You Moved to Office 365

Now What?

Sean Metcalf
Founder, Trimarc
ABOUT
❖ Founder Trimarc ([Trimarc.io](https://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 (2018)
❖ Speaker: Black Hat, Blue Hat, BSides, DEF CON, DerbyCon, Shakacon, Sp4rkCon, Troopers
❖ Security Consultant / Researcher
❖ AD Enthusiast - Own & Operate [ADSecurity.org](https://ADSecurity.org) (Microsoft platform security info)
AGENDA
• The “Cloud”
• Attacking the Cloud
• Auditing
• Administration
• Cloud Security Controls
• Controlling Access
• Password Insight
• Cloud Security “Tune Up”
• Office 365 Subscriptions & Capability
• Best Practices & Wrap-up
• BONUS: Testing Defenses

Sean Metcalf (@PyroTek3) TrimarcSecurity.com
I’m working on slides for my @BSidesCharm talk called “You moved to Office 365, Now What?”
What would you like me to include?

Yeah I do cloud stuff too.
It’s like AD, just in Azure 😊
Responses by Category

- Logging: 10
- Security Features & Controls: 7
- ADFS: 5
- Misc: 4
- Protocol Control: 2

[ Sean Metcalf | @PyroTek3 | TrimarcSecurity.com ]
Moving to the Microsoft Cloud

• Sign up for Office 365 – first one in gets Global Admin!
• Configure Azure AD Connect to synchronize users & groups
• Move Exchange mail to Exchange Online (keep 1 Exchange server on-prem for management)
• Update mail flow
• ...

[ Sean Metcalf | @PyroTek3 | TrimarcSecurity.com ]
The Cloud Is Magic!
“The cloud is more secure since _____ spends millions every year on cloud security”
Internal Network

Intranet (LAN)

DMZ

Router (WAN)
Anywhere Cloud Access

SaaS Applications

Office Portal

portal.office.com

Exchange Online
Multi-Tenant

outlook.office365.com
outlook.office.com

Yammer

Yammer.com

Azure AD (eSTS)

login.microsoftonline.com
Azure Active Directory in the Marketplace

Every Office 365 and Microsoft Azure customer uses Azure Active Directory

- 17.5M organizations
- 1.1B identities
- 634K 3rd party apps in Azure AD
- 90K paid Azure AD / EMS customers
- 450B monthly authentications
- 90% of Fortune 500 companies

Source: Microsoft Ignite Conference 2018
https://myignite.techcommunity.microsoft.com/sessions/64565?source=sessions
Cloud Active Directory?

**On-premises Active Directory**
- Authentication, Directory, & Management
- AD Forest for single entity
- Internal corporate network
- Authentication
  - Kerberos
  - NTLM
- LDAP
- Group Policy

**Azure AD (Office 365)**
- Identity
- Designed for multi-tenant
- Cloud/web-focused
- Authentication
  - SAML 2.0
  - OpenID Connect
  - OAuth 2.0
  - WS-Federation
- REST API: AD Graph API
# Attackers Love the Cloud

The threats are real, global, and target all of us.

### Common Passwords Attempted in Password Spray Attacks

<table>
<thead>
<tr>
<th>Password</th>
<th>SPRING</th>
<th>2018</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summer</td>
<td>September</td>
<td>1234</td>
</tr>
<tr>
<td>Winter</td>
<td>Football</td>
<td>Your Company Name</td>
</tr>
</tbody>
</table>

1.29 Billion Authentication blocked in August 2018

81% of data breaches involved weak, default, or stolen passwords

Source: Microsoft Ignite Conference 2018

[ Sean Metcalf | @PyroTek3 | TrimarcSecurity.com ]
Attacks on the Cloud

300% increase in identity attacks over the past year.

Source: Microsoft Ignite Conference 2018
https://myignite.techcommunity.microsoft.com/sessions/64523?source=sessions

[ Sean Metcalf | @PyroTek3 | TrimarcSecurity.com ]
Alert (TA18-086A)
Brute Force Attacks Conducted by Cyber Actors

Original release date: March 27, 2018 | Last revised: March 28, 2018

Systems Affected
Networked systems

Overview

According to information derived from FBI investigations, malicious cyber actors are increasingly using a style of brute force attack known as password spraying against organizations in the United States and abroad.

On February 2018, the Department of Justice in the Southern District of New York, indicted nine Iranian nationals, who were associated with the Mabna Institute, for computer intrusion offenses related to activity described in this report. The techniques and activity described herein, while characteristic of Mabna actors, are not limited solely to use by this group.

The Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI) are releasing this Alert to provide further information on this activity.

Description

In a traditional brute-force attack, a malicious actor attempts to gain unauthorized access to a single account by guessing the password. This can quickly result in a targeted account getting locked-out, as commonly used account-lockout policies allow three to five bad attempts during a set period of time. During a password-spray attack (also known as the “low-and-slow” method), the malicious actor attempts a single password against many accounts before moving on to attempt another password. This method can work in areas where account-lockout policies are not used, or when account-lockout policies do not effectively prevent access.
Cloud Attack Timeline

Source: Microsoft Ignite Conference 2018

1. Day 1 – 11: Attacker compromises privileged user's non MFA-enabled account.


3. Day 137 – 143: Attackers create rules on Contoso’s SharePoint and email to automate data exfiltration to a cloud storage solution.

4. Day 16 – 163: Attacker uses stolen credentials to VPN into corporate network.


https://myignite.techcommunity.microsoft.com/sessions/64523?source=sessions
Attacking the Cloud: Password Spraying

MailSniper
https://github.com/dafthack/MailSniper

MailSniper is a penetration testing tool for searching through email in a Microsoft Exchange environment for specific terms (passwords, insider intel, network architecture information, etc.). It can be used as a non-administrative user to search their own email, or by an Exchange administrator to search the mailboxes of every user in a domain.

MailSniper also includes additional modules for password spraying, enumerating users/domains, gathering the Global Address List from OWA and EWS, and checking mailbox permissions for every Exchange user at an organization.

For more information about the primary MailSniper functionality check out this blog post.

For more information about additional MailSniper modules check out these blog posts:

- GAL & Password Spraying
- Invoke-OpenInboxFinder

Download the MailSniper Field Manual to quickly reference various MailSniper functions.

[ Sean Metcalf | @PyroTek3 | TrimarcSecurity.com ]
Attacking the Cloud: Password Spraying

Password Spraying the OWA portal at https://outlook.office365.com/owa/. Sit tight...
5 threads remaining

[*] Now spraying the OWA portal at https://outlook.office365.com/owa/
[*] Current date and time: 11/04/2018 09:59:26

[ Sean Metcalf | @PyroTek3 | TrimarcSecurity.com ]
EWS Capability

- Availability
- Bulk Transfer
- Delegate Management
- Exchange Store Search
- Exchange Search
- Federated Sharing Folder
- Inbox Rules Item
- Mail Tips Messaging
- Records Management
- Message Tracking Notification
- Service Configuration Synchronization
- Unified Messaging User Configuration Utility
Attacking the Cloud: Password Spraying

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

5 threads remaining
[oooooooooooooooooooooooooooooooooooooo]

>> -userlist 'C:\Temp\0365\UserList.txt' -OutFile 'c:\temp\0365\ews-sprayed-creds.txt' -password 'Password99!'

[*] Now spraying the EWS portal at https://outlook.office365.com/EWS/Exchange.asmx
[*] Current date and time: 11/04/2018 09:56:01
[*] Trying Exchange version Exchange2010
Attacking the Cloud: Password Spraying

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

5 threads remaining.

[*] A total of 1 credentials were obtained.
Results have been written to c:\temp\0365\ews-sprayed-creds.txt.
[*] Now spraying the EWS portal at https://outlook.office365.com/EWS/Exchange.asmx
[*] Current date and time: 11/04/2018 10:30:20
[*] Trying Exchange version Exchange2010
[*] SUCCESS! User:TrimarcRD.com\DarthVader@TrimarcRD.com Password:Summer2018!
[*] A total of 1 credentials were obtained.
Results have been written to c:\temp\0365\ews-sprayed-creds.txt.
[*] Now spraying the EWS portal at https://outlook.office365.com/EWS/Exchange.asmx
[*] Current date and time: 11/04/2018 10:30:34
[*] Trying Exchange version Exchange2010
[*] SUCCESS! User:TrimarcRD.com\HanSolo@TrimarcRD.com Password:Password99!
[*] A total of 1 credentials were obtained.
Results have been written to c:\temp\0365\ews-sprayed-creds.txt.
[*] Now spraying the EWS portal at https://outlook.office365.com/EWS/Exchange.asmx
[*] Current date and time: 11/04/2018 10:30:48
[*] Trying Exchange version Exchange2010
[*] SUCCESS! User:TrimarcRD.com\JangoFett@TrimarcRD.com Password:Password#99
[*] A total of 1 credentials were obtained.
Results have been written to c:\temp\0365\ews-sprayed-creds.txt.
[*] Now spraying the EWS portal at https://outlook.office365.com/EWS/Exchange.asmx
[*] Current date and time: 11/04/2018 10:31:01
[*] Trying Exchange version Exchange2010
Attacking the Cloud: Password Spraying

Now spraying the EWS portal at https://outlook.office365.com/EWS/Ex

Current date and time: 11/04/2018 10:31:16

Trying Exchange version Exchange2010

SUCCESS! User:TrimarcRD.com\Leia@TrimarcRD.com Password:Password99

A total of 1 credentials were obtained.

Results have been written to c:\temp\O365\ews-sprayed-creds.txt.
# Attacking the Cloud: Password Spraying

<table>
<thead>
<tr>
<th>Date/Time</th>
<th>Username</th>
<th>Service</th>
<th>Result</th>
</tr>
</thead>
</table>
### Attacking the Cloud: Password Spraying

<table>
<thead>
<tr>
<th>Basic info</th>
<th>Device info</th>
<th>MFA info</th>
<th>Conditional Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Request Id</td>
<td>b6c4fd5c-a7b0-4d75-ba65-5ba429789700</td>
<td></td>
<td>IP address 137.135.</td>
</tr>
<tr>
<td>Correlation Id</td>
<td>c8dec77b-2c4c-4071-8a7c-4bed95359c01</td>
<td></td>
<td>Location Washington, Virginia, US</td>
</tr>
<tr>
<td>User</td>
<td>Leia</td>
<td></td>
<td>Date 11/4/2018, 10:31:29 AM</td>
</tr>
<tr>
<td>Username</td>
<td><a href="mailto:leia@trimarcrd.com">leia@trimarcrd.com</a></td>
<td></td>
<td>Status Success</td>
</tr>
<tr>
<td>User ID</td>
<td>2a8165e3-296c-4168-aa52-968bce5f1ef0</td>
<td></td>
<td>Client App Other clients; Older Office clients</td>
</tr>
<tr>
<td>Application</td>
<td>Office 365 Exchange Online</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Application ID</td>
<td>00000002-0000-0ff1-ce00-000000000000</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Attacking the Cloud: Password Spraying

<table>
<thead>
<tr>
<th>Basic info</th>
<th>Device info</th>
<th>MFA info</th>
<th>Conditional Access</th>
<th>Troubleshooting and support</th>
</tr>
</thead>
<tbody>
<tr>
<td>Request Id</td>
<td>b6c4fd5c-a7b0-4d75-ba65-5ba475769700</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Correlation Id</td>
<td>8603d100-6135-45d1-956b-e8f360d99e6f</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>User</td>
<td>Leia</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Username</td>
<td><a href="mailto:leia@trimarcrd.com">leia@trimarcrd.com</a></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>User ID</td>
<td>2a8165e3-296c-4168-aa52-968bce5f1ef0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Application</td>
<td>Office 365 Exchange Online</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Application ID</td>
<td>00000002-0000-0ff1-ce00-000000000000</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IP address</td>
<td>137.135</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Location</td>
<td>Washington, Virginia, US</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Date</td>
<td>11/4/2018, 10:31:11 AM</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Status</td>
<td>Failure</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sign-in error code</td>
<td>50126</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Failure reason</td>
<td>Invalid username or password or Invalid on-premise username or password.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Client App</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ISP</td>
<td>Microsoft Corporation</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IP Geolocation Information</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Continent</td>
<td>North America (NA)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Country</td>
<td>United States (US)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>City</td>
<td>Washington</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

[ Sean Metcalf | @PyroTek3 | TrimarcSecurity.com ]
Cloud Auditing

[ Sean Metcalf | PyroTek3 | TrimarcSecurity.com ]
## Microsoft Cloud Auditing

<table>
<thead>
<tr>
<th>Audit Item</th>
<th>Category</th>
<th>Enabled by Default</th>
<th>Retention</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Activity</td>
<td>Office 365 Security &amp; Compliance Center</td>
<td>No</td>
<td>90 days</td>
</tr>
<tr>
<td>Admin Activity</td>
<td>Office 365 Security &amp; Compliance Center</td>
<td>No</td>
<td>90 days</td>
</tr>
<tr>
<td>Mailbox Auditing</td>
<td>Exchange Online</td>
<td>No*</td>
<td>90 days</td>
</tr>
<tr>
<td>Sign-in Activity</td>
<td>Azure AD</td>
<td>Yes</td>
<td>30 days (AAD P1)</td>
</tr>
</tbody>
</table>
| Users at Risk         | Azure AD                                | Yes                | 7 days  
|                        |                                         |                     | 30 days (AAD P1)     |
| Risky Sign-ins        | Azure AD                                | Yes                | 7 days  
|                        |                                         |                     | 30 days (AAD P1)     |
|                       |                                         |                     | 90 days (AAD P2)     |
| Azure MFA Usage       | Azure AD                                | Yes                | 30 days              |
| Directory Audit       | Azure AD                                | Yes                | 7 days  
|                        |                                         |                     | 30 days (Azure AD P1/P2) |

* Microsoft is gradually enabling mailbox auditing for tenants.
Enable User & Admin Activity Auditing

Audit log search

To use this feature, turn on auditing so we can start recording user and admin activity in your organization. When you turn this on, activity will be recorded to the Office 365 audit log and available to view in a report.

Need to find out if a user deleted a document or if an admin reset someone’s password? Search the Office 365 audit log to find out what the users and admins in your organization have been doing. You’ll be able to find activity related to email, groups, documents, permissions, directory services, and much more. Learn more about searching the audit log.

Search

Activities

Show results for all activities

Start date

2018-10-20

End date

2018-10-28

Results

| Date | IP address | User | Activity | Item | Detail |

Run a search to view results
Enable User & Admin Activity Auditing

Audit log search

We're preparing the Office 365 audit log. You'll be able to search for user and admin activity in a couple of hours.

Need to find out if a user deleted a document or if an admin reset someone's password? Search the Office 365 audit log to find out what the users and admins in your organization have been doing. You'll be able to find activity related to email, groups, documents, permissions, directory services, and much more. Learn more about searching the audit log

Search

Show results for all activities

Start date

2018-10-20

00:00

End date

2018-10-28

00:00

Run a search to view results

[ Sean Metcalf | @PyroTek3 | TrimarcSecurity.com ]
Get Mailbox Auditing

```powershell
PS C:\> Get-Mailbox -ResultSize Unlimited -Filter {RecipientTypeDetails -eq "UserMailbox"} | FL Name,Audit*

<table>
<thead>
<tr>
<th>Name</th>
<th>AuditEnabled</th>
<th>AuditLogAgeLimit</th>
<th>AuditAdmin</th>
<th>AuditDelegate</th>
<th>AuditOwner</th>
</tr>
</thead>
<tbody>
<tr>
<td>SeanMetcalf</td>
<td>False</td>
<td>90.00:00:00</td>
<td>{Update, MoveToDeletedItems, SoftDelete, HardDelete}</td>
<td>{Update, MoveToDeletedItems, SoftDelete, HardDelete}</td>
<td>{Update, MoveToDeletedItems, SoftDelete, HardDelete}</td>
</tr>
<tr>
<td>hailey</td>
<td>False</td>
<td>90.00:00:00</td>
<td>{Update, MoveToDeletedItems, SoftDelete, HardDelete}</td>
<td>{Update, MoveToDeletedItems, SoftDelete, HardDelete}</td>
<td>{Update, MoveToDeletedItems, SoftDelete, HardDelete}</td>
</tr>
</tbody>
</table>
```
Enable Mailbox Auditing

```powershell
Get-Mailbox -ResultSize Unlimited -Filter {RecipientTypeDetails -eq "UserMailbox"} | ` Set-Mailbox -AuditEnabled $true -AuditOwner MailboxLogin,HardDelete,SoftDelete

Get-Mailbox -ResultSize Unlimited -Filter {RecipientTypeDetails -eq "UserMailbox"} | ` FL Name,Audit*
```

<table>
<thead>
<tr>
<th>Name</th>
<th>SeanMetcalf</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>AuditEnabled</strong></td>
<td>True</td>
</tr>
<tr>
<td>AuditLogAgeLimit</td>
<td>90.00:00:00</td>
</tr>
<tr>
<td>AuditAdmin</td>
<td>Update, MoveToDeletedItems, SoftDelete, HardDelete...</td>
</tr>
<tr>
<td>AuditDelegate</td>
<td>Update, MoveToDeletedItems, SoftDelete, HardDelete...</td>
</tr>
<tr>
<td>AuditOwner</td>
<td>SoftDelete, HardDelete, MailboxLogin</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name</th>
<th>bailey</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>AuditEnabled</strong></td>
<td>True</td>
</tr>
<tr>
<td>AuditLogAgeLimit</td>
<td>90.00:00:00</td>
</tr>
<tr>
<td>AuditAdmin</td>
<td>Update, MoveToDeletedItems, SoftDelete, HardDelete...</td>
</tr>
<tr>
<td>AuditDelegate</td>
<td>Update, MoveToDeletedItems, SoftDelete, HardDelete...</td>
</tr>
<tr>
<td>AuditOwner</td>
<td>SoftDelete, HardDelete, MailboxLogin</td>
</tr>
</tbody>
</table>

[ Sean Metcalf | @PyroTek3 | TrimarcSecurity.com ]
Getting Office 365 Logs in Your SIEM

### SIEM server integration Microsoft 365

A SIEM server can receive data from a wide variety of Microsoft 365 services and applications. The following table lists several Microsoft 365 services and applications along with SIEM server inputs and where to go to learn more about SIEM server integration.

<table>
<thead>
<tr>
<th>Microsoft 365 Service or Application</th>
<th>SIEM server inputs</th>
<th>Resources to learn more</th>
</tr>
</thead>
<tbody>
<tr>
<td>Office 365 Advanced Threat Protection or Office 365 Threat Intelligence</td>
<td>Audit logs</td>
<td>SIEM integration with Office 365 Advanced Threat Protection</td>
</tr>
<tr>
<td>Microsoft Cloud App Security</td>
<td>Log integration</td>
<td>SIEM integration with Microsoft Cloud App Security</td>
</tr>
<tr>
<td>Office 365 Cloud App Security</td>
<td>Log integration</td>
<td>Integrate your SIEM server with Office 365 Cloud App Security</td>
</tr>
<tr>
<td>Windows Defender Advanced Threat Protection</td>
<td>Log integration</td>
<td>Pull alerts to your SIEM tools</td>
</tr>
<tr>
<td>Azure Security Center (Threat Protection and Threat Detection)</td>
<td>Alerts</td>
<td>Azure Security data export to SIEM - Pipeline Configuration - Preview</td>
</tr>
<tr>
<td>Azure Active Directory Identity Protection</td>
<td>Audit logs</td>
<td>Integrate Azure Active Directory audit logs</td>
</tr>
<tr>
<td>Azure Advanced Threat Analytics</td>
<td>Log integration</td>
<td>ATA SIEM log reference</td>
</tr>
</tbody>
</table>
Getting Office 365 Logs in Your SIEM

### Important

You must be an Office 365 global administrator or have the security administrator role assigned for the Security & Compliance Center to set up SIEM integration with Office 365 Advanced Threat Protection. Audit logging must be turned on for your Office 365 environment. To get help with this, see [Turn Office 365 audit log search on or off](https://docs.microsoft.com/en-us/office365/securitycompliance/siem-server-integration).

Azure Sentinel (Preview)

- Cloud native SIEM
- Aggregates data from various sources (on-prem & multiple clouds)
- Microsoft analytics to help detect threats
- Built-in orchestration with connectors to other systems.

[ Sean Metcalf | @PyroTek3 | TrimarcSecurity.com ]
Azure Sentinel Detection via GitHub

<table>
<thead>
<tr>
<th>Branch: master</th>
<th>Azure-Sentinel / Detections /</th>
<th>Create new file</th>
<th>Find file</th>
<th>History</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>AWSCloudTrail : change technique to tactic</td>
<td>a month ago</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>AzureActivity : change technique to tactic</td>
<td>a month ago</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>CommonSecurityLog : change technique to tactic</td>
<td>a month ago</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>DnsEvents : change technique to tactic</td>
<td>a month ago</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>MultipleDataSources : Adding in Ajeet’s for March</td>
<td>25 days ago</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>OfficeActivity : OfficeActivity detections and hunting from ashwin (#141)</td>
<td>11 days ago</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>SecurityEvent : Updating list of WellKnownGroupSID to include DNSAdmins and DnsUpdat... (</td>
<td>23 days ago</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>SigninLogs : Azure portal brute force (#136)</td>
<td>24 days ago</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Syslog : change technique to tactic</td>
<td>a month ago</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>VMCConnection : Adding a couple of interesting queries I threw together while doing r... (</td>
<td>11 days ago</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>W3CISLog : pushing initial version of PrivAccountTracking and some minor fixes</td>
<td>28 days ago</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>readme.md : Updating Detections Readme</td>
<td>2 months ago</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Uncommon processes/files - bottom 5%

<table>
<thead>
<tr>
<th>QUERY</th>
<th>DESCRIPTION</th>
<th>PROVIDER</th>
<th>DATA SOURCE</th>
<th>RES.</th>
<th>TACTIC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Uncommon processes/files - bottom 5%</td>
<td>Shows the top 5% processes seen running for the first time.</td>
<td>Microsoft</td>
<td>SecurityEvent</td>
<td>12</td>
<td></td>
</tr>
<tr>
<td>Script usage summary (percentage)</td>
<td>Daily summary of os scripts run across the environment.</td>
<td>Microsoft</td>
<td>SecurityEvent</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>Summary of users creating uncommon accounts</td>
<td>Summarizes users of uncommon &amp; unusual accounts.</td>
<td>Microsoft</td>
<td>SecurityEvent</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Office365 authentications</td>
<td>Shen’s authentication volume by user agent and IP.</td>
<td>Office365</td>
<td>SecurityEvent</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>New processes observed in last 24 hours</td>
<td>Shen’s new processes observed in the last 24 hours.</td>
<td>Microsoft</td>
<td>SecurityEvent</td>
<td>80</td>
<td></td>
</tr>
<tr>
<td>Summary of failed login attempts</td>
<td>A summary of failed attempts that can be used to infer potential threats.</td>
<td>Microsoft</td>
<td>SecurityEvent</td>
<td>80</td>
<td></td>
</tr>
<tr>
<td>Anomalous Azure AD logs based on authentication</td>
<td>This query over Azure AD sign-in activity highlights anomalous activity.</td>
<td>Microsoft</td>
<td>SignIns</td>
<td>12</td>
<td></td>
</tr>
<tr>
<td>Process executed from base64 encoded PE</td>
<td>Process executed from base64 encoded PE file head seen in the logs.</td>
<td>Microsoft</td>
<td>SecurityEvent</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Process executed from base64 encoded PE</td>
<td>Process executed from base64 encoded PE file head seen in the logs.</td>
<td>Microsoft</td>
<td>SecurityEvent</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Summary of users creating new user accounts</td>
<td>New user accounts may be an attack vector providing the attacker.</td>
<td>Microsoft</td>
<td>SecurityEvent</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>User and Group enumeration</td>
<td>The query finds attempts to list users or groups within the domain.</td>
<td>Microsoft</td>
<td>SecurityEvent</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Hosts with new logons</td>
<td>Shen’s new accounts that have logged on to a host.</td>
<td>Microsoft</td>
<td>SecurityEvent</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Malware in the recycle bin</td>
<td>Finding attacks hiding malware in the recycle bin.</td>
<td>Microsoft</td>
<td>SecurityEvent</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Downloading files</td>
<td>Malware writers often use windows system process to download files.</td>
<td>Microsoft</td>
<td>SecurityEvent</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Accounts and user Agents associated with malware</td>
<td>Summary of user accounts and user Agents associated with malware.</td>
<td>Microsoft</td>
<td>SecurityEvent</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Azure AD sign-ins from new locations</td>
<td>New Azure AD sign-in locations today versus historic.</td>
<td>Microsoft</td>
<td>SignIns</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>PowerShell downloads</td>
<td>Finds PowerShell execution events that could imply malicious activity.</td>
<td>Microsoft</td>
<td>SecurityEvent</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Sharepoint downloads</td>
<td>Shen’s volume of documents uploaded to or downloaded.</td>
<td>Microsoft</td>
<td>SecurityEvent</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Summary of user logins by logon type</td>
<td>Comparing successful and unsuccessful logins may indicate potential threats.</td>
<td>Microsoft</td>
<td>SecurityEvent</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>SSH brute force attacks</td>
<td>Identifies anomalies in known ssh login attempts.</td>
<td>Microsoft</td>
<td>SecurityEvent</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>

**Query Information**

```plaintext
let start=datetimestring("2019-02-23T18:26:13.832Z");
let end=datetimestring("2019-02-23T18:26:21.801Z");
let processexecution[securityevent]
  set processeseventsecurityevent =
  where EventIdGenerated > start and TimeGenerated < end
<table>
<thead>
<tr>
<th>EventIDGenerated</th>
<th>Event ID</th>
<th>Event Time</th>
<th>Severity</th>
<th>ProcessName</th>
<th>EventCode</th>
<th>SecurityEvent</th>
</tr>
</thead>
<tbody>
<tr>
<td>45688</td>
<td>45688</td>
<td>2019-02-23</td>
<td>Critical</td>
<td>Executable</td>
<td>45688</td>
<td>SecurityEvent</td>
</tr>
</tbody>
</table>
```

**Entities**

- Timestamp
- EventIDGenerated

**Tactics**

**Execution**

The execution tactic represents techniques that result in execution of adversary-controlled code on a local or remote system.

**Initial Access**

The initial access tactic represents the vector accesses used to gain an initial foothold within a network.

**Persistence**

Resistance to persistence tactics represents the adversaries ability to establish a persistent presence on a network.

**Privilege Escalation**

Privilege escalation is the result of actions that allows an adversary to obtain a higher level of permissions on a system.
Azure Sentinel Hunting via GitHub
Now spraying the EWS portal at https://outlook.office365.com/EWS/Exchange.asmx

Current date and time: 04/26/2019 18:42:16

SUCCESS! User:TrimarcRD.com\DarthVader@trimarcrd.com Password:TheForce19!

A total of 1 credentials were obtained.

Results have been written to C:\Temp\CloudAttackScripts\owa-sprayed-creds.txt.

Now spraying the EWS portal at https://outlook.office365.com/EWS/Exchange.asmx

Current date and time: 04/26/2019 18:41:54

SUCCESS! User:TrimarcRD.com\BobaFett@trimarcrd.com Password:Mandalorian19!

SUCCESS! User:TrimarcRD.com\JangoFett@trimarcrd.com Password:Mandalorian19!

A total of 2 credentials were obtained.

Results have been written to C:\Temp\CloudAttackScripts\owa-sprayed-creds.txt.

Now spraying the EWS portal at https://outlook.office365.com/EWS/Exchange.asmx

Current date and time: 04/26/2019 18:41:34

Trying Exchange version Exchange2010

SUCCESS! User:TrimarcRD.com\ObiWanKenobi@trimarcrd.com Password:WinterisComing19!

A total of 1 credentials were obtained.

Results have been written to C:\Temp\CloudAttackScripts\owa-sprayed-creds.txt.
Azure Sentinel Password Spray Detection

Case ID: 0000000-0000-0000-0000-000000000000

Alerts

Search: X

Severity: Informational, Low, Medium, High, Critical

<table>
<thead>
<tr>
<th>ALERT NAME</th>
<th>ALERT ID</th>
<th>PRODUCT NAME</th>
<th>CREATION TIME</th>
<th>TIME FRAME</th>
<th>NUMBER OF ENTITIES</th>
<th>HITS</th>
</tr>
</thead>
</table>

Run

Time range: Custom

Script:

```sql
where ResultType != 0
where ResultDescription == "Invalid username or password or Invalid on-premise username or password."
where ClientAppUsed == "Other clients; Older Office clients"
extend AccountCustomEntity = UserPrincipalName
extend IPCustomEntity = IPAddress
```
<table>
<thead>
<tr>
<th>TimeGenerated (UTC...)</th>
<th>Source</th>
<th>OperationName</th>
<th>Identity</th>
<th>ResultDescription</th>
<th>ClientAppUsed</th>
<th>Location</th>
<th>IPAdd...</th>
<th>AppDisplayName</th>
</tr>
</thead>
<tbody>
<tr>
<td>2019-04-26T22:45:33.674</td>
<td>Azure AD</td>
<td>Sign-in activity</td>
<td>Han Solo</td>
<td>Invalid username or password or invalid on-premise username or password or pass...</td>
<td>Other clients; Older Office clients</td>
<td>US</td>
<td>69.12</td>
<td>Office 365</td>
</tr>
<tr>
<td>2019-04-26T22:43:29.129</td>
<td>Azure AD</td>
<td>Sign-in activity</td>
<td>Lendo Calrissian</td>
<td>Invalid username or password or invalid on-premise username or pass...</td>
<td>Other clients; Older Office clients</td>
<td>US</td>
<td>69.13</td>
<td>Office 365</td>
</tr>
<tr>
<td>2019-04-26T22:43:08.325</td>
<td>Azure AD</td>
<td>Sign-in activity</td>
<td>Lendo Calrissian</td>
<td>Invalid username or password or invalid on-premise username or pass...</td>
<td>Other clients; Older Office clients</td>
<td>US</td>
<td>69.13</td>
<td>Office 365</td>
</tr>
<tr>
<td>2019-04-26T22:41:17.777</td>
<td>Azure AD</td>
<td>Sign-in activity</td>
<td>Bailey</td>
<td>Invalid username or password or invalid on-premise username or pass...</td>
<td>Other clients; Older Office clients</td>
<td>US</td>
<td>69.13</td>
<td>Office 365</td>
</tr>
<tr>
<td>2019-04-26T22:41:03.764</td>
<td>Azure AD</td>
<td>Sign-in activity</td>
<td>Lendo Calrissian</td>
<td>Invalid username or password or invalid on-premise username or pass...</td>
<td>Other clients; Older Office clients</td>
<td>US</td>
<td>69.12</td>
<td>Office 365</td>
</tr>
<tr>
<td>2019-04-26T22:40:55.951</td>
<td>Azure AD</td>
<td>Sign-in activity</td>
<td>Bailey</td>
<td>Invalid username or password or invalid on-premise username or pass...</td>
<td>Other clients; Older Office clients</td>
<td>US</td>
<td>69.13</td>
<td>Office 365</td>
</tr>
<tr>
<td>2019-04-26T22:40:41.185</td>
<td>Azure AD</td>
<td>Sign-in activity</td>
<td>Han Solo</td>
<td>Invalid username or password or invalid on-premise username or pass...</td>
<td>Other clients; Older Office clients</td>
<td>US</td>
<td>69.13</td>
<td>Office 365</td>
</tr>
<tr>
<td>2019-04-26T22:40:17.015</td>
<td>Azure AD</td>
<td>Sign-in activity</td>
<td>Han Solo</td>
<td>Invalid username or password or invalid on-premise username or pass...</td>
<td>Other clients; Older Office clients</td>
<td>US</td>
<td>69.13</td>
<td>Office 365</td>
</tr>
<tr>
<td>2019-04-26T22:39:32.624</td>
<td>Azure AD</td>
<td>Sign-in activity</td>
<td>ObiWan Kenobi</td>
<td>Invalid username or password or invalid on-premise username or pass...</td>
<td>Other clients; Older Office clients</td>
<td>US</td>
<td>69.13</td>
<td>Office 365</td>
</tr>
<tr>
<td>2019-04-26T22:39:29.039</td>
<td>Azure AD</td>
<td>Sign-in activity</td>
<td>Lendo Calrissian</td>
<td>Invalid username or password or invalid on-premise username or pass...</td>
<td>Other clients; Older Office clients</td>
<td>US</td>
<td>69.13</td>
<td>Office 365</td>
</tr>
<tr>
<td>2019-04-26T22:39:29.039</td>
<td>Azure AD</td>
<td>Sign-in activity</td>
<td>Lendo Calrissian</td>
<td>Invalid username or password or invalid on-premise username or pass...</td>
<td>Other clients; Older Office clients</td>
<td>US</td>
<td>69.13</td>
<td>Office 365</td>
</tr>
<tr>
<td>2019-04-26T22:39:27.047</td>
<td>Azure AD</td>
<td>Sign-in activity</td>
<td>Han Solo</td>
<td>Invalid username or password or invalid on-premise username or pass...</td>
<td>Other clients; Older Office clients</td>
<td>US</td>
<td>69.13</td>
<td>Office 365</td>
</tr>
<tr>
<td>2019-04-26T22:39:27.047</td>
<td>Azure AD</td>
<td>Sign-in activity</td>
<td>Han Solo</td>
<td>Invalid username or password or invalid on-premise username or pass...</td>
<td>Other clients; Older Office clients</td>
<td>US</td>
<td>69.13</td>
<td>Office 365</td>
</tr>
<tr>
<td>2019-04-26T22:39:20.268</td>
<td>Azure AD</td>
<td>Sign-in activity</td>
<td>Bailey</td>
<td>Invalid username or password or invalid on-premise username or pass...</td>
<td>Other clients; Older Office clients</td>
<td>US</td>
<td>69.13</td>
<td>Office 365</td>
</tr>
<tr>
<td>2019-04-26T22:39:20.268</td>
<td>Azure AD</td>
<td>Sign-in activity</td>
<td>Bailey</td>
<td>Invalid username or password or invalid on-premise username or pass...</td>
<td>Other clients; Older Office clients</td>
<td>US</td>
<td>69.13</td>
<td>Office 365</td>
</tr>
<tr>
<td>2019-04-26T22:39:03.266</td>
<td>Azure AD</td>
<td>Sign-in activity</td>
<td>Han Solo</td>
<td>Invalid username or password or invalid on-premise username or pass...</td>
<td>Other clients; Older Office clients</td>
<td>US</td>
<td>69.13</td>
<td>Office 365</td>
</tr>
<tr>
<td>2019-04-26T22:36:03.266</td>
<td>Azure AD</td>
<td>Sign-in activity</td>
<td>Han Solo</td>
<td>Invalid username or password or invalid on-premise username or pass...</td>
<td>Other clients; Older Office clients</td>
<td>US</td>
<td>69.13</td>
<td>Office 365</td>
</tr>
<tr>
<td>2019-04-26T22:35:45.788</td>
<td>Azure AD</td>
<td>Sign-in activity</td>
<td>ObiWan Kenobi</td>
<td>Invalid username or password or invalid on-premise username or pass...</td>
<td>Other clients; Older Office clients</td>
<td>US</td>
<td>69.13</td>
<td>Office 365</td>
</tr>
<tr>
<td>2019-04-26T22:35:45.788</td>
<td>Azure AD</td>
<td>Sign-in activity</td>
<td>ObiWan Kenobi</td>
<td>Invalid username or password or invalid on-premise username or pass...</td>
<td>Other clients; Older Office clients</td>
<td>US</td>
<td>69.13</td>
<td>Office 365</td>
</tr>
</tbody>
</table>
Azure Sentinel Pricing

Pricing details

There will be no charges specific to Azure Sentinel during the preview. Pricing for Azure Sentinel will be announced in the future and a notice will be provided prior to the end of the preview. Should you choose to continue using Azure Sentinel after the notice period, you will be billed at the applicable rates.

Data import from Office 365 is free. You need to be a licensed customer of Office 365 for this data import. Even during preview additional charges may be incurred related to data ingestion, automation workflows or customization of machine learning models.  


Log Analytics

Log Analytics is billed per gigabyte (GB) of data ingested into the service.

<table>
<thead>
<tr>
<th>FEATURE</th>
<th>FREE UNITS INCLUDED</th>
<th>PRICE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Ingestion</td>
<td>5 GB per customer per month(^1)</td>
<td>$2.30 per GB</td>
</tr>
<tr>
<td>Data Retention</td>
<td>31 days(^2)</td>
<td>$0.10 per GB per month</td>
</tr>
</tbody>
</table>

\(^1\)The first 5 GB of data ingested per customer to the Azure Log Analytics service every month is offered free.
\(^2\)Every GB of data ingested into your Azure Log Analytics workspace is retained at no charge for the first 31 days.

Please note: Service Map solution is billed for data ingested by the Dependency Agent into the Service Map platform and the Log Analytics service. Data ingested by the Dependency Agent is billed per Log analytics prices listed above. Billing for data ingested into the Service Map platform is not enabled yet and will be billed starting August 1, 2019.
(Google) Chronicle Backstory

- Runs on Google infrastructure.
- No charges based on data volume.
- Designed for multi-petabyte analytics.

[Sean Metcalf | @PyroTek3 | TrimarcSecurity.com]

https://chronicle.security/products/backstory/
Protecting Cloud Administration
According to Microsoft, Only ___% of ALL (Office 365/Azure AD) Admin Accounts require MFA.

As of September 2018

[ Sean Metcalf | @PyroTek3 | TrimarcSecurity.com ]
According to Microsoft, Only 1.8% of ALL (Office 365/Azure AD) Admin Accounts require MFA.

As of September 2018
Cloud Administration Protection

- Only cloud admin accounts are in privileged groups.
- Require all cloud admin accounts to use MFA (Microsoft Authenticator only).

```powershell
$userCredential = Get-Credential
Import-Module MSOnline
Connect-MsolService -Credential $userCredential

$auth = New-Object -TypeName Microsoft.Online.Administration.StrongAuthenticationRequirement
$auth.RelyingParty = "*

$auth.State = "Enabled"
$auth.RememberDevicesNotIssuedBefore = (Get-Date)

# Enable MFA on all Users
Get-MsolUser -All | Where {$__.userprincipalname -like "*admin*"} | 
Foreach {Set-MsolUser -UserPrincipalName $__.UserPrincipalName -StrongAuthenticationRequirements $auth }
```

[ Sean Metcalf | @PyroTek3 | TrimarcSecurity.com ]
Cloud Administration Protection via Baseline Policy

While managing custom conditional access policies requires an Azure AD Premium license, baseline policies are available in all editions of Azure AD.

This policy requires **multi-factor authentication (MFA)** for the following directory roles:

- Global Administrator
- SharePoint Administrator
- Exchange Administrator
- Conditional Access Administrator
- Security Administrator
- Helpdesk Administrator/Password Administrator
- Billing Administrator
- User Account Administrator

This policy also blocks legacy authentication.

**Learn more**

**Enable policy**
- Use policy immediately
- Do not use policy

**Users**

Select the users to exempt from...
“Break Glass” Cloud Admin Account

• New account designated as the Microsoft Cloud Admin account.
• Has permanent membership in the most privileged groups.
• Is excluded from most security controls: MFA and Conditional Access policies.
• Has a strong password (16 characters, for now).
• Only used in emergencies.
• All other cloud admin accounts have strong security controls (MFA, etc.)
Azure AD Privileged Identity Management

Azure AD PIM is a Premium feature that enables you to limit standing admin access to privileged roles and much more. **Learn more**

**Limit standing access**

PIM allows you to make users eligible for roles, which means they only have access when necessary.

**Discover who has access**

Using the built-in wizard, you can easily discover users with permanent privileged role assignments and make them eligible.

**Review privileged access**

With Access Reviews, you can choose delegates or have users attest for themselves if they still need access to privileged roles.

---

**Do more with Azure AD Privileged Identity Management**

- Require Multi-Factor Authentication
- Log service/ticket numbers when activating
- Schedule activations for a specific date
- Require approval workflow to activate
- Receive notifications when users are assigned
- Configure and resolve alerts for privileged roles
Leverage PIM to Minimize Admin Rights
### My roles - Azure AD roles

<table>
<thead>
<tr>
<th>Role Name</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Administrator</td>
<td>Permanently assigned</td>
</tr>
<tr>
<td>Global Administrator</td>
<td>Permanently assigned</td>
</tr>
<tr>
<td>Privileged Role Administrator</td>
<td>Permanently assigned</td>
</tr>
</tbody>
</table>

### Activate
- Azure AD roles
- Azure resource roles

### Troubleshooting + Support
- Troubleshoot
- New support request
Leverage PIM to Minimize Admin Rights

<table>
<thead>
<tr>
<th>ROLE</th>
<th>ACTIVATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>DARTH VADER [<a href="mailto:DARTHVADER@TRIMARCRCRD.COM">DARTHVADER@TRIMARCRCRD.COM</a>]</td>
<td></td>
</tr>
<tr>
<td>Exchange Administrator</td>
<td>Eligible</td>
</tr>
<tr>
<td>Conditional Access Administrator</td>
<td>Eligible</td>
</tr>
<tr>
<td>EXADMIN [<a href="mailto:EXADMIN@TRIMARCRCRD.COM">EXADMIN@TRIMARCRCRD.COM</a>]</td>
<td></td>
</tr>
<tr>
<td>Exchange Administrator</td>
<td>Permanent</td>
</tr>
<tr>
<td>Teams Service Administrator</td>
<td>Permanent</td>
</tr>
<tr>
<td>Skype for Business Administrator</td>
<td>Permanent</td>
</tr>
<tr>
<td>Teams Communications Administrator</td>
<td>Permanent</td>
</tr>
<tr>
<td>SharePoint Service Administrator</td>
<td>Permanent</td>
</tr>
</tbody>
</table>
Microsoft Cloud Security Controls

YOUR SECURITY ACCESS CONTROLS...

GRATEFULLY ACCEPTED

[ Sean Metcalf | @PyroTek3 | TrimarcSecurity.com ]
<table>
<thead>
<tr>
<th>Security Control</th>
<th>Required Subscription</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multi-Factor Authentication for Office 365</td>
<td>Office 365</td>
</tr>
<tr>
<td>Azure Multi-Factor Authentication</td>
<td>Azure AD P1 or Additional cost per user/ per authentication</td>
</tr>
<tr>
<td>Conditional Access</td>
<td>Azure AD P1</td>
</tr>
<tr>
<td>Privileged Identity Management (PIM)</td>
<td>Azure AD P2 (only admin accounts need this)</td>
</tr>
<tr>
<td>Azure AD Password Protection (On-Prem or custom banned password list)</td>
<td>Azure AD P1</td>
</tr>
<tr>
<td>Azure Identity Protection</td>
<td>Azure AD P2</td>
</tr>
<tr>
<td>Azure ATP (for on-prem AD)</td>
<td>Enterprise Mobility + Security 5 suite (EMS E5)</td>
</tr>
</tbody>
</table>
Office 365 E5 does not provide Azure AD Premium features

Enterprise Mobility + Security 5 suite (EMS E5) does
Trimarc - Overview
Azure Active Directory

Sign-ins

What's new in Azure AD
Stay up to date with the latest release notes and blog posts.
Azure Identity Protection

• Included with Azure AD Premium (P2)
• Have to “install” via the Azure Marketplace (portal.azure.com)
• Dashboard covering identity risk.
• Provides automatic remediation of “risky” sign-ins
Azure AD Identity Protection

- 4 users have a high risk level.

**Overview**
- Users flagged for risk: 34 out of 433 users (7.85%)
- Risk events:
  - High: 2
  - Medium: 36
  - Low: 0
  - Closed: 89

**Vulnerabilities**
- Medium: 398 (Users without multi-factor authentication registration)
- Medium: 1 (Roles don't require multi-factor authentication for activation)
- Low: 10 (Administrators aren't using their privileged roles)
- Low: 31 (There are too many global administrators)

**Configure**
- Multi-factor authentication registration
- User risk policy
- Sign-in risk policy

**Settings**
- Alerts
- Weekly Digest
- Pin to dashboard
Enable Risk-based Policies

- Requires Azure Identity Protection (Azure AD P2)
- Assigns a risk level during sign-in
- Risk level determines action
  - Force password change
  - Require MFA registration
  - MFA for higher risk authentication
Enable Sign-in Risk Policy

Is this a “risky sign-in”?

- Anonymous IP
- Unfamiliar location

Sign-in risk

Select the sign-in risk level

- Low and above
- Medium and above
- High
Enable User Risk Remediation Policy

Policy name
User risk remediation policy

Assignments

- Users
  - All users

- Conditions
  - User risk

Controls

- Access
  - Require password change

Review

- Estimated impact
  - Number of users impacted

What’s the chance the account is compromised?
- Some detected in real-time
- ~14 day learning period

Sign-in risk

Select the sign-in risk level
- Low and above
- Medium and above
- High

Enforce Policy
[ On Off ]
Enable User Risk Remediation Policy

If you want to require MFA for risky sign-ins, you should:

1. Enable the multi-factor authentication registration policy for the affected users.

2. Require the affected users to sign in to a non-risky session to perform an MFA registration.

Completing these steps ensures that multi-factor authentication is required for a risky sign-in.

The sign-in risk policy is:

- Applied to all browser traffic and sign-ins using modern authentication.

- Not applied to applications using older security protocols by disabling the WS-Trust endpoint at the federated IDP, such as ADFS.

Controlling Access
## Azure AD Conditional Access

- Enforce different rules on authentication/access based on a variety of conditions.
- Control access based on:
  - Sign-in activity (anomalies?)
  - Network location (corporate network vs internet)
  - Device (AAD Joined?)
  - Application
- Requires Azure AD P1

<table>
<thead>
<tr>
<th>When this happens</th>
<th>Then do this</th>
<th>Conditional access policy</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Conditions</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Access controls</td>
</tr>
</tbody>
</table>

[ Sean Metcalf | @PyroTek3 | TrimarcSecurity.com ]
Conditional Access

https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/overview

[ Sean Metcalf | @PyroTek3 | TrimarcSecurity.com ]
Baseline Protection (Preview)

• Set of predefined conditional access policies.
• First Baseline Protection Policy: Require MFA for admins
• While baseline policies are in preview, enable “Automatically enable policy in the future” so the policy is automatically enabled once the policy reaches General Availability.
• Available for all Azure AD users (AAD Premium not required).
Legacy Authentication

Why Block Legacy Authentication?

- 350K compromised accounts in April 2018 due to password spray, 200K in the last month.
- Nearly 100% of password spray attacks we see are from legacy authentication
- Blocking legacy authentication reduces compromise rate by 66%
- [https://aka.ms/PasswordSprayBestPractices](https://aka.ms/PasswordSprayBestPractices)

Source: Microsoft Ignite Conference 2018
Legacy vs Modern Authentication

**Legacy Auth**
- Office 2010 and older
- Office 2013 (requires patch + reg key to support modern auth)
- Clients that use mail protocols such as IMAP/SMTP/POP
- Older PowerShell modules

**Modern Auth**
- Office 2013 (requires enabling)
- Office 2016 (PC & Mac)
- Outlook Mobile
- iOS 11 Mail app
Step 1: Understand the usage of Legacy Authentication in your organization

- Use sign in logs to examine current usage. Filter by Client App (add column if you do not see it)
- POP, IMAP, MAPI, SMTP and ActiveSync go to Exchange Online
- “Other Clients” shows SharePoint and Exchange Web Services
- You can export/download the sign in logs, sort by Client App and identify the top offenders

Source: Microsoft Ignite Conference 2018
Disable Legacy Auth
Disable Service Access

- Outlook on the Web (OWA)
- Outlook desktop (MAPI)
- Exchange Web Services (EWS)
- Mobile (Exchange ActiveSync)
- IMAP
- POP
Azure AD Connect Health - ADFS

ADFS External Smart Lockout

• Update ADFS servers to Windows Server 2016 (or 2019).
• Provides enhanced protection against on-prem AD lockouts during external password spray attacks.
• External Smart Lockout: Locks out attackers while allows valid users access.
• ADFS 2019
  • Independent lockout thresholds for familiar & unfamiliar locations.
  • Smart lockout audit mode while still leveraging soft lockout.
• External Lockout Best Practice Configuration (ADFS 2016):
  • `Set-AdfsProperties -EnableExtranetLockout $true -ExtranetLockoutThreshold 15 -ExtranetObservationWindow (new-timespan -Minutes 30) -ExtranetLockoutRequirePDC $false`

Gaining Password Insight

I DON'T ALWAYS USE A SECURE PASSWORD

BU7WH3N1DO

www.hawaii.edu/infosec/ncsam.html

[ Sean Metcalf | @PyroTek3 | TrimarcSecurity.com ]
Password Hash Sync, What & Why?

- Azure AD Connect provides capability.
- Requests password hashes from Active Directory Domain Controllers on-prem.
- Hashes these hashes (MD4+salt+PBKDF2+HMAC-SHA256)
- Sends to Azure AD tenant.
- Microsoft can identify & flag Azure AD users with bad passwords (& Dark Web).

[ Sean Metcalf | @PyroTek3 | TrimarcSecurity.com ]
Azure AD Smart Lockout

• Smart lockout uses cloud intelligence to identify & lockout attackers guessing passwords.

• Determines logon activity differences between valid users & attackers.

• Included in all versions of Azure AD ("free").

[Sean Metcalf | @PyroTek3 | TrimarcSecurity.com]

Azure AD Password Protection

- Global banned password list (All users)
- Custom banned password list (Azure AD P1)
- Dynamic banned passwords (All Users)
  - Letter substitution
  - Fuzzy matching (shorter versions of banned passwords)
  - Substring matching
  - Scoring: <5 points = blocked

https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-password-ban-bad
Azure AD Premium Password Protection

- On-prem Active Directory solution.
- Requires Azure AD P1, DCs running 2012+, & DFSR (SYSVOL replication).
- Microsoft Password Filter deployed to DCs.
- 1-2 Proxy servers configured in the AD forest.
- Blocks >500 commonly used passwords (plus > 1M pw character substitution).
- Audit or Enforce password restrictions.
- Usage reporting (Get-AzureADPasswordProtectionSummaryReport)

https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-password-ban-bad-on-premises
Azure AD Premium Password Protection

Authentication methods (Preview) - Password protection (Preview)

Manage

Password protection (Preview)

Custom smart lockout

Lockout threshold: 10
Lockout duration in seconds: 60

Custom banned passwords

Enforce custom list: Yes

Custom banned password list:
Trimarc
Washington
DCUnited

Password protection for Windows Server Active Directory

Enable password protection on Windows Server Active Directory: Yes
Mode: Enforced
Azure AD Premium
Password Protection
Azure ATP

• Cloud based security solution for on-prem Active Directory.
• Requires licensing (Enterprise Mobility + Security 5 suite (EMS E5))
• Effectively Microsoft Advanced Threat Analytics (ATA) in the cloud.
• Azure ATP client “sensor” installed on Domain Controllers.
Azure ATP
Microsoft Cloud Security
“Tune Up”

MUCH IMPROVE

VERY BETTER

[ Sean Metcalf | @PyroTek3 | TrimarcSecurity.com ]
Secure Score

Your Secure Score is:
248
of 483

Your Secure Score

Secure Score figures out what Office 365 services you are using, then looks at your configuration and behaviors and compares it to a baseline asserted by Microsoft. If your configuration and behaviors are in line with best practices, you will get points, which you can track over time. More importantly, you will be able to quickly determine what things you can do to reduce their risk.
Secure Score

You should enable MFA for all of your Azure AD privileged roles because a breach of any of those accounts can lead to a breach of any of your data. We found that you had 1 admin out of 1 that did not have MFA enabled. If you enable MFA for those 1 admin accounts, your score will go up 50 points.

Threats
- Password Cracking
- Account Breach
- Elevation of Privilege

Compliance Controls
- ISO 27015:2014 - Control C.9.4.2, A.10.8
- CSA CCM301: Control DSI-02
- GDPR - Control 6.8.5

Compare your score

<table>
<thead>
<tr>
<th>Action Category</th>
<th>Identity</th>
<th>User Impact</th>
<th>Implementation Cost</th>
<th>Action Score</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Low</td>
<td>Low</td>
<td></td>
<td>0/50</td>
</tr>
</tbody>
</table>

64 Secure Score
37 Office 365 Seat Size Average Score
0 Please Select Industry Type
31 Office 365 Average Secure Score

Seat size this tenant belongs to is 6 - 99 seats
Enable Client Rules Forwarding Block

What am I about to change?

There are several ways today that a bad actor can use external mail forwarding to exfiltrate data.

1. Client created external mail forwarding Rules, such as the Outlook desktop client.
2. Admins can set up external mail forwarding for a user via setting ForwardingSmtpAddress on a user object.
3. Admins can create external transport rules to forward messages.
4. Client created ForwardingSmtpAddress via Outlook Web Access Interface

This Security Control action will help mitigate Client created external mail forwarding rules.

A simple mitigation is to, on each Remote Domain, including the Default to disallow Auto-Forwarding. This is a global setting and applies to every email sent from within a Tenant, as a result it is a very broad approach, which does not allow white listing. More details can be found here. RBAC roles can be used to achieve a similar result.

Using a properly configured Transport Rule we can control the impact of data exfiltration via Client created external mail forwarding rules. This approach has a couple of advantages:

1. Clients will receive a custom NDR message, useful for highlighting to end users external forwarding rules they may have not known existed (accidental exfiltration), or external forwarding rules created by a bad actor on a compromised mailbox.
2. Allows a whitelist of users or groups to be configured to allow business approved exceptions to the policy.
3. Provides some mitigation, for when an Admin account has been used to create a Remote Domain with auto-forwarding enabled to specific namespace to exfiltrate data.
4. Provides some mitigation, for when an Admin account has been used to alter the Default Remote Domain settings.

This Security Control will create a transport rule of the type AutoForward, mitigating the use of client-side forwarding rules.

Enable Client Rules Forwarding Block Complete

You have successfully created the transport rule that blocks the use of client-side forwarding rules. We found that you had 0 Rules out of 0 that did have blocks enabled.

Your score will increase by 20 points within 24 hours. We found that you had 0 Rules out of 0 that did have blocks enabled.
# Secure Score – Highest Priority Items

<table>
<thead>
<tr>
<th>Action</th>
<th>Score Increase</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable MFA for Azure AD privileged roles</td>
<td>50</td>
</tr>
<tr>
<td>Enable MFA for users</td>
<td>30</td>
</tr>
<tr>
<td>Enable sign-in risk policy</td>
<td>30</td>
</tr>
<tr>
<td>Enable user risk policy</td>
<td>30</td>
</tr>
<tr>
<td>Enable Client Rules Forwarding Block</td>
<td>20</td>
</tr>
<tr>
<td>Enable Cloud App Security Console</td>
<td>20</td>
</tr>
<tr>
<td>Enable Data Loss Prevention policies</td>
<td>20</td>
</tr>
<tr>
<td>Enable Microsoft Intune Mobile Device Management</td>
<td>20</td>
</tr>
<tr>
<td>Enable policy to block legacy authentication</td>
<td>20</td>
</tr>
<tr>
<td>Ensure all users are registered for multi-factor authentication</td>
<td>20</td>
</tr>
<tr>
<td>Review permissions &amp; block risky OAuth applications connected</td>
<td>20</td>
</tr>
<tr>
<td>Set automated notification for new OAuth applications connected</td>
<td>20</td>
</tr>
<tr>
<td>Set automated notifications for new and trending cloud applications</td>
<td>20</td>
</tr>
</tbody>
</table>

**Recommended ASAP**

**Additional subscription required**

[ Sean Metcalf | @PyroTek3 | TrimarcSecurity.com ]
Your Identity Secure Score

26/223

Your score is above the average for your company's industry.

<table>
<thead>
<tr>
<th>Trimarc R&amp;D</th>
<th>26</th>
</tr>
</thead>
<tbody>
<tr>
<td>Industry average</td>
<td>-1</td>
</tr>
<tr>
<td>Typical 6-99 person co...</td>
<td>26</td>
</tr>
</tbody>
</table>

Improvement actions

<table>
<thead>
<tr>
<th>NAME</th>
<th>SCORE IMPACT</th>
<th>USER IMPACT</th>
<th>IMPLEMENTATION COST</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable MFA for Azure AD privileged roles</td>
<td>50</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>Enable MFA for users</td>
<td>30</td>
<td>Moderate</td>
<td>Moderate</td>
</tr>
<tr>
<td>Enable sign-in risk policy</td>
<td>30</td>
<td>Moderate</td>
<td>Moderate</td>
</tr>
<tr>
<td>Enable user risk policy</td>
<td>30</td>
<td>Moderate</td>
<td>Moderate</td>
</tr>
<tr>
<td>Ensure all users are registered for multi-factor authentication</td>
<td>20</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>Do not allow users to grant consent to unmanaged applications</td>
<td>10</td>
<td>Moderate</td>
<td>Low</td>
</tr>
<tr>
<td>Enable policy to block legacy authentication</td>
<td>10</td>
<td>Moderate</td>
<td>Moderate</td>
</tr>
</tbody>
</table>
Manage advanced alerts

Your subscription allows you to use Office 365 Cloud App Security!

Take advantage of features such as:

- Alerts - Create alerts and investigate anomalous and suspicious behavior
- Productivity app discovery - Gain visibility into how Office 365 and other productivity cloud services are being used
- App permissions - View and control which apps have been granted permissions to your Office 365 environment

Investigate identity behavior across cloud apps

Go to Office 365 Cloud App Security
Learn more about Office 365 Cloud App Security

Office 365 Cloud App Security is powered by Microsoft Cloud App Security service which is a separate online service
- Privacy & Cookies
- Terms
### Policies

<table>
<thead>
<tr>
<th>Policy</th>
<th>Count</th>
<th>Severity</th>
<th>Category</th>
<th>Action</th>
<th>Modified</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unusual file share activity (by user)</td>
<td>0</td>
<td><img src="https://trimarcsecurity.com/media/severity-icon-orange.png" alt="" /></td>
<td>Threat detection</td>
<td><img src="https://trimarcsecurity.com/media/status-icon-active.png" alt="Status Icon" /></td>
<td>Oct 24, 2018</td>
</tr>
<tr>
<td>Unusual file download (by user)</td>
<td>0</td>
<td><img src="https://trimarcsecurity.com/media/severity-icon-orange.png" alt="" /></td>
<td>Threat detection</td>
<td><img src="https://trimarcsecurity.com/media/status-icon-active.png" alt="Status Icon" /></td>
<td>Oct 24, 2018</td>
</tr>
<tr>
<td>Multiple failed login attempts</td>
<td>0</td>
<td><img src="https://trimarcsecurity.com/media/severity-icon-orange.png" alt="" /></td>
<td>Threat detection</td>
<td><img src="https://trimarcsecurity.com/media/status-icon-active.png" alt="Status Icon" /></td>
<td>Oct 24, 2018</td>
</tr>
<tr>
<td>Unusual file deletion activity (by user)</td>
<td>0</td>
<td><img src="https://trimarcsecurity.com/media/severity-icon-orange.png" alt="" /></td>
<td>Threat detection</td>
<td><img src="https://trimarcsecurity.com/media/status-icon-active.png" alt="Status Icon" /></td>
<td>Oct 24, 2018</td>
</tr>
<tr>
<td>Activity from suspicious IP addresses</td>
<td>0</td>
<td><img src="https://trimarcsecurity.com/media/severity-icon-orange.png" alt="" /></td>
<td>Threat detection</td>
<td><img src="https://trimarcsecurity.com/media/status-icon-active.png" alt="Status Icon" /></td>
<td>Oct 24, 2018</td>
</tr>
<tr>
<td>Activity from anonymous IP addresses</td>
<td>0</td>
<td><img src="https://trimarcsecurity.com/media/severity-icon-orange.png" alt="" /></td>
<td>Threat detection</td>
<td><img src="https://trimarcsecurity.com/media/status-icon-active.png" alt="Status Icon" /></td>
<td>Oct 24, 2018</td>
</tr>
</tbody>
</table>
Office 365 Subscriptions (Capability & Cost)

SERVICE COSTS WHAT IT COSTS.

IT'S THE PEACE OF MIND YOU PAY PREMIUM FOR

[ Sean Metcalf | @PyroTek3 | TrimarcSecurity.com ]
# Office 365 Enterprise Tiers

<table>
<thead>
<tr>
<th>Enterprise 1 (E1) - $8 user/month</th>
<th>Enterprise 3 (E3) - $20 user/month</th>
<th>Enterprise 5 (E5) - $35 user/month</th>
</tr>
</thead>
<tbody>
<tr>
<td>50 GB mailbox</td>
<td>50 GB mailbox</td>
<td>100 GB mailbox</td>
</tr>
<tr>
<td>File storage and sharing with 1 TB OneDrive storage</td>
<td>Unlimited personal cloud storage</td>
<td>Unlimited personal cloud storage</td>
</tr>
<tr>
<td>No Office installed apps</td>
<td>Desktop versions of Office applications (One license covers 5 phones, 5 tablets, and 5 PCs or Macs per user)</td>
<td>Desktop versions of Office applications (One license covers 5 phones, 5 tablets, and 5 PCs or Macs per user)</td>
</tr>
<tr>
<td></td>
<td>eDiscovery with in-place search, hold, and export</td>
<td>eDiscovery with in-place search, hold, and export</td>
</tr>
<tr>
<td></td>
<td>Customer Lockbox</td>
<td>Office ATP</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Auto classification, smart import, and more with Advanced Data Governance</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Office 365 Cloud App Security</td>
</tr>
</tbody>
</table>

[ Sean Metcalf | @PyroTek3 | TrimarcSecurity.com ]
Azure Active Directory Options

• Free
• Basic: $1 per user monthly
  • No object limit & Basic reports
• P1: $6 per user monthly
  • Self-Service Group and app Management
  • Self Service Password Reset/Change/Unlock
  • Two-way sync between on-prem & Azure AD
  • Multi-Factor Authentication (Cloud and On-premises (MFA Server))
  • Cloud App Discovery
  • Conditional Access based on group, location, and device state
  • Connect Health
  • Microsoft Cloud App Security integration
  • MDM auto-enrollment
• P2: $9 per user monthly
  • Includes P1 features
  • Identity Protection
  • Privileged Identity Management
  • Access Reviews

### Enterprise Mobility + Security Options

<table>
<thead>
<tr>
<th>Plan</th>
<th>Features</th>
<th>Price per User per Month</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Azure AD P1: $6</strong></td>
<td><a href="#">Azure Active Directory Premium P1</a></td>
<td><a href="#">Intune</a></td>
</tr>
<tr>
<td><strong>E3</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>E5</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

[Sean Metcalf | @PyroTek3 | TrimarcSecurity.com]
Approximate Microsoft Cloud Cost ($26 - $50 user/month)

- **Office 365 E3 & Azure AD**
  - Office 365 E3 ($20) + Azure AD P1 ($6) = $26/user/month
  - Office 365 E3 ($20) + Azure AD P2 ($9) = $29/user/month

- **Office 365 E5 & Azure AD**
  - Office 365 E5 ($35) + Azure AD P1 ($6) = $41/user/month
  - Office 365 E5 ($35) + Azure AD P2 ($9) = $44/user/month

- **Office 365 E3 & Enterprise Mobility + Security**
  - Office 365 E3 ($20) + Enterprise Mobility + Security E3 ($8.74) = ~$29/user/month
  - Office 365 E3 ($20) + Enterprise Mobility + Security E5 ($14.80) = ~$35/user/month

- **Office 365 E5 & Enterprise Mobility + Security**
  - Office 365 E5 ($35) + Enterprise Mobility + Security E3 ($8.74) = ~$44/user/month
  - Office 365 E5 ($35) + Enterprise Mobility + Security E5 ($14.80) = ~$50/user/month

*Note: Plan for Azure AD P2 for all admin accounts to leverage PIM*
Mini Celebration Time!
@markmorow can we get more than 16 character passwords in Azure AD? Like maybe 30?
cc: @NerdPyle

Note:
I wasn’t the only one asking for this.
Though I did pester Microsoft a lot...
Reset password

Password Admin-created

- Auto-generate password
- Let me create the password

Password *

- Make this user change their password when they first sign in

You need to create a strong password 8-256 characters long that combines at least three of the following: uppercase letters, lowercase letters, symbols, and numbers.

Reset Cancel
Reset password

Password

Admin-created

- Auto-generated
- Let me create

Password *

- Make this use

You need to create a strong password 8-256 characters long that combines at least three of the following: uppercase letters, lowercase letters, symbols, and numbers.

Reset  Cancel
Reset password

Old password

Password

- Auto-generate password
- Let me create the password

Create new password

Password

- Make this user create the password

Your password can't be longer than 16 characters.
Note:
Microsoft has not announced anything about this, so the increased password character length is likely still being rolled out. Consider this a limited “Preview” ;)}
Cloud Security Best Practices
Microsoft Cloud Recommendations Summary

• Disable user access protocols that aren't required - goal is Modern Auth with MFA.
• Enable user and admin activity logging in Office 365 (UnifiedAuditLogIngestionEnabled).
• Enable mailbox activity auditing on all O365 mailboxes.
• Review the recommendations in Office Secure Score and implement as many as possible.
• Enable “Password Hash Sync”
• Enable self-service password reset
• Ensure all users are registered for MFA
• Enable MFA for all users
• Enable sign-in & user risk policy
• Conditional Access: Block Legacy Auth (most attacks leverage legacy auth)
• Monitor App registrations.
• Audit consented permissions for apps & user access to apps

[ Sean Metcalf | @PyroTek3 | TrimarcSecurity.com ]
Microsoft Cloud: Protecting Admin Accounts

• Enforce MFA on all admin accounts
• Many of the basics remain the same
  • Least privilege is key and poorly understood in many cloud implementations
  • Least access, use the security features provided by the cloud
  • Cloud admin workstations – treat same as privileged users
• Limit admin role membership and monitor group membership. PIM can help.
Summary

• The cloud isn’t inherently secure.

• 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.

• Cloud features change regularly. This talk is likely already out of date...

Slides: Presentations.ADSecurity.org

Sean Metcalf (@Pyrotek3) sean [@] TrimarcSecurity.com

www.ADSecurity.org TrimarcSecurity.com
BONUS: Testing Defenses

https://docs.microsoft.com/en-us/office365/securitycompliance/attack-simulator
Simulate the Attack: Password Spray

Configure Password Attack

Confirm

Please confirm your settings: Users: bailey@trimarcrd.com BobaFett@TrimarcRD.com DarthVader@TrimarcRD.com HanSolo@TrimarcRD.com JangoFett@TrimarcRD.com JoeUser@TrimarcRD.com Leia@TrimarcRD.com ObiWanKenobi@TrimarcRD.com Yoda@TrimarcRD.com

Are you sure you want proceed with your password attack?

Back Finish Cancel
Simulate the Attack: Password Spray

Password Spray Attack

Attack Details

A password spray attack against an organization is typically done by running a list of commonly used passwords against a list of valid Office 365 user accounts. Typically, the attacker crafts one password to try against all of the known user accounts. If the attack is not successful, the attacker will try again using another carefully crafted password, usually with a waiting period between attempts to avoid policy-based account lockout triggers.

Current Attack Status

TrimarcRD Password Spray Attack (Winter2018!)

33% of user accounts attempted
1 of 9 users have been compromised

Terminate Attack
Simulate the Attack: Password Spray

Attack details

Report: TrimarcRD Password Spray Attack (Winter2018!)

11/3/2018, 8:08:20 PM to 11/3/2018, 8:09:10 PM

The results from the Password Spray attack scenario are shown below. These results indicate the success of the attack and susceptibility of employees to this attack vector.

- Total users targeted: 9
- Successful attempts: 1
- Overall Success Rate: 11%

For this attack, 1 of 9 users were found to be susceptible to Password Spray attacks.

Compromised Users

BobaFett@TrimarcRD.com
Simulate the Attack: Password Attack

Please confirm your settings: Users: bailey@trimarcRD.com BobaFett@trimarcRD.com DarthVader@trimarcRD.com HanSolo@trimarcRD.com JangoFett@trimarcRD.com JoeUser@trimarcRD.com Leia@trimarcRD.com ObiWanKenobi@trimarcRD.com Yoda@trimarcRD.com

Are you sure you want proceed with your password attack?

[ Back ] [ Finish ] [ Cancel ]
Simulate the Attack: Password Attack

Brute Force Password (Dictionary Attack)  Account Breach

A brute-force attack dictionary is an automated, trial-and-error method of generating multiple passwords guesses from a dictionary file against a user’s password.

TrimarcRD Password Attack

22% of user accounts attempted
1 of 9 users have been compromised

[ Sean Metcalf | @PyroTek3 | TrimarcSecurity.com ]
Simulate the Attack: Password Attack

Brute Force Password (Dictionary Attack)

Password cracking techniques are used to guess a user's password by trying many variations with a computer. Once an attacker has the user name and password for a user, the attacker will generally be able to sign in to Office 365 and gain access to additional information, such as other user accounts and sensitive information. Brute-force attacks work by calculating every possible combination that could make up a password and testing to see if it is the correct password. As the password's length increases, the amount of time, on average, to find the correct password increases exponentially. This means short passwords can usually be discovered rather quickly, but longer passwords may take decades to discover. Two types of brute-force password attacks exist: a dictionary attack using a well-known list of passwords, and an exhaustive attack, where combinations are tried sequentially. Attack simulator uses a dictionary list attack, allowing modifications of frequency between attacks and the number of attempts. If a password is discovered, the password itself is not shown; only an indication that a password was discovered will be shown.
Simulate the Attack: Password Attack

Attack details

Report: TrimarcRD Password Attack

11/3/2018, 8:01:54 PM to 11/3/2018, 8:04:41 PM

The results from the Brute Force Password attack scenario are shown below. These results indicate the success of the attack and susceptibility of employees to this attack vector.

- Total users targeted: 9
- Successful attempts: 6
- Overall Success Rate: 67%

For this attack, 6 of 9 users were found to be susceptible to Brute Force Password attacks.

Compromised Users

- BobaFett@TrimarcRD.com
- DarthVader@TrimarcRD.com
- HanSolo@TrimarcRD.com
- JangoFett@TrimarcRD.com
- JoeUser@TrimarcRD.com
- Leia@TrimarcRD.com
Simulate the Attack: Phishing Attack

Provide a name to the campaign

Name
Prize Giveaway

Please select a template in the list...

Payroll Update
Simulate the Attack: Phishing Attack

Please provide email details

From (Name)
TrimarcRD Payroll Update

From (Email)
payrollservices@payrolltooling.com

Phishing Login server URL
http://portal.payrolltooling.com

Custom Landing Page URL
If you use a custom landing page for user awareness after an attack, enter your URL here.

Subject
Urgent - Update Your Payroll Details

Back  Next  Cancel
Simulate the Attack: Phishing Attack

Email body

$(username), Your payroll details need updating, please click below to start.

UPDATE YOUR ACCOUNT DETAILS

Dear $(username),

We have recently upgraded our payroll system, as a security measure we need you to confirm your bank routing number details for you.

Please review and enter your routing number details at the link above $(username) by clicking on the "Update Your Account Details" button.
Simulate the Attack: Phishing Attack

Spear Phishing (Credentials Harvest)   Account Breach

A spear-phishing attack is a targeted attempt to acquire sensitive information, such as user names, passwords, and credit card information, by masquerading as a trusted entity. This attack will use a URL to attempt to obtain user names and passwords.
Simulate the Attack: Phishing Attack

TrimarcRD Payroll Update

Urgent - Update Your Payroll Details

Joe User, Your payroll details need update.

Security & Compliance

Threat management

Attack simulator

[ Sean Metcalf | @PyroTek3 | TrimarcSecurity.com ]
Dear Joe User,

We have recently upgraded our payroll system, as a security measure we need you to confirm your bank routing number details for your account nominated to receive your salary.

Please review and enter your routing number details at the link above Joe User - by clicking on the “Update Your Account Details” button above.

Failure to update your account details will result in delays with your salary being processed. Please make sure to update the details at least 5 days before the next Payroll cycle to avoid an unnecessary delay in processing.

Please let us know if you have any questions.

Thank you.
Sign in

Email, phone, or Skype

This connection is not secure. Logins entered here could be compromised. Learn More

No account? Create one!

Can't access your account?
You have been redirected to this web page as a recent message you opened was part of a Phishing awareness test being run by your Organization. You will be contacted shortly by your Administrators for some follow up training on security best practices. In the meantime some high-level information is presented below to help you remain safe.

Why are we talking about Phishing?
Phishing happens to everybody. It's a huge problem, and it’s getting bigger. In fact, a 2016 study reports that 91% of cyberattacks and the resulting data breach begin with a phishing email. These attacks are becoming more frequent and sophisticated. So much so that one online article states that 97% of people world-wide could not identify a sophisticated phishing attack. And, it's not just your work accounts at risk. These phishers will hack things like your banking, utilities, insurance information and even Facebook, Twitter, and Instagram accounts.
Report: Payroll Update


The results from the Spear Phishing attack scenario are shown below. These results indicate the success of the attack and susceptibility of employees to this attack vector.

<table>
<thead>
<tr>
<th>Total users targeted</th>
<th>Fastest Click</th>
<th>Fastest Credentials</th>
</tr>
</thead>
<tbody>
<tr>
<td>9</td>
<td>5 minutes 31 seconds</td>
<td>11 minutes 58 seconds</td>
</tr>
<tr>
<td>Successful attempts</td>
<td>Average Click</td>
<td>Average Credentials</td>
</tr>
<tr>
<td>1</td>
<td>8 minutes 14 seconds</td>
<td>11 minutes 58 seconds</td>
</tr>
<tr>
<td>Overall Success Rate</td>
<td>Click Success Rate</td>
<td>Credential Success Rate</td>
</tr>
<tr>
<td>11%</td>
<td>22%</td>
<td>11%</td>
</tr>
</tbody>
</table>

For this attack, 1 of 9 users were found to be susceptible to Spear Phishing attacks.

Compromised Users

JangoFett@trimarcid.com
Credential supplied: 11/3/2018, 8:49:07 PM
Link clicked: 11/3/2018, 8:47:46 PM

JoeUser@trimarcid.com
Link clicked: 11/3/2018, 8:43:00 PM