How do you do Incident Response for your Azure Active Directory?

Thomas Detzner
Mark Morowczynski (@markmorow)
Program Managers – Identity Division
Agenda

Password Spray
Finding Legacy Authentication
Blocking Legacy Authentication
Go Do’s!
One Day

- “Hey do you have a minute?” – Account Executive
- “Hey do you have a few mins, can I run something by you?” - IAM architect
- “Hey can we do a quick call...immediately?” - CISO
<table>
<thead>
<tr>
<th>Email</th>
<th>Winter</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="mailto:Josi@contoso.com">Josi@contoso.com</a></td>
<td>Winter2019!</td>
</tr>
<tr>
<td><a href="mailto:Chance@wingtiptoys.com">Chance@wingtiptoys.com</a></td>
<td>Winter2019!</td>
</tr>
<tr>
<td><a href="mailto:Rami@fabrikam.com">Rami@fabrikam.com</a></td>
<td>Winter2019!</td>
</tr>
<tr>
<td><a href="mailto:TomH@cohowinery.com">TomH@cohowinery.com</a></td>
<td>Winter2019!</td>
</tr>
<tr>
<td><a href="mailto:AnitaM@cohovineyard.com">AnitaM@cohovineyard.com</a></td>
<td>Winter2019!</td>
</tr>
<tr>
<td><a href="mailto:EitokuK@cpandl.com">EitokuK@cpandl.com</a></td>
<td>Winter2019!</td>
</tr>
<tr>
<td><a href="mailto:Ramanujan@Adatum.com">Ramanujan@Adatum.com</a></td>
<td>Winter2019!</td>
</tr>
<tr>
<td><a href="mailto:Maria@Treyresearch.net">Maria@Treyresearch.net</a></td>
<td>Winter2019!</td>
</tr>
<tr>
<td><a href="mailto:LC@adverture-works.com">LC@adverture-works.com</a></td>
<td>Winter2019!</td>
</tr>
<tr>
<td><a href="mailto:EW@alpineskihouse.com">EW@alpineskihouse.com</a></td>
<td>Winter2019!</td>
</tr>
<tr>
<td><a href="mailto:info@blueyonderairlines.com">info@blueyonderairlines.com</a></td>
<td>Winter2019!</td>
</tr>
<tr>
<td><a href="mailto:AiliS@fourthcoffee.com">AiliS@fourthcoffee.com</a></td>
<td>Winter2019!</td>
</tr>
<tr>
<td><a href="mailto:MM39@litwareinc.com">MM39@litwareinc.com</a></td>
<td>Winter2019!</td>
</tr>
<tr>
<td><a href="mailto:Margie@margiestravel.com">Margie@margiestravel.com</a></td>
<td>Winter2019!</td>
</tr>
<tr>
<td><a href="mailto:Ling-Pi997@proseware.com">Ling-Pi997@proseware.com</a></td>
<td>Winter2019!</td>
</tr>
<tr>
<td><a href="mailto:PabloP@fineartschool.net">PabloP@fineartschool.net</a></td>
<td>Winter2019!</td>
</tr>
<tr>
<td><a href="mailto:GiseleD@tailspintoys.com">GiseleD@tailspintoys.com</a></td>
<td>Winter2019!</td>
</tr>
<tr>
<td><a href="mailto:Luly@worldwideimporters.com">Luly@worldwideimporters.com</a></td>
<td>Winter2019!</td>
</tr>
</tbody>
</table>
730,000+
Compromised accounts due to password spray in the last 4 months
Percentage of password spray attacks coming from legacy protocols
Let’s Agree on Terminology

- Basic authentication
  - Application collects the user’s credentials and sends them to authenticate the user

- Modern authentication
  - Application presents the authenticating user with a browser where they authenticate to the authentication service

- Legacy authentication
  - How we refer to Basic authentication when the credentials are sent to the Application’s service, not the Auth Service
Legacy Authentication, Examples

- Mail clients that use legacy authentication
  - Office 2010 and older
  - Office 2013 by default (can use modern auth with reg key)
  - Clients using older mail protocols (POP, IMAP, SMTP, etc)
    (Most mobile mail apps, Windows Mail, ...)

Legacy Authentication, Examples

Mail clients that use legacy authentication:
- Office 2010 and older
- Office 2013 by default (can use modern auth with reg key)
- Clients using older mail protocols (POP, IMAP, SMTP, etc.) (Most mobile mail apps, Windows Mail, …)
Legacy Authentication, Examples

- Mail clients that use legacy authentication
  - Office 2010 and older
  - Office 2013 by default (can use modern auth with reg key)
  - Clients using older mail protocols (POP, IMAP, SMTP, etc)
    (Most mobile mail apps, Windows Mail, ...)

- Older PowerShell Modules
Legacy Authentication, Examples

- Mail clients that use legacy authentication
  - Office 2010 and older
  - Office 2013 by default (can use modern auth with reg key)
  - Clients using older mail protocols (POP, IMAP, SMTP, etc) (Most mobile mail apps, Windows Mail, …)

- Older PowerShell Modules

- Lesser known culprits: Room Phones, Service Accounts
Modern Authentication (Web Flow)

- Ability to apply other controls (MFA challenge, Device state check, Session restrictions, ...)
- Get SSO with other logins on the machine.
- Applies to mobile devices as well (MAM Policies)
- More information about the user’s login endpoint, this makes Identity Protection more effective
Agenda

Password Spray
Finding Legacy Authentication
Blocking Legacy Authentication
Go Do’s!
Finding Legacy Authentication In Azure AD

- Sign In Logs to examine usage
- POP, IMAP, MAPI, SMTP and ActiveSync go to EXO
- “Other Clients” shows SharePoint and EWS
- If you are federated this will only show SUCCESSFUL events

<table>
<thead>
<tr>
<th>USERNAME</th>
<th>APPLICATION</th>
<th>SIGN-IN STATUS</th>
<th>CLIENT APP</th>
<th>CONDITIONAL ACCEPTANCE</th>
</tr>
</thead>
<tbody>
<tr>
<td>audrey.oliwer@wingt...</td>
<td>Azure Portal</td>
<td>Success</td>
<td>Browser</td>
<td>Success</td>
</tr>
<tr>
<td>audrey.oliwer@wingt...</td>
<td>Azure Portal</td>
<td>Failure</td>
<td>Browser</td>
<td>Success</td>
</tr>
<tr>
<td>audrey.oliwer@wingt...</td>
<td>Azure Portal</td>
<td>Failure</td>
<td>Browser</td>
<td>Failure</td>
</tr>
<tr>
<td>audrey.oliwer@wingt...</td>
<td>Azure Portal</td>
<td>Failure</td>
<td>Unknown</td>
<td>Not Applied</td>
</tr>
<tr>
<td>hannahhanhaha@v...</td>
<td>Microsoft App Acc...</td>
<td>Success</td>
<td>Browser</td>
<td>Success</td>
</tr>
<tr>
<td>Barbara Kess</td>
<td>Barbara Kess</td>
<td>Success</td>
<td>Browser</td>
<td>Not Applied</td>
</tr>
<tr>
<td>Barbara Kess</td>
<td>Barbara Kess</td>
<td>Failure</td>
<td>Unknown</td>
<td>Not Applied</td>
</tr>
<tr>
<td>Barbara Kess</td>
<td>Barbara Kess</td>
<td>Failure</td>
<td>Unknown</td>
<td>Not Applied</td>
</tr>
</tbody>
</table>
Finding Password Spray due to Legacy Authentication in ADFS/Federation Provider

ADFS Audit 411


For 2016+, Audit 1203

Azure AD Connect Health Risky IP Report

<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>
Azure AD + Azure Monitoring =

- **Store (JSON)**: Storing massive amounts of unstructured data using Azure Blob Storage.
- **Push to SIEM**: Big data streaming platform and event ingestion service using Azure EventHub.
- **Analyze**: Collects telemetry to retrieve and analyze data using Azure Log Analytics.

Additional components include:
- **Download/Script**: Database/SIEM Pull (JSON) using Reporting API.
- **Azure AD**
- **Azure Monitor**
Azure AD + Azure Monitoring = Azure Sentinel

Azure AD

Azure Log Analytics
Azure AD Logs into SIEM

• 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 (aka.ms/aad2splunk)
    • Sumo Logic (aka.ms/aad2sumo)
    • IBM QRadar (aka.ms/aad2QRadar)
    • ArcSight (aka.ms/aad2Archsight)
    • SysLog (aka.ms/aad2Syslog)

• Azure Log Analytics or Azure Sentinel
  • https://docs.microsoft.com/en-us/azure/sentinel/connect-azure-active-directory
Azure Workbooks & Azure Sentinel

- Built-In Queries under Workbooks
- Sign-In Errors, Conditional Access and Legacy Auth

**Sign-ins using Legacy Auth**

- All Sign-ins: 38
  - Success: 38

**Legacy Auth Sign-in Details**

<table>
<thead>
<tr>
<th>User</th>
<th>Sign-in Status</th>
<th>Sign-in Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Edward Huntington</td>
<td>Success</td>
<td>6 hours ago</td>
</tr>
<tr>
<td>Edward Huntington</td>
<td>Success</td>
<td>9 hours ago</td>
</tr>
<tr>
<td>Edward Huntington</td>
<td>Success</td>
<td>31 hours ago</td>
</tr>
<tr>
<td>Edward Huntington</td>
<td>Success</td>
<td>2 days ago</td>
</tr>
<tr>
<td>Other clients: IMAP</td>
<td>Success</td>
<td></td>
</tr>
</tbody>
</table>
Azure Workbooks & Azure Sentinel

- Built-In Queries under Insights
- Sign-In Errors, Conditional Access and Legacy Auth!
- Can export these queries to use in Azure Sentinel or SIEM as well
Azure Workbooks & Azure Sentinel

**Sign-ins using Legacy Auth**

- TimeRange: Last 14 days
- Apps: All
- Users: All
- Protocols: All

### Legacy Auth Sign-ins by App and Protocol

<table>
<thead>
<tr>
<th>Name</th>
<th>Sign-in Count</th>
<th>Trend</th>
<th>Failure Count</th>
<th>User Interrupted Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Office 365</td>
<td>38</td>
<td><img src="image" alt="Graph" /></td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Other clients: IMAP</td>
<td>38</td>
<td><img src="image" alt="Graph" /></td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
### Azure Workbooks & Azure Sentinel

#### Log Analytics workspace Logs Query

```plaintext
let data = SignInLogs
| where AppDisplayName in (\{Apps\}) or '*' in (\{Apps\})
| where UserDisplayName in (\{Users\}) or '*' in (\{Users\})
| extend errorCode = toint(Status.errorCode)
| extend SignInStatus = case(errorCode == 0, "Success",
                           errorCode == 50058, "Interrupt",
                           errorCode == 50140, "Interrupt",
                           errorCode == 51006, "Interrupt",
                           errorCode == 50059, "Interrupt",
                           errorCode == 65001, "Interrupt",
                           errorCode == 52001, "Interrupt"
                      )
```

#### Legacy Auth Sign-ins by App and Protocol

<table>
<thead>
<tr>
<th>Name</th>
<th>Sign-in Count</th>
<th>Trend</th>
<th>Failure Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Office 365</td>
<td>38</td>
<td><img src="image" alt="Trend Chart" /></td>
<td>0</td>
</tr>
<tr>
<td>Other clients, IMAP</td>
<td>38</td>
<td><img src="image" alt="Trend Chart" /></td>
<td>0</td>
</tr>
</tbody>
</table>
Agenda

Password Spray
Finding Legacy Authentication
Blocking Legacy Authentication
Go Do’s!
Blocking Legacy Auth in Exchange

Disable services at the mailbox level


Authentication Policies


Client IP Block


```
PS 0:
Set-OrganizationConfig -IPListBlocked 41.204.224.0/24,41.203.78.0/24
```
ADFS Extranet and Smart Lockout

• Extranet Lockout
  • Window Server 2012R2
  • Doesn’t pass the authentication request to Active Directory when threshold reached
  • Prevents brute force but user can still be locked out from extranet

• Smart Lockout
  • Windows Server 2016 and 2019
  • Keeps track of IP of valid logins
  • Prevents brute force, denial of service and some password spray
  • https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/operations/configure-ad-fs-extranet-smart-lockout-protection
Blocking Authorization in ADFS/Federation Provider

Authorization Rules

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

```c
{Type == "http://schemas.microsoft.com/ws/2012/01/insidecorporatenetwork", Value == "false"]
&& c1: [Type == "http://schemas.microsoft.com/2012/01/requestcontext/claims/x-ms-endpoint-absolute-path", Value == "/adfs/services/trust/*.*"]
&& c2: [Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/groupsid", Value == "((?!);
=> issue(Type = "http://schemas.microsoft.com/authorization/claims/deny", Value = "DenyUsersWithClaim");
```
Blocking Legacy Authentication in Azure AD

Block those that are NOT using FIRST
- Block Today with Conditional Access
- Requires Azure AD P1

Update Clients / Apps

Only Service Accounts / Apps should remain
- Ring fence those

FYI:
Legacy auth support for Exchange Online being deprecated on October 13th, 2020. Impacts:
- Exchange ActiveSync (EAS)
- IMAP
- POP
- Remote PowerShell
Agenda

Password Spray
Finding Legacy Authentication
Blocking Legacy Authentication
Go Do’s!
I migrated our northern data center to the cloud.

But the cloud stopped working and I can't find the phone number for our cloud guy. I so... whatever.

You lost our data center? That's one way to look at it.
Go Dos!

- Confirm Modern Authentication is enabled, move to Office 2016
- Enable Mailbox auditing, ALL auditing
  - Required if tenant was created **BEFORE Jan 2019**
- If you are Federated with ADFS, deploy **Smart Lockout**
- Make sure you have Azure AD Connect Health for ADFS installed
- Find and understand Legacy Auth Usage in your organization
  - Integrated Azure AD logs with your SIEM or use Log Analytics or Azure Sentinel
Go Dos!

- Start shutting it down by scenario
  - Every end user who is *not* using a Legacy Auth should have it shut down at the Application level
  - Every service account that needs it should, have only the protocol it uses, possibly constrained by IP
  - If you had legacy clients as your standard enterprise clients, build a plan for Modern Auth. This is the biggest identity risk facing your organization today.
  - Ask for forgiveness, not permission

- Modernize your password policy [https://aka.ms/passwordguidance](https://aka.ms/passwordguidance)
  - Use the Azure AD Banned Password List (works with AD too!)
  - Deploy Azure AD Password Protection to your on premises
  - [https://aka.ms/deploypasswordprotection](https://aka.ms/deploypasswordprotection)
Bonus Content: I’ve been Legacy Auth’ed! Help me!

- Figure out what was exfiltrated/access/changed
  - Search the audit log in the Security & Compliance Center
  - Use Search-UnifiedAuditLog

- Bonus link: Looking for malicious behavior in O365
Contact

Thomas Detzner
tdetzner@microsoft.com

Mark Morowczynski (  markmorow)
markmoro@microsoft.com

Program Managers – Identity Division