



# Cloudy Vision: How Cloud Integration Complicates Security

Sean Metcalf  
Trimarc

# Sean Metcalf

- Founder Trimarc ([Trimarc.io](https://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, Troopers
- Security Consultant / Researcher
- AD Enthusiast - Own & Operate [ADSecurity.org](https://adsecurity.org) (Microsoft platform security info)

# Agenda

- The Cloud
- Cloud Security Challenges
- Getting into Cloud Security
- Cloud Service Discovery
- Attacking Federation
- Attacking On-Prem Cloud Integration
- Attacking Cloud Administration
- Cloud App Permission Exploitation



# **The Cloud Is Magic!**









# Anywhere Cloud Access

## SaaS Applications



## Azure AD (eSTS)



login.microsoftonline.com



# Azure Active Directory in the Marketplace

Every Office 365 and Microsoft Azure customer uses Azure Active Directory

17.5<sub>M</sub>

organizations



1.1<sub>B</sub>

identities



634<sub>k</sub>

3<sup>rd</sup> party apps  
in Azure AD



90<sub>k</sub>

paid Azure AD /  
EMS customers



450<sub>B</sub>

monthly  
authentications



90%

of Fortune 500  
companies



Source: Microsoft Ignite Conference 2018

<https://myignite.techcommunity.microsoft.com/sessions/64565?source=sessions>

Sep 2018

# Cloud Active Directory?

## **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
  - SAML 2.0
  - OpenID Connect
  - OAuth 2.0
  - WS-Federation
- REST API: AD Graph API

# Attackers Love the Cloud

## Common Passwords Attempted in Password Spray Attacks

Password	Spring	2018
Summer	September	1234
Winter	Football	Your Company Name

The threats are real, global, and target all of us

**1.29 Billion**

Authentications blocked in August 2018

**81%** of data breaches involved weak, default, or stolen passwords

Source: Microsoft Ignite Conference 2018

# Cloud Security Challenges





# 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.
- What services and data is private vs what's public isn't always obvious.
- Different paradigm.
- General lack of knowledge.

# Getting Into Cloud Security

- Microsoft, Amazon AWS, & Google GCP
- IAAS or SAAS?
  - Infrastructure As A Service (IAAS)
  - Service As A Service (SAAS)
- Microsoft: Office 365 and Azure.
- Barriers:
  - Cost
  - Rapid Pace (can be an advantage – find a niche & **own it!**).
  - Each vendor's solution is very different (naming, capability, etc).

# Acme Corporation

- Company founded in 1808.
- Global company headquartered in Las Vegas, Nevada.
- Largest manufacturer & distributor of anvils in the world.
- 500k users in 140 countries (anvils are big business).
- Started thinking about moving all on-prem infrastructure cloud (except manufacturing systems).
- Just hired a new visionary CIO...

**ACME AMERICAN WROUGHT ANVILS**

**THEY RING LIKE A BELL.** No other make, English or American, surpasses our ACME in design, material or finish. It is well known in the shops of the world, and at home, for its sound of steel gives it the best and warranted reputation. None has sufficient strength or stability and perfect finish; like few anvils, it rings clear, true and loud, and is used in a special instance in that there gives notice of workmen's plans, and its perfect finish and perfect shape. The sound of the anvil and the ring of the bell are the best and the best of the world.

**WE HAVE THE EXCLUSIVE SALE OF THE ACME.** We have the right of the factory that makes them, and get them in the best of the world in the best of the world. We and your world, like everyone, in the world, we have the best of the world in the best of the world.



**ONLY 92c 15c**

**You Save More Money**

The low prices on hardware in our catalog are lower still in this book. Over 3,000 hardware items reduced.

Local Phone 15c

Priority #1:  
We're going to the cloud!



Wile E. Coyote  
CIO  
Acme Corporation



# Attacking The Cloud



# Cloud Discovery

## What can we find?



# Cloud Recon: DNS MX Records

- Proofpoint (pphosted)
- Microsoft Office 365: DOMAIN-COM.mail.protection.outlook.com
- Cisco Email Security (iphmx)
- Message Labs
- Mimecast
- Google Apps (G Suite):  
\*.google OR \*.gmail.com
- FireEye (fireeyecloud.com)
- ForcePoint (mailcontrol.com)

Name	Value
----	-----
pphosted.com	296
outlook.com	186
iphmx.com	67
message1abs.com	60
mimecast.com	57
google.com	25
fireeyecloud.com	9
mailcontrol.com	6
googlemail.com	5

# Cloud Recon: DNS TXT Records

**MS = Microsoft Office 365**

**Google-Site-Verification = G Suite**

**Docusign = Docusign digital signatures**

**Adobe IDP**

**Amazonses = Amazon Simple Email**

**Facebook**

**Atlassian-\* = Atlassian services**

**GlobalSign**

**AzureWebsites = Microsoft Azure**

**Dropbox**

MS	851
google-site-verification	509
docusign	247
adobe-idp-site-verification	210
amazonses	158
facebook-domain-verification	141
atlassian-domain-verification	111
globalsign-domain-verification	109
v	76
azurewebsites	48
dropbox-domain-verification	24
cisco-ci-domain-verification	22
Dynatrace-site-verification	16
have-i-been-pwned-verification	11
status-page-domain-verifica...	7
OSIAGENTREGURL	7
workplace-domain-verification	6
bugcrowd-verification	5
yandex-verification	4
cisco-site-verification	4



# Cloud Recon: Acme DNS TXT Records

What do we know about Acme's Cloud Config?

- **Office 365** (MS=7274734)
- Atlassian
- Cisco
- Citrix
- Docusign
- Dropbox
- Facebook
- Google Site
- Team Viewer
- WebEx

```
PS C:\WINDOWS\system32> (Resolve-DnsName 'th
v=spf1 include:spf.protection.outlook.com -a
atlassian-domain-verification=JjxTtv2u8dg+QZ
ciscocidomainverification=2947343fd5dab85a29
citrix-verification-code=a5da5637-df88-4bbb-
docusign=034562ewrg5a-9143-4342-8659-39c2452
v=verifydomain MS=7274734
dropbox-domain-verification=f7wuqiwe73b8
facebook-domain-verification=22dsh0s45wegw2y
google-site-verification=jnpwbxwt0PexFgvJB3q
teamviewer-sso-verification=e6d38470a1a4fa98
webexdomainverification=7943253ade-03459-443
```

# Cloud Recon: Acme DNS TXT Records

One Misconfig (JIRA) to Leak Them All- Including NASA and Hundreds of Fortune 500 Companies!



Avinash Jain (@logicbomb\_1) Follow

Aug 2 · 7 min read

[https://medium.com/@logicbomb\\_1/one-misconfig-jira-to-leak-them-all-including-nasa-and-hundreds-of-fortune-500-companies-a70957ef03c7](https://medium.com/@logicbomb_1/one-misconfig-jira-to-leak-them-all-including-nasa-and-hundreds-of-fortune-500-companies-a70957ef03c7)



Products For teams Support

Try free

Buy now



Features

Enterprise

Pricing

Try it free

where due to some misconfiguration issues in JIRA, their internal user data, their name, email ids, their project details on which they were working, assignee of those projects and various other information were getting exposed.

# Cloud Recon: Federation

No standard naming for FS.  
Some are hosted in the cloud.

DNS query for:

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

```
Name       : adfs.██████████.com
QueryType  : A
TTL        : 299
Section    : Answer
IP4Address : ██████████

Name       : sso.██████████.com
QueryType  : A
TTL        : 899
Section    : Answer
IP4Address : ██████████

Name       : sts.██████████.com
QueryType  : A
TTL        : 86399
Section    : Answer
IP4Address : ██████████

Name       : okta.██████████.com
QueryType  : CNAME
TTL        : 299
Section    : Answer
NameHost   : ██████████.okta.com

Name       : ██████████.okta.com
QueryType  : CNAME
TTL        : 299
Section    : Answer
NameHost   : hammer-crtrs.okta.com

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



# Attacking Federation

Identity

## How to steal identities – federated style

Federation is effectively Cloud Kerberos.

Own the Federation server, own organizational cloud services.

Token & Signing certificates  $\sim$  KRBGT (think Golden Tickets)

DEF CON 25 (July 2017)



# Attacking Federation: Forging SAML Tokens

## THREAT RESEARCH BLOG POST

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

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

### ADFSpoof

<https://github.com/fireeye/adfs spoof>

A python tool to forge AD FS security tokens.

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

### Detailed Description

ADFSpoof has two main functions:

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

This tool is meant to be used in conjunction with ADFSdump. ADFSdump runs on an AD FS server and outputs important



# Attacking Federation: ADFS Persistence

## *I Am ADFS and So Can You*

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

### Adapt or die

- Kill/suspend service, replace DLL, restart
- Verify success!
- Depending on adapter:
  - Different methods to patch
  - Different logging methods
- Same knowledge can be used dynamically
  - In-memory patching stealthy, more technically complex
  - Doesn't persistent restarts without a persistent "shim"

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

## **I AM AD FS AND SO CAN YOU**

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

**Douglas Bienstock and Austin Baker**

Principal Consultants, FireEye Mandiant

# Attacking Federation: ADFS Persistence

I Am ADFS and So Can You

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

Adapt or die

Process Explorer Search

Handle or DLL substring: duo

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

- Same know
- In-memor
- Doesn't pe

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

# Federation Server Attack Detection & Defense

- Protect federation servers (ADFS) like Domain Controllers (Tier 0).
- Protect federation certificates.
- Consolidate and correlate federation server, AD, and Azure AD logs to provide insight into user authentication to Office 365 services.
- Correlate Federation token request with AD authentication to ensure a user performed the complete auth flow.

# On-Prem: AD to Cloud Sync

- AD provides Single Sign On (SSO) to cloud services.
- Most organizations aren't aware of all cloud services active in their environment.
- Some directory sync tools synchronizes all users & attributes to cloud services.
- Most sync engines only require AD user rights to send user and group information to cloud service.
- If you have Office 365, you almost certainly have Azure AD Connect synchronizing on-prem AD user to Azure AD.

# On-Prem: AD to Cloud Sync



active directory sync directory tool



Images



Videos



Shopping

About 32,500,000 results (0.58 seconds)



# 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
<ul style="list-style-type: none"><li>• Replicate Directory Changes</li><li>• Replicate Directory Changes All</li></ul>	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        : cdc66dd0-65e2-40bc-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
```

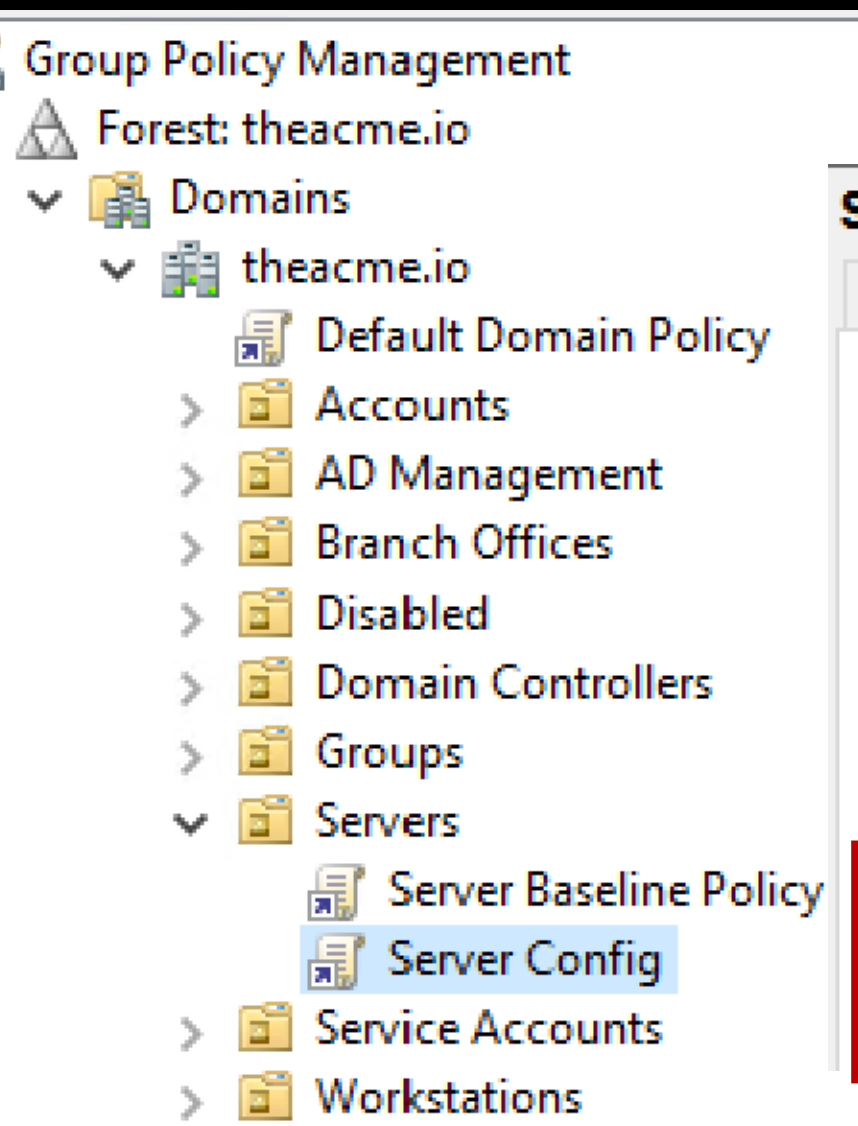


# On-Prem: Acme's Azure AD Connect

```
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  
GPONDisplayName   : 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



## 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	Read (from Security Filtering)
Domain Admins (ACME\Domain Admins)	Edit settings, delete, modify security
Enterprise Admins (ACME\Enterprise Admins)	Edit settings, delete, modify security
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.

# 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:

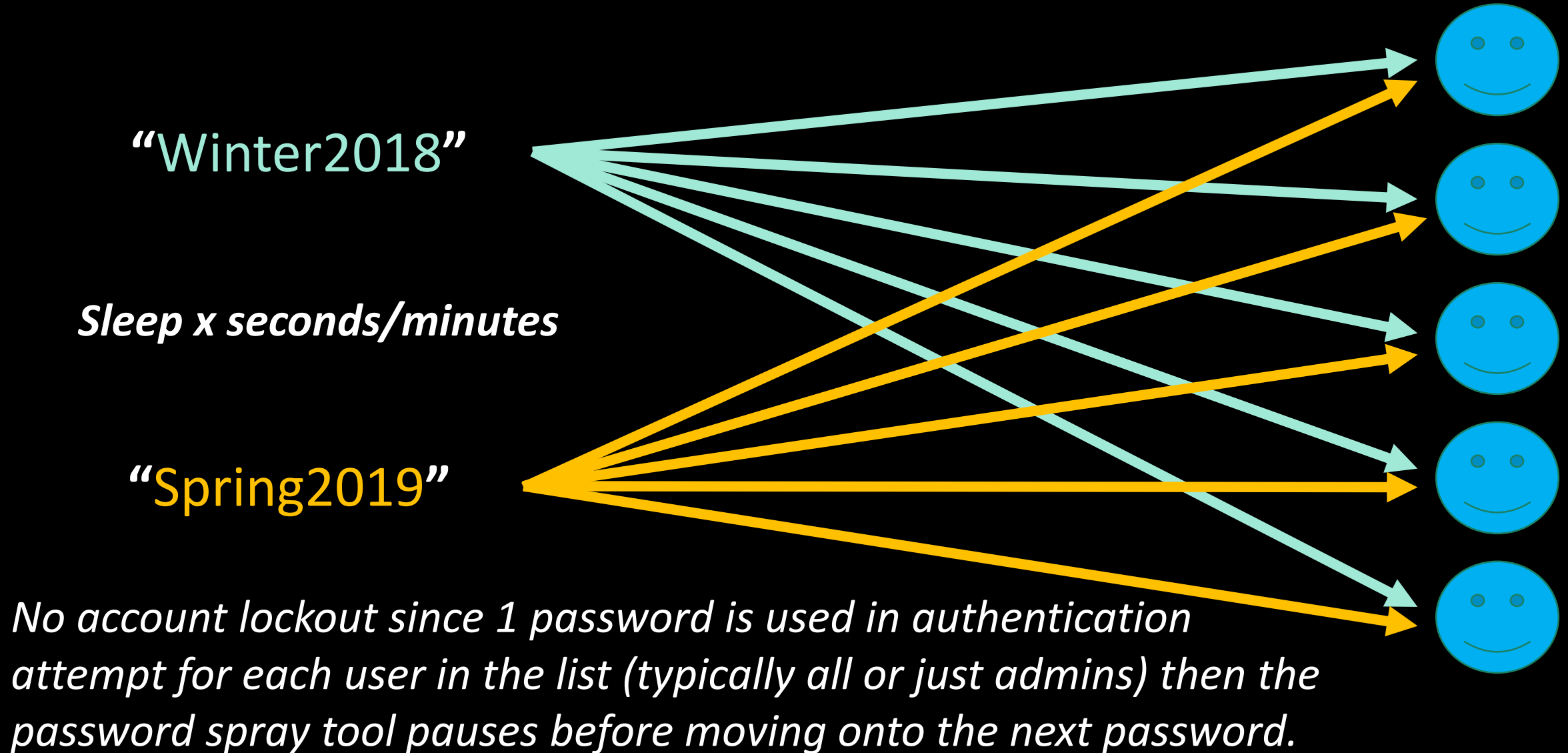
- Azure AD user can enumerate all user accounts & admin group membership with access to Office 365 services (the internet by default).
- User enumeration\* often possible without an account!



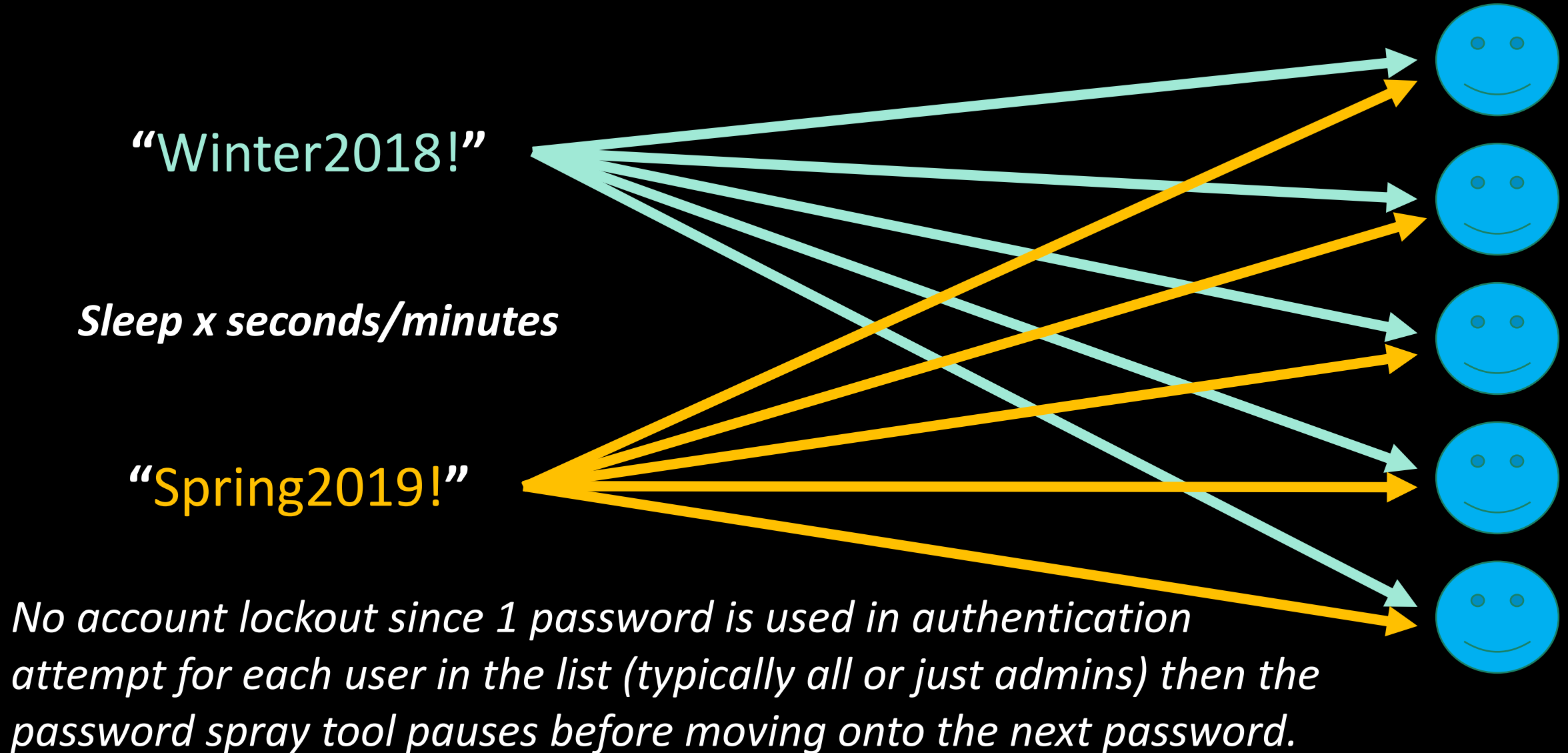
# Azure AD User Enumeration

- 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>

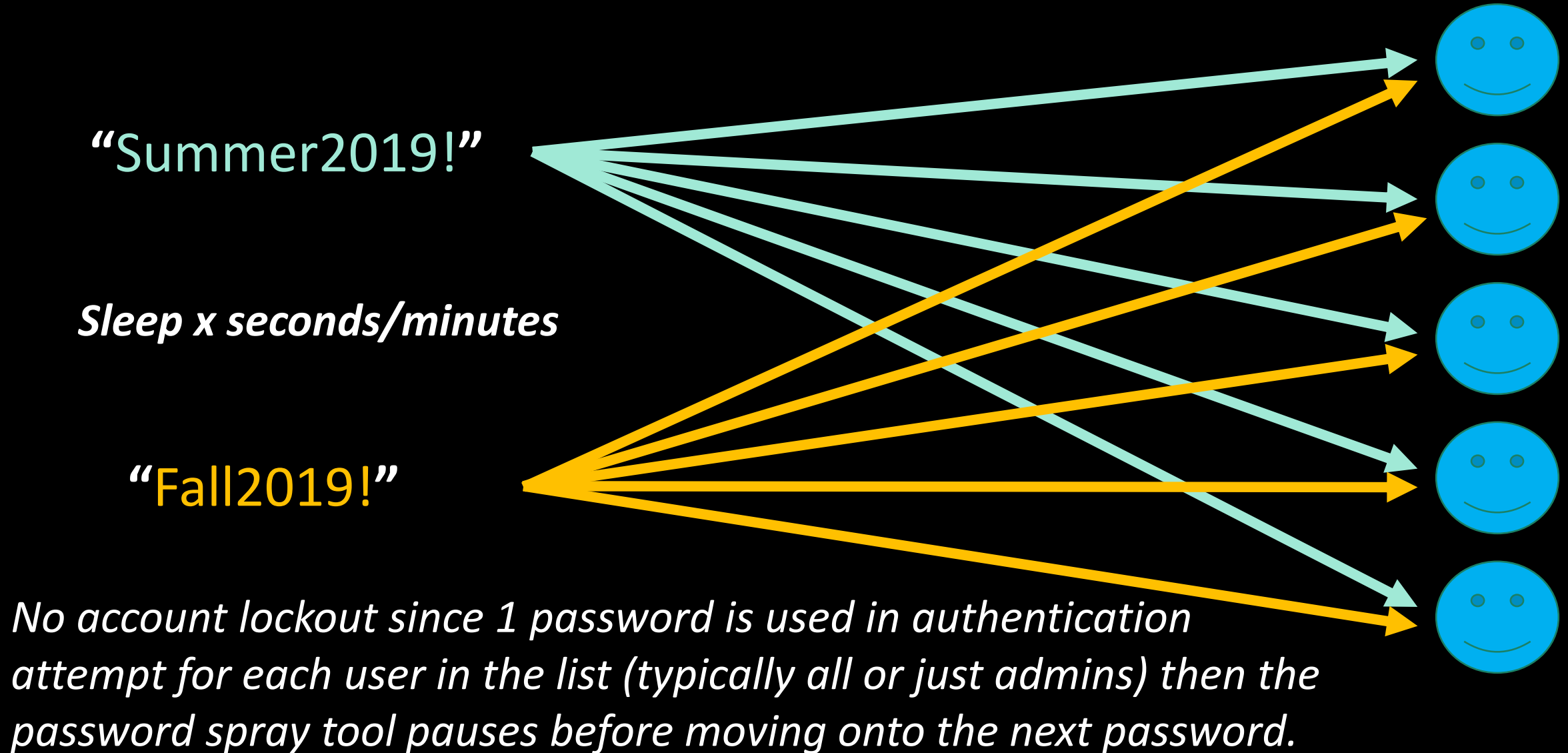
# Password Spraying Overview



# Password Spraying Overview



# Password Spraying Overview



# Attacking the Cloud: 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-0365.ps1
```

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

```
5 threads remaining
```

```
[ooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooo
```

```
+ 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)*



# 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

Acme Corporation - Sign-ins						
Azure Active Directory						
<a href="#">Download</a> <a href="#">Export Data Settings</a> <a href="#">Troubleshoot</a> <a href="#">Refresh</a>   <a href="#">Columns</a>   <a href="#">Got feedback?</a>						
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	
8/2/2019, 12:06:04 AM	Boba Fett	Office 365 Exchang...	Failure	52.168.138.234	Not Applied	

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

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
8/2/2019, 12:02:06 AM	Boba Fett	Office 365 Exchang...	Failure	52.168.138.234	Not Applied
8/2/2019, 12:04:11 AM	Boba Fett	Office 365 Exchang...	Success	52.168.138.234	Not Applied

*\*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 password	
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

# 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

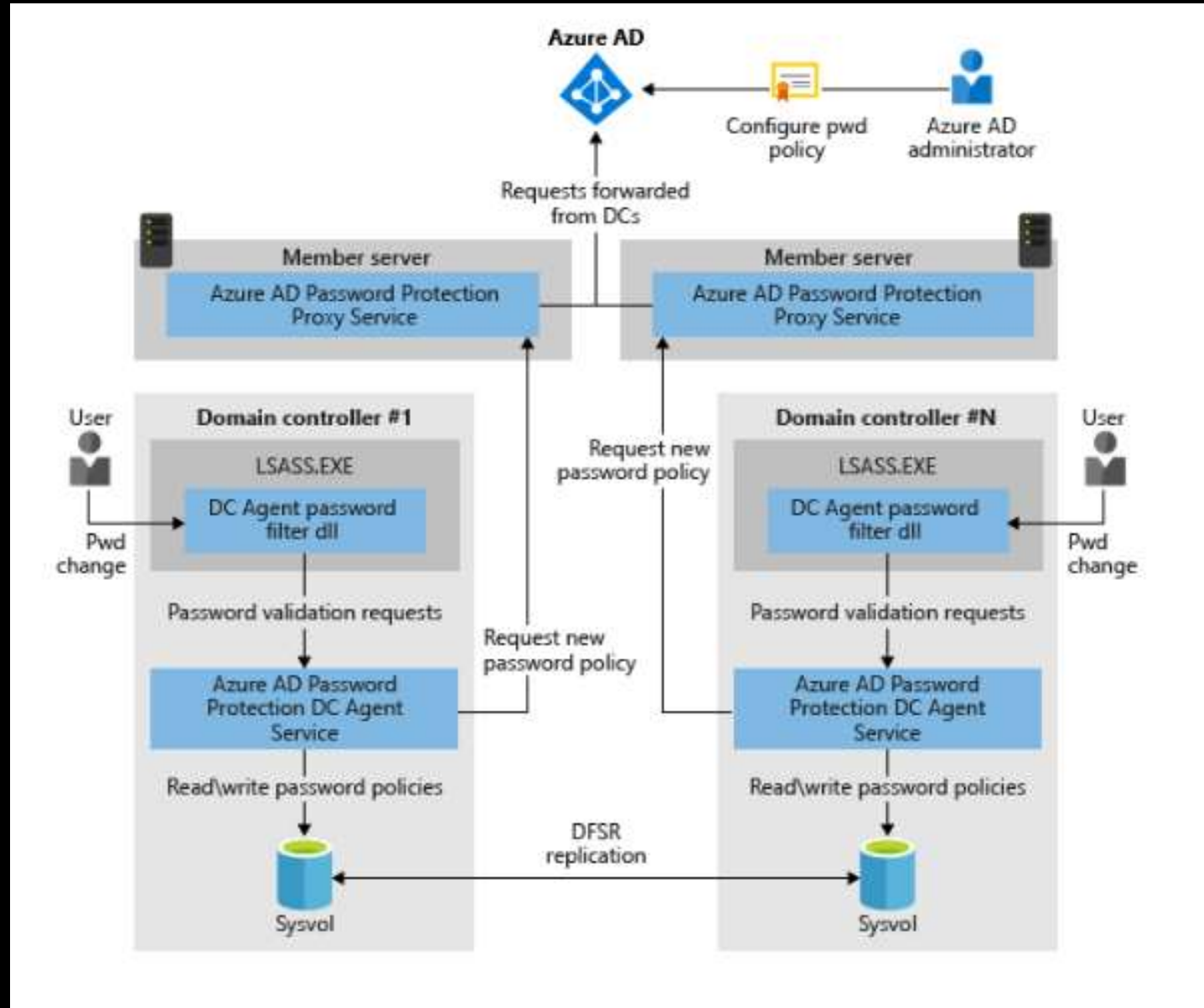
# Password Spraying Defense (ADFS)

- 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



# Attacking Cloud Administration

A promotional banner for Black Hat USA 2018. The background features a dark, stormy sky with a large, bright moon on the right and silhouettes of mountains at the bottom. The text is white and yellow.

**black hat**  
USA 2018  
AUGUST 4-9, 2018  
MANDALAY BAY / LAS VEGAS

From Workstation to Domain Admin:  
Why Secure Administration Isn't Secure and How to Fix It

Sean Metcalf  
CTO, Trimarc

🐦 #BHUSA / 🌐 BLACKHATEVENTS

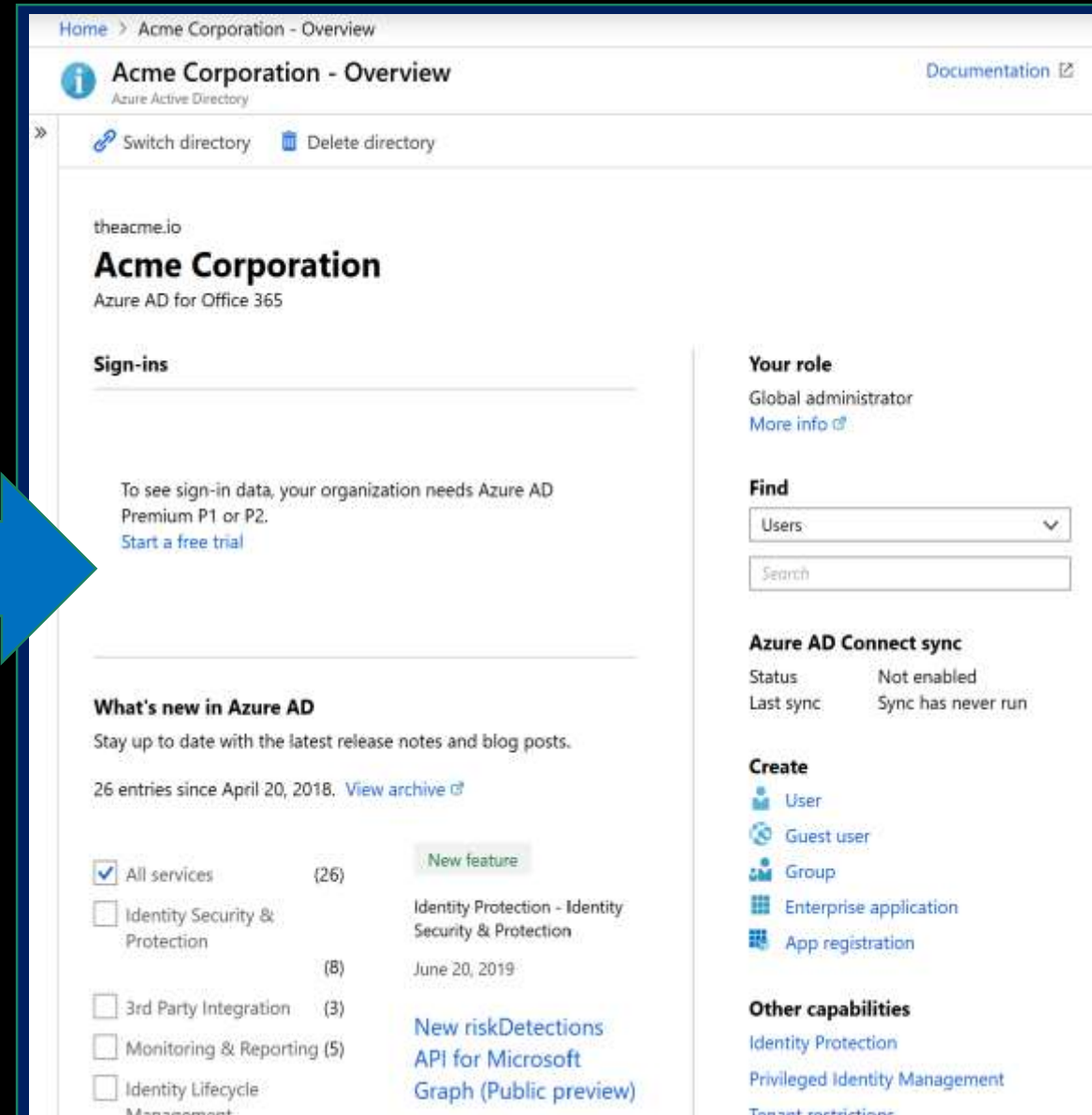
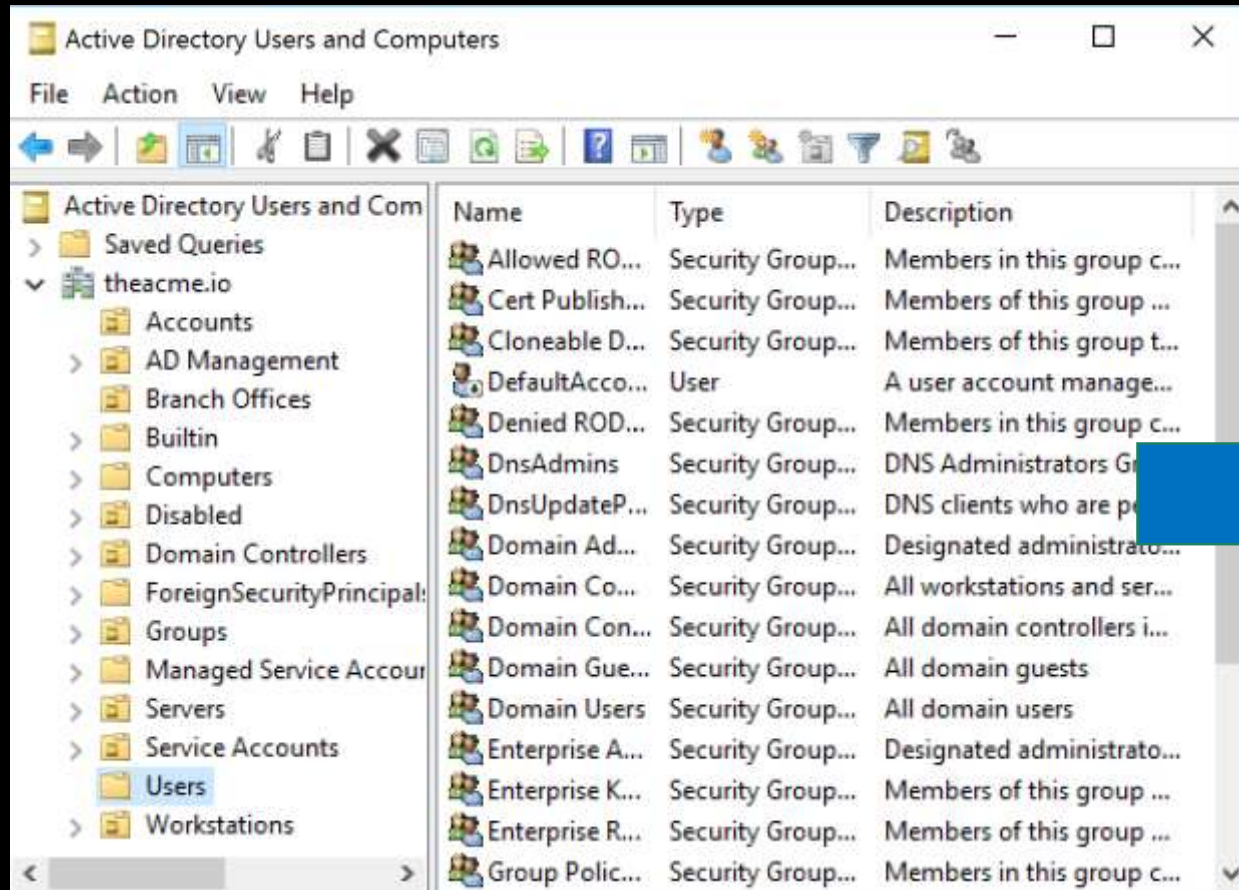
## Exploiting Active Directory Administrator Insecurities




Sean Metcalf (@Pyrotek3)  
s e a n @ a d s e c u r i t y . o r g  
[www.ADSecurity.org](http://www.ADSecurity.org)



# From On-Prem to Cloud Administration



# Attacking Cloud Administration

 **Global administrator - Assignments**  
All roles

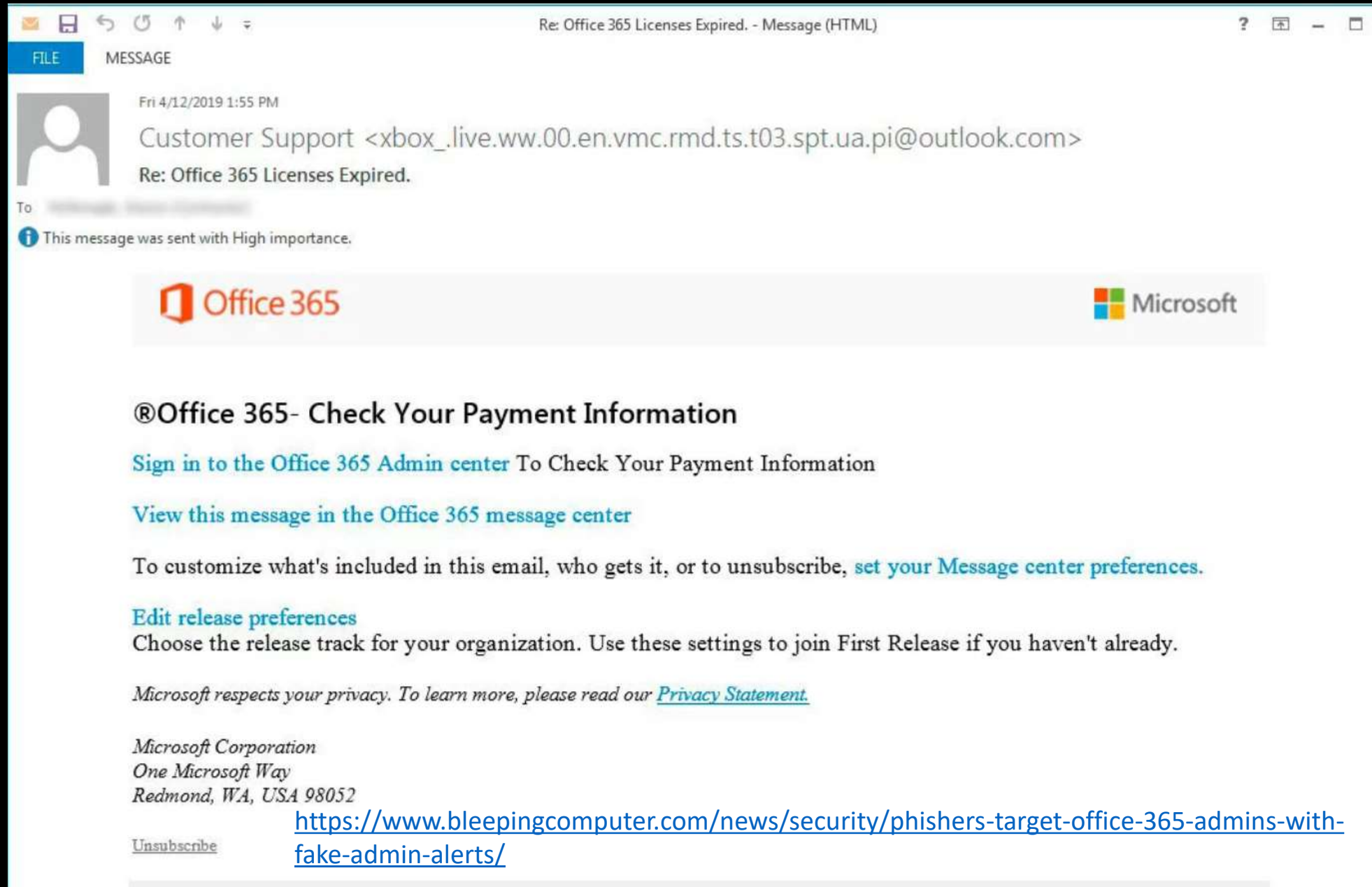
[+ Add assignment](#) [✕ Remove assignment](#) [🔄 Refresh](#) [🔗 Manage in PIM](#) | [💙 Got feedback?](#)

Search

Type

NAME	USERNAME	TYPE	SCOPE
Sean Metcalf	sean@theacmeio.onmicrosoft.com	User	Directory
Mark Morowczynski	mark@theacme.io	User	Directory
Sean Metcalf	seanmetcalf@theacme.io	User	Directory
Han Solo	hansolo@theacme.io	User	Directory
Boba Fett	SUCCESS! User:theacme.io\bobafett@theacme.io Password:Mandalorian19!		
Mace Windu	mace@theacme.io	User	Directory
Thrawn	SUCCESS! User:theacme.io\thrawn@theacme.io Password:Summer2019!		

# Attacking Cloud Administration



# 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.

# Global Reader

*Members have read-only access to reports, alerts, and can see all the configuration and settings.*

*The primary difference between Global Reader and Security Reader is that an Global Reader can access **configuration and settings**.*

- View-Only Retention Management
- View-Only Manage Alerts
- View-Only Device Management
- View-Only IB Compliance Management
- View-Only DLP Compliance Management
- Security Reader
- Service Assurance View
- View-Only Audit Logs
- View-Only Record Management
- View-Only Recipients



# Cloud Administration – Finding a Weakness

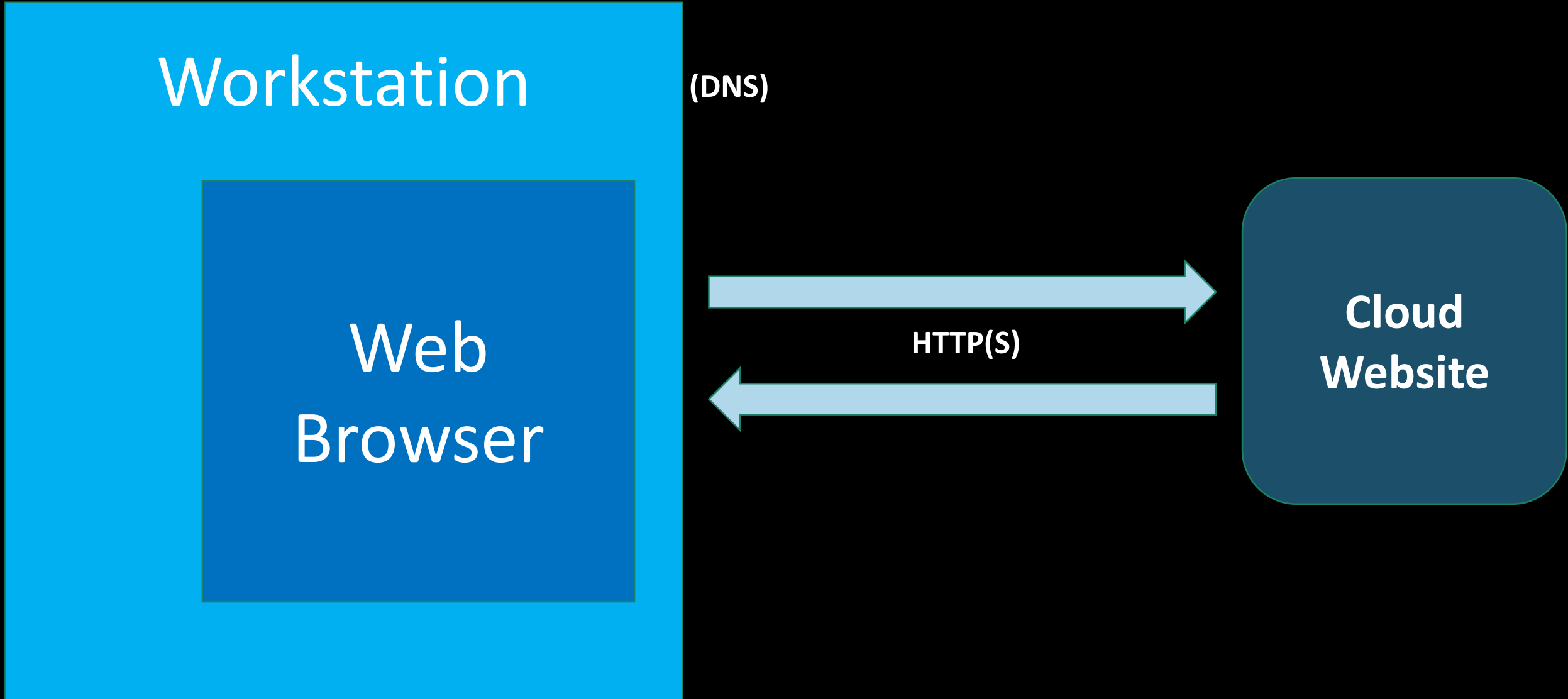
Workstation

(DNS)

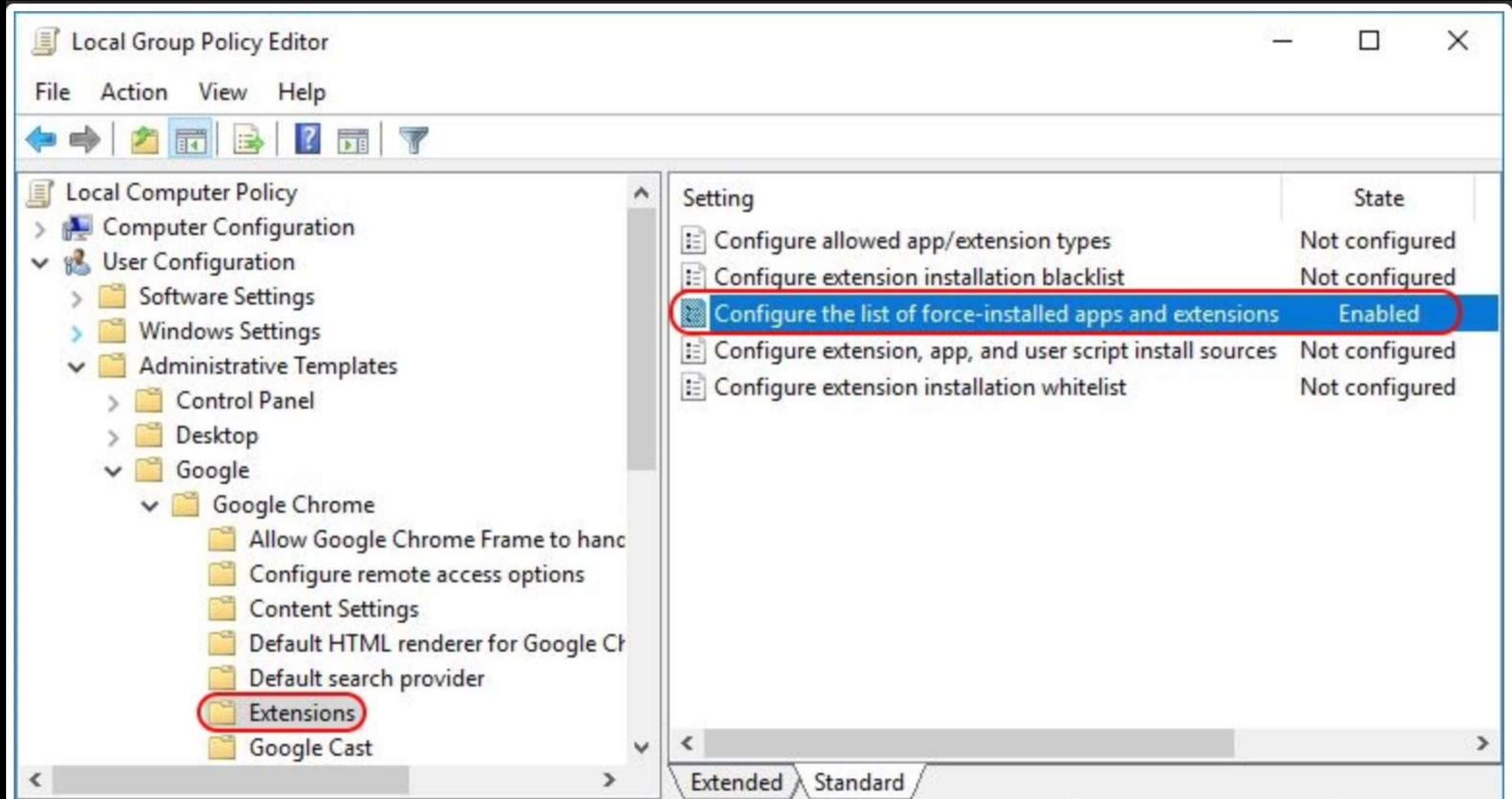
Web  
Browser

HTTP(S)

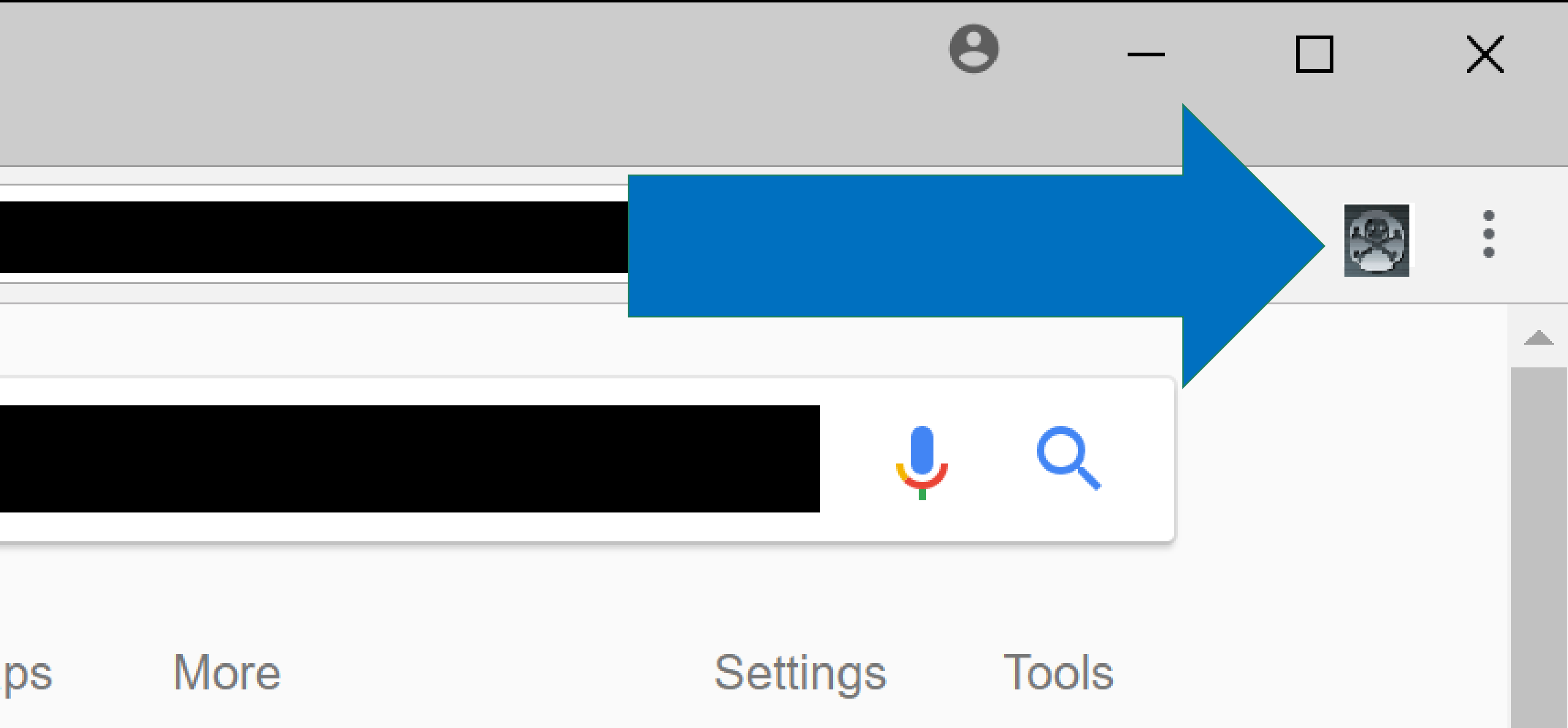
Cloud  
Website



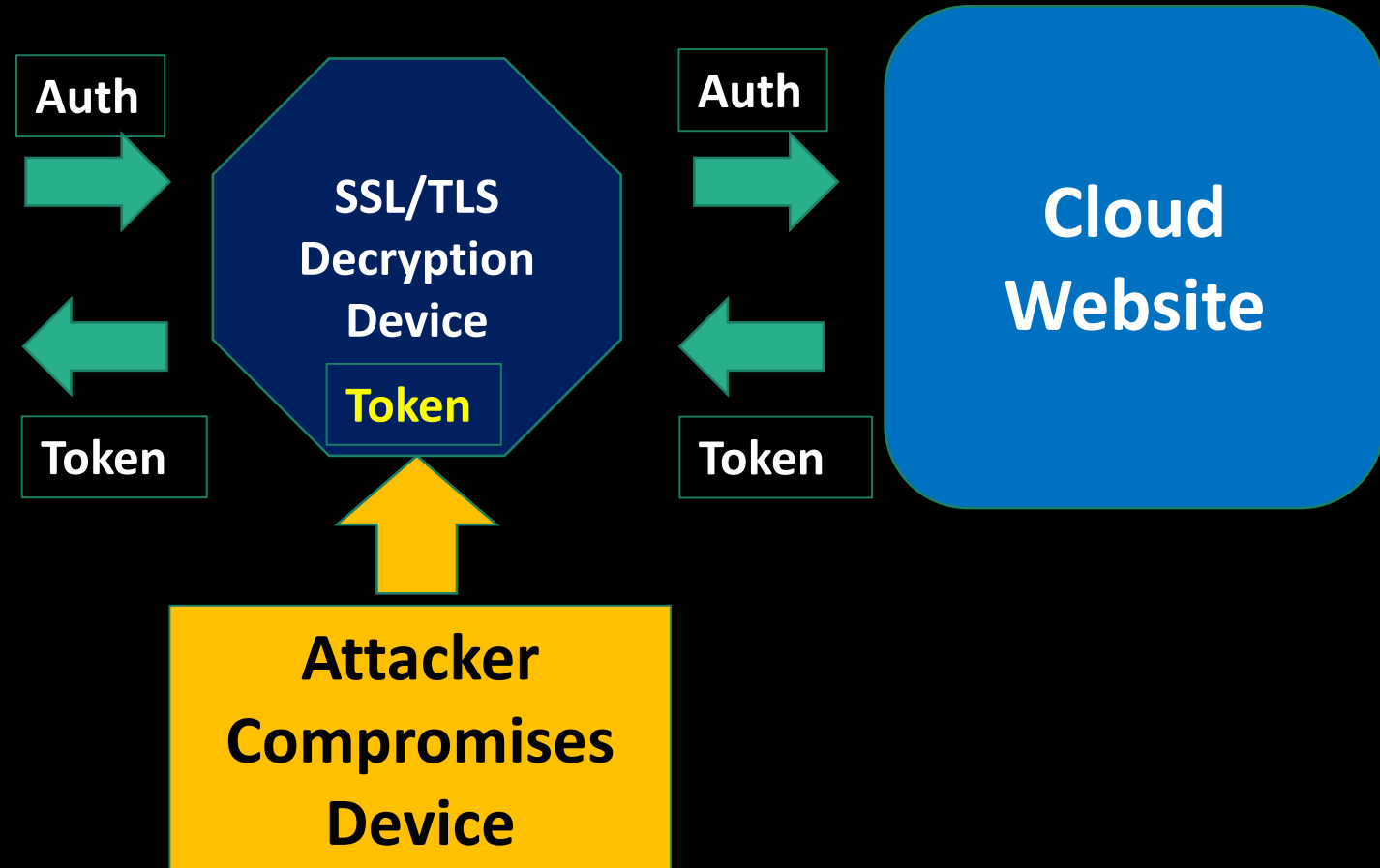
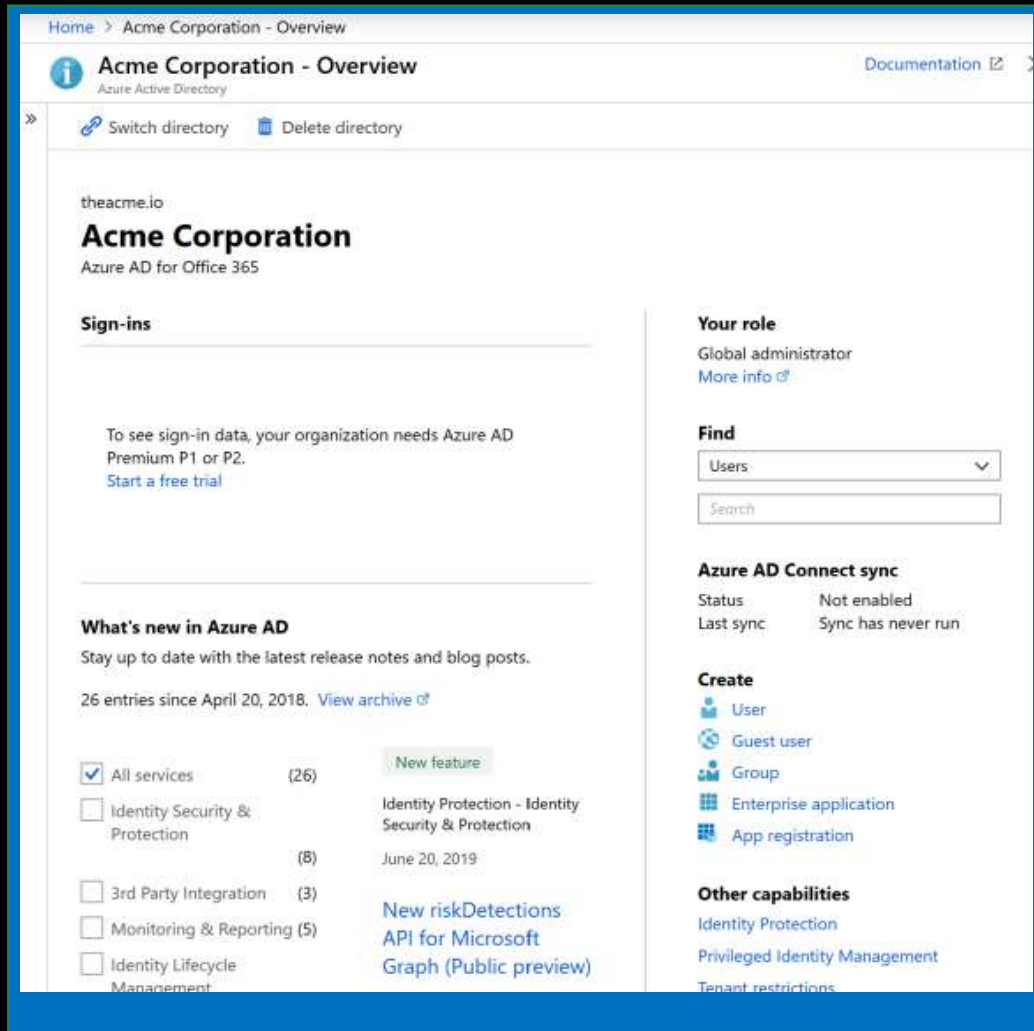
# Attacking Cloud Administration: Token Theft



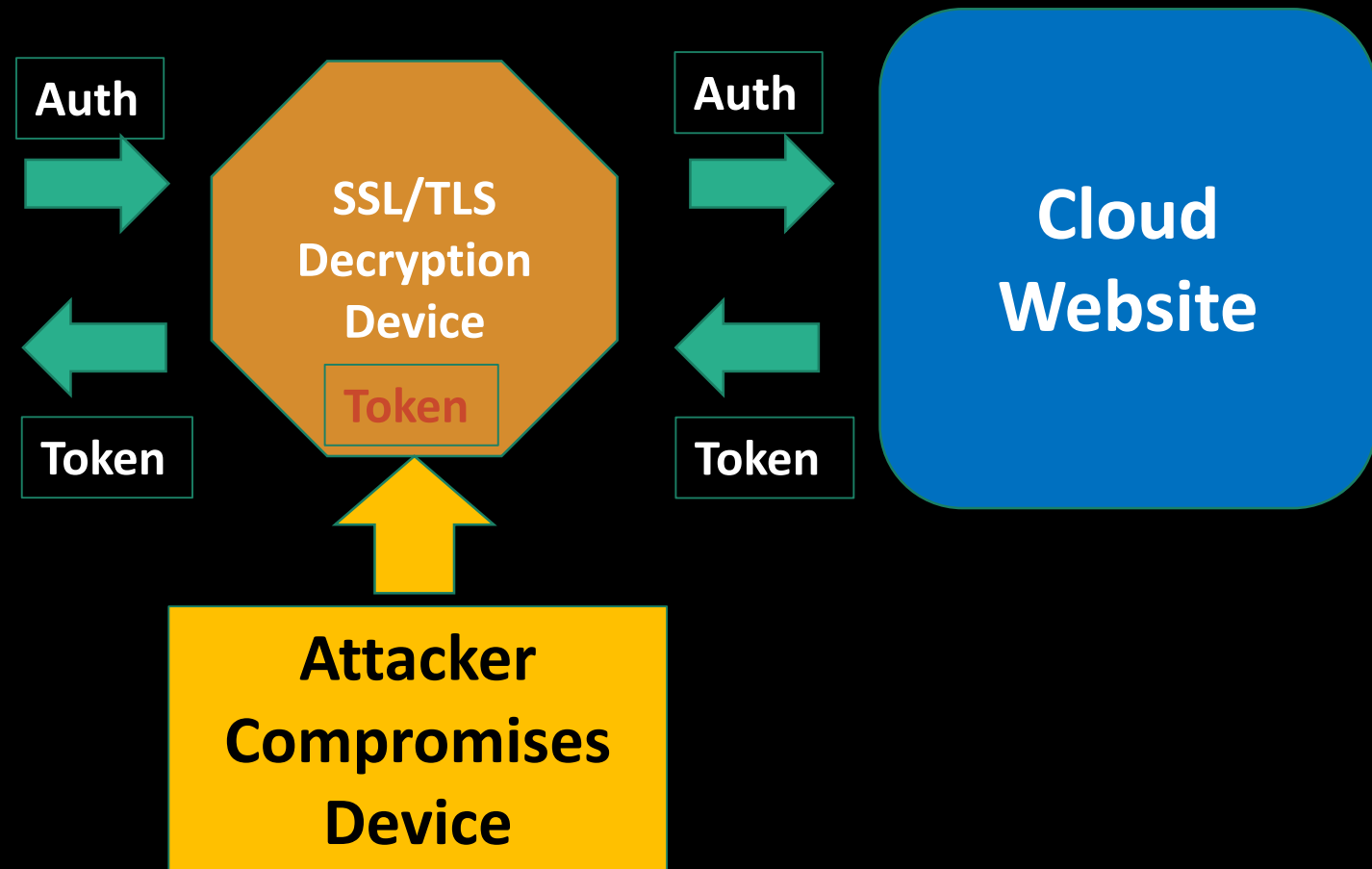
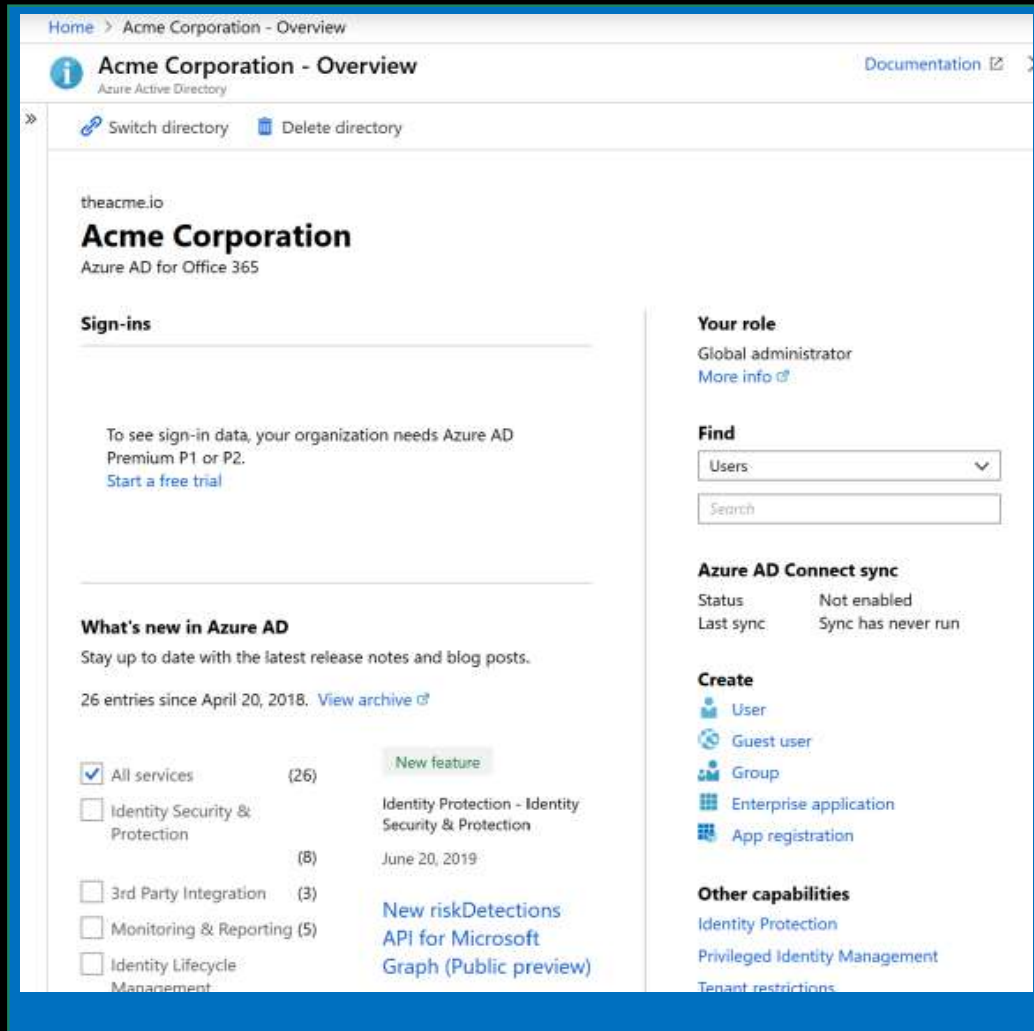
# Attacking Cloud Administration: Token Theft



# Attacking Cloud Administration: Token Theft



# Attacking Cloud Administration: Token Theft





# Attacking Cloud Administration: Token Theft

<https://aad.portalazure.com/>

Home > Acme Corporation - Overview

**Acme Corporation - Overview**  
Azure Active Directory

Switch directory Delete directory

theacme.io

**Acme Corporation**  
Azure AD for Office 365

**Sign-ins**

To see sign-in data, your organization needs a Premium P1 or P2.  
[Start a free trial](#)

**What's new in Azure AD**  
Stay up to date with the latest release notes and blog posts.  
26 entries since April 20, 2018. [View archive](#)

☒ All services (26) New feature

☐ Identity Security & Protection (8)

☐ 3rd Party Integration (3)

☐ Monitoring & Reporting (5)

☐ Identity Lifecycle Management

**Azure AD Connect sync**  
Status Not enabled  
Last sync Sync has never run

**Create**

- User
- Guest user
- Group
- Enterprise application
- App registration

**Other capabilities**

- Identity Protection
- Privileged Identity Management
- Tenant restrictions



<https://aad.portal.azure.com/>

Home > Acme Corporation - Overview

**Acme Corporation - Overview**  
Azure Active Directory

Switch directory Delete directory

theacme.io

**Acme Corporation**  
Azure AD for Office 365

**Sign-ins**

To see sign-in data, your organization needs a Premium P1 or P2.  
[Start a free trial](#)

**What's new in Azure AD**  
Stay up to date with the latest release notes and blog posts.  
26 entries since April 20, 2018. [View archive](#)

☒ All services (26) New feature

☐ Identity Security & Protection (8)

☐ 3rd Party Integration (3)

☐ Monitoring & Reporting (5)

☐ Identity Lifecycle Management

**Azure AD Connect sync**  
Status Not enabled  
Last sync Sync has never run

**Create**

- User
- Guest user
- Group
- Enterprise application
- App registration

**Other capabilities**

- Identity Protection
- Privileged Identity Management
- Tenant restrictions

<https://github.com/kgretzky/evilginx2>

# 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	luceskywalker	TheForce19	luceskywalker@Plus.com



# Password Reuse/Replay Detection

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

HavelBeenPwned.com

';--have i been pwned?

Check if you have an account that has been compromised in a data breach

Domain name

enter the domain you'd like to search

Subscribe me

☒

Notification email

enter your email address

Security

Overview (Preview)

Identity Secure Score

Conditional Access

MFA

Users flagged for risk

Risk events

Authentication methods

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

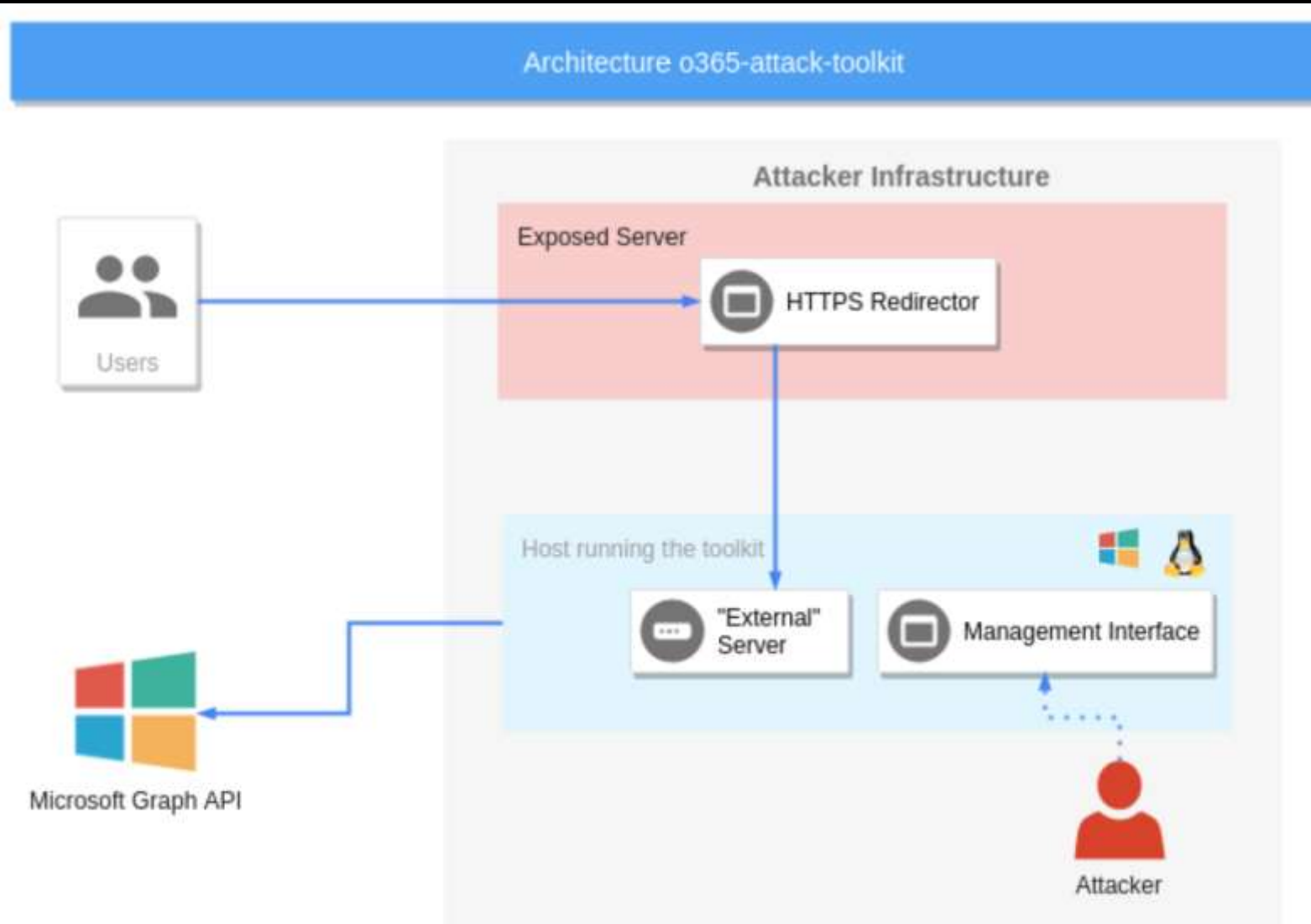
# Turn on Azure AD Connect Password Hash Sync

- 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”

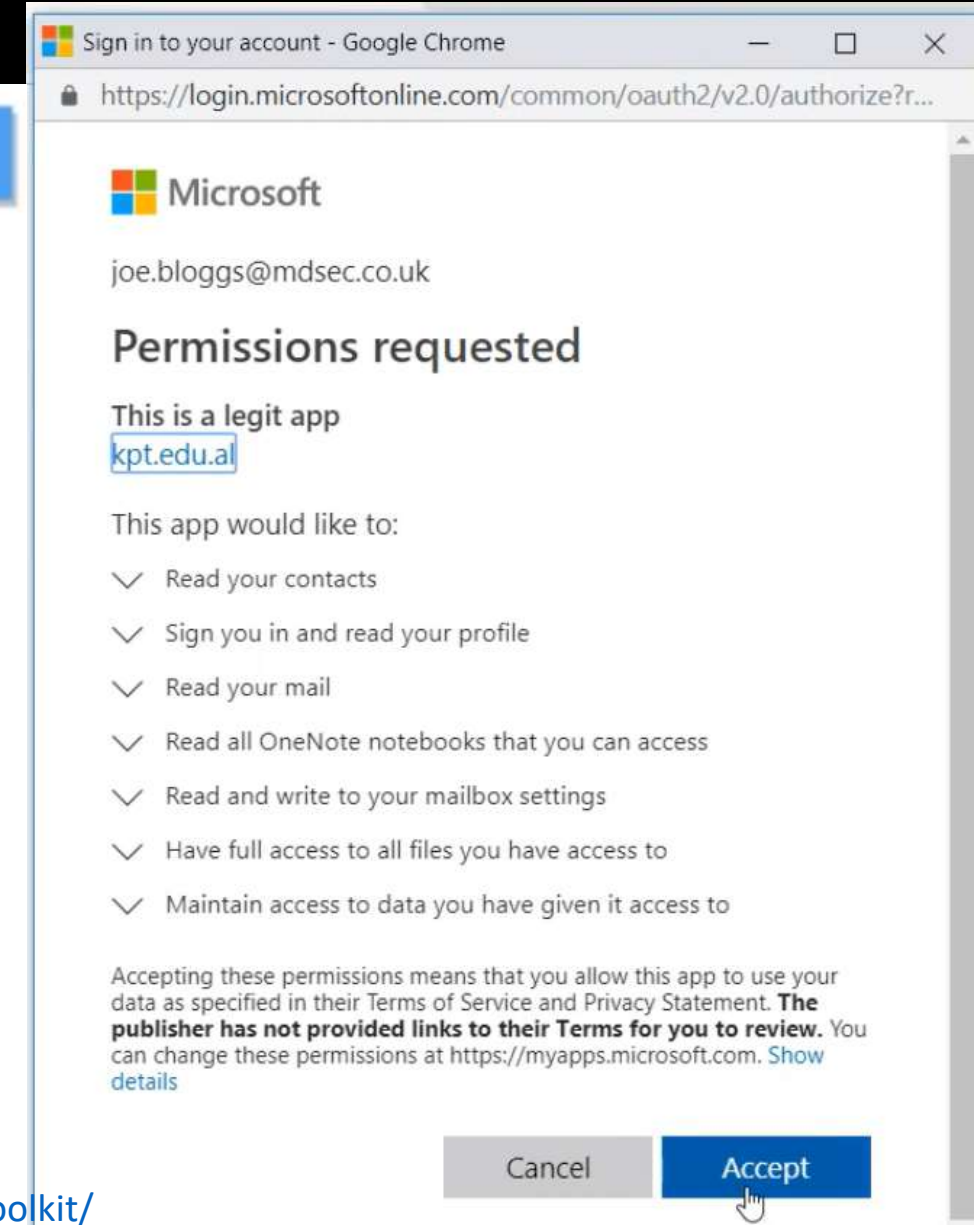
# Attacking the Cloud: App PrivEsc & Persistence

- 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.

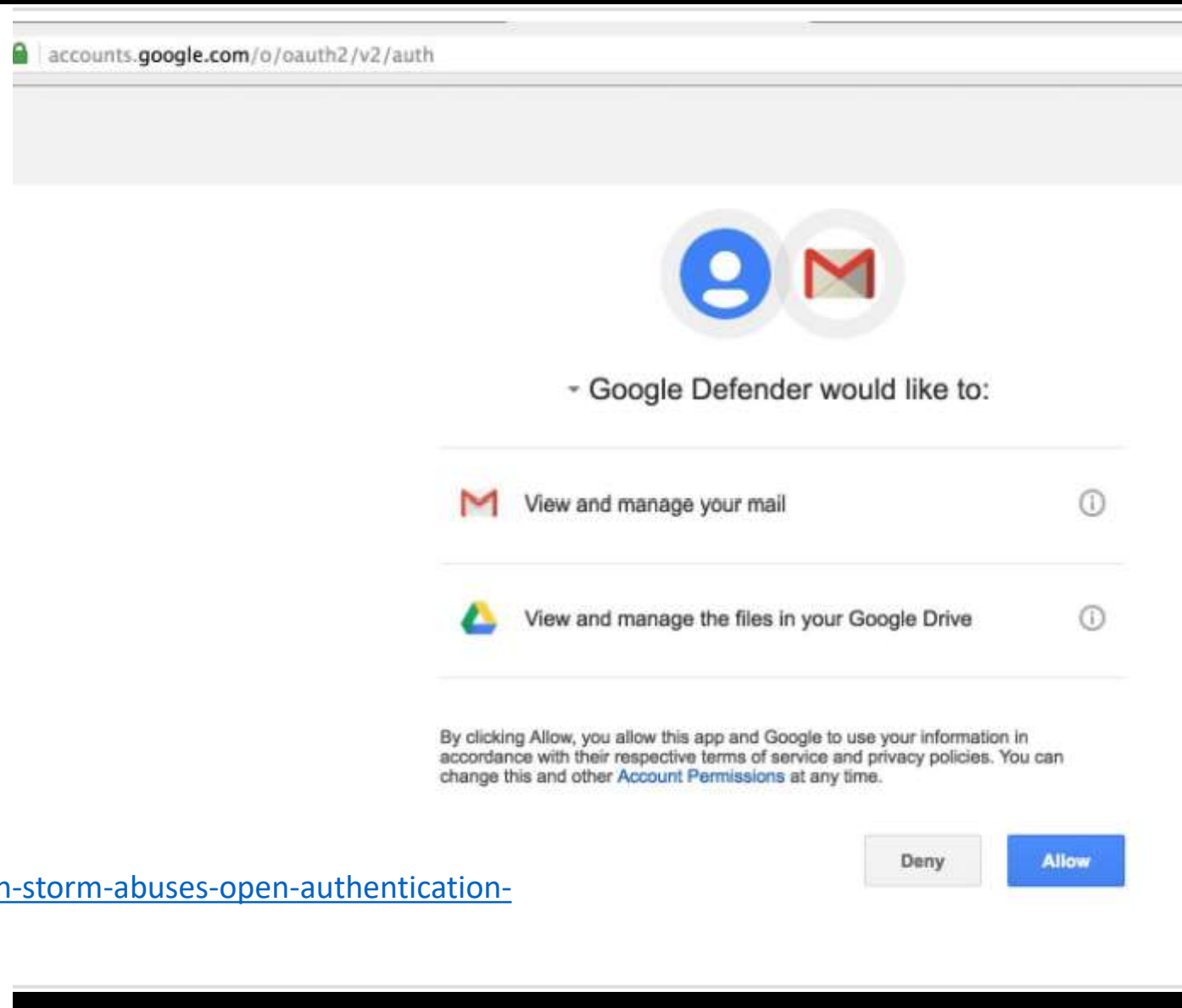
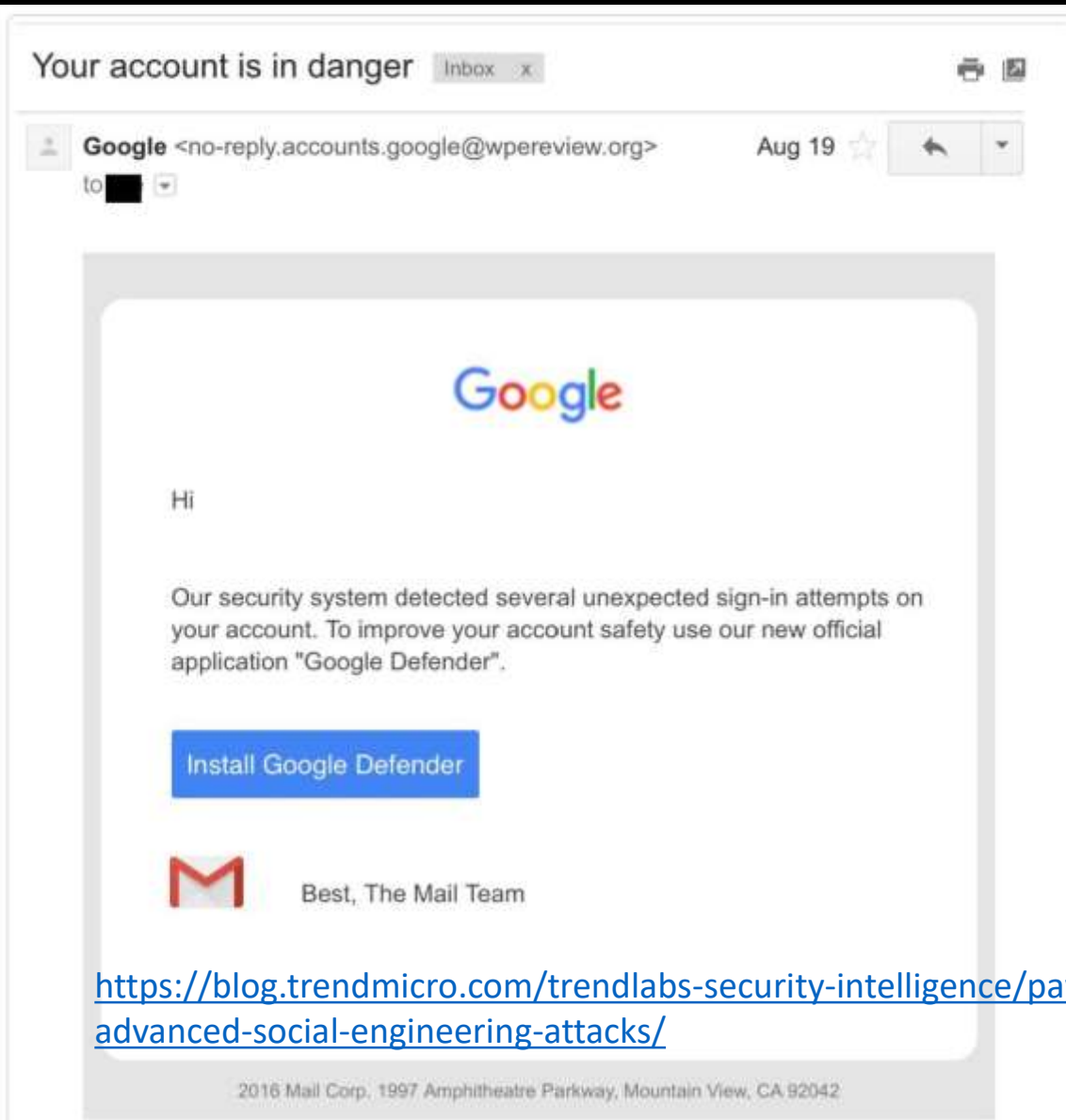
# Illicit Consent Grant Attack: MDSec O365 Attack Toolkit



<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.



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
- ✓ 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

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](#)

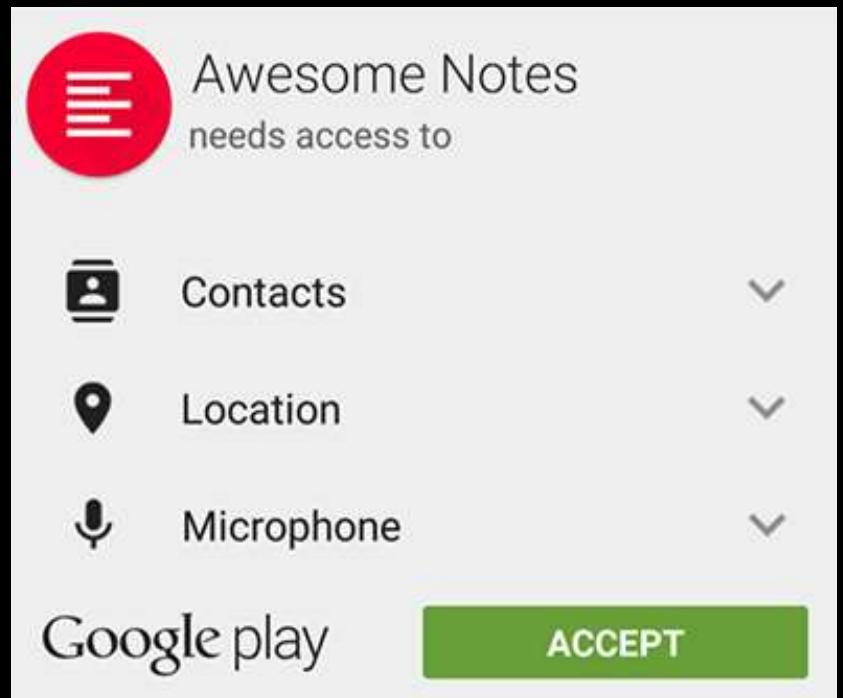
Cancel

Accept

# 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>

## 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](#)

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

# What's Next? Assemble Your Team



More in-depth Microsoft Cloud defense recommendations:

<https://adsecurity.org/?p=4179>



# 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.



# Phase 2 Go Do Soon Security Checklist

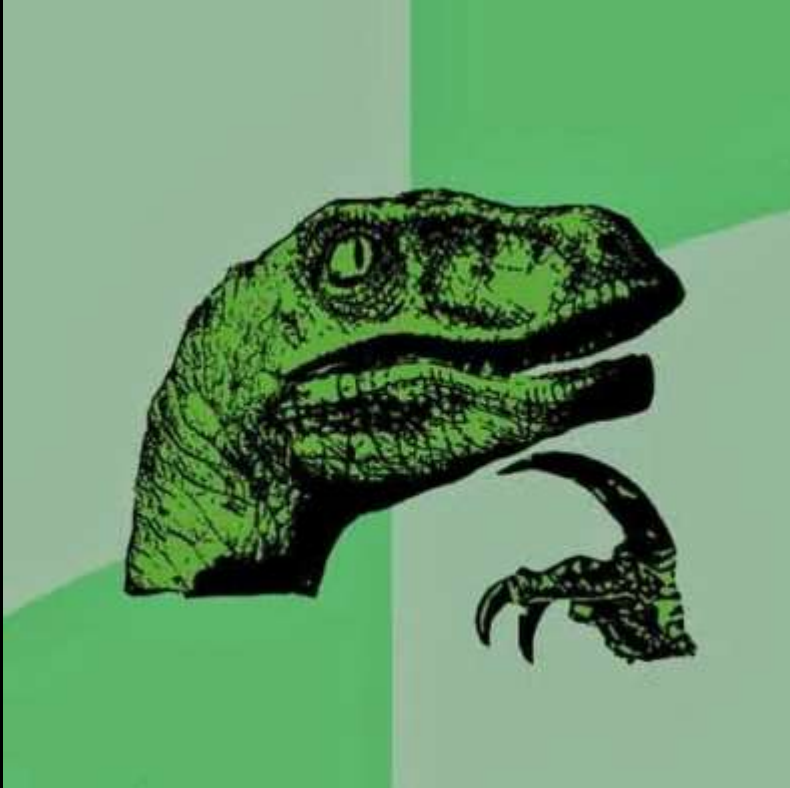
- ☐ Enable self-service password reset (SSPR).
- ☐ Enable MFA for all users via Conditional Access or Risk Based.
- ☐ Disable Legacy Authentication Entirely via Conditional Access
- ☐ FIDO for admin accounts
- ☐ Follow admin account best practices for cloud admins
- ☐ Audit consented permissions for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

# Conclusion

**The Cloud Is Magic!**



# Conclusion



- Cloud is a new paradigm that requires special attention (& resources).
- The cloud isn't inherently secure.
- Security responsibilities are shared between provider and customer.
- There are many security features and controls that are available.
- Security controls need to be researched, tested, and implemented.
- Security in the cloud may cost extra.

Slides: [Presentations.ADSecurity.org](http://Presentations.ADSecurity.org)

Sean Metcalf (@Pyrotek3)  
sean@adsecurity.org  
[www.ADSecurity.org](http://www.ADSecurity.org)  
[TrimarcSecurity.com](http://TrimarcSecurity.com)