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

Ian Farr
Ian Parramore
Program Managers – Identity Division
Agenda

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

- “Have you heard anything from Customer X? Something seems to be going on?” – Colleague

- “Have you heard anything from Customer X? Something seems to be going on?” – Account Executive

- “…” – Customer

Sunday...

- “Help, we’re in the middle of a breach!” – Customer
Password Spray

Josi@contoso.com
Chance@wingtiptoy.com
Rami@fabrikam.com
TomH@cohowinery.com
AnitaM@cohovineyard.com
EitokuK@cpandl.com
Ramanujan@Adatum.com
Maria@Treyresearch.net
LC@adventure-works.com
EW@alpineskihouse.com
info@blueyonderairlines.com
AiliS@fourthcoffee.com
MM39@litwareinc.com
Margie@margiestravel.com
Ling-Pi997@proseware.com
PabloP@fineartschool.net
GiseleD@tailspintoys.com
Luly@worldwideimporters.com

Newyear2020!
730,000+

Compromised accounts due to password spray
(last 4 months)
~100%
Percentage of password spray attacks from legacy protocols
Let’s agree on **terminology**

- **Basic Authentication**
  - Application collects username and password and sends it to an auth service.

- **Legacy Authentication**
  - Basic authentication where credentials are sent to an auth service.
  - Can only present username / password.
  - No support for MFA, richer client / auth service interface.

- **Modern Authentication**
  - Application presents authenticating user with browser to authenticate to authentication service.
  - Ability to apply other controls – e.g., MFA, trusted device, session.
Legacy Authentication, examples...

- Mail clients that use Legacy Auth
  - 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
Legacy Authentication, examples:

- Mail clients that use Legacy Auth
- 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
Legacy Authentication, examples...

- Mail clients that use Legacy Auth
- 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

- Lesser known culprits: Room Phones, Service Accounts
Agenda

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

- Sign-In Logs
- POP, IMAP, MAPI, SMTP and ActiveSync go to EXO
- “Other Clients” = SharePoint and EWS
- Federated domains WON’T show FAILED authentications
Finding Password Spray due to Legacy Authentication in ADFS

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 Monitor =

- Store (JSON)
  - Storing massive amounts of unstructured data
    - Azure Blob Storage

- Push to SIEM
  - Big data streaming platform and event ingestion service
    - Azure EventHub

- Analyze
  - Collects telemetry to retrieve and analyze data
    - Azure Log Analytics

- Download
- Script
- Database / SIEM
  - Pull (JSON)
- Reporting API
- Azure AD
Azure AD + Azure Monitor = 💖

Diagram:
- Azure AD
- Azure Log Analytics
- Azure Sentinel

Connections:
- Azure AD to Azure Log Analytics
- Azure Log Analytics to Azure Sentinel
Azure AD Logs into SIEM

- Pull from Azure AD Graph API
- 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
Azure Log Analytics Workbooks

- Built-In Queries
  - Sign-Ins, Conditional Access, App Consent Audit and Legacy Auth!
Azure Log Analytics Workbooks – Edit Mode

```
let data = SigninLogs
| where AppDisplayName in {{Apps}} or +++ in {{Apps}}
| where UserId in {{Users}} or +++ in {{Users}}
| extend CAstatus = case(ConditionalAccessStatus == "success", "Successful",
  ConditionalAccessStatus == "failure", "Failed",
  ConditionalAccessStatus == "notApplied", "Not applied",
  isempty(ConditionalAccessStatus), "Not applied",
  "Disabled")
| mexpand ConditionalAccessPolicies
| extend CAGrantControlName = tostring(ConditionalAccessPolicies.enforcedGrantControls[8])
| extend CAGrantControl = case(CAGrantControlName contains "MFA", "Require MFA",
  CAGrantControlName contains "Terms of Use", "Require Terms of Use",
  CAGrantControlName contains "Privacy", "Require Privacy Statement",
  CAGrantControlName contains "Device", "Require Device Compliant",
  CAGrantControlName contains "Azure AD Joined", "Require Hybrid Azure AD Joined Device",
  CAGrantControlName contains "Apps", "Require Approved Apps",
  "Other")

data
| summarize Count = dcount(Id) by CAstatus
| join kind = inner (data
  | make-series Trend = dcount(Id) default = 0 on TimeGenerated in range([TimeRange:start], [TimeRange:end], [TimeRange:grain]) by CAstatus}
```
Azure Sentinel Workbooks

Azure AD Audit logs
Azure AD Sign-in logs
Insecure Protocols
Agenda

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

Disable services at mailbox level


Authentication Policies


Client IP Block


```bash
PS 0:
New-AuthenticationPolicy -Name "Block Basic Authentication"
```
ADFS Extranet and Smart Lockout

- Smart Lockout
  - Windows Server 2016 and 2019
  - Keeps track of IP of valid logins
  - Prevents brute force, denial of service and some password spray

- Extranet Lockout
  - Window Server 2012 R2
  - Doesn’t pass authentication request to Active Directory when threshold reached
  - Prevents brute force but user can still be locked out from extranet
Blocking Authorisation in ADFS / Federation Provider

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

https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/operations/access-control-policies-w2k12
Blocking Legacy Authentication in Azure AD

- Block **today** with Conditional Access
- Only Service Accounts / apps should remain
  - Ring-fence and **protect**
- Report Only mode
  - “Audit Only” policy mode
  - Evaluate impact before switching on

https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-report-only
Agenda

Password Spray
Finding Legacy Authentication
Blocking Legacy Authentication

Go Do’s!
Go Dos!

- Confirm Modern Auth is enabled
  - Enable MFA / Go Passwordless / Device Trust

- Enable Mailbox auditing - ALL auditing!
  - Required if tenant created **BEFORE Jan 2019**

- If Federated with ADFS, deploy Smart Lockout

- Find and understand Legacy Auth usage in organization
  - Integrate Azure AD logs with your SIEM or use Log Analytics or Azure Sentinel
Go Dos!

· Start shutting down by scenario
  · Every end user *not* using Legacy Auth should have legacy auth shut down at app level
  · Every service account that needs Legacy Auth should have be constrained to only the protocol it uses
    · Possibly constrained by IP
  · If enterprise clients are Legacy Auth clients, build a plan for Modern Auth
  · Ask for forgiveness, not permission

· Modernize your password policy
  · [https://aka.ms/passwordguidance](https://aka.ms/passwordguidance)
  · Deploy Azure AD Password Protection to on premises
    · [https://aka.ms/deploypasswordprotection](https://aka.ms/deploypasswordprotection)

· Five steps to secure your Identity infrastructure
Bonus Content: I’ve been Legacy Auth’ed! Help me!

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

- Bonus link: looking for malicious behavior in O365

- Best practices for defending against password spray attacks
Contact

Ian Farr
ianfarr@microsoft.com

Ian Parramore
ianparr@microsoft.com

Program Managers – Identity Division