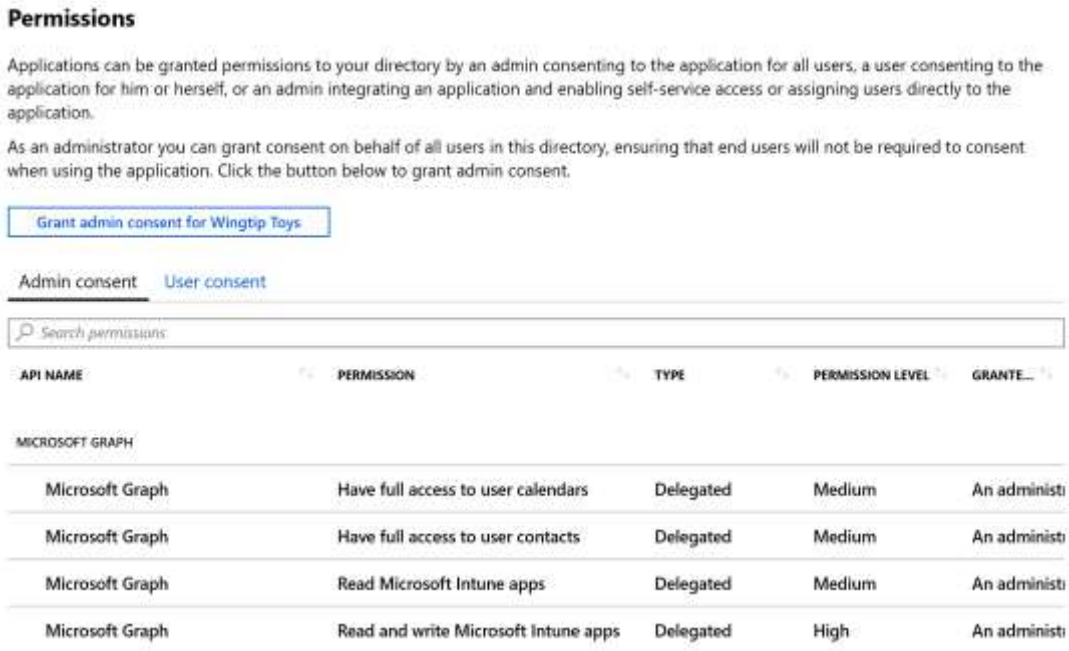
- Read and write all applications
- Read and write directory data
- Use Exchange Web Services with full access to all mailboxes
- Read and write calendars in all mailboxes
- Read and write contacts in all mailboxes
- Read and write all user mailbox settings
- Read and write mail in all mailboxes
- Send mail as any user
- Read all users' full profiles
- 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
  https://gist.github.com/psignoret/41793f8c6211d2df5051d77ca3728c09



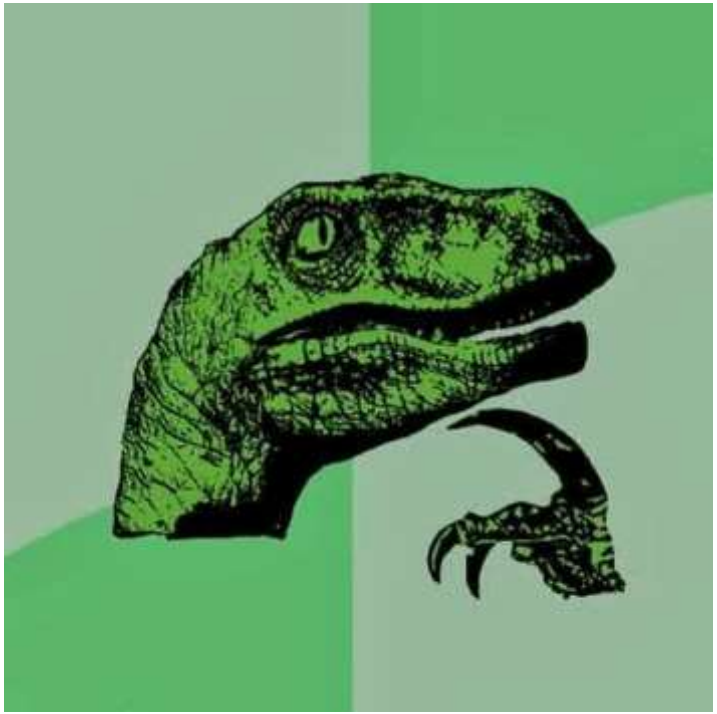
O365 Phase 1 Go Do Right Now Checklist

- ❑ 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.

Slides: Presentations.ADSecurity.org

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