A Holistic Approach to Defending Business Email Compromise (BEC) Attacks

SANS DFIR SUMMIT 2021

Korstiaan Stam, Founder Invictus Incident Response

Agenda

01 Past

Overview of the work done on BEC in the past

02 Present

Current state of affairs regarding BEC, what is happening and what can we do as defenders

03 Holistic approach

What is a holistic approach and why do you need it

04 BEC Guide

An intro to the BEC Guide and how you can use it to detect and respond to BEC attacks

05 Future

A look into my crystal ball for BEC attacks and what can be done to combat the problem

About Me

Professional

- Worked at PwC and led the IR team also worked at Northwave
- Part-time cyber security lecturer in Amsterdam
- Recently started my own IR firm

Personal

- Like to learn new stuff and keep myself busy
- Try to blog and do some more CTFs

INVICTUS
INCIDENT RESPONSE

1 The past
A brief history lesson

SANS SUMMIT 2019

In Prague my former colleagues presented on the topic of “Responding to Business Email Compromises”

Office365 Extractor

The Office 365 Extractor is a tool to reliably acquire the Unified Audit Log in Office 365 environments for forensic analysis.

Splunk app

In response to the huge amount of BEC cases I developed a Splunk application that helps with ”automatic” detection of suspicious events in the Unified Audit Log.

Complexity

A lot of the BEC cases were relatively straightforward, forward emails wait for the opportunity to intervene.

2 The present
What is happening right now?

Red team developments

Lots of tooling available to ”pentest” Office 365 environments:

- MSOLSpray
- Ruler
- O365 Attack toolkit
- MailSniper
- Attack Simulator by Microsoft

Blue team developments

New tooling available to investigate and defend your environments:

- CrowdStrike Reporting Tool for Azure
- HAWK, for quick triage
- DFIR-O365RC, acquisition tool from ANSSI
- NotRuler
- MITRE ATT&CK now includes cloud specific techniques
- MailItemsAccessed logging for E5 customers

3 Holistic Approach

Old approach

- Search for indicators of compromise based on the story of the engagement
- Perform checks based on your knowledge of BEC Tactics, Techniques & Procedures

Pros:

- Quick

Cons:

- You might miss stuff
- Inconsistent results
- Standardization is difficult

Holistic approach

- Combine the good of the old approach and;
- Perform a set of pre-determined checks regardless of the incident story
- Leverage threat intelligence

Pros:

- (More) Complete
- Consistent results

Cons:

- Need to stay updated on the latest TTPs and make sure procedures are continuously updated

4 BEC Guide

Developed in 2020/2021 at PwC with my former colleagues

- Joey Rentenaar
- Curtis Hanson
- Anna Laskai

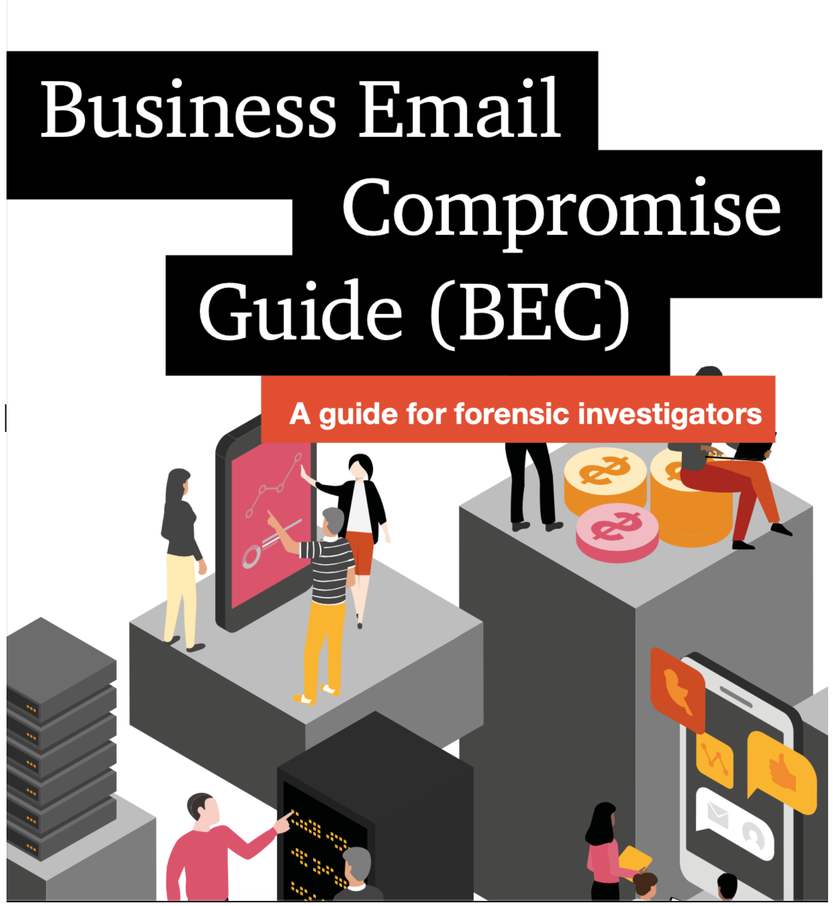
https://github.com/PwC-IR/Business-Email-Compromise-Guide

Intention of the guide is to provide digital responders with the knowledge and tools to investigations

- Great success ☺
- Not known everywhere

Guide consists of 10 steps

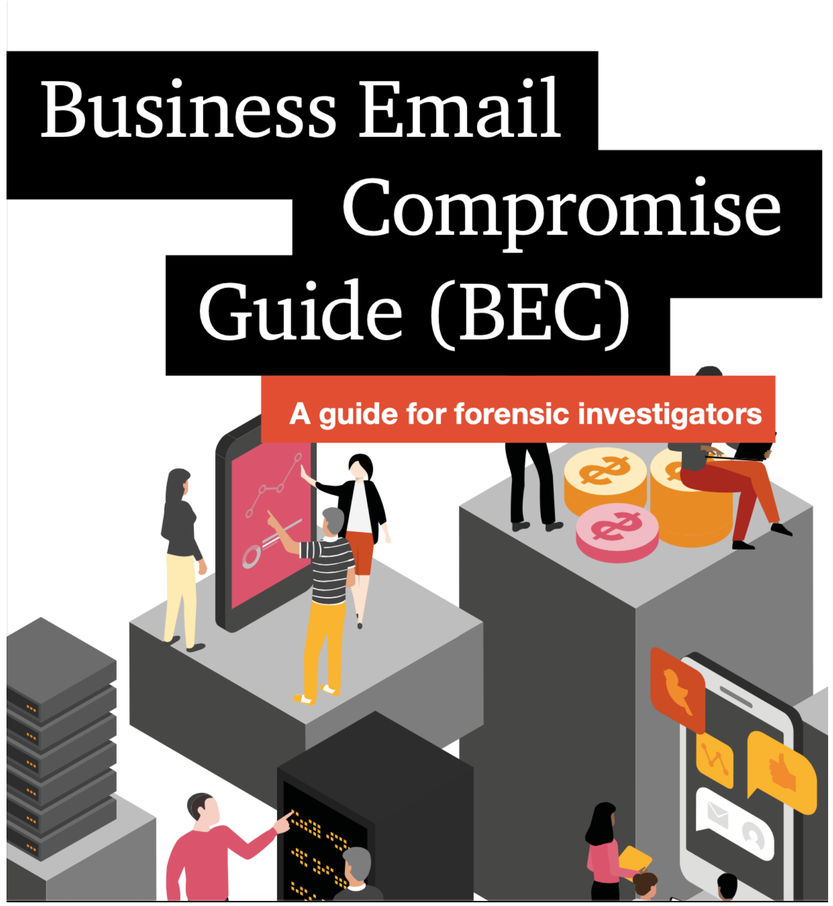
- Can be used as blueprint for your holistic approach
- It’s not limited to Office 365 environments
- AFAIK the guide is currently not maintained



4 BEC Guide

In this talk we will be discussing a subset of the documented steps:

- Step 1 - Investigation Kickoff
- Step 2 - Preparation & Collection
- Step 3 - Forwarding Rules
- Step 4 - Login activity
- Step 5 - Permission changes
- **Step 6 - OAuth2 Abuse**
- Step 7 - Evasion techniques
- **Step 8 - Assess Data Accessed or Exfiltrated**
- Step 9 - Threat Intelligence, Phishing Emails and Malware
- **Step 10 - Recommendations**



Step 4 - Login activity

Overview

Description

Login activity, particularly suspicious logins attempts are expected if a threat actor has accessed or is attempting to access the victim's environment. The UAL captures details for every login performed by a user and are useful for identifying suspicious activity, such as brute force attacks.

How

Threat actors typically leverage the following methods to get access to an environment:

- (Spear)phishing
- Password Spraying
- Brute-Force attacks

Detection

Unified Audit Log (UAL)

- MailboxLogin
- UserLoggedIn
- UserLoginFailed

Look for anomalous user-agents:

- CBAInProd
- Ruler

Look for anomalous IP-addresses:

- Unexpected locations
- One IP-address logging into multiple accounts in short amount of time
- Multiple IP-addresses logging into one account in short amount of time

Multi Factor Authentication (MFA)

- UserStrongAuthClientAuthNRequiredInterrupt

Step 4 - Login activity
Brute Force attacks

Brute force attack

Brute-force attacks often result in account lockouts, because too many logins occur over a short period of time, lock-out events are recorded in the UAL.

UserId	Reason	ClientIP	UserAgent
GradyA@dutchmasterz.onmicrosoft.com	IdsLocked	80.114.221.214	Mozilla/5.0 (Linux; Android 11; Pixel 3a) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.134 Mobile Safari/537.36 Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.114 Safari/537.36 Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
MiriamG@dutchmasterz.onmicrosoft.com	IdsLocked	80.114.221.214	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36

Step 4 - Login activity
Brute Force attacks

Brute force attack

A smarter threat actor will use multiple IP-addresses and apply a time interval between the subsequent attempts to prevent lock-out.

ClientIP	UserId	UserAgent
109.36.130.165	GradyA@dutchmasterz.onmicrosoft.com	Mozilla/5.0 (Linux; Android 11; Pixel 3a) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.134 Mobile Safari/537.36
178.85.138.132	GradyA@dutchmasterz.onmicrosoft.com	Mozilla/5.0 (Linux; Android 10; SM-N960F) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.120 Mobile Safari/537.36
80.114.221.214	GradyA@dutchmasterz.onmicrosoft.com MiriamG@dutchmasterz.onmicrosoft.com	Mozilla/5.0 (Linux; Android 11; Pixel 3a) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.134 Mobile Safari/537.36 Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.114 Safari/537.36 Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36

Step 6 – OAuth2 Abuse

Overview

Description

BEC threat actors abuse OAuth applications in order to gain access to a victim's account without using a victim's credentials. OAuth is a way of authorizing third-party applications to login into user accounts such as social media and webmail.

How

Threat actors typically leverage the following methods to trick users with fake applications:

- Gain access to the environment, register a new application
- Send an email requesting permissions for the new application
- After user allows permissions, threat actor can impersonate the user and their permissions without the need for a password or MFA

Detection

Unified Audit Log (UAL)

- Add application
- Consent to application
- Add app role assignment grant to user
- Add OAuth2PermissionGrant

Alternatively:

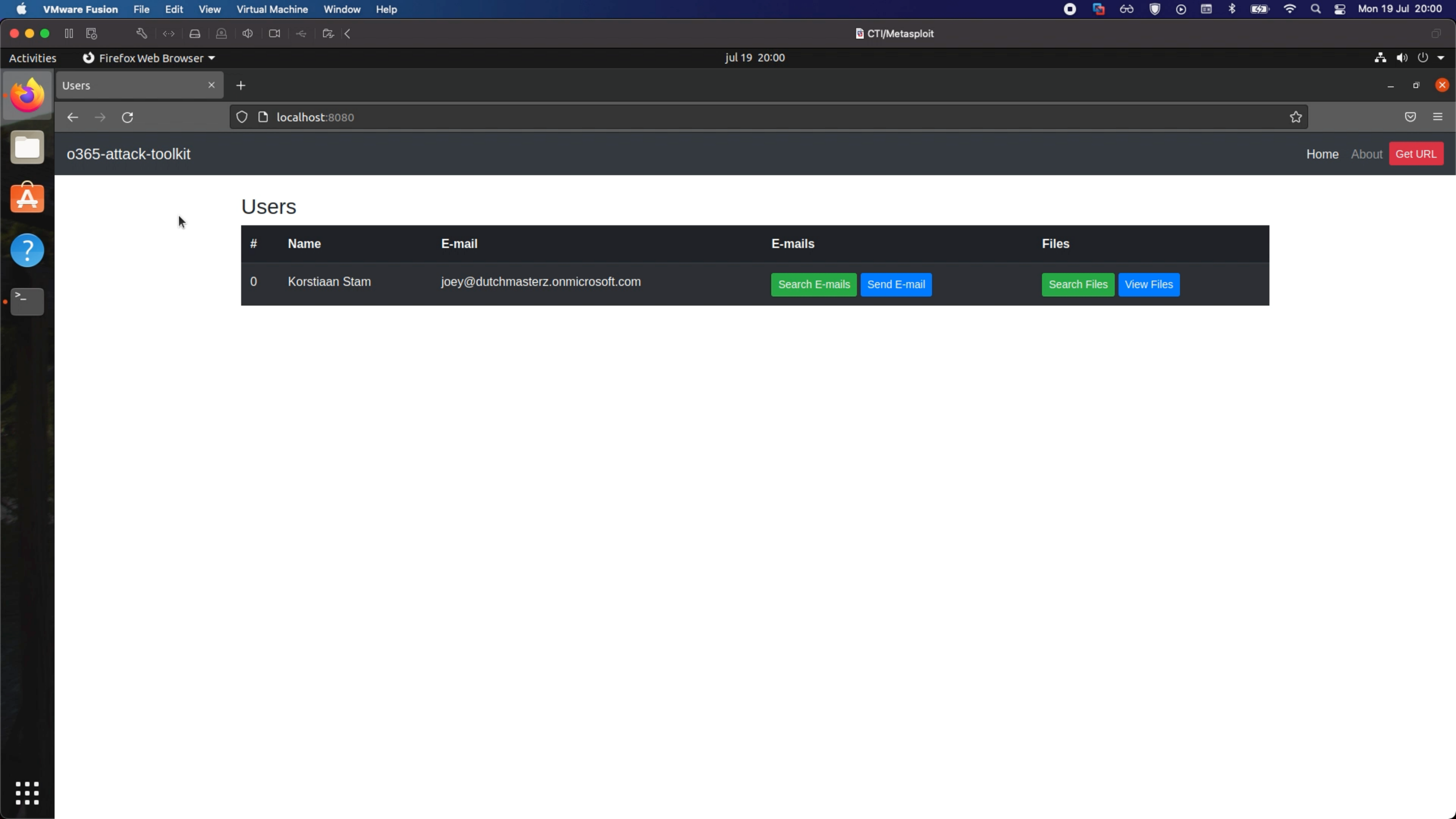
- Go to the Azure portal - User-Applications
- Get-AzureADPSPermissionGrants
- Crowdstrike CRT

Step 6 – OAuth2 Abuse
Malicious app registration and usage

Example attack

1. Threat actor registers a new malicious OAuth2 app
2. Threat actor sends phishing email requesting the permissions for the malicious app from the user(s)
3. User grants permissions
4. Threat actor has access to account/emails of user

Test if for yourself with the 0365 toolkit from MDSec:
https://github.com/mdsecactivebreach/o365-attack-toolkit


VMware Fusion File Edit View Virtual Machine Window Help
Mon 19 Jul 20:00
CTI/Metasploit
Activities
Firefox Web Browser
jul 19 20:00
Users
localhost:8080
o365-attack-toolkit
Home
About
Get URL
Users
Name E-mail E-mails Files
0 Korstiaan Stam joey@dutchmasterz.onmicrosoft.com
Search E-mails
Send E-mail
Search Files
View Files

Step 6 – OAuth2 Abuse
Malicious app registration and usage

Detection & Response

1. Threat actor registers a new malicious OAuth2 app

Applications added to Azure

CreationTime	SourceAccount	AppDetails
2021-07-12T11:54:32	joey@dutchmasterz.onmicrosoft.com	AppAddress=[{ "AddressType": 0, "Address": "http://localhost:30662/gettoken", "ReplyAddressClientType": 1, "ReplyAddressIndex": null, "IsReplyAddressDefault": false }] AppId=["842cef72-745d-463c-8b49-ce16ccc5ebd2"] AvailableToOtherTenants=[true] DisplayName=["sisai"] Included Updated Properties=AppAddress, AppId, AvailableToOtherTenants, DisplayName, RequiredResourceAccess RequiredResourceAccess=[{ "ResourceAppId": "00000003-0000-0000-c000-000000000000", "RequiredAppPermissions": [{ "EntitlementId": "e1fe6dd8-ba31-4d61-89e7-88639da4683d", "DirectAccessGrant": false, "ImpersonationAccessGrants": [20]

* Event only generated when the malicious application is created in the environment you are investigating

** Microsoft Portal – App Registrations contains all registered applications with AppId

Step 6 – OAuth2 Abuse

Malicious app registration and usage

Detection & Response

2. Threat actor sends phishing email asking users for permissions for the malicious app
3. User grants permissions to application

Permissions assigned to application by users

14m ago

CreationTime	Operation	AppId	User	Application Permissions
2021-07-12T11:51:27	Consent to application.	768fb398-1e3f-4a25-8989-2141f5eb5ebd	joey@dutchmasterz.onmicrosoft.com	ConsentAction.Permissions=[] => [[Id: BuKXIHEpH0-uoibcqwjFowX827gP2l9It2x9H5IJxp8, ClientId: 2097e206-2971-4f1f-aea2-26dcab08c5a3, PrincipalId: , ResourceId: b8dbfc05-da0f-485f-b76c-7d1f9209c69f, ConsentType: AllPrincipals, Scope: User.Read User.ReadBasic.All User.Read.All Group.Read.All Group.ReadWrite.All], [Id: BuKXIHEpH0-uoibcqwjFo-sb3saOFPZDjHMp2EIy5pk, ClientId: 2097e206-2971-4f1f-aea2-26dcab08c5a3, PrincipalId: , ResourceId: c6de1beb-148e-43f6-8c73-29d84232e699, ConsentType: AllPrincipals, Scope: User.Read]];
2021-07-12T11:58:23	Consent to application.	842cef72-745d-463c-8b49-ce16ccc5ebd2	AlexW@dutchmasterz.onmicrosoft.com	ConsentAction.Permissions=[] => [[Id: IEWH5_WxIEWP8TxaMYUdIOsb3saOFPZDjHMp2EIy5pn-RqaVzOOKSKlIG6Trx7ET, ClientId: e7874520-b1f5-4520-8ff1-3c5a31851d20, PrincipalId: 95a646fe-e3cc-488a-a948-1ba4ebc7b113, ResourceId: c6de1beb-148e-43f6-8c73-29d84232e699, ConsentType: Principal, Scope: offline_access Contacts.Read User.Read Mail.Read Mail.Send Files.ReadWrite.All Files.Read Files.Read.All openid profile]];
2021-07-12T11:59:10	Consent to application.	842cef72-745d-463c-8b49-ce16ccc5ebd2	joey@dutchmasterz.onmicrosoft.com	ConsentAction.Permissions=[] => [[Id: IEWH5_WxIEWP8TxaMYUdIOsb3saOFPZDjHMp2EIy5pnLAYCdWaFSQqOhwtxonzIq, ClientId: e7874520-b1f5-4520-8ff1-3c5a31851d20, PrincipalId: 9d8001cb-a159-4252-a3a1-c2dc689f322a, ResourceId: c6de1beb-148e-43f6-8c73-29d84232e699, ConsentType: Principal, Scope: offline_access Contacts.Read User.Read Mail.Read Mail.Send Files.ReadWrite.All Files.Read Files.Read.All openid profile]];
2021-07-12T12:05:19	Consent to application.	Application_05b9401d-262a-4cc8-969b-c78cec87aacf	AlexW@dutchmasterz.onmicrosoft.com	ConsentAction.Permissions=[] => [[Id: AAAAAAAAAAAAAAAAAAAAAOsb3saOFPZDjHMp2EIy5pn-RqaVzOOKSKlIG6Trx7ET, ClientId: 00000000-0000-0000-0000-000000000000, PrincipalId: 95a646fe-e3cc-488a-a948-1ba4ebc7b113, ResourceId: c6de1beb-148e-43f6-8c73-29d84232e699, ConsentType: Principal, Scope: offline_access Contacts.Read User.Read Mail.Read Mail.Send Files.ReadWrite.All Files.Read Files.Read.All openid profile email]];
2021-07-12T12:06:03	Consent to application.	395a1045-4185-43f1-ba4f-2b889bf7416b	joey@dutchmasterz.onmicrosoft.com	ConsentAction.Permissions=[] => [[Id: AAAAAAAAAAAAAAAAAAAAAOsb3saOFPZDjHMp2EIy5pnLAYCdWaFSQqOhwtxonzIq, ClientId: 00000000-0000-0000-0000-000000000000, PrincipalId: 9d8001cb-a159-4252-a3a1-c2dc689f322a, ResourceId: c6de1beb-148e-43f6-8c73-29d84232e699, ConsentType: Principal, Scope: offline_access Contacts.Read User.Read Mail.Read Mail.Send Files.ReadWrite.All Files.Read Files.Read.All openid profile]];

Step 6 – OAuth2 Abuse
Malicious app registration and usage

Detection & Response

4. Threat actor performs activities within App context such as reading emails

Operations by application

1m ago

Operation	count
MailItemsAccessed	7
Update service principal.	6
UserLoginFailed	6
Add app role assignment grant to user.	4
Consent to application.	4
Add application.	1
Add owner to application.	1
Add service principal.	1

Step 8 – Data Access/Exfiltration

Overview

Description

One of the biggest challenges during a BEC investigation is determining which emails or data has been accessed by a threat actor. Logs that help determine which emails were accessed, copied and/or exfiltrated may be missing or unavailable.

How

Threat actors might exfiltrate data for extortion attempts as seen in ransomware. Or to target clients of yours with legitimate documents there are a lot of good uses for threat actors.

- Manual searching of mailboxes
- Another method used by threat actors is leveraging the built-in eDiscovery suite
- Synchronize a mailbox to an ‘Offline’ mailbox

Detection

Unified Audit Log (UAL) only for E5!

- MailItemsAccessed

Two types of activity recorded:

- Bind access

Used for individual messages being accessed

- Sync access

Activity recorded related to applications syncing email messages using a client, such as Outlook on desktop

eDiscovery activity is recorded under:

- eDiscovery search started or exported

Step 8 – Data Access/Exfiltration

Data exfiltrated

Email access through malicious app

Threat actor gained access through the usage of a malicious application and able to read emails

1. Search for Bind activity within the MailItemsAccessed operation
2. Determine the malicious app using ClientAppId
3. Determine what emails were accessed based on the InternetMessageId

Some important notes for the Bind operation within the MailItemsaccessed Operation.

- Aggregated data covers a period of 2 minutes
- InternetMessageId can be used to identify individual emails
- Number of operations within an event captured in field ‘Operation Count’
- Operation stops logging if more than 1000 records are recorded within 24 hour

Step 8 – Data Access/Exfiltration

Data exfiltrated

Bind access to email through malicious app

1. Search for Bind activity within the MailItemsAccessed operation
2. Determine the malicious app using AppId

Bind access

CreationTime	ClientAppId	InternetMessageId	Owner	Operation Count	Folder Path	SourceIPAddress
2021-07-12T11:59:32	842cef72-745d-463c-8b49-ce16ccc5ebd2	<3c8225af9b384ba69c41ae5b312ba716-JFBVALKQOJXWILKCJQZFA7CPGM3DKTLFONZWCZ3FINSW45DFOJ6E2Q2ENFTWK43UL4YDMMBWGIYXYU3NORYA====@microsoft.com>	joey@dutchmasterz.onmicrosoft.com	5	\Inbox	40.126.32.99
2021-07-12T11:59:32	842cef72-745d-463c-8b49-ce16ccc5ebd2	<8ec082cba1374a06b0c8e7dd27baaf2d-JFBVALKQOJXWILKNK4YVA7CPGM3DKTLFONZWCZ3FINSW45DFOJ6E2ZLTONQWOZKDMVXHIZLSL5GUGMRWG44TKMT4KNWXI4A=@microsoft.com>	joey@dutchmasterz.onmicrosoft.com	5	\Inbox	40.126.32.99
2021-07-12T11:59:32	842cef72-745d-463c-8b49-ce16ccc5ebd2	<c40964d3525d4baab2802d1a65406798-JFBVALKQOJXWILKNK4YVA7CPGM3DKTLFONZWCZ3FINSW45DFOJ6E2Q2ENFTWK43UL4YDKMRTGIYXYU3NORYA====@microsoft.com>	joey@dutchmasterz.onmicrosoft.com	5	\Inbox	40.126.32.99
2021-07-12T11:59:32	842cef72-745d-463c-8b49-ce16ccc5ebd2	<d81dd510c1f145de9407b0b4fb2578cf-JFBVALKQOJXWILKNK4YVA7CPGM3DKTLFONZWCZ3FINSW45DFOJ6E2Q2ENFTWK43UL4YDOMJRGIYXYU3NORYA====@microsoft.com>	joey@dutchmasterz.onmicrosoft.com	5	\Inbox	40.126.32.99
2021-07-12T11:59:32	842cef72-745d-463c-8b49-ce16ccc5ebd2	<e4b519b753f8464bb33508ef284d02ff-JFBVALKQOJXWILKCJQZFA7CPGM3DKTLFONZWCZ3FINSW45DFOJ6E2Q2ENFTWK43UL4YDIMRVGIYXYU3NORYA====@microsoft.com>	joey@dutchmasterz.onmicrosoft.com	5	\Inbox	40.126.32.99

3. Determine what emails were accessed using PowerShell

```
Get-MessageTrackingLog –MessageID ‘InternetMessageId’
                    OR
Start-HistoricalSearch –Startdate <date> -EndDate <date> -ReportTitle <String> -
ReportType MessageTrace –MessageID ‘InternetMessageId’
                    OR
```

Step 8 – Data Access/Exfiltration

Data exfiltrated

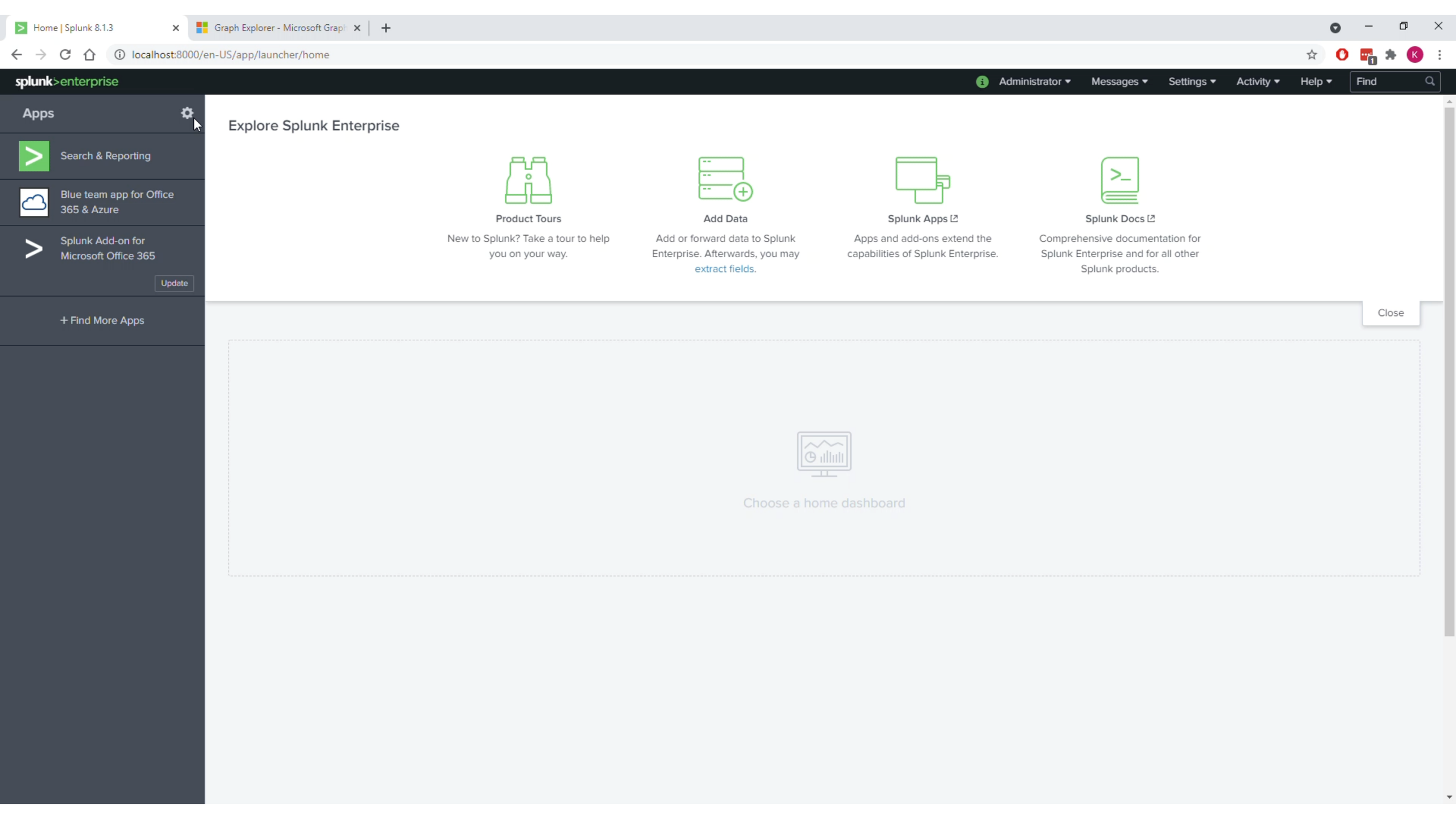
Demo

Use Data Accessed Investigator in Splunk app

&

Graph Explorer (https://developer.microsoft.com/en-us/graph/graph-explorer)

Query used: https://graph.microsoft.com/v1.0/me/messages?$filter=internetMessageId eq **‘InternetMessageId’**


Home | Splunk 8.1.3
Graph Explorer - Microsoft Graph
localhost:8000/en-US/app/launcher/home
splunk>enterprise
Administrator
Messages
Settings
Activity
Help
Find
Apps
Search & Reporting
Blue team app for Office 365 & Azure
Splunk Add-on for Microsoft Office 365
Update
+ Find More Apps
Explore Splunk Enterprise
Product Tours
New to Splunk? Take a tour to help you on your way.
Add Data
Add or forward data to Splunk Enterprise. Afterwards, you may extract fields.
Splunk Apps
Apps and add-ons extend the capabilities of Splunk Enterprise.
Splunk Docs
Comprehensive documentation for Splunk Enterprise and for all other Splunk products.
Close
Choose a home dashboard

Step 8 – Data Access/Exfiltration

Data exfiltrated

Sync operation with Outlook client

Threat actor performs an offline sync operation to download all emails

Sync access

<1m ago

CreationTime	MailboxOwnerUPN	Item.ParentFolder.Name	SourceIP	ClientInfoString	ClientProcess
2021-06-14T10:48:43	joey@dutchmasterz.onmicrosoft.com	Inbox	34.99.76.45	Client=MSExchangeRPC	OUTLOOK.EXE
2021-06-14T10:48:55	joey@dutchmasterz.onmicrosoft.com	Problèmes de synchronisation	34.99.76.45	Client=MSExchangeRPC	OUTLOOK.EXE
2021-06-14T10:48:55	joey@dutchmasterz.onmicrosoft.com	1	34.99.76.45	Client=MSExchangeRPC	OUTLOOK.EXE
2021-06-14T10:48:56	joey@dutchmasterz.onmicrosoft.com	Archive	34.99.76.45	Client=MSExchangeRPC	OUTLOOK.EXE
2021-06-14T10:48:56	joey@dutchmasterz.onmicrosoft.com	Historique des conversations	34.99.76.45	Client=MSExchangeRPC	OUTLOOK.EXE
2021-06-14T10:48:56	joey@dutchmasterz.onmicrosoft.com	Problèmes de synchronisation	34.99.76.45	Client=MSExchangeRPC	OUTLOOK.EXE
2021-06-14T10:48:57	joey@dutchmasterz.onmicrosoft.com	Deleted Items	34.99.76.45	Client=MSExchangeRPC	OUTLOOK.EXE

Step 10 –Recommendations

Overview

The below technical recommendations are based on personal experiences and security best practices. There are almost certainly other recommendations that can be implemented at an organization but these are considered ‘easy wins’.

1. Enable Multi-Factor Authentication (MFA)
2. Ensure mailbox audit logging enabled for all accounts
3. Enforce a strong password policy
4. Forward Office 365 logging to a centralized location
5. Perform regular checks on (active) forwarding rules
6. Perform regular checks on registered applications
7. Block mail forwarding to external domains
8. Disable legacy protocol authentication when appropriate
9. Security awareness training

5 The future
What is next?

More BEC attacks

There are no signs of BEC attacks slowing down. Insurers report that BEC and Ransomware are the Top 2 attacks in terms of damage.

BEC & APT

As seen for instance in SolarWinds attack the email environment remains a great initial access vector. More advanced threat actors will be targeting your email environment.

Increased complexity

With the attention of APTs for online email environments expect more advanced attacks leveraging trusts in AzureAD and application attacks.

5 The future
What you can do to be prepared

Splunk app updated

I have updated my Splunk application and it contains more and better dashboards to detect and respond to BEC attacks.
https://github.com/invictus-ir/Blue-team-app-Office-365-and-Azure

Dataset for researchers

One of the most time-consuming things is testing out use cases and having realistic incident data. Together with my colleagues over the years we have created a superset of AuditRecords, cleaned it up a bit by removing some IP-addresses it contains all kinds of weird activity. Use at your own risk.
https://github.com/invictus-ir/o365_dataset

THANK YOU

Korstiaan Stam (@korstiaans)
Founder, Invictus Incident Response
E: korstiaan@invictus-ir.com
W: invictus-ir.com

Resources

Splunk App:

- https://github.com/invictus-ir/Blue-team-app-Office-365-and-Azure
- https://splunkbase.splunk.com/app/4667/

Dataset:

- https://github.com/invictus-ir/o365_dataset

BEC Guide:

- https://github.com/PwC-IR/Business-Email-Compromise-Guide