Sean Metcalf   Mark Morowczynski
Trimarc       Microsoft

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

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)
About

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
- AskPFEPplat Blog, Azure AD Identity Blog

Mark Morowczynski
@markmorow
Markmoro@microsoft.com
Agenda

• “Sample Customer” Cloud On-boarding Process
• Attacker Recon
• Attacking the Cloud
• Defending the Cloud
• Go Do’s!
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…
Priority #1: We're going to the cloud!

Wile E. Coyote
CIO
Acme Corporation
Acme Project Team Members

- 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 Recon

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)
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

<table>
<thead>
<tr>
<th>Domain Name</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>MS</td>
<td>851</td>
</tr>
<tr>
<td>google-site-verification</td>
<td>509</td>
</tr>
<tr>
<td>docusign</td>
<td>247</td>
</tr>
<tr>
<td>adobe-idp-site-verification</td>
<td>210</td>
</tr>
<tr>
<td>amazonses</td>
<td>158</td>
</tr>
<tr>
<td>facebook-domain-verification</td>
<td>141</td>
</tr>
<tr>
<td>atlassian-domain-verification</td>
<td>111</td>
</tr>
<tr>
<td>globalsign-domain-verification</td>
<td>109</td>
</tr>
<tr>
<td>V</td>
<td>76</td>
</tr>
<tr>
<td>azurewebsites</td>
<td>48</td>
</tr>
<tr>
<td>dropbox-domain-verification</td>
<td>24</td>
</tr>
<tr>
<td>cisco-ci-domain-verification</td>
<td>22</td>
</tr>
<tr>
<td>Dynatrace-site-verification</td>
<td>16</td>
</tr>
<tr>
<td>have-i-been-pwned-verification</td>
<td>11</td>
</tr>
<tr>
<td>status-page-domain-verification</td>
<td>7</td>
</tr>
<tr>
<td>OSIAGENTREGURL</td>
<td>7</td>
</tr>
<tr>
<td>workplace-domain-verification</td>
<td>6</td>
</tr>
<tr>
<td>bugcrowd-verification</td>
<td>5</td>
</tr>
<tr>
<td>yandex-verification</td>
<td>4</td>
</tr>
<tr>
<td>cisco-site-verification</td>
<td>4</td>
</tr>
</tbody>
</table>
Cloud Recon: Acme DNS TXT Records

What do we know about Acme’s Cloud Config?

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

```
PS C:\WINDOWS\system32> (Resolve-DnsName -Name acme.com) | Set-DnsServerPreference -Preference 0 -Server .

v=spf1 include:spf.protection.outlook.com
atlassian-domain-verification=JjxTtv2u
atlassian-domain-verification=JjxTtv2u
Cisco
Cisco
Cisco
ciscocidomainverification=2947343fd5da6c777c03cb0a32fb0

citrix-verification-code=a5da5637-df88-46b2-a672-00f7c6b1e002
docusign=034562ewrg5a-9143-4342-8659-3v=verifydomain
MS=7274734
Dropbox
Dropbox
dropbox-domain-verification=f7wuqiwe73
Facebook
Facebook
Facebook
Facebook
GoogleSite
GoogleSite
GoogleSite
GoogleSite
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

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.
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
On-Prem: AD to Cloud Sync
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>
</tbody>
</table>

| 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 |
On-Prem: Acme’s Azure AD Connect

```powershell
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 tenant 'theacmeio.onmicrosoft.com'. This account must have directory replication permissions in Azure Active Directory and write permission on certain attributes to enable Hybrid Deployment.
| DistinguishedName                                | CN=MSOL_trd977930921,OU=Service Accounts,DC=theacme,DC=io
| Enabled                                          | True
| GivenName                                        | 
| Name                                             | MSOL_trd977930921
| ObjectClass                                      | user
| ObjectGUID                                       | cdc6dd0-65e2-40bc-bc60-461408831036
| SamAccountName                                   | MSOL_trd977930921
| SID                                              | S-1-5-21-143179592-3749324205-2095737646-1138 |
On-Prem: Acme’s Azure AD Connect

```
PS C:\> Invoke-ACLScanner -ResolveGUIDs `n  -ADSpPath 'DC=theacme,DC=io' `n  | where {($_.IsInherited -eq $False) -AND `n  ($_.ObjectType -like 'DS-Replication*')} `n  | select ObjectDN,IdentityReference,AccessControlType,`n  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>

<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

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

Description: Account created by the Windows Azure Active Directory Sync Service 'trd977930921' running on computer 'AZURESYNC' configured to use 'theacmeio.onmicrosoft.com'. This account must have directory and write permission on certain attributes to enable Azure AD Connect.

DistinguishedName: CN=MSOL_trd977930921,OU=Service Accounts,DC=theacme,DC=io

Enabled: True

```powershell
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 -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-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.
AD Recon vs Azure AD Recon

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

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

• Office 365 Authentication Page (Python) [Account Discovery]
  • https://github.com/LMGsec/o365creeper

• OWA (Golang)
  • https://github.com/busterb/msmailprobe

• ActiveSync (Python)
  • https://bitbucket.org/grimhacker/office365userenum/src

• MSOnline/AzureAD PowerShell Module (PowerShell)
  • https://github.com/nyxgeek/o365recon
Password Spraying Overview

“Winter2019”

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

“Winter2019!”

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.
Attacking the Cloud: Password Spraying

• Ruler (Exchange) [Golang]
  • https://github.com/sensepost/ruler/wiki/Brute-Force

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

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

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

Legacy Authentication enables O365 Password Spraying

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

PS C:\> C:\temp\Spray-0365.ps1

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


[*] Now spraying the EWS portal at https://outlook.office365.com/EWS/Exchange.asmx
[*] Current date and time: 08/02/2019 04:01:04
[*] Trying Exchange version Exchange2010
[*] A total of 0 credentials were obtained.
Results have been written to C:\temp\owa-sprayed-creds.txt.
[*] Now spraying the EWS portal at https://outlook.office365.com/EWS/Exchange.asmx
[*] Current date and time: 08/02/2019 04:01:35
[*] Trying Exchange version Exchange2010
[*] SUCCESS! User: theacme.io\thrawn@theacme.io Password: Summer2019!
[*] A total of 1 credentials were obtained.
Results have been written to C:\temp\owa-sprayed-creds.txt.
[*] Now spraying the EWS portal at https://outlook.office365.com/EWS/Exchange.asmx
[*] Current date and time: 08/02/2019 04:01:58
[*] Trying Exchange version Exchange2010
[*] A total of 0 credentials were obtained.
Results have been written to C:\temp\owa-sprayed-creds.txt.
[*] Now spraying the EWS portal at https://outlook.office365.com/EWS/Exchange.asmx
[*] Current date and time: 08/02/2019 04:02:21
[*] Trying Exchange version Exchange2010
[*] A total of 0 credentials were obtained.
Results have been written to C:\temp\owa-sprayed-creds.txt.
[*] Now spraying the EWS portal at https://outlook.office365.com/EWS/Exchange.asmx
[*] Current date and time: 08/02/2019 04:02:22
[*] Trying Exchange version Exchange2010
[*] A total of 0 credentials were obtained.
Attacking the Cloud: Password Spraying

Now spraying the EWS portal at https://outlook.office365.com/EWS/Exchange.asmx
Current date and time: 08/02/2019 04:01:35
Trying Exchange version Exchange2010
SUCCESS! User: theacme.io\thrawn@theacme.io Password: Summer2019!
A total of 1 credentials were obtained.

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

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

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

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

Access denied

You do not have access

Soon...

To see sign-in data, upgrade your organization's subscription. License status: Azure AD Free

Start a free Premium Trial
# Detecting Password Spraying

<table>
<thead>
<tr>
<th>Date/Time</th>
<th>Username</th>
<th>App/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, 9:09:06 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, 9:09:01 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, 9:09:00 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

### Azure AD Sign-in Logs

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

<table>
<thead>
<tr>
<th>Date/Time</th>
<th>Username</th>
<th>Application</th>
<th>Outcome</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>8/2/2019, 12:02:06 AM</td>
<td>Boba Fett</td>
<td>Office 365 Exchange Online</td>
<td>Failure</td>
<td>52.168.138.234</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>52.168.138.234</td>
</tr>
</tbody>
</table>
## Detecting Password Spraying

### Basic info

<table>
<thead>
<tr>
<th><strong>Request ID</strong></th>
<th>8e270d9b-9dc4-41c5-9273-e69395680400</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Correlation ID</strong></td>
<td>94558595-8ecc-484b-b7a6-6eaa3e9d74e</td>
</tr>
<tr>
<td><strong>User</strong></td>
<td>Boba Fett</td>
</tr>
<tr>
<td><strong>Username</strong></td>
<td><a href="mailto:bobafett@theacme.io">bobafett@theacme.io</a></td>
</tr>
<tr>
<td><strong>User ID</strong></td>
<td>5688de1a-10ec-4b5c-b98d-73cfff32c27f0</td>
</tr>
<tr>
<td><strong>Application</strong></td>
<td>Office 365 Exchange Online</td>
</tr>
<tr>
<td><strong>Application ID</strong></td>
<td>00000002-0000-0ff1-ce00-000000000000</td>
</tr>
</tbody>
</table>

| **IP address** | 52.168.138.234 |
| **Location** | Washington, Virginia, US |
| **Date** | 8/2/2019, 12:02:06 AM |
| **Status** | Failure |
| **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 |

### 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**
From On-Prem to Cloud Administration

Active Directory Users and Computers

Acme Corporation - Overview

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.

Existing entries:
- All services (24)
- Identity Security & Protection (8)
- 3rd Party Integration (3)
- Monitoring & Reporting (5)
- Identity Lifecycle Management

New features:
- Identity Protection - Identity Security & Protection
- New riskDetections API for Microsoft Graph (Public preview)
# Attacking 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>SUCCESS!</td>
<td>User</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>SUCCESS!</td>
<td>User</td>
</tr>
</tbody>
</table>
Attacking Cloud Administration

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

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.

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

From Global Admin to **Global Reader**

- Currently in Public 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.

Cloud Administration – Finding a Weakness

Diagram:
- Workstation
  - Web Browser
- Cloud Website
  - HTTP(S)
  - (DNS)
Attacking Cloud Administration: Token Theft
Attacking Cloud Administration: Token Theft
Attacking Cloud Administration: Token Theft
Attacking Cloud Administration: Token Theft
Attacking Cloud Administration: Token Theft

https://github.com/kgretzky/evilginx2
Password Reuse/Replay

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

30f8c8134437da0c0232eeca20bd7992c00bce74:
df272defef6127aeaec5c47c7ceed028c39354df:
c886b08ad18cd650b1bc4a7612a0742a2257a41e:
bd01669b5883f24e8e55930efeb098fb5a873d96:
ef60e1915933c7c5abde3cb160f45bf1963e3525:
991db9efcfa06ae837a4d433b6ba2777256e1af8:
4b757d2f8f7036f8119739e4b82b2c7875f4a987:
13a7bc6d374dccc55334a756a7fb9bf4f1b46c7d:
a4404ac0b635faa6264658fc960836a308427c90:
546684e9d6df2f217db45229b4fa63c5d51f26729:
54cd6a7aaf905ac2145942f65a03fa7c54cf3ea9:
fb88038b760bc428e4847831aad572339c2e8ecd:
c0b796b5d6a936b8c30351a27f30b8f1a3109a:

 SHA1

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

\[ \text{'--have i been pwned?} \]

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**: (Check box)
- **Notification email**: enter your email address

### Risk Event:
- **Risk Level**: High
- **Detection Type**: Offline
- **Risk Event Type**: Users with leaked credentials

---

![Password Hash Sync](image-url)
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

• 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
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!
Admin Accounts with MFA Sept 2017: 0.7%

Admin Accounts with MFA Sept 2018: 1.7%

Admin Accounts with MFA Oct 2019: 8.2%

91.8% of admins with NO MFA
Protect Cloud Admin Accounts

• Good: Turn MFA on!
• Better: Conditional Access
• 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](https://aka.ms/deploymentplans)
Future Protection

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
FIDO2 in Azure AD

Public Preview July 2019

• Edge, Chrome, 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!
Strong Authentication with **FIDO2 security key**

1. User plugs FIDO2 security key into computer
2. Windows detects FIDO2 security key
3. Windows device sends auth request
4. Azure AD sends back nonce
5. User completes gesture to unlock private key stored in security key’s secure enclave
6. FIDO2 security key signs nonce with private key
7. PRT token request with signed nonce is sent to Azure AD
8. Azure AD verifies FIDO key signature
9. Azure AD returns PRT to enable access to cloud resources
FIDO2 public preview expanding to Hybrid environments (Early 2020)
User authenticates to Azure AD with a FIDO2 security key.

Azure AD checks the tenant for a Kerberos server key matching the user’s on-premises AD Domain.
- Azure AD Generates a partial Kerberos Ticket Granting Ticket (TGT) for the users on-premises AD Domain. The TGT contains only the user SID. No authorization data (groups) are included in the TGT.

The partial TGT is returned to the Windows along with Azure AD Primary Refresh Token (PRT).

Windows contacts on-premises AD Domain Controller and trades the partial TGT for a full TGT.

Windows now has Azure AD PRT and a full Active Directory TGT.
# Audit Consented Permissions for All Apps

## 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]

<table>
<thead>
<tr>
<th>API NAME</th>
<th>PERMISSION</th>
<th>TYPE</th>
<th>PERMISSION LEVEL</th>
<th>GRANTEE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Graph</td>
<td>Have full access to user calendars</td>
<td>Delegated</td>
<td>Medium</td>
<td>An administrator</td>
</tr>
<tr>
<td>Microsoft Graph</td>
<td>Have full access to user contacts</td>
<td>Delegated</td>
<td>Medium</td>
<td>An administrator</td>
</tr>
<tr>
<td>Microsoft Graph</td>
<td>Read Microsoft Intune apps</td>
<td>Delegated</td>
<td>Medium</td>
<td>An administrator</td>
</tr>
<tr>
<td>Microsoft Graph</td>
<td>Read and write Microsoft Intune apps</td>
<td>Delegated</td>
<td>High</td>
<td>An administrator</td>
</tr>
</tbody>
</table>
### Audit Consented Permissions for All Apps

<table>
<thead>
<tr>
<th>PERMISSION</th>
<th>TYPE</th>
<th>PERMISSION LEVEL</th>
<th>GRANTED BY</th>
<th>TOTAL USERS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sign users in</td>
<td>Delegated</td>
<td>Medium</td>
<td></td>
<td>15</td>
</tr>
<tr>
<td>Sign in and read user profile</td>
<td>Delegated</td>
<td>Low</td>
<td></td>
<td>7</td>
</tr>
<tr>
<td>Read and write access to user profile</td>
<td>Delegated</td>
<td>Unknown</td>
<td></td>
<td>14</td>
</tr>
<tr>
<td>Read all users’ basic profiles</td>
<td>Delegated</td>
<td>Low</td>
<td></td>
<td>14</td>
</tr>
<tr>
<td>Read and write access to user mail</td>
<td>Delegated</td>
<td>High</td>
<td></td>
<td>14</td>
</tr>
<tr>
<td>Read and write user and shared mail</td>
<td>Delegated</td>
<td>High</td>
<td></td>
<td>3</td>
</tr>
</tbody>
</table>

**User(s)**

- Caleb Baker
  - calebb@wingtiptoysonline.com

- Rajat Luthra
  - rluthra@wingtiptoysonline.com
Audit App Permissions with PowerShell

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

Review both:
• Delegated permissions (OAuth2PermissionGrants)
• Application permissions (AppRoleAssignments).

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

https://gist.github.com/psignoret/41793f8c6211d2df5051d77ca3728c09
Breach Replay Defenses

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 Notpeya, The Most Devasting Cyberattack In History
- 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

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

5.5+ billion
Leaked credentials processed

14.2+ million
Leaked credentials matched

82%
Azure AD active tenants with PHS – Sept 2018

91%
Azure AD active tenants with PHS – Oct 2019
Phishing Defenses

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..
Phishing Defenses

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
ADFS Monitoring

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!

<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>

• ADFS 2016 or ADFS 2019 Turn On Smart Lockout
Password Spray Defense

Modernize your password policy

• People choose “strong” but easily guessable passwords
  • November2019! or Winter2019!
• https://aka.ms/passwordguidance
• NIST 800-63B
Azure AD Banned Password Policy

- Applies to on-prem AD as well!

- [https://aka.ms/deploypassword protection](https://aka.ms/deploypassword protection)

Custom smart lockout
- Lockout threshold: 10
- Lockout duration in seconds: 70

Custom banned passwords
- Enforce custom list: Yes
- Custom banned password list:
  - seahawks
  - mariners
  - sounders
  - redmond
  - washington

Password protection for Windows Server Active Directory
- Enable password protection on Windows Server Active Directory: Yes
- Mode: Enforced
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
Legacy Authentication and Password Spray

Nearly 100% of password spray attacks are using legacy authentication

• 730,000+ Compromised accounts due to password spray in last 4 months
• Federated with Azure AD/O365
  • IDP is responsible for authentication, including legacy auth!
• https://aka.ms>PasswordSprayBestPractices
Blocking Legacy Authentication in Exchange

- Disable services at the mailbox level

- Authentication Policies

- Client IP Block
Blocking Authorization in ADFS/Federation

- Authorization rules
  - Very rich expressions using ADFS claims language
  - Happens after authentication
  - Applies to ALL applications behind Azure AD
• First, if you have users NOT using Legacy Auth protocols.
  • Block with Conditional Access
    • Requires Azure AD P1

• Update Clients

• Only Service Accounts / Apps should remain

• Legacy auth for EXO being deprecated on Oct 13th, 2020

• Ensure you have coverage for all device type scenarios (Question 7)
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.

Slides:
Presentations.ADSecurity.org

Mark Morowczynski
@markmorow
Markmoro@microsoft.com

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

• 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://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
• SprayingToolkit
  • 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
References

- Azure AD Baseline Policies
  - [https://aka.ms/aadbaseline](https://aka.ms/aadbaseline)
- Azure AD Deployment Plans
  - [https://aka.ms/deploymentplans](https://aka.ms/deploymentplans)
- Azure AD FIDO2
  - [http://aka.ms/fido2docs](http://aka.ms/fido2docs)
- Azure AD App Consent Script
  - [https://gist.github.com/psignoret/41793f8c6211d2df5051d77ca3728c09](https://gist.github.com/psignoret/41793f8c6211d2df5051d77ca3728c09)
- Azure AD Password Hash Sync
  - [http://aka.ms/aadphs](http://aka.ms/aadphs)
- Wired-The Untold Story Of Notpaya, The Most Devasting Cyberattack In History
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

- 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

• Exchange Authentication Policies

• Exchange Client IP Block

• Azure AD Conditional Access Q&A

• ADFS Smart Lockout