Legacy Authentication and Password Spray, Understanding and Stopping Attackers Favorite TTPs in Azure AD

Mark Morowczynski @markmorow
Ramiro Calderon @ramiroclld
Principal Program Manager- Identity Division
Who We Are?

Identity Product Group,
Customer Experience (CXP) Team
SANS STI Student
How Many People have Azure Active Directory?
Agenda

What is Legacy Authentication
How To Find Legacy Authentication In Your Environment
Successfully Blocking Legacy Auth
Legacy Authentication

Basic authentication

- Typically a single factor (username/password)
- Applications and protocols don’t support Multi-Factor Authentication

Federated with Azure AD/O365

- IDP is responsible for authentication, including basic auth!
Legacy Authentication, Examples

Clients that use legacy authentication

(can use modern authentication methods with newer clients)


Modern Authentication (Web Flow)

More tools to protect resources
Ability to handle an MFA challenge/response
Can include additional information about the device (Hybrid Domain Join)
Applies to mobile devices as well (MAM Policies)
More information an attacker has to guess correctly to spoof (this is good news for us!)

User Agent, Application Target
Email client connects to EXO with basic auth U/P
EXO queries Azure AD for tenant config -> Federated
EXO sends an Auth request to on-prem IdP
EXO sends the SAML token to Azure AD
Azure AD validates IDP token and evaluates CA policies
Azure AD issues token to EXO
EXO returns mail-service specific content
Modernize your password policy

People choose “strong” but easily guessable passwords. June2019! Or Summer2019!

https://aka.ms/passwordguidance

NIST 800-63B

Implement Azure AD Banned Password Policy

Applies to on-prem AD as well!

https://aka.ms/deploypasswordprotection
Password Spray

Common password used against many, many accounts.

Basic Attacker—Same Source IP, Same Password

Intermediate Attacker—Multiple IPs, Same Password

Advanced Attacker—Multiple IPs, different likely passwords

About 1% of users will fall victim to this O365 Attack Simulator can do this!

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@tailspintoy.com
Luly@worldwideimporters.com
Bjorn@woodgrovebank.com
NK@lucernepublishing.com
Legacy Authentication and Password Spray In The Real World

August 2018- 200k accounts compromised due to password spray
January 2019- 158k accounts compromised due to password spray
February 2019- 143k accounts compromised due to password spray
March 2019- 278k accounts compromised due to password spray
April 2019- 125k accounts compromised due to password spray

Nearly 100% of password spray attacks we see are from legacy authentication

Blocking legacy auth reduces compromise rate by 66%

https://aka.ms/PasswordSprayBestPractices
Agenda

What is Legacy Authentication

How To Find Legacy Authentication In Your Environment

Successfully Blocking Legacy Auth
Identity Protection
Role Based Access Control
Core Store
Azure Active Directory

Authentication flows
Authorization flows
Authentication Services
Conditional Access Engine
Identity Protection

AD FS Audits
Azure AD Connect Health Reports
Azure AD Sign in reports
Azure AD Risk Events
Exchange Mailbox Audits

Legacy Authentication
Client Network
Microsoft Cloud Services
Office 365
U/P App Cache

Unauthenticated
Authenticated
Authorized

How?  Where?  Find!  Stop!
Finding 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>104.206.238.9</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>
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 the SUCCESFUL
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 as well
Finding The Damage of Legacy Authentication in Exchange Online

First, enable all mailbox logging

Required if tenant was created **BEFORE** Jan 2019


Figure out what was exfiltrated/access/changed

Bonus link: Looking for malicious behavior in O365
Agenda

What is Legacy Authentication
How To Find Legacy Authentication In Your Environment
Successfully Blocking Legacy Auth
Identity Protection

Role Based Access Control

Core Store

Azure Active Directory

Authentication Services

Conditional Access Engine

Conditional Access Policies

Exchange Online

Mailbox Auth Lockdown

Authentication Policies

Client IP Block

AD FS

Extranet Soft Lockout

Extranet Smart Lockout

AD FS AuthZ rules

Azure AD

Conditional Access Policies

How? Where? Find! Stop!

Microsoft Cloud Services

Office 365

U/P App Cache

Client Network

IDP

On-premises

DC

Legacy Authentication

Microsoft Cloud Services

Azure Active Directory
Blocking Legacy Auth in Exchange

Disable services at the mailbox level


Authentication Policies


Client IP Block

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
Blocking Legacy Auth In Azure AD

Block those that are NOT using FIRST
Block Today with Conditional Access
Requires Azure AD P1
Update Clients
Only Service Accounts / Apps should remain
FYI, Basic Auth Support for EWS will be decommissioned by October 2020
Go Dos!

Confirm Modern Authentication is enabled

Enable Mailbox auditing, all auditing

Find Legacy Auth Usage

  Block those that are NOT using Legacy protocols

  Setup a dashboard to monitor continuous usage

Restrict Legacy Auth usage to corpnet if possible, to start

Modernize your password policy https://aka.ms/passwordguidance

  Use the Azure AD Banned Password List (works with AD too!)

    https://aka.ms/deploypasswordprotection

Start updating clients, disabling legacy protocols and blocking with Azure AD Conditional Access
Questions

Mark Morowczynski @markmorow
Ramiro Calderon @ramiroclld
Principal Program Managers