TEC TALKS

The Experts Conference

Sponsored by Quest®

TheExpertsConference.com

Office 365 & Azure Active Directory: 10 Security Actions to Take Now

Sean Metcalf
Microsoft Certified Master
Founder & CTO, Trimarc Security LLC

TEC | The Experts Conference

Sponsored by Quest®

TEC 2020
in Atlanta

The live in-person AD and Office 365 training of the year!

November 17-18, 2020

www.TheExpertsConference.com

Hybrid Active Directory Security

Office 365

Migration and Modernization

RANDY FRANKLIN SMITH
Windows Security Subject Matter Expert
UltimateITSecurity.com

SEAN METCALF
Microsoft Certified Master, Founder & CTO
Trimarc Security, LLC

CHRIS MCNULTY
Sr. Product Manager
Microsoft

DAVID KENNEDY
Founder & CEO
TrustedSEC

TEC

The Experts Conference

Sponsored by Quest®

SEAN METCALF

Microsoft Certified Master

Founder & CTO, Trimarc Security, LLC

I will be speaking at TEC 2020. • **REGISTER NOW AND JOIN ME!**

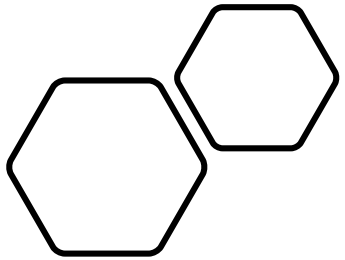
ABOUT

- Founder Trimarc (Trimarc.io), a professional services company that helps organizations better secure their Microsoft platform, including the Microsoft Cloud.
- Microsoft Certified Master (MCM) Directory Services
- Microsoft MVP
- Speaker: Black Hat, Blue Hat, BSides, DEF CON, DerbyCon, Shakacon, Sp4rkCon, TEC, Troopers
- Security Consultant / Researcher
- AD Enthusiast - Own & Operate ADSecurity.org (Microsoft platform security info)

AGENDA

- Introduction
- Azure AD & Office 365 Common Attacks
  - Password Spray
  - Password Reuse/Breach Replay
  - Consent Abuse
- Securing Azure AD & Office 365: Security Actions to Take Now
- Conclusion

Azure AD & Office 365 Common Attacks



Common Attacks: Password Spray

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

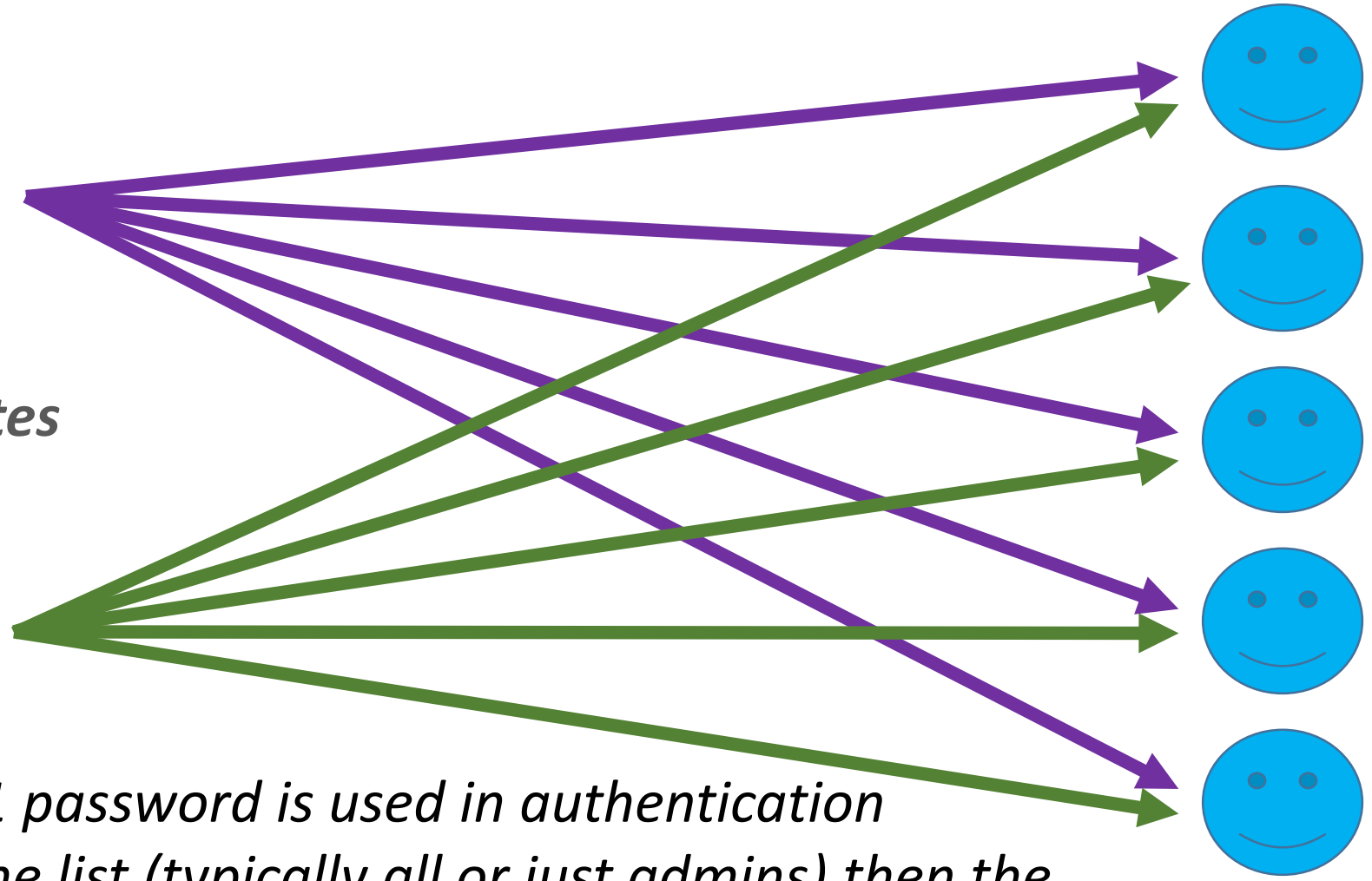
Azure AD user can enumerate all user accounts & admin group membership with access to Office 365 services (the internet by default).

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

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
    [oooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooo

    + 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
```

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.
```

Detecting Password Spraying

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 subscri… …icense status: Azure AD Free

Start a free Premium Trial

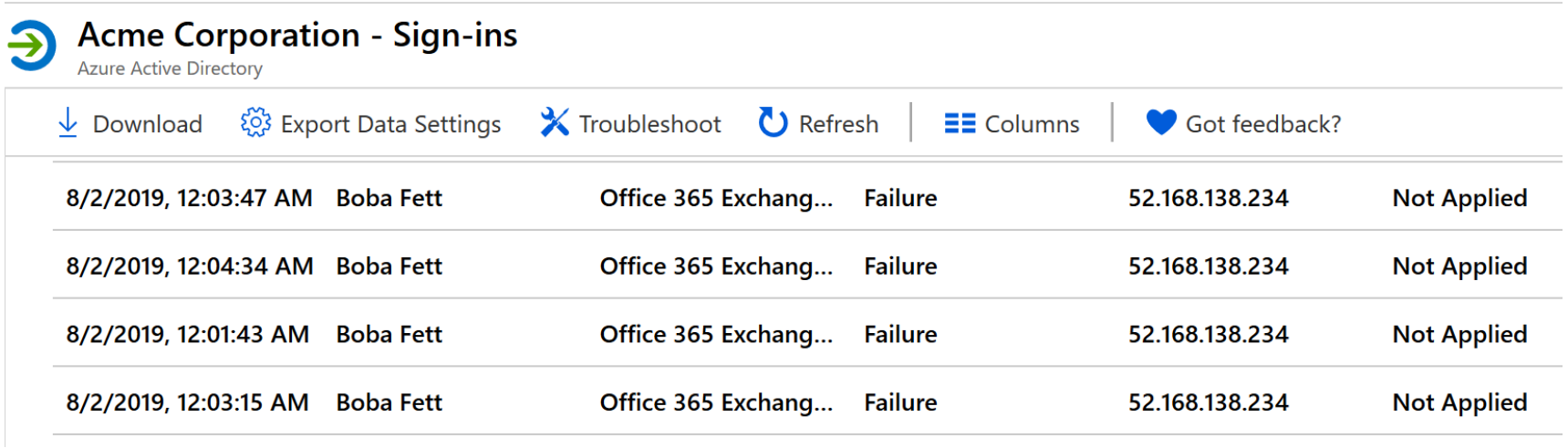
Soon…

Detecting Password Spraying

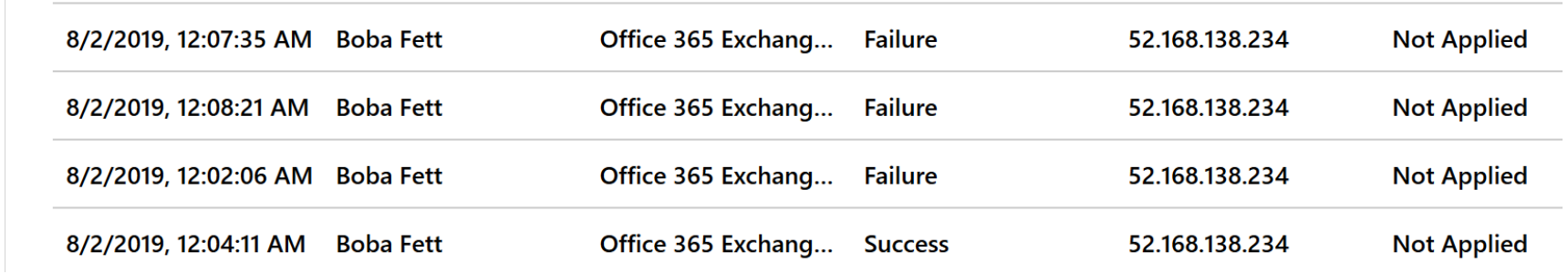
8/1/2019, 9:09:12 PM	Thrawn	Office 365 Exchange On...	Failure	52.168.138.234
8/1/2019, 9:09:11 PM	Qui-Gon Jinn	Office 365 Exchange On...	Failure	52.168.138.234
8/1/2019, 9:09:11 PM	Lando Calrissian	Office 365 Exchange On...	Failure	52.168.138.234
8/1/2019, 9:09:07 PM	Boba Fett	Office 365 Exchange On...	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

Basic info | Device info | MFA info | Conditional Access | Troubleshooting and support

Request ID	8e270d9b-9dc4-41c5-9273-e69395680400	IP address	52.168.138.234
Correlation ID	94558595-8ecc-484b-b7a6-6eaaa3e9d74e	Location	Washington, Virginia, US
User	Boba Fett	Date	8/2/2019, 12:02:06 AM
Username	bobafett@theacme.io	Status	Failure
User ID	5688de1a-10ec-4b5c-b98d-73cff3c2e7f0	Sign-in error code	50126
Application	Office 365 Exchange Online	Failure reason	Invalid username or password or Invalid on-premise username or passwor
Application ID	00000002-0000-0ff1-ce00-000000000000	Client app	Other clients; Older Office clients

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

Common Attacks: Breach Replay

Password Reuse/Replay

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

Reply Retweet Favorite

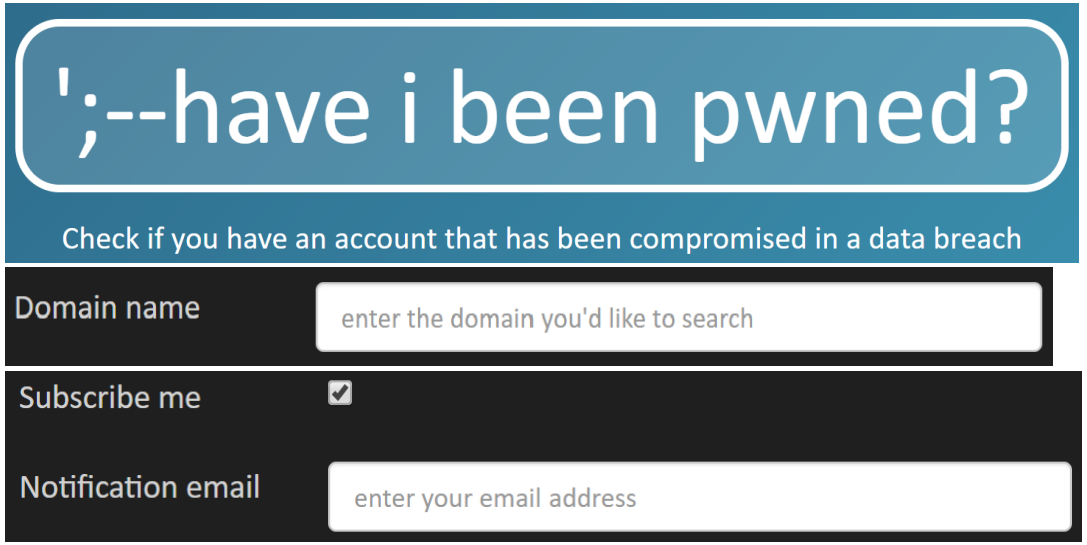
```
30f8c8134437da0c0232eeca20bd7992c00bce74:
df272dfef6127aeaecc5c47c7ceed028c39354df:
c886b08ad18cd650b1bc4a7612a0742a2257a41e:
bd01669b5883f24ebe55930efeb098fb5a873d96:
ef60e1915933c7c5abde3cb160f45bf1963e3525:
991db9efcfa06ae837a4d433b6ba2777256e1af8:
4b757d2f8f7036f8119739e4b82bc27875f4a987:
13a7bc6d3d74dcc5533d0a756a7b9bf4f1b46c7d:
a4404ac0b635faa6264658fc960836a308427c90:
546684e9d6d2f217db45229b4fa63c5d51f26729:
54cd6a7aaf905ac2145942f65a03fa7c54cf3ea9:
fb88038b760bc428e4847831aad572339c2e8ecd:
c06bbe76b5dfa96cb8c0351a227f30b8f1a3109a:
a067d0f50263bc845b31c70b6882ae91ed27a2c:
```

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 Report

RISK LEVEL	DETECTION TYPE	RISK EVENT TYPE	RISK EVENTS CLOSED
High	Offline	Users with leaked credentials	2 of 2

Common Attacks: Consent Abuse

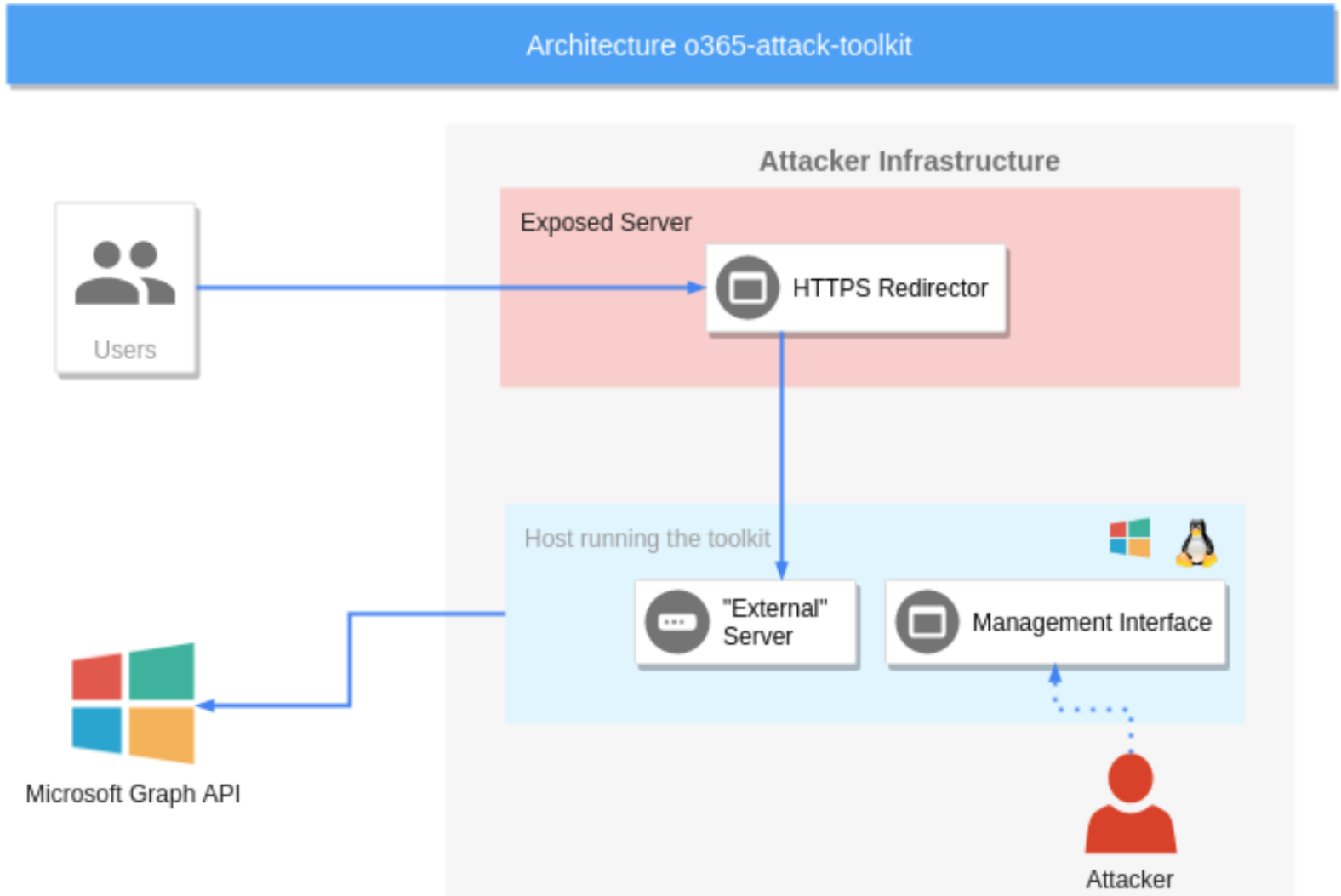
Consent Abuse

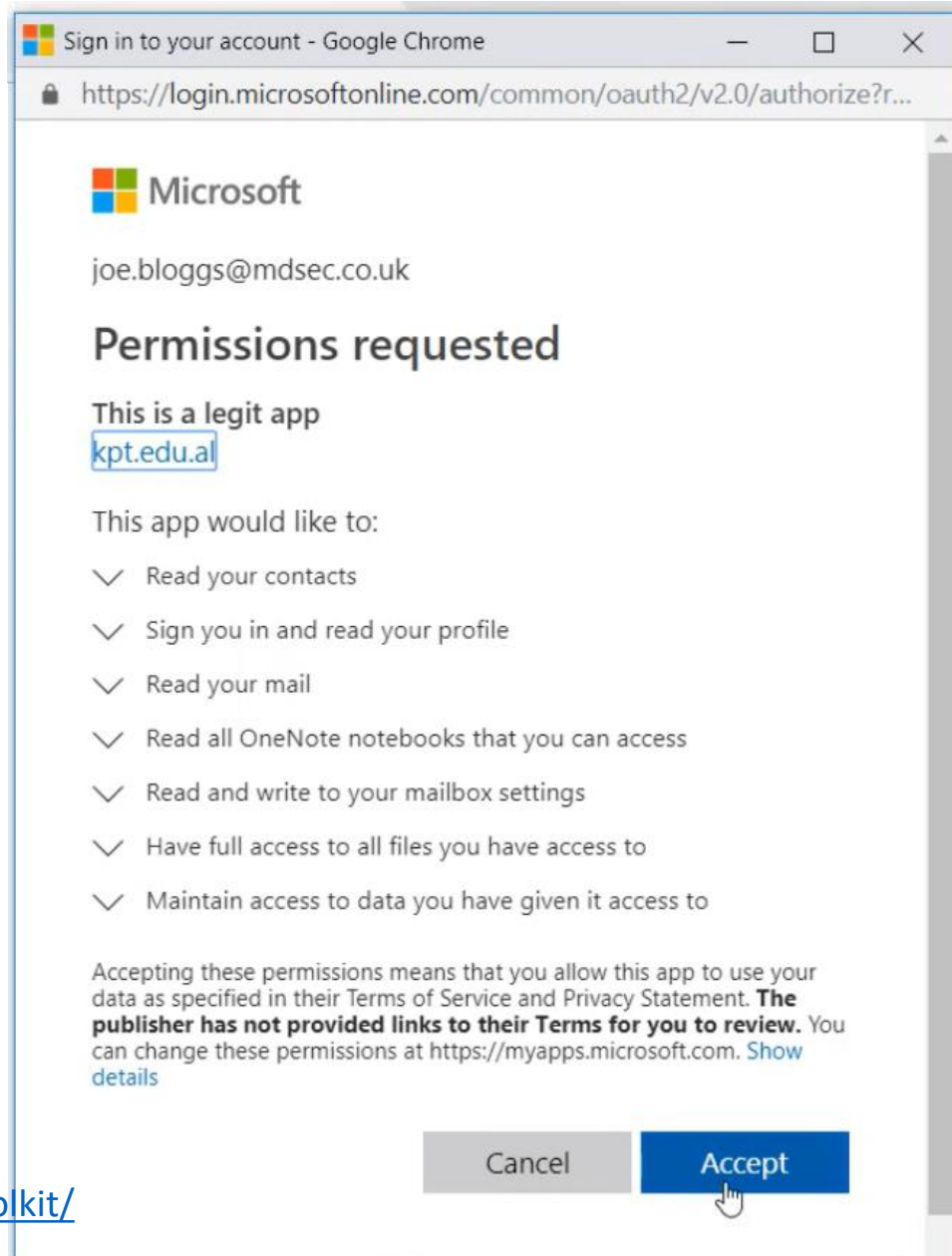
Users fooled into granting permissions to an app that looks like a familiar app.

FireEye PwnAuth

MDSec Office 365 Toolkit

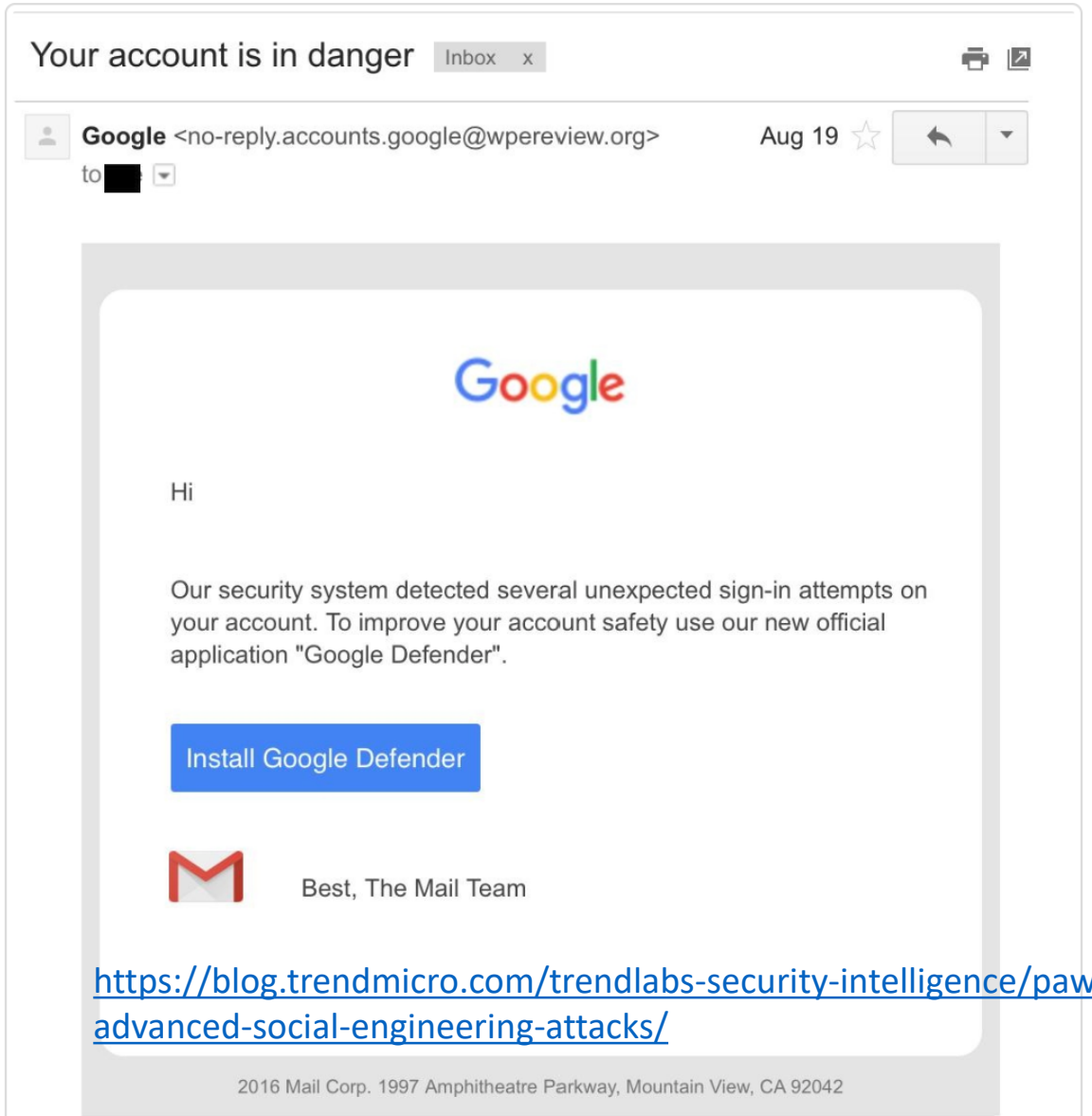
Illicit Consent Grant Attack: MDSec O365 Attack Toolkit

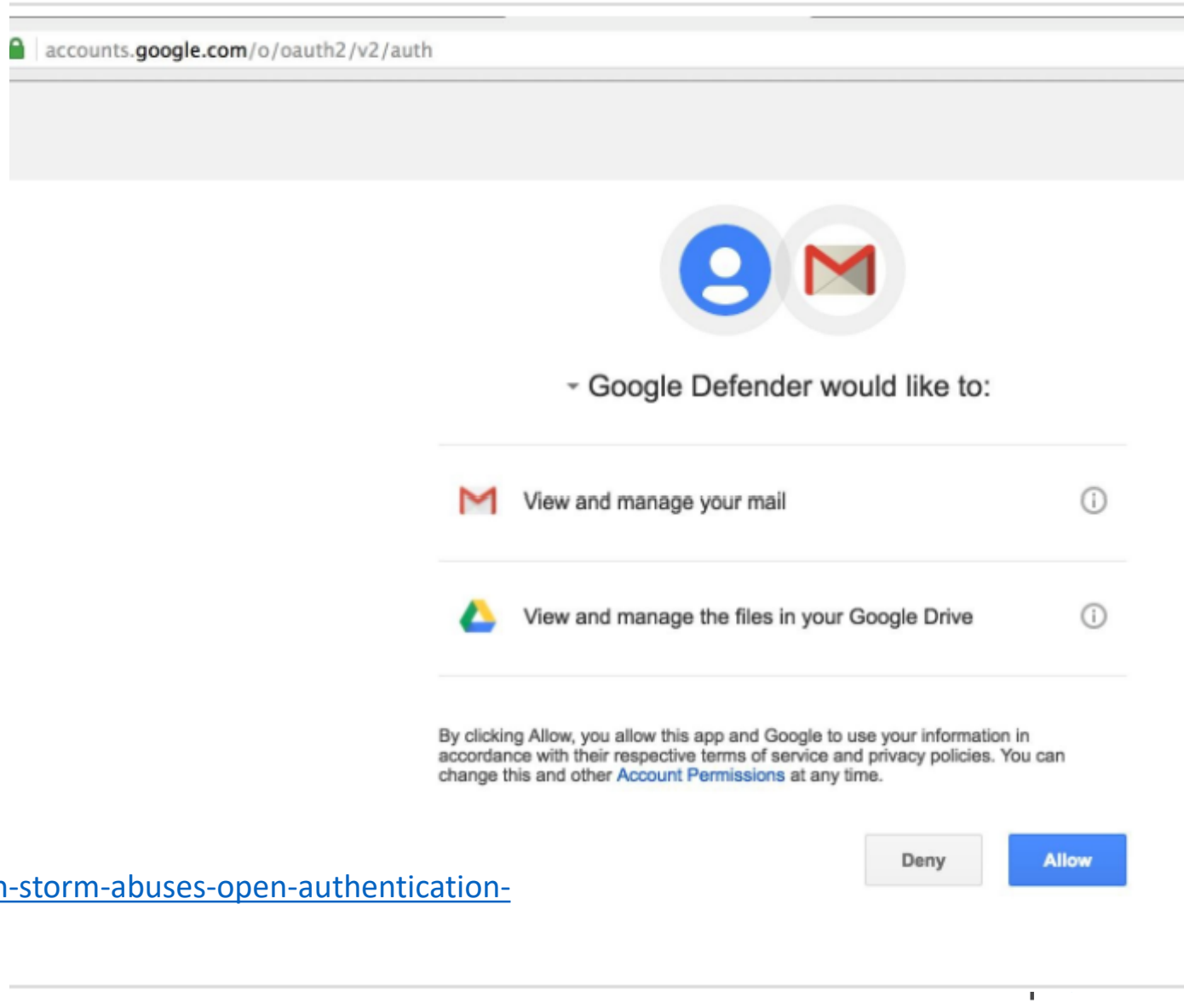




https://www.mdsec.co.uk/2019/07/introducing-the-office-365-attack-toolkit/

Illicit Consent Grant Attack: Pawn Storm

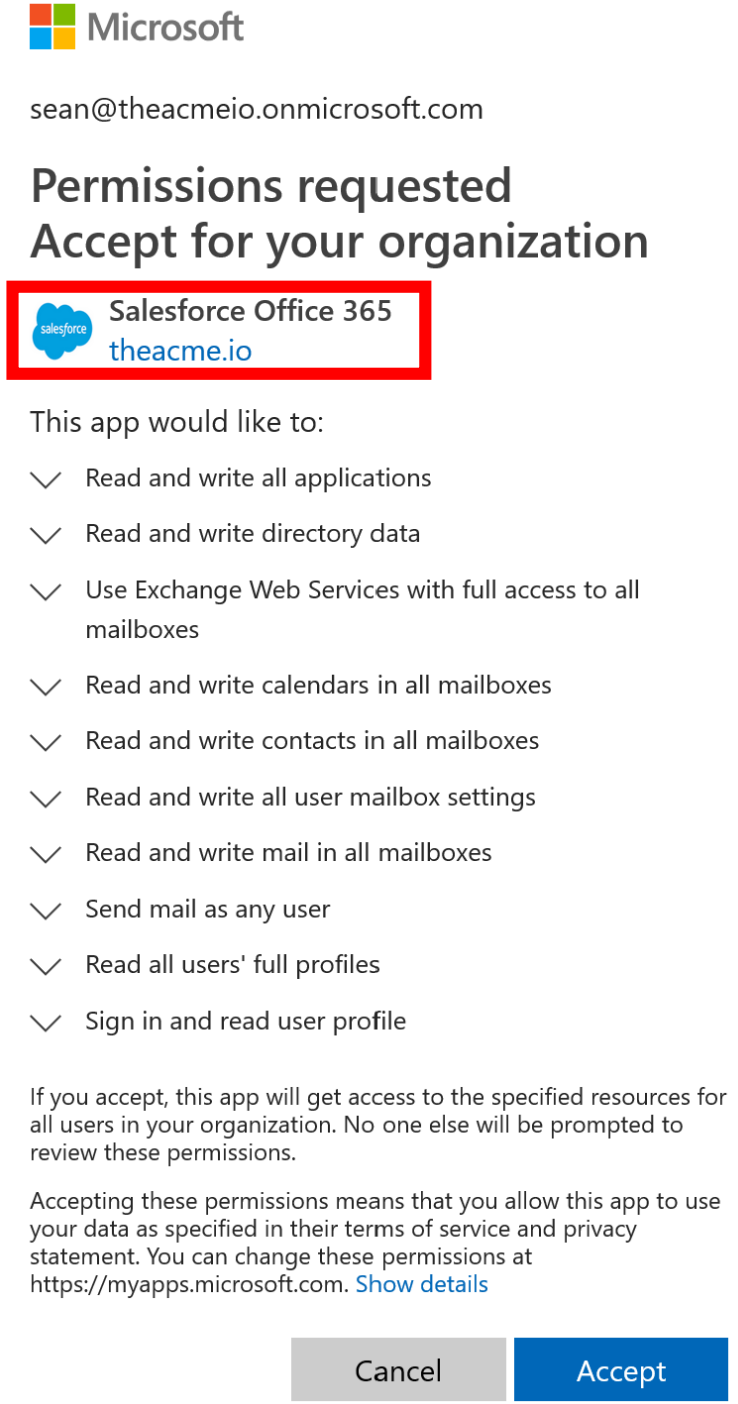




https://blog.trendmicro.com/trendlabs-security-intelligence/pawn-storm-abuses-open-authentication-advanced-social-engineering-attacks/

Enterprise App Permissions

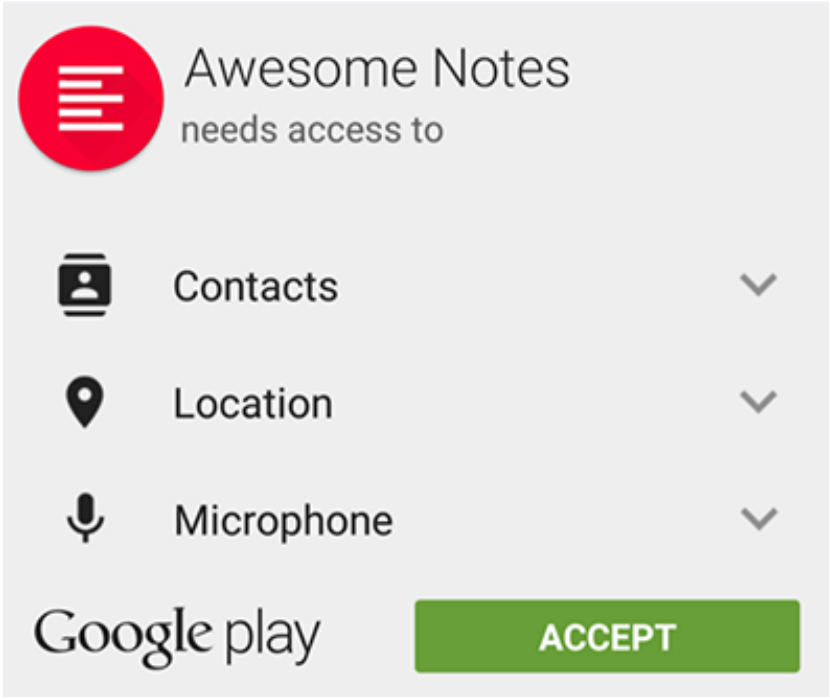
- Enterprise App (tenant-wide) permissions can be granted by Admins.
- Ideal persistence technique since app permissions not reviewed like group membership.



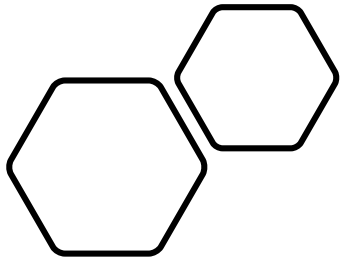
Enterprise App Permissions

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



Security Actions to Take Now



Limit Global Admins (2 to 4)

“Report” Accounts Should use Global Reader

Multi-Factor Authentication (MFA) for All Role Admins

Global Admins First, Preferably with Microsoft Authenticator App (no SMS/text)

Use Azure Privileged Identity Management (PIM)

Requires Azure AD P2 for Accounts using PIM (only)

1. Control Role Groups with PIM

- Global Admin
- Privileged Role Admin
- User Admin
- Security Admin
- Authentication Admin
- Application Admin
- Conditional Access Admin

These roles can control Office 365 admin accounts/groups/system. List is not comprehensive.

2. Control Service Admin Roles with PIM

- Exchange Admin
- SharePoint Admin
- Teams Admin
- Skype for Business Admin
- Intune Admin

These roles control Office 365 services & can access data. List is not comprehensive.

Identify Role Group Membership

```powershell
# Sample PowerShell Code. Provided without warranty or support.
Import-Module AzureAD
Connect-AzureAD

$AzureADDirectoryRole = Get-AzureADDirectoryRole
Write-Output "Discovered $($AzureADDirectoryRole.Count) Active Azure AD Roles"
Write-Output "============================================================="
Write-Output ""

$AzureADRoleGroupReport = @()
ForEach ($AzureADDirectoryRoleItem in $AzureADDirectoryRole)
 {
    $RoleGroupMembers = @()
    [array]$RoleGroupMembers = Get-AzureADDirectoryRoleMember -ObjectId
$AzureADDirectoryRoleItem.ObjectId

    Write-Output "Azure AD Role $($AzureADDirectoryRoleItem.DisplayName)
Membership ($($RoleGroupMembers.Count) members):"
    $RoleGroupMembers | % {$_.UserPrincipalName}
    Write-Output " "
 }
```

```
Discovered 18 Active Azure AD Roles
============================================================

Azure AD Role Application Administrator Membership (0 members):

Azure AD Role Device Administrators Membership (0 members):

Azure AD Role Intune Service Administrator Membership (2 members):
sean@trimarcrd.com
DevAdmin@trimarcrd.com

Azure AD Role Device Managers Membership (1 members):

Azure AD Role Security Administrator Membership (1 members):
sean@trimarcrd.com

Azure AD Role SharePoint Service Administrator Membership (2 members):
DarthVader@TrimarcRD.com
exadmin@trimarcrd.com

Azure AD Role Privileged Role Administrator Membership (1 members):
sean@trimarcrd.com

Azure AD Role Teams Communications Support Specialist Membership (0 members):

Azure AD Role Global Reader Membership (3 members):
TrimarcMCSA@trimarcrd.com
sadiki@trimarcrd.com
scottb@trimarcrd.com

Azure AD Role Exchange Service Administrator Membership (1 members):
exadmin@trimarcrd.com

Azure AD Role Directory Writers Membership (1 members):

Azure AD Role Billing Administrator Membership (0 members):

Azure AD Role Lync Service Administrator Membership (1 members):
exadmin@trimarcrd.com

Azure AD Role Conditional Access Administrator Membership (0 members):

Azure AD Role Teams Communications Administrator Membership (1 members):
exadmin@trimarcrd.com

Azure AD Role Teams Service Administrator Membership (2 members):
BobaFett@TrimarcRD.com
exadmin@trimarcrd.com

Azure AD Role Security Reader Membership (1 members):
TrimarcMCSA@trimarcrd.com

Azure AD Role Company Administrator Membership (2 members):
sean@trimarcrd.com
jason@trimarcrd.com
```

Secure Global Admin Authentication

Create & Use Dedicated Admin Accounts for (Office 365) Administration

Require MFA (& PIM)

Use Cloud Admin Workstations

Configure for FIDO2 authentication

Configure 2 Emergency “break-glass” Global Admin Accounts

1 should be excluded from MFA.

1 should be excluded from Conditional Access policies.

Both should have a FIDO2 key configured for authentication (in safe).

Audit logon activity.

Protect Azure AD Connect Server (& ADFS) like a DC

AAD Connect Service Account is Highly Privileged in Azure AD & AD

Azure AD Connect Server Location

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


Description       : Account created by the Windows Azure Active Directory Sync tool with installation identifier
                    'trd977930921' running on computer 'AZURESYNC' configured to synchronize to tenant
                    'theacmeio.onmicrosoft.com'. This account must have directory replication permissions in the local Active
                    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
```

```
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
SamAccountName    : AZURESYNC$
```

Ensure Azure AD Connect is Running the Current Version

6 versions released in 2019.
Versions older than 18 months will be deprecated.

```
Import-Module MSOnline
Connect-MsolService
(Get-MsolCompanyInformation).DirSyncClientVersion
```

Review Application Permissions & Consent

Review Tenant-Wide Permission (Admin) Consent

Security

- Conditional Access
- Permissions
- Token encryption (Preview)

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

Search permissions

API NAME	PERMISSION	TYPE	PERMISSION LEVEL	GRANTE...
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

Review Per-User Permission (User) Consent

User consent

	PERMISSION	TYPE	PERMISSION LEVEL	GRANTE...
h	Sign users in	Delegated	Medium	15 total us...
h	Sign in and read user profile	Delegated	Low	7 total use...
h	Read and write access to user profile	Delegated	Unknown	14 total us...
h	Read all users' basic profiles	Delegated	Low	14 total us...
h	Read and write access to user mail	Delegated	High	14 total us...
h	Read and write user and shared mail	Delegated	High	3 total use...

User(s)

Search by name or email

Caleb Baker
calebb@wingtiptoysonline.com

Rajat Luthra
rluthra@wingtiptoysonline.com

Audit App Permissions with PowerShell

.\Get-AzureADPSPermissions.ps1 | Export-Csv -Path "permissions.csv" -NoTypeInformation

Review both:

- Delegated permissions (OAuth2PermissionGrants)
- Application permissions (AppRoleAssignments).

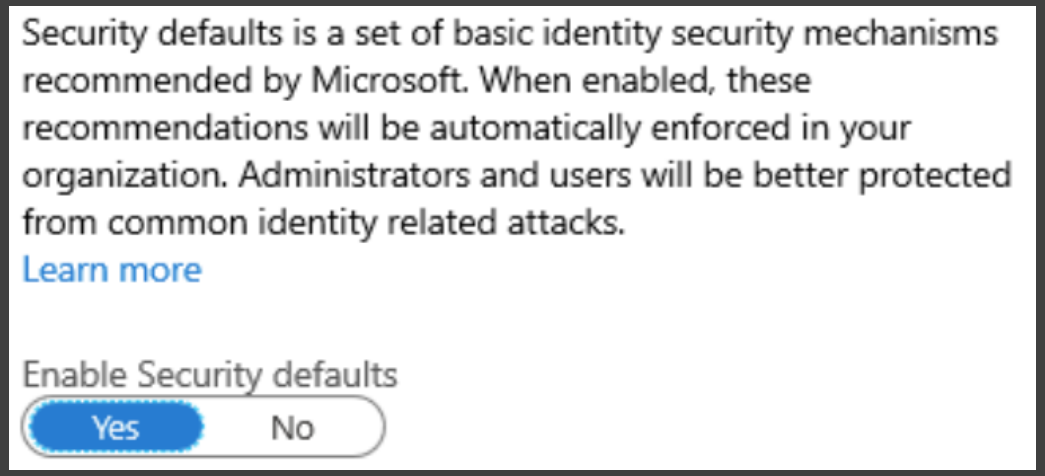
*Courtesy of Philippe Signoret

Review output, especially:

- consents that are of ConsentType of 'AllPrincipals'.
- discrete permissions that each delegated permission or application has
- specific users that have consents granted. If high profile or high impact users have inappropriate consents granted, you should investigate further.
- ClientDisplayName for apps that seem suspicious.

https://gist.github.com/psignoret/41793f8c6211d2df5051d77ca3728c09

Enable Security Defaults



If Not Currently Leveraging Conditional Access Policies
(Enabled on Tenants Created after Oct 22nd, 2019)

Security Defaults

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

Leverage Conditional Access Policies

1

Limit/Disable Legacy Authentication

2

Enforce MFA for Role Members

3

Restrict Access to Office 365 Services & SAAS Apps

Monitor Azure AD & Office 365 Logs

Pull Logs into Existing SIEM or Leverage Azure Sentinel

Review Microsoft Secure Score

Work on "Quick Wins" – items with low user impact & low effort.

Microsoft Secure Score

Microsoft Secure Score has made some updates to your available improvement actions. Learn more

Explore new features and give feedback on Microsoft Secure Score's updated experience, in preview now! Try the preview version

Overview | Improvement actions | History

Your secure score

Total score: 116 / 303

Microsoft Secure Score analyzes the protection state of your identities, data, devices, apps, and infrastructure.

Identity **111** / 203

Protection state of your Azure AD accounts and roles

Data **5** / 35

Protection state of your Office 365 documents

Device No data to show

Protection state of your devices

Apps **0** / 65

Protection state of your email and cloud apps

Infrastructure No data to show

Protection state of your Azure resources

Learn more about Microsoft Secure Score

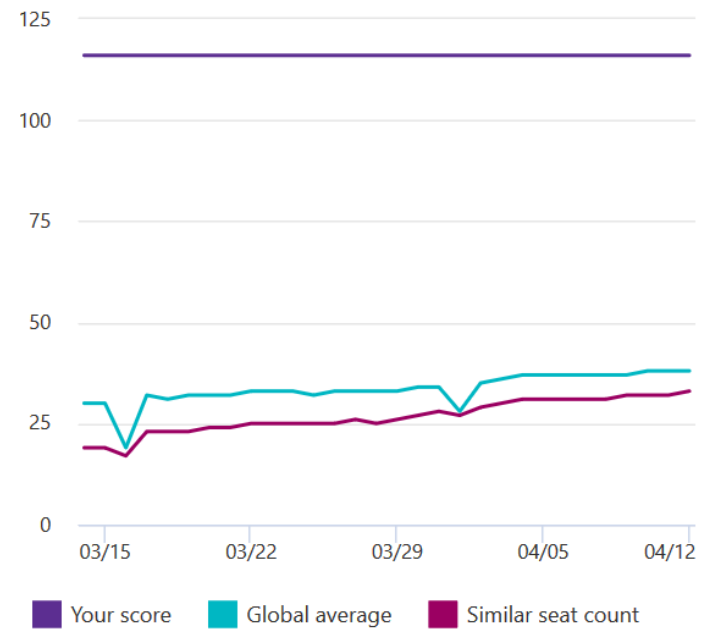
Get your score using Microsoft Graph API

History

0 points in 30 days

Total score

Your secure score over time and how you compare to other organizations.



View history

Overview | **Improvement actions** | History

Actions you can take to improve your Microsoft Secure Score. Score updates may take up to 24 hours.

Export

15 items | Search | Filter | Group by

Applied filters: Status: Not completed

Improvement action	Rank	Score	Category	User impact	Implementation cost	Portal	Status	Notes
Require MFA for administrative roles	1	25/50	Identity	Low	Low	Azure Active Directory	Not completed	-
Enable Password Hash Sync if hybrid	9	0/10	Identity	Low	Low	Azure Active Directory	Not completed	-
Ensure all users can complete multi-factor authenti...	12	9/30	Identity	High	High	Azure Active Directory	Not completed	-
Enable self-service password reset	20	0/5	Identity	Moderate	Moderate	Azure Active Directory	Not completed	-
Do not allow users to grant consent to unmanage...	35	0/10	Identity	Moderate	Low	Azure Active Directory	Not completed	-
Apply IRM protections to documents	41	0/5	Data	Moderate	Moderate	Azure Active Directory	Not completed	-
Delete/block accounts not used in last 30 days	51	0/1	Identity	Moderate	Low	Azure Active Directory	Not completed	-
Apply Data Loss Prevention policies	54	0/20	Data	Moderate	Moderate	Microsoft Information ...	Not completed	-
Set automated notifications for new OAuth applica...	57	0/20	Apps	Moderate	Low	Microsoft Cloud App S...	Not completed	-
Enable policy to block legacy authentication	68	0/20	Identity	Moderate	Moderate	Azure Active Directory	Not completed	-
Set automated notifications for new and trending ...	75	0/15	Apps	Moderate	Low	Microsoft Cloud App S...	Not completed	-
Create a custom activity policy to discover suspicio...	80	0/10	Apps	Moderate	Low	Microsoft Cloud App S...	Not completed	-
Discover trends in shadow IT application usage	82	0/5	Apps	Low	Moderate	Microsoft Cloud App S...	Not completed	-
Use Cloud App Security to detect anomalous beha...	107	0/15	Apps	Low	Low	Microsoft Cloud App S...	Not completed	-
Turn on customer lockbox feature	127	0/5	Data	Moderate	Moderate	Exchange Online	Not completed	-

Microsoft Secure Score

Microsoft Secure Score has made some updates to your available improvement actions. Learn more

Explore new features and give feedback on Microsoft Secure Score's updated experience, in preview now! Try the preview version

Overview | **Improvement actions** | History

Actions you can take to improve your Microsoft Secure Score. Score updates may take up to 24 hours.

Export | 15 items | Search | Filter | Group by

Applied filters: Status: Not completed

Improvement action	Rank	Score	Category	User impact	Implementation cost	Portal	Status	Notes
Require MFA for administrative roles	1	25/50	Identity	Low	Low	Azure Active Directory	Not completed	-
Enable Password Hash Sync if hybrid	9	0/10	Identity	Low	Low	Azure Active Directory	Not completed	-
Discover trends in shadow IT application usage	82	0/5	Apps	Low	Moderate	Microsoft Cloud App S...	Not completed	-
Use Cloud App Security to detect anomalous beha...	107	0/15	Apps	Low	Low	Microsoft Cloud App S...	Not completed	-
Enable self-service password reset	20	0/5	Identity	Moderate	Moderate	Azure Active Directory	Not completed	-
Do not allow users to grant consent to unmanage...	35	0/10	Identity	Moderate	Low	Azure Active Directory	Not completed	-
Apply IRM protections to documents	41	0/5	Data	Moderate	Moderate	Azure Active Directory	Not completed	-
Delete/block accounts not used in last 30 days	51	0/1	Identity	Moderate	Low	Azure Active Directory	Not completed	-
Apply Data Loss Prevention policies	54	0/20	Data	Moderate	Moderate	Microsoft Information ...	Not completed	-
Set automated notifications for new OAuth applica...	57	0/20	Apps	Moderate	Low	Microsoft Cloud App S...	Not completed	-
Enable policy to block legacy authentication	68	0/20	Identity	Moderate	Moderate	Azure Active Directory	Not completed	-
Set automated notifications for new and trending ...	75	0/15	Apps	Moderate	Low	Microsoft Cloud App S...	Not completed	-
Create a custom activity policy to discover suspicio...	80	0/10	Apps	Moderate	Low	Microsoft Cloud App S...	Not completed	-
Turn on customer lockbox feature	127	0/5	Data	Moderate	Moderate	Exchange Online	Not completed	-
Ensure all users can complete multi-factor authenti...	12	9/30	Identity	High	High	Azure Active Directory	Not completed	-

Other Regular Review Items

- Review Microsoft 365 Security Center reports
  https://security.microsoft.com/homepage
- Review Exchange Forms/Rules for potentially malicious settings.
  https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/detect-and-remediate-outlook-rules-forms-attack?view=o365-worldwide
- Review Illicit Consent Grants
  https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/detect-and-remediate-illicit-consent-grants?view=o365-worldwide
- Review Exchange Online mailbox permissions for unusual/unintended configuration (Get-ExoMailboxPermission)
  https://docs.microsoft.com/en-us/powershell/module/exchange/powershell-v2-module/get-exomailboxpermission?view=exchange-ps

Office 365 Security Checklist

1. Limit Global Admins to <5.
2. Enforce Multi-Factor Authentication (MFA) for All Role Admins.
3. Use Azure Privileged Identity Management (PIM).
    1. Control Role Groups with PIM
    2. Control Service Admin Roles with PIM
4. Secure Global Admin Authentication.
    1. Separate Admin Account
    2. Require MFA
    3. Use Cloud Admin Workstations
    4. Configure for FIDO2 authentication
5. Configure 2 Emergency Global Admin Accounts.
6. Protect Azure AD Connect Server like a DC.
7. Ensure Azure AD Connect is Running the Current Version.
8. Configure Security Defaults OR Conditional Access policies.
9. Review Application Permissions & Consent.
10. Monitor Azure AD & Office 365 Logs.
11. Review Microsoft Secure Score
12. Determine if Tenant Restrictions makes sense.

Sean Metcalf (@Pyrotek3)
sean @ Trimarc Security .com
www.ADSecurity.org
TrimarcSecurity.com

References

- Protect Global Admins
  https://docs.microsoft.com/en-us/office365/enterprise/protect-your-global-administrator-accounts
- Admin Roles in Office 365
  https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/directory-assign-admin-roles
- Review Role Membership in the portal
  https://portal.azure.com/#blade/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/RolesAndAdministrators
- Azure PIM documentation
  https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/
- Review PIM configuration
  https://portal.azure.com/#blade/Microsoft_Azure_PIMCommon/ResourceMenuBlade/quickstart/resourceId//resourceType/tenant/provider/aadroles
- Create 2 emergency (break-glass) administrator accounts
  https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/directory-emergency-access
- Protect Azure AD Connect like a DC
  https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-install-prerequisites
- Ensure Azure AD Connect is running the current version
  https://docs.microsoft.com/en-us/azure/active-directory/hybrid/reference-connect-version-history
- Azure AD Permissions Review Script
  https://gist.github.com/psignoret/41793f8c6211d2df5051d77ca3728c09
- Azure AD Security Defaults
  https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/concept-fundamentals-security-defaults
- Configure Tenant Restrictions
  https://techcommunity.microsoft.com/t5/azure-active-directory-identity/new-enhanced-access-controls-in-azure-ad-tenant-restrictions-is/ba-p/245194
- 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/

TEC TALKS

The Experts Conference

Sponsored by Quest®

TheExpertsConference.com

Q&A: Enter in the Q&A feature.

Register for TEC at TheExpertsConference.com