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
Some things start with Twitter…
Some things start with Twitter…

Sean Metcalf @PyroTek3 · Aug 8, 2018
Replying to @markmorow @BlackHatEvents and @azuread
Yes! Let's do that!

Mark Morowczynski @markmorow
Replying to @PyroTek3 and @BlackHatEvents
We should do one next year on @azuread
9:57 PM · Aug 8, 2018 · Twitter for iPhone
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 & distributer 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 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…
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
What do we know about Acme’s Cloud Config?

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

```bash
PS C:\WINDOWS\system32> (Resolve-DnsName -v=spf1 include:spf.protection.outlook.atlassian-domain-verification=JjxTtv2uciscocoidomainverification=2947343fd5dacitrix-verification-code=a5da5637-df88docusign=034562ewrg5a-9143-4342-8659-3
v=verifydomain MS=7274734
dropbox-domain-verification=f7wuqiwe73facebook-domain-verification=22dsh0s45google-site-verification=jnpwbxWt0PexFteamviewer-sso-verification=e6d38470a1webexdomainverification=7943253ade-034
```
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

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.
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 \(\sim\) KRBTGT (think Golden Tickets)
**THREAT RESEARCH BLOG POST**

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


**ADFSpoof**

https://github.com/fireeye/adxspooff

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 AD FS state data (the encrypted PFX file).
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"
Attacking Federation: ADFS Persistence

I Am ADFS and So Can You

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

Same knowledge

- In-memory
- Doesn't persist

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"))
    {
    }
}
• 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.
active directory sync directory tool

About 32,500,000 results (0.58 seconds)
On-Prem: AD to Cloud Sync

active directory sync directory tool
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
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>
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 the Azure AD 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

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

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

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-6ACB-495D-97E6-2AEC89ED91A8}
GPOType      : GroupPolicyPreferences
On-Prem: Acme’s Azure AD Connect

Group Policy Management
Forest: theacme.io

Domains

Server Config
Scope | Details | Settings | Delegation

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


[*] 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:thecacme.io\thrawn@thecacme.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 04:04:04
[*] 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

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\boba@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 to Azure AD Premium P1 or P2.

License status: Azure AD Free

Start a free Premium Trial
**Detecting Password Spraying**

<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>Name</th>
<th>Activity</th>
<th>Result</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>8/1/2019</td>
<td>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</td>
<td>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</td>
<td>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</td>
<td>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</td>
<td>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</td>
<td>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</td>
<td>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</td>
<td>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</td>
<td>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</td>
<td>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</td>
<td>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</td>
<td>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</td>
<td>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


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, 12:02:06 AM Boba Fett Office 365 Exchange Online Failure 52.168.138.234 Not Applied


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

### Basic info

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Request ID</td>
<td>8e270d9b-9dc4-41c5-9273-e69395680400</td>
</tr>
<tr>
<td>Correlation ID</td>
<td>94558595-8ecc-484b-b7a6-6eaaa3e9d74e</td>
</tr>
<tr>
<td>User</td>
<td>Boba Fett</td>
</tr>
<tr>
<td>Username</td>
<td><a href="mailto:bobafett@theacme.io">bobafett@theacme.io</a></td>
</tr>
<tr>
<td>User ID</td>
<td>5688de1a-10ec-4b5c-b98d-73cffe3c7e7f0</td>
</tr>
<tr>
<td>Application</td>
<td>Office 365 Exchange Online</td>
</tr>
<tr>
<td>Application ID</td>
<td>00000002-0000-0ff1-ce00-000000000000</td>
</tr>
<tr>
<td>IP address</td>
<td>52.168.138.234</td>
</tr>
<tr>
<td>Location</td>
<td>Washington, Virginia, US</td>
</tr>
<tr>
<td>Date</td>
<td>8/2/2019, 12:02:06 AM</td>
</tr>
<tr>
<td>Status</td>
<td>Failure</td>
</tr>
<tr>
<td>Sign-in error code</td>
<td>50126</td>
</tr>
<tr>
<td>Failure reason</td>
<td>Invalid username or password or Invalid on-premise username or password</td>
</tr>
<tr>
<td>Client app</td>
<td>Other clients; Older Office clients</td>
</tr>
</tbody>
</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**
Attacking Cloud Administration

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

Sean Metcalf
CTO, Trimarc
From On-Prem to Cloud Administration
## Global administrator - Assignments

**All roles**

<table>
<thead>
<tr>
<th>Add assignment</th>
<th>Remove assignment</th>
<th>Refresh</th>
<th>Manage in PIM</th>
<th>Got feedback?</th>
</tr>
</thead>
</table>

<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@theacme.io.onmicrosoft.com">sean@theacme.io.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><strong>SUCCESS! User:theacme.io\<a href="mailto:bobafett@theacme.io">bobafett@theacme.io</a> Password:Mandalorian19!</strong></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><strong>SUCCESS! User:theacme.io\<a href="mailto:thrawn@theacme.io">thrawn@theacme.io</a> Password:Summer2019!</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Attacking Cloud Administration

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.

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.
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

Cloud Administration – Finding a Weakness

Workstation

Web Browser

(DNS)

HTTP(S)

Cloud Website
Local Group Policy Editor

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

Setting
- 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
Attacking Cloud Administration: Token Theft

SSL/TLS Decryption Device

Attacker Compromises Device

Cloud Website

Auth

Token

SSL/TLS Decryption Device

Auth

Token

Token

Auth

Token
Attacking Cloud Administration: Token Theft

SSL/TLS Decryption Device

Auth

Token

Cloud Website

Attacker Compromises Device

Token

Auth

Token

Auth
Attacking Cloud Administration: Token Theft

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

Microsoft Azure

Auth

Evil Proxy

Token

https://github.com/kgretzky/evilginx2
Our team is currently looking into reports of stolen passwords. Stay tuned for more.

Password Reuse/Replay

SHA1

112. Han Solo hansolo LeiaIKnow19! hansolo@theacme.io
113. Luke Skywalker lukeskywalker TheForce19 lukeskywalker@Plus.com
Password Hash (of the AD Hash) Sync Enabled: Users with Leaked Credential Report

HaveIBeenPwned.com

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

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
  • 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
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

![Cartoon image with a dog saying "This is fine." during a fire]
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](http://aka.ms/fido2docs)
- Go try this in your test tenant!
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

Admin consent | User consent

Search permissions

<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></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Microsoft Graph</td>
<td>Have full access to user calendars</td>
<td>Delegated</td>
<td>Medium</td>
<td>An admini</td>
</tr>
<tr>
<td>Microsoft Graph</td>
<td>Have full access to user contacts</td>
<td>Delegated</td>
<td>Medium</td>
<td>An admini</td>
</tr>
<tr>
<td>Microsoft Graph</td>
<td>Read Microsoft Intune apps</td>
<td>Delegated</td>
<td>Medium</td>
<td>An admini</td>
</tr>
<tr>
<td>Microsoft Graph</td>
<td>Read and write Microsoft Intune apps</td>
<td>Delegated</td>
<td>High</td>
<td>An admini</td>
</tr>
</tbody>
</table>
Audit Consented Permissions for All Apps

<table>
<thead>
<tr>
<th>PERMISSION</th>
<th>TYPE</th>
<th>PERMISSION LEVEL</th>
<th>GRANTE...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sign users in</td>
<td>Delegated</td>
<td>Medium</td>
<td>15 total users...</td>
</tr>
<tr>
<td>Sign in and read user profile</td>
<td>Delegated</td>
<td>Low</td>
<td>7 total users...</td>
</tr>
<tr>
<td>Read and write access to user profile</td>
<td>Delegated</td>
<td>Unknown</td>
<td>14 total users...</td>
</tr>
<tr>
<td>Read all users' basic profiles</td>
<td>Delegated</td>
<td>Low</td>
<td>14 total users...</td>
</tr>
<tr>
<td>Read and write access to user mail</td>
<td>Delegated</td>
<td>High</td>
<td>14 total users...</td>
</tr>
<tr>
<td>Read and write user and shared mail</td>
<td>Delegated</td>
<td>High</td>
<td>3 total users...</td>
</tr>
<tr>
<td>Search email</td>
<td>Delegated</td>
<td>High</td>
<td>7 total users...</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*
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>
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
### 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
Modernize your password policy

• People choose “strong” but easily guessable passwords
  • August2019! or Summer2019!
• https://aka.ms/passwordguidance
• NIST 800-63B
• Applies to on-prem AD as well!

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

---

Azure AD Banned Password Policy

**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
• 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](https://aka.ms/PasswordSprayBestPractices)
• Disable services at the mailbox level

• Authentication Policies

• Client IP Block
• 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
  - 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)
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.
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.
The Cloud Is Magic!
• 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
• 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
• 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
• 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 Notpeya, 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](https://aka.ms/passwordguidance)
- NIST 800-63 Password Guidance
- Azure AD Banned Password for Active Directory
  - [https://aka.ms/deploypasswordprotection](https://aka.ms/deploypasswordprotection)
- Azure AD Banned Password Policy Scoring
- FRS to DFSR Migration
  - [http://aka.ms/dfsrmig](http://aka.ms/dfsrmig)
• 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

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