Cloudy Vision:
How Cloud Integration Complicates Security

Sean Metcalf
Trimarc
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)
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
Azure Active Directory in the Marketplace

Every Office 365 and Microsoft Azure customer uses Azure Active Directory

17.5M organizations
1.1B identities
634K 3rd party apps in Azure AD
90K paid Azure AD / EMS customers
450B monthly authentications
90% of Fortune 500 companies

Source: Microsoft Ignite Conference 2018
https://myignite.techcommunity.microsoft.com/sessions/64565?source=sessions
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

<table>
<thead>
<tr>
<th>Common Passwords Attempted in Password Spray Attacks</th>
<th>The threats are real, global, and target all of us</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Password</strong></td>
<td>Spring</td>
</tr>
<tr>
<td><strong>Summer</strong></td>
<td>September</td>
</tr>
<tr>
<td><strong>Winter</strong></td>
<td>Football</td>
</tr>
</tbody>
</table>

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

Wile E. Coyote
CIO
Acme Corporation
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 *.googlemail.com
- FireEye (fireeyecloud.com)
- ForcePoint (mailcontrol.com)

<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>pphosted.com</td>
<td>296</td>
</tr>
<tr>
<td>outlook.com</td>
<td>186</td>
</tr>
<tr>
<td>iphmx.com</td>
<td>67</td>
</tr>
<tr>
<td>message labs.com</td>
<td>60</td>
</tr>
<tr>
<td>mimecast.com</td>
<td>57</td>
</tr>
<tr>
<td>google.com</td>
<td>25</td>
</tr>
<tr>
<td>fireeyecloud.com</td>
<td>9</td>
</tr>
<tr>
<td>mailcontrol.com</td>
<td>6</td>
</tr>
<tr>
<td>googlemail.com</td>
<td>5</td>
</tr>
</tbody>
</table>
Cloud Recon: DNS TXT Records

**MS** = Microsoft Office 365

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

**Docusign** = Docusign digital signatures

Adobe IDP

**Amazon**ses = Amazon Simple Email

Facebook

Atlassian-*= Atlassian services

GlobalSign

**Azure**Websites = Microsoft Azure

Dropbox
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
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

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
How to steal identities – federated style

Federation is effectively Cloud Kerberos.
Own the Federation server, own organizational cloud services.
Token & Signing certificates \(\approx\) KRBTGT (think Golden Tickets)
Attacking Federation: Forging SAML Tokens

THREAT RESEARCH BLOG POST
Golden SAML: Newly Discovered Attack Technique Forges Authentication to Cloud Apps


ADFSpoof
https://github.com/fireeye/adfspoof
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 configuration data.
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"

I AM ADFS 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/

```csharp
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"))
    {
    }
    if (string.IsNullOrEmpty(text))
    {
        // Handle empty or null 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 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:

<table>
<thead>
<tr>
<th>Permission</th>
<th>Used for</th>
</tr>
</thead>
<tbody>
<tr>
<td>Replicate Directory Changes</td>
<td>Password sync</td>
</tr>
<tr>
<td>Replicate Directory Changes All</td>
<td></td>
</tr>
<tr>
<td>Read/Write all properties User</td>
<td>Import and Exchange hybrid</td>
</tr>
<tr>
<td>Read/Write all properties iNetOrgPerson</td>
<td>Import and Exchange hybrid</td>
</tr>
<tr>
<td>Read/Write all properties Group</td>
<td>Import and Exchange hybrid</td>
</tr>
<tr>
<td>Read/Write all properties Contact</td>
<td>Import and Exchange hybrid</td>
</tr>
<tr>
<td>Reset password</td>
<td>Preparation for enabling password writeback</td>
</tr>
</tbody>
</table>
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 permission in Microsoft Directory and write permission on certain attributes to enable Hybrid Deployment.

DistinguishedName: CN=MSOL_trd977930921,OU=Service Accounts,DC=theacme,DC=io
Enabled: True
GivenName: 
Name: MSOL_trd977930921
ObjectClass: user
ObjectGUID: cdcb6dd0-65e2-40bc-bc60-461408831036
SamAccountName: MSOL_trd977930921
SID: S-1-5-21-143179592-3749324205-2095737646-1138
On-Prem: Acme’s Azure AD Connect

```powershell
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
```

<table>
<thead>
<tr>
<th>ObjectDN</th>
<th>DC=theacme,DC=io</th>
</tr>
</thead>
<tbody>
<tr>
<td>IdentityReference</td>
<td>ACME\MSOL_trd977930921</td>
</tr>
<tr>
<td>AccessControlType</td>
<td>Allow</td>
</tr>
<tr>
<td>ActiveDirectoryRights</td>
<td>ExtendedRight</td>
</tr>
<tr>
<td>ObjectType</td>
<td>DS-Replication-Get-Changes-All</td>
</tr>
</tbody>
</table>

```
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
```

<table>
<thead>
<tr>
<th>ObjectDN</th>
<th>DC=theacme,DC=io</th>
</tr>
</thead>
<tbody>
<tr>
<td>IdentityReference</td>
<td>ACME\MSOL_trd977930921</td>
</tr>
<tr>
<td>AccessControlType</td>
<td>Allow</td>
</tr>
<tr>
<td>ActiveDirectoryRights</td>
<td>ExtendedRight</td>
</tr>
<tr>
<td>ObjectType</td>
<td>DS-Replication-Get-Changes</td>
</tr>
</tbody>
</table>
```
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 for 'theacmeio.onmicrosoft.com'. This account must have directory and write permission on certain attributes to enable Azure AD Connect.

DistinguishedName : CN=MSOL_trrd977930921,OU=Service Accounts,DC=theacme,DC=io

PS C:\> get-adcomputer AzureSync

DistinguishedName : CN=AZURESYNC,OU=Servers,DC=theacme,DC=io
On-Prem: Acme’s Azure AD Connect

PS C:\> Find-GPOComputerAdmin -O>Name '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-6ACB-495D-97E6-2AEC89ED91A8\}
GPOType       : GroupPolicyPreferences
On-Prem: Acme’s Azure AD Connect

Server Config

These groups and users have the specified permission for this GPO

Groups and users:

<table>
<thead>
<tr>
<th>Name</th>
<th>Allowed Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authenticated Users</td>
<td>Read (from Security Filtering)</td>
</tr>
<tr>
<td>Domain Admins (ACME\Domain Admins)</td>
<td>Edit settings, delete, modify security</td>
</tr>
<tr>
<td>Enterprise Admins (ACME\Enterprise Admins)</td>
<td>Edit settings, delete, modify security</td>
</tr>
<tr>
<td>ENTERPRISE DOMAIN CONTROLLERS</td>
<td>Read</td>
</tr>
<tr>
<td>Server Tier 1 (ACME\Server Tier 1)</td>
<td>Edit settings</td>
</tr>
<tr>
<td>Server Tier 2 (ACME\Server Tier 2)</td>
<td>Edit settings</td>
</tr>
<tr>
<td>Server Tier 3 (ACME\Server Tier 3)</td>
<td>Edit settings, delete, modify security</td>
</tr>
</tbody>
</table>
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
No account lockout since 1 password is used in authentication attempt for each user in the list (typically all or just admins) then the password spray tool pauses before moving onto the next password.
Password Spraying Overview

“Winter2018!”

Sleep x seconds/minutes

“Spring2019!”

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

“Summer2019!”

Sleep x seconds/minutes

“Fall2019!”

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.
Attacking the Cloud: Password Spraying

- Ruler (Exchange) [Golang]

- SprayingToolkit (Lync/Skype for Business/OWA) [Python]
  - [https://github.com/byt3bl33d3r/SprayingToolkit](https://github.com/byt3bl33d3r/SprayingToolkit)

- LyncSniper (Lync/Skype for Business) [PowerShell]
  - [https://github.com/mdsecresearch/LyncSniper](https://github.com/mdsecresearch/LyncSniper)

- MailSniper (OWA/EWS) [PowerShell]
  - [https://github.com/dafthack/MailSniper](https://github.com/dafthack/MailSniper)

*Legacy Authentication enables O365 Password Spraying*

*Legacy = Outlook <=2010, POP, IMAP, SMTP, etc*
Attacking the Cloud: Password Spraying

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

5 threads remaining

User: theacme.io\thrawn@theacme.io Password: Summer2019!

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

A total of 0 credentials were obtained.

Results have been written to C:temp\owa-sprayed-creds.txt.
Attacking the Cloud: Password Spraying

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.

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

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

[*] Now spraying the EWS portal at https://outlook.office365.com/EWS/Exchange.asmx
[*] Current date and time: 08/02/2019 04:05:34
[*] Trying Exchange version Exchange2010
[*] SUCCESS! User:theacme.io\bailey@theacme.io Password:Password1
[*] A total of 1 credentials were obtained.
Detecting Password Spraying

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

<table>
<thead>
<tr>
<th>Date</th>
<th>Username</th>
<th>Service</th>
<th>Status</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>8/1/2019, 9:09:12 PM</td>
<td>Thrawn</td>
<td>Office 365 Exchange On...</td>
<td>Failure</td>
<td>52.168.138.234</td>
</tr>
<tr>
<td>8/1/2019, 9:09:11 PM</td>
<td>Qui-Gon Jinn</td>
<td>Office 365 Exchange On...</td>
<td>Failure</td>
<td>52.168.138.234</td>
</tr>
<tr>
<td>8/1/2019, 9:09:11 PM</td>
<td>Lando Calrissian</td>
<td>Office 365 Exchange On...</td>
<td>Failure</td>
<td>52.168.138.234</td>
</tr>
<tr>
<td>8/1/2019, 9:09:07 PM</td>
<td>Boba Fett</td>
<td>Office 365 Exchange On...</td>
<td>Failure</td>
<td>52.168.138.234</td>
</tr>
<tr>
<td>8/1/2019, 9:09:06 PM</td>
<td>Obi-Wan Kenobi</td>
<td>Office 365 Exchange On...</td>
<td>Failure</td>
<td>52.168.138.234</td>
</tr>
<tr>
<td>8/1/2019, 9:09:06 PM</td>
<td>Leia</td>
<td>Office 365 Exchange On...</td>
<td>Failure</td>
<td>52.168.138.234</td>
</tr>
<tr>
<td>8/1/2019, 9:09:06 PM</td>
<td>Rey</td>
<td>Office 365 Exchange On...</td>
<td>Failure</td>
<td>52.168.138.234</td>
</tr>
<tr>
<td>8/1/2019, 9:09:06 PM</td>
<td>Kylo</td>
<td>Office 365 Exchange On...</td>
<td>Failure</td>
<td>52.168.138.234</td>
</tr>
<tr>
<td>8/1/2019, 9:09:01 PM</td>
<td>Padme Amidala</td>
<td>Office 365 Exchange On...</td>
<td>Failure</td>
<td>52.168.138.234</td>
</tr>
<tr>
<td>8/1/2019, 9:09:01 PM</td>
<td>Bailey</td>
<td>Office 365 Exchange On...</td>
<td>Failure</td>
<td>52.168.138.234</td>
</tr>
<tr>
<td>8/1/2019, 9:09:00 PM</td>
<td>Han Solo</td>
<td>Office 365 Exchange On...</td>
<td>Failure</td>
<td>52.168.138.234</td>
</tr>
<tr>
<td>8/1/2019, 9:09:00 PM</td>
<td>Adm Ackbar</td>
<td>Office 365 Exchange On...</td>
<td>Failure</td>
<td>52.168.138.234</td>
</tr>
<tr>
<td>8/1/2019, 9:08:53 PM</td>
<td>Finn</td>
<td>Office 365 Exchange On...</td>
<td>Failure</td>
<td>52.168.138.234</td>
</tr>
</tbody>
</table>

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

| Date/Time          | Username  | Service                  | Result   | IP Address     | Conditional
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>8/2/2019, 12:03:47 AM</td>
<td>Boba Fett</td>
<td>Office 365 Exchange...</td>
<td>Failure</td>
<td>52.168.138.234</td>
<td>Not Applied</td>
</tr>
<tr>
<td>8/2/2019, 12:04:34 AM</td>
<td>Boba Fett</td>
<td>Office 365 Exchange...</td>
<td>Failure</td>
<td>52.168.138.234</td>
<td>Not Applied</td>
</tr>
<tr>
<td>8/2/2019, 12:01:43 AM</td>
<td>Boba Fett</td>
<td>Office 365 Exchange...</td>
<td>Failure</td>
<td>52.168.138.234</td>
<td>Not Applied</td>
</tr>
<tr>
<td>8/2/2019, 12:03:15 AM</td>
<td>Boba Fett</td>
<td>Office 365 Exchange...</td>
<td>Failure</td>
<td>52.168.138.234</td>
<td>Not Applied</td>
</tr>
<tr>
<td>8/2/2019, 12:03:04 AM</td>
<td>Boba Fett</td>
<td>Office 365 Exchange...</td>
<td>Failure</td>
<td>52.168.138.234</td>
<td>Not Applied</td>
</tr>
<tr>
<td>8/2/2019, 12:08:21 AM</td>
<td>Boba Fett</td>
<td>Office 365 Exchange Online</td>
<td>Failure</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8/2/2019, 12:02:06 AM</td>
<td>Boba Fett</td>
<td>Office 365 Exchange Online</td>
<td>Failure</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8/2/2019, 12:04:11 AM</td>
<td>Boba Fett</td>
<td>Office 365 Exchange Online</td>
<td>Success</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*Azure AD Sign-in Logs require Azure AD Premium (P1 or P2)*
## Detecting Password Spraying

### Basic info

<table>
<thead>
<tr>
<th>Request ID</th>
<th>Correlation ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>8e270d9b-9dc4-41c5-9273-e69395680400</td>
<td>94558595-8ecc-484b-b7a6-6eaa3e9d74e</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>User</th>
<th>Username</th>
<th>User ID</th>
<th>Application</th>
<th>Application ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Boba Fett</td>
<td><a href="mailto:bobafett@theacme.io">bobafett@theacme.io</a></td>
<td>5688de1a-10ec-4b5c-b98d-73cf3c2e7f0</td>
<td>Office 365 Exchange Online</td>
<td>00000000-0000-0000-0000-000000000000</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IP address</th>
<th>Location</th>
<th>Date</th>
<th>Status</th>
<th>Sign-in error code</th>
</tr>
</thead>
</table>

**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!

<table>
<thead>
<tr>
<th>TIMESTAMP</th>
<th>TRIGGER TYPE</th>
<th>IP ADDRESS</th>
<th>BAD PASSWORD ERROR COUNT</th>
<th>EXTRANET LOCKOUT ERROR COUNT</th>
<th>UNIQUE USERS ATTEMPTED</th>
</tr>
</thead>
<tbody>
<tr>
<td>2/28/2018 6:00 PM</td>
<td>hour</td>
<td>104.208.238.9</td>
<td>0</td>
<td>284</td>
<td>14</td>
</tr>
<tr>
<td>2/28/2018 6:00 PM</td>
<td>hour</td>
<td>104.44.252.135</td>
<td>0</td>
<td>27</td>
<td>1</td>
</tr>
<tr>
<td>2/28/2018 6:00 PM</td>
<td>hour</td>
<td>168.61.144.85</td>
<td>0</td>
<td>164</td>
<td>2</td>
</tr>
</tbody>
</table>
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](http://aka.ms/dfsrmig))

- **Deploy in Audit Mode first**

- Passwords are fuzzy matched, substring matched & scored. Must be 5 or higher

- After passwords have been changed, look to extend password age
Attacking Cloud Administration

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

Sean Metcalf
CTO, Trimarc

Exploiting Active Directory Administrator Insecurities

Sean Metcalf (@Pyrotek3)
sean@adsecurity.org
www.ADSecurity.org
From On-Prem to Cloud Administration
### Global administrator - Assignments

<table>
<thead>
<tr>
<th>Name</th>
<th>Username</th>
<th>Type</th>
<th>Scope</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sean Metcalf</td>
<td><a href="mailto:sean@theacmeio.onmicrosoft.com">sean@theacmeio.onmicrosoft.com</a></td>
<td>User</td>
<td>Directory</td>
</tr>
<tr>
<td>Mark Morowczynski</td>
<td><a href="mailto:mark@theacme.io">mark@theacme.io</a></td>
<td>User</td>
<td>Directory</td>
</tr>
<tr>
<td>Sean Metcalf</td>
<td><a href="mailto:seanmetcalf@theacme.io">seanmetcalf@theacme.io</a></td>
<td>User</td>
<td>Directory</td>
</tr>
<tr>
<td>Han Solo</td>
<td><a href="mailto:hansolo@theacme.io">hansolo@theacme.io</a></td>
<td>User</td>
<td>Directory</td>
</tr>
<tr>
<td>Boba Fett</td>
<td>theacme.io\<a href="mailto:bobafett@theacme.io">bobafett@theacme.io</a></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mace Windu</td>
<td><a href="mailto:mace@theacme.io">mace@theacme.io</a></td>
<td>User</td>
<td>Directory</td>
</tr>
<tr>
<td>Thrawn</td>
<td>theacme.io\<a href="mailto:thrawn@theacme.io">thrawn@theacme.io</a></td>
<td>User</td>
<td>Directory</td>
</tr>
</tbody>
</table>

**SUCCESS! User: theacme.io\bobafett@theacme.io Password: Mandalorian19!**

**SUCCESS! User: theacme.io\thrawn@theacme.io Password: Summer2019!**
Attacking Cloud Administration

Customer Support <xbox_live ww.00.en.vmc.rmd.ts.t03.spt.ua.pi@outlook.com>
Re: Office 365 Licenses Expired.

To: [email redacted]

This message was sent with High importance.

Office 365

©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

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

Web Browser

Cloud Website

(DNS)

HTTP(S)
Attacking Cloud Administration: Token Theft

![Local Group Policy Editor screenshot showing the configuration setting for Google Chrome extensions.](image-url)
Attacking Cloud Administration: Token Theft
Attacking Cloud Administration: Token Theft

SSL/TLS Decryption Device

Cloud Website

Attacker Compromises Device

Auth

Token

Auth

Token

Auth

Token

Attacker Compromises Device

SSL/TLS

Decryption

Device

Cloud

Website

Attacker

Compromises

Device

Auth

Token

Auth

Token

Attacker Compromises Device

SSL/TLS

Decryption

Device

Cloud Website

Attacker Compromises Device
Attacking Cloud Administration: Token Theft
Attacking Cloud Administration: Token Theft

https://github.com/kgretzky/evilginx2
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 whiteliste 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.

Replay

112. Han Solo hansolo LeiaIKnow19! hansolo@theacme.io
113. Luke Skywalker lukeskywalker TheForce19 lukeskywalker@Plus.com
Password Reuse/Replay Detection

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

HaveIBeenPwned.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

<table>
<thead>
<tr>
<th>RISK LEVEL</th>
<th>DETECTION TYPE</th>
<th>RISK EVENT TYPE</th>
<th>RISK EVENTS CLOSED</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>Offline</td>
<td>Users with leaked credentials</td>
<td>2 of 2</td>
</tr>
</tbody>
</table>
Turn on Azure AD Connect Password Hash Sync

- Leaked Credential Reporting
  - Dark Web, Law Enforcement, and Security Researchers
- When something catastrophic happens
  - WannaCry, NotPetya
- 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
  • 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

Enterprise App Permissions

• Enterprise App (tenant-wide) permissions can be granted by Admins.

• Ideal persistence technique since app permissions not reviewed like group membership.
Enterprise App Permissions

This app would like to:

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

Awesome Notes
needs access to

- Contacts
- Location
- Microphone

Google play
ACCEPT
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
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

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