Business Email Compromise Guide (BEC)

A guide for forensic investigators

pwc

Summary

The Business Email Compromise Guide sets out to describe 10 steps for performing a Business Email Compromise (BEC) investigation, including, but not limited to, an Office 365 environment. Each step is intended to guide an individual through the process of identifying, collecting and analysing activity commonly associated with BEC intrusions. The process begins with the prerequisites of an investigation to direct the scope, followed by the preparation and collection of data necessary for analysis. Intermediate steps cover different analysis techniques to identify suspicious and common BEC tactics, tooling and procedures (TTPs). The final step includes remediation measures to help mitigate and recover from current or future BEC related intrusions. Overall, this guide attempts to equip cyber security professionals with the necessary knowledge to handle a BEC investigation from start to finish.

Key Takeaways

- Define the scope of an investigation and direct the investigative process by using questions and a checklist.
- Preparation is critical for success. It should be known which logs are available, how to extract them, and possess adequate permissions for collecting such logs.
- Forwarding rules are one of the most common tactics observed in BEC investigations.
- Identifying suspicious login activity is useful for assessing initial access and lateral movement.
- Permission changes on existing or newly created accounts often indicate the threat actor established persistence, and could indicate the scope of an investigation is wider than initially assessed.
- BEC threat actors can be adaptive and innovative in their tactics, such as abusing OAuth applications or other vulnerabilities.
- Assessing which emails or data has been accessed and/or exfiltrated is critical for determining the impact on an organisation, including but not limited to financial losses, privacy implications and reputational damages.
- Threat intelligence is an important part of the investigative process, which supports understanding a threat actor's overall tradecraft, and identifying phishing emails.
- BEC intrusions are typically opportunistic and attribution is difficult.
- There are some simple and effective steps to mitigate BEC intrusions.

Table of contents

Introduction

Business Email Compromise (BEC) is a type of scam targeting executives or employees authorized to make payments by tricking the victim into transferring money to fraudulent accounts. BEC is synonymous with CEO fraud and Email Account Compromise (EAC). The US Federal Bureau of Investigation (FBI) estimates that approximately USD 1.7 billion dollars has been lost to BEC between 2013 and 2019.[1] The average loss per victim is USD 72,000,[2] but there are many publicly documented cases of victims losing millions in a single instance.[3] BEC scams do not often require advanced techniques or tooling, but rely on social engineering techniques to manipulate victims. The simplicity of the scam, as well as the potentially high financial gain is what lends towards the persistence and prevalence of BEC attacks. It is highly likely that anyone working in the field of digital forensics, incident response or threat intelligence is bound to be involved in a BEC investigation.

The challenges faced in our initial BEC investigations were greatly exacerbated by the lack of technical information and tooling publicly available. So, through trial and error, we developed the necessary knowledge and tooling to help handle BEC investigations. This Guide sets out to share that knowledge, tooling and experience.

We have compiled first-hand accounts and open source materials to create an extensive but non-exhaustive guide for any cyber security professional conducting a BEC investigation. This guide focuses on steps applicable to investigations within an Office 365 environment; however, many of the steps are not mutually exclusive to an Office 365 environment and are representative of the threat actor's overall tradecraft which could be applicable to any BEC investigation. We hope this document supports others and helps disrupt BEC threat actors, while building trust in society. Hopefully, other organizations in this field follow our approach and share their knowledge, in order to tackle important problems and help those in need.

[1] '2019 Internet Crime Report', FBI, https://pdf.ic3.gov/2019_IC3Report.pdf (11 February 2020)
[2] '2019 Internet Crime Report', FBI, https://pdf.ic3.gov/2019_IC3Report.pdf (11 February 2020)
[3] 'Investment Firm Hit by BEC Scam', Bank Info Security, https://www.bankinfosecurity.com/investment-firm-hit-by-bec-scam-a-14287 (15 May 2020)

Step 1

Investigation Kickoff

BEC investigations often begin with limited details, such as someone stole money or attempted to steal money. A technical investigation is kicked off to determine what happened and the impact to the victim. All investigations differ but follow the same intrusion analysis process: begin at the first sign of malicious activity, work forward to identify the worst, and then go back and fill in the missing pieces to generate a complete picture of the intrusion. Throughout this process are questions that need to be answered and used to both define the scope of an investigation and guide the investigative process. This section outlines those typical questions, alongside providing a checklist of actions for a BEC investigation.

1.1 Investigative Questions

There are common questions that arise during a BEC investigation, which we have mapped to relevant sections in this guide. It may not be possible to answer all of the questions because an investigation encounters missing logs, data or information. Some questions require completing multiple steps before being able to determine an answer. In fact, some questions may even require an investigation to be nearly completed before a proper assessment is made. There are questions that could be irrelevant to a specific investigation, but we have written this Guide to include some of the most common questions that arise in a BEC investigation.

Question	Guide
Which logs are available?	Step 1 - Administrator Audit Log and Unified Audit Log
How to collect relevant logs?	Step 1 - Collection Methods
What accounts were compromised and/or accessed?	Step 2 - Forwarding Rules Step 3 - Login Activity Step 4 - Permission changes

Is there indication that the threat actor is still in the environment or maintains access?	Step 2 - Forwarding Rules Step 3 - Login Activity Step 4 - Permission changes Step 5 - OAuth2 Abuse Step 6 - Other suspicious activity Step 7 - Assess Data
When did the intrusion begin?	Step 3 - Login Activity Step 5 - OAuth2 Abuse Step 8 - Threat Intelligence, Phishing Emails and Malware
How long did the threat actor maintain access?	Step 2 - Forwarding Rules Step 3 - Login Activity Step 4 - Permission changes Step 5 - OAuth2 Abuse Step 6 - Other suspicious activity Step 7 - Assess Data Step 8 - Threat Intelligence, Phishing Emails
What data was accessed and/or exfiltrated by the threat actor?	Step 7 - Assess Data
Is there someone internal involved?	Step 2 - Forwarding Rules Step 3 - Login Activity Step 8 - Threat Intelligence, Phishing Emails and Malware
Is this a targeted attack and who is responsible?	Step 8 - Threat Intelligence, Phishing Emails and Malware
How to prevent future attacks?	Step 9 - Recommendations

1.2 Checklist

The following checklist is non-exhaustive but consists of action to take in a BEC investigation:

Step 1: Investigation Kickoff

○ Define the scope of an investigation.

Step 2: Preparation and Collection

○ Available logs based on retention policy (e.g., 90 days and is that within scope).

○ Collect Admin Audit Log.

○ Collect Unified Audit Log.

○ Collect Message Trace Log.

Step 3: Forwarding Rules

○ Name of the forwarding rule(s).

○ Forwarding rule(s) using the RSS folder, etc.

○ Email addresses used by the threat actor (e.g., non-business account, etc.).

Step 4: Login Activity

○ Suspicious Logins (e.g., Unknown IPs or odd country locations).

○ Indications of brute force attempts (e.g., multiple back-to-back failed login attempts).

○ Events showing username guesses.

Step 5: Permission Changes

○ New users being created.

○ Users being added to administrator groups/roles.

○ Users given permissions to other mailboxes.

Step 6: OAuth2 Abuse

○ Check for odd applications in the application list abusing OAuth.

○ Check for recent Oauth2 permissions given to applications in the UAL.

○ Applications with admin consent in the environment.

Step 7: Evasion Techniques

○ Audit Log has been disabled.

○ Items being shared with individuals outside of the organization.

○ eDiscovery alerts.

Step 8: Data Accessed

○ Identify sessions belonging to the threat actor.

○ Identify email messages accessed by the threat actor.

○ Data exfiltrated by a malicious forwarding rule.

○ Impact analysis based on the emails accessed.

Step 9: Threat Intelligence, Phishing Email and Malware

○ Domain of sender and receiver.

○ Email headers.

○ Email content (e.g., malicious attachments, links, fake signatures, etc.).

Step 10: Recommendations

○ ‘Strong’ passwords and password policy.

○ Multi-Factor Authentication (MFA).

○ Mailbox audit logging is enabled.

○ Block forwarding to external domains.

Step 2

Preparation & Collection

An important step in a BEC investigation is preparation and collection methods. This step has become even more important as many engagements are occurring remotely. Log availability and collection methods could differ or not be viable for a particular investigation. While this section focuses on Office 365, there are several techniques that could be applicable to other environments. This section sets out to explain what Office 365 logs are relevant to a BEC investigation, how they can be collected, and what is required to complete the collection.

2.1 Unified Audit Log (UAL)

The UAL is a critical piece of evidence in a BEC investigation because it is a centralized source for all Office 365 events. The UAL contains at least 76 categories of data, including events from Azure, Exchange, SharePoint, OneDrive, and Skype.[1]

2.1.1 Roles and Permissions

An account is needed with sufficient permissions to collect the mentioned logs. This action is often overlooked and forgotten until collection is attempted. Requesting and implementing the correct permissions is necessary to avoid these setbacks. Microsoft has the following description on what roles are needed to extract the UAL:

“You have to be assigned the View-Only Audit Logs or Audit Logs role in Exchange Online to search the Office 365 audit log. By default, these roles are assigned to the Compliance Management and Organization Management role groups on the Permissions page in the Exchange admin center. To give a user the ability to search the Office 365 audit log with the minimum level of privileges, you can create a custom role group in Exchange Online, add the View-Only Audit Logs or Audit Logs role, and then add the user as a member of the new role group. For more information, see Manage role groups in Exchange Online.”[2]

During our investigations we often ask for a Global Reader account with Audit Log roles assigned, which can be accomplished via the following steps:

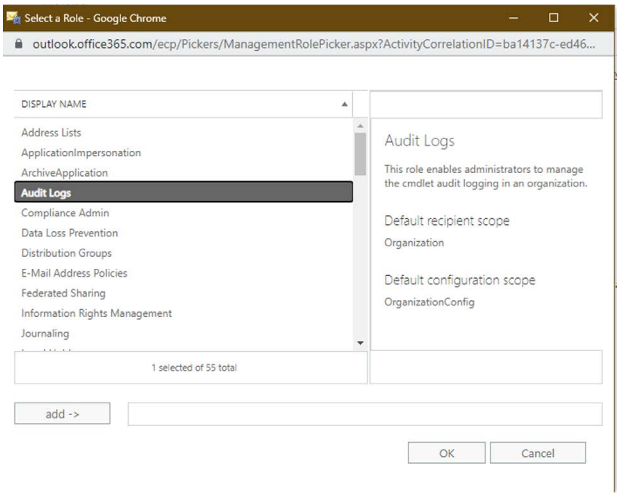
1. Create a new user account in the Microsoft 365 admin center (admin.microsoft.com);
2. Assign the new user ‘Global Reader’ role;
3. Go to Exchange admin center (protect.microsoft.com);
4. Click on ‘+’ to create a new ‘Role Group’, pick a name, and add the Audit Log role; and
5. Add the user to the new group.

[1] ‘Responding to Business Email Compromise Part 2, Korstiaan Stam, LinkedIn https://www.linkedin.com/pulse/responding-business-email-compromise-part-2-korstiaan-stam/ (25 April 2019)

[2] ‘Search the audit log in the compliance center’, Microsoft, https://docs.microsoft.com/en-us/microsoft-365/compliance/search-the-audit-log-in-security-and-compliance?view=o365-worldwide (13 October 2020)

2.1.2 Logs, Record Types and Artifacts

There are multiple types of records that can be extracted in an investigation. It is typically best practice to extract the complete UAL if possible because it assists in providing a complete picture and timeline of the incident. However, this option is not always viable and certain cases require a more targeted approach to triage the incident.



Select a Role - Google Chrome

outlook.office365.com/ecp/Pickers/ManagementRolePicker.aspx?ActivityCorrelationID=ba14137c-ed46...

DISPLAY NAME

Address Lists
ApplicationImpersonation
ArchiveApplication
Audit Logs
Compliance Admin
Data Loss Prevention
Distribution Groups
E-Mail Address Policies
Federated Sharing
Information Rights Management
Journaling

1 selected of 55 total

Audit Logs

This role enables administrators to manage the cmdlet audit logging in an organization.

Default recipient scope

Organization

Default configuration scope

OrganizationConfig

Figure 1- Add the Audit Logs role

The Complete UAL

The UAL contains at least 76 categories of data and it is recommended to extract the complete UAL. However, a major caveat with collecting the complete UAL is the acquisition time can be quite long. Large organisations often have millions of events and extracting a complete UAL with so many events can take more time than is expected or budgeted. If time is a concern, using another method that only extracts the suspected victim logs is possible and typically provides enough context to triage an incident.

Specific or Groups of RecordTypes

RecordTypes contain specific events for different services within Office 365. This method allows a user to choose which events to extract instead of the complete UAL. For example, a user can extract logs only containing information related to Exchange and ignore logs for Skype, SharePoint, etc. This method of extraction is popular when companies use SharePoint, which generates a high number of events. Extracting RecordTypes and eliminating irrelevant logs will decrease the time required for the extraction process. A full list of RecordTypes is provided in Appendix A.[3]

Specific Artifacts

The specific artifacts method is usually reserved for triaging because it provides only limited information necessary in an investigation. For example, a user can extract forwarding rules to do a quick spot check for malicious activity, but this method misses other relevant information needed to complete the investigation. Extracting specific artifacts can be accomplished with tools, such as HAWK.[4] HAWK is a PowerShell based tool and is discussed below.

2.1.3 Collection Methods

Once the type of logs needed for an investigation are determined, there are three main options for extracting them from the UAL:

- Security Compliance Center;
- Office 365 Management API; and
- Search-UnifiedAuditLog cmdlet.

[3] The list provided is a combination of RecordTypes publicly listed by Microsoft and first-hand research conducted by our Incident Response team. Microsoft often updates and removes RecordTypes, and it is recommended to monitor this activity and cross reference any changes with the data provided in Appendix A.

[4] https://github.com/Canthv0/hawk

Both the Security Compliance Center and Office 365 Management API have limitations. The Security Compliance Center only allow extraction of 5,000 sorted records or 50,000 unsorted records at a time. In our experience, BEC investigations almost always have more than 50,000 records. In fact, it is quite common to have several million records. Therefore, extracting 5,000 or 50,000 records at a time, creates a repetitive and inefficient process that results in dozens of separate excel files. The API possesses limited history, which is a result of tests we ran extracting records through the API. We have built our own solution on top of the Search-UnifiedAuditLog cmdlet, since this avoids the mentioned limitations and is a reliable way to extract the entire UAL.

2.1.4 Office 365 Extractor

The Office 365 Extractor is a tool created by our team to avoid the limitations incurred by the Security Compliance Center and Office 365 Management API. The Office 365 Extractor allows for acquisition of the complete UAL or Specific Record Types, and addresses the exporting records limit by automatically creating a new session every time the 5,000 sorted record limit is reached. The script extracts all of the defined logs into a single CSV file(s) and saves it to the LogDirectory.

The following is a general workflow for investigating a BEC case with the Office 365 Extractor:

1. Download and execute script;
2. Determine scope and time interval;
3. Choose extraction type; and
4. Begin acquisition.

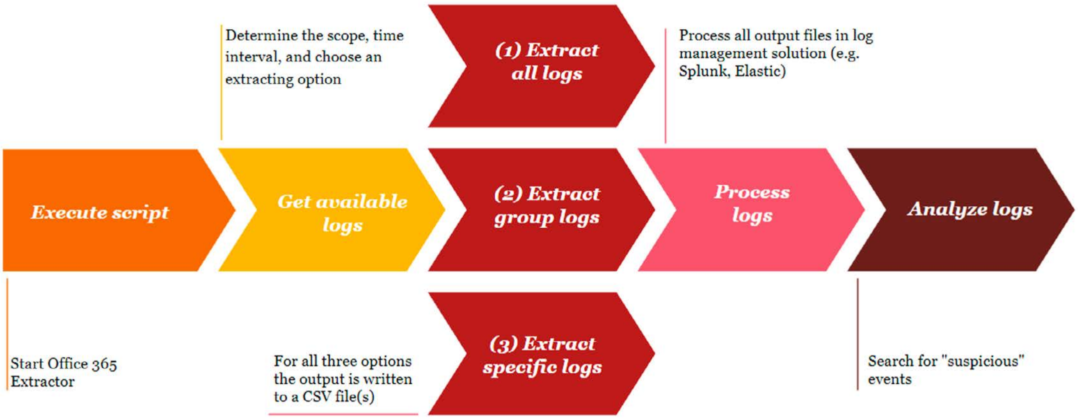
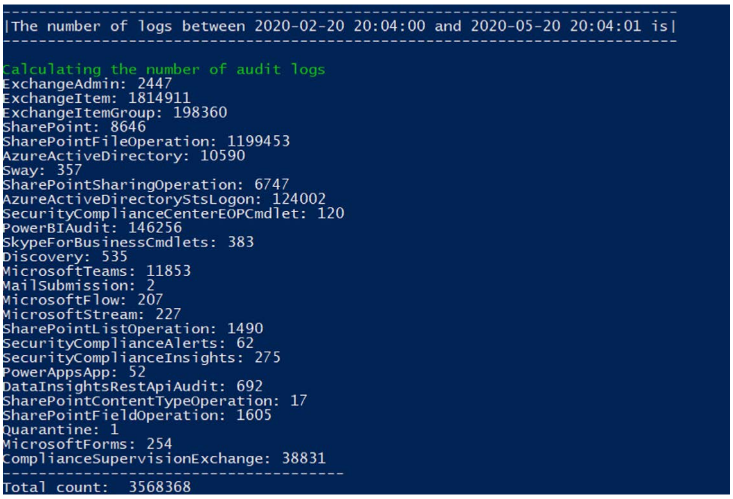

Determine the scope, time interval, and choose an extracting option
(1) Extract all logs
Process all output files in log management solution (e.g. Splunk, Elastic)
Execute script
Get available logs
(2) Extract group logs
Process logs
Analyze logs
Start Office 365 Extractor
For all three options the output is written to a CSV file(s)
(3) Extract specific logs
Search for "suspicious" events

Figure 2 - Workflow for investigating a BEC case

1. **Download and Execute the Office 365 Extractor**
   Download the Office 365_Extractor.ps1 script from our Github page: https://github.com/PwC-IR/Office-365-Extractor and run the script with PowerShell.

2. **Determine Scope and Interval**
   At the start of an investigation it is often unknown which log sources are available or how many logs exist. This information is required to determine the scope and time interval for the Office 365 Extractor. The scope includes the total amount and type of records available and the time period of interest. To determine the scope, choose the first option of the script that indicates the available logging from the 76 different log types.

Start by running the Office365 Extractor, and selecting option one in the menu: *Show available log sources and amount of logging*. The output of the script provides an overview of which logs are available and their relative amounts (see image below).



```
-----------------------------------------------------------------------------
|The number of logs between 2020-02-20 20:04:00 and 2020-05-20 20:04:01 is|
-----------------------------------------------------------------------------

Calculating the number of audit logs
ExchangeAdmin: 2447
ExchangeItem: 1814911
ExchangeItemGroup: 198360
SharePoint: 8646
SharePointFileOperation: 1199453
AzureActiveDirectory: 10590
Sway: 357
SharePointSharingOperation: 6747
AzureActiveDirectoryStsLogon: 124002
SecurityComplianceCenterEOPCmdlet: 120
PowerBIAudit: 146256
SkypeForBusinessCmdlets: 383
Discovery: 535
MicrosoftTeams: 11853
MailSubmission: 2
MicrosoftFlow: 207
MicrosoftStream: 227
SharePointListOperation: 1490
SecurityComplianceAlerts: 62
SecurityComplianceInsights: 275
PowerAppsApp: 52
DataInsightsRestApiAudit: 692
SharePointContentTypeOperation: 17
SharePointFieldOperation: 1605
Quarantine: 1
MicrosoftForms: 254
ComplianceSupervisionExchange: 38831
----------------------------------------
Total count:  3568368
```

Figure 3 - Output of available log sources and amount of logging

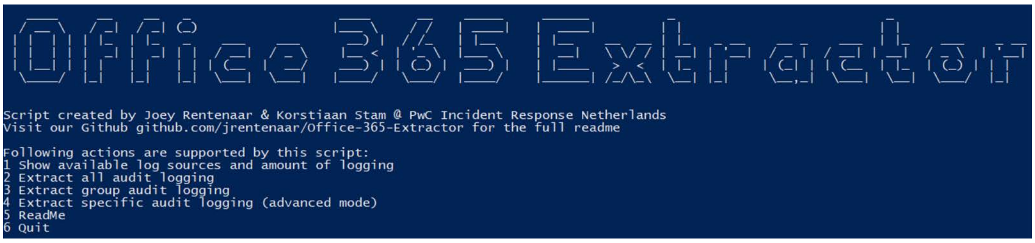
The above information should be supplemented with answering the following questions in an attempt to determine the scope:

How much time is available for the acquisition?
The best practice is to acquire the complete UAL. However, acquisition of the complete UAL can take multiple days which may not be a viable option. If time is limited, then it is not recommended to extract the complete UAL, but only focus on Specific or Groups of RecordTypes.

What information is relevant for the investigation?
In most BEC intrusions the investigation is centered around the Exchange environment, which means not all logs need to be extracted only Specific or Groups of RecordTypes. There are exceptions, and if time permits, it is best practice to extract the complete UAL to capture a complete picture and timeline of the incident.

When did the incident likely occur?
Depending on the Office 365 license of a victim, logs are either available for the last 90 days (E3 license) or 365 days (E5 license). Knowing the general timeframe of when an incident occured can help reduce time wasted extracting data not relevant to an investigation. For example, rather than extracting the last 90 days of events, a user can extract the last 10 days from when the incident likely occurred. This approach saves time and resources, but could miss indicators relevant to an investigation if the intrusion occurred outside of the estimated time frame.

Should the focus be on all users or specific users?
The Office 365 Extractor provides an option to extract events for specific user(s). This approach limits the acquisition to only relevant victims and reduces acquisition time. Best practice is to extract the complete UAL, since the scope of an investigation can expand as analysis is conducted, which could require data from other victims.

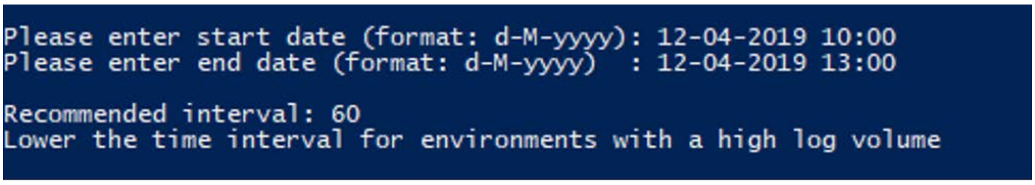


```
Script created by Joey Rentenaar & Korstiaan Stam @ PwC Incident Response Netherlands
Visit our Github github.com/jrentenaar/Office-365-Extractor for the full readme

Following actions are supported by this script:
1 Show available log sources and amount of logging
2 Extract all audit logging
3 Extract group audit logging
4 Extract specific audit logging (advanced mode)
5 ReadMe
6 Quit
```

Figure 4 - Office 365 Extractor Main menu

Once the scope is determined, define the relevant start and end date of the investigation in the Office365 Extractor. It is also necessary to designate a time interval between the start and end dates, which closely reflect the time it takes to reach 5,000 records. The reason for setting a time interval is because Office 365 Extractor addresses the exporting records limit by automatically creating a new session every time the 5,000 record limit is reached. However, regardless of whether a long or short interval is chosen, the script adapts to the amount of logs in a given time frame and guarantees that all logs are extracted. We recommend 60 minutes as a default time interval but this amount may vary based on your investigation. Once the scope and interval are determined, the next step is acquiring the desired record type. After the time interval is provided the script will give you the option to provide specific users. If you only need to acquire the events for specific users you can select this option, if not select all users.



```
Please enter start date (format: d-M-yyyy): 12-04-2019 10:00
Please enter end date (format: d-M-yyyy)  : 12-04-2019 13:00

Recommended interval: 60
Lower the time interval for environments with a high log volume
```

Figure 5 - Select dates and interval

3. **Choose Exaction Type**
Complete UAL: The following groups are pre-configured in the Office 365 Extractor. Selecting one of the groups all RecordTypes in the group will be extracted automatically:

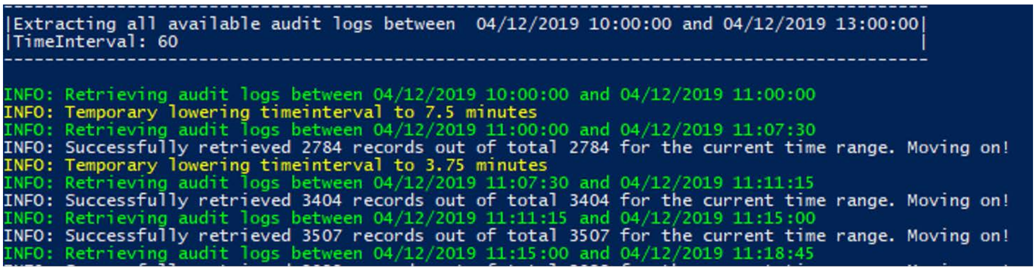
Input group name script	RecordTypes in group
All Exchange logging	ExchangeAdmin, ExchangeAggregatedOperation, ExchangeItem, ExchangeItemGroup, ExchangeItemAggregated, ComplianceDLPExchange, ComplianceSupervisionExchange, MipAutoLabelExchangeItem
All Azure logging	AzureActiveDirectory, AzureActiveDirectoryAccountLogon, AzureActiveDirectoryStsLogon
All Sharepoint logging	ComplianceDLPSharePoint, SharePoint, SharePointFileOperation, SharePointSharingOperation, SharepointListOperation, ComplianceDLPSharePointClassification, SharePointCommentOperation, SharePointListItemOperation, SharePointContentTypeOperation, SharePointFieldOperation, MipAutoLabelSharePointItem, MipAutoLabelSharePointPolicyLocation
All Skype logging	SkypeForBusinessCmd, SkypeForBusinessPSTNUsage, SkypeForBusinessUsersBlocked

Specific Audit Logs: Extract individual data sets from the 46 available record types. This process can be reproduced for any number of specific logs, which are written to separate CSV files. We recommend extracting at least the following RecordTypes:

O365 Service	RecordType	Description	Important artifacts
Exchange	ExchangeAdmin	Contains Exchange admin audit data.	Forwarding activity
	ExchangeItem	Contains Exchange mailbox audit data.	Forwarding activity, mailbox permission changes
Azure	AzureActive Directory	Contains AD logging.	Login activity (Brute force, MFA errors, suspicious logins)

A full list of RecordTypes is provided in Appendix A.[5] After selecting the acquisition option the script will extract all the required log events. The output files are hashed using the SHA256 algorithm. This allows the audit logs to be used as evidence and maintain a proper chain of custody. Hashing is considered best practice for digital forensic practitioners as it reduces the chance of evidence being tampered with and maintains the integrity of the data over time.

2.1.5 HAWK



```
-------------------------------------------------------------------------------------
|Extracting all available audit logs between  04/12/2019 10:00:00 and 04/12/2019 13:00:00|
|TimeInterval: 60                                                                    |
-------------------------------------------------------------------------------------

INFO: Retrieving audit logs between 04/12/2019 10:00:00 and 04/12/2019 11:00:00
INFO: Temporary lowering timeinterval to 7.5 minutes
INFO: Retrieving audit logs between 04/12/2019 11:00:00 and 04/12/2019 11:07:30
INFO: Successfully retrieved 2784 records out of total 2784 for the current time range. Moving on!
INFO: Temporary lowering timeinterval to 3.75 minutes
INFO: Retrieving audit logs between 04/12/2019 11:07:30 and 04/12/2019 11:11:15
INFO: Successfully retrieved 3404 records out of total 3404 for the current time range. Moving on!
INFO: Retrieving audit logs between 04/12/2019 11:11:15 and 04/12/2019 11:15:00
INFO: Successfully retrieved 3507 records out of total 3507 for the current time range. Moving on!
INFO: Retrieving audit logs between 04/12/2019 11:15:00 and 04/12/2019 11:18:45
```

Figure 6 - Terminal output during extracting

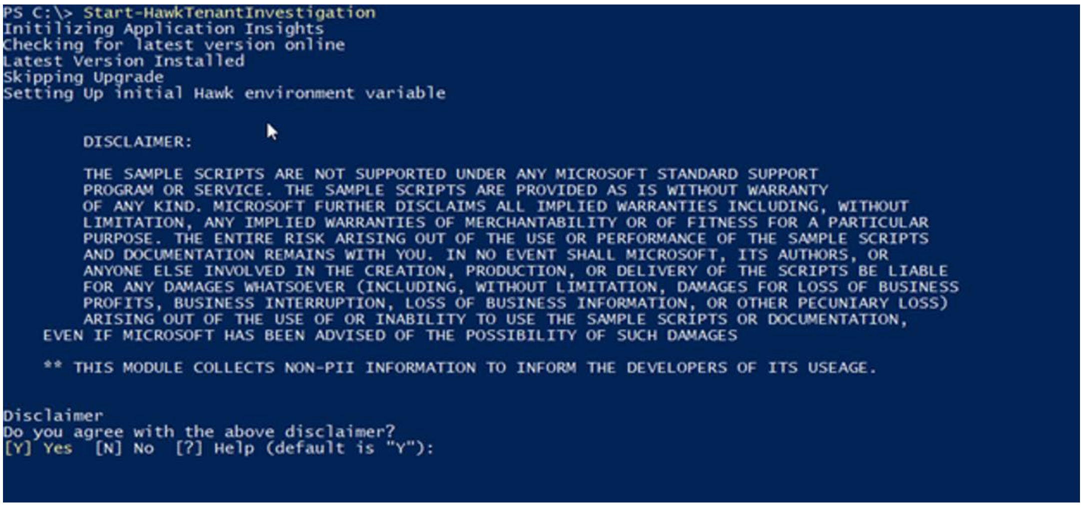
While the Office 365 Extractor does not support the extraction of specific artifacts, there are tools for this task. HAWK is a PowerShell based tool used for gathering information related to Office 365 intrusions, such as specific artifacts.[6] Running HAWK creates an audit report that includes the following information:

- CAS Mailbox Info;
- User login events with IP addresses;
- Mailbox Audit Report;
- User Mailbox Forwarding Information;
- User Inbox Rules Information;
- Mailbox Info;
- Mailbox Statistics; and
- Azure Authentication logs report.

[5] The list provided is a combination of RecordTypes publicly listed by Microsoft and first-hand research conducted by our Incident Response team. Microsoft often updates and removes RecordTypes, and it is recommended to monitor this activity and cross reference any changes with the data provided in Appendix A.

[6] Canthv0, Github, https://github.com/Canthv0/hawk

As briefly mentioned, extracting specific artifacts is typically reserved for triaging and spot checks for malicious activity. A comprehensive investigation is likely to use one of the other methods discussed above.



```
PS C:\> Start-HawkTenantInvestigation
Initilizing Application Insights
Checking for latest version online
Latest Version Installed
Skipping Upgrade
Setting Up initial Hawk environment variable


        DISCLAIMER:

        THE SAMPLE SCRIPTS ARE NOT SUPPORTED UNDER ANY MICROSOFT STANDARD SUPPORT
        PROGRAM OR SERVICE. THE SAMPLE SCRIPTS ARE PROVIDED AS IS WITHOUT WARRANTY
        OF ANY KIND. MICROSOFT FURTHER DISCLAIMS ALL IMPLIED WARRANTIES INCLUDING, WITHOUT
        LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR OF FITNESS FOR A PARTICULAR
        PURPOSE. THE ENTIRE RISK ARISING OUT OF THE USE OR PERFORMANCE OF THE SAMPLE SCRIPTS
        AND DOCUMENTATION REMAINS WITH YOU. IN NO EVENT SHALL MICROSOFT, ITS AUTHORS, OR
        ANYONE ELSE INVOLVED IN THE CREATION, PRODUCTION, OR DELIVERY OF THE SCRIPTS BE LIABLE
        FOR ANY DAMAGES WHATSOEVER (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS
        PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, OR OTHER PECUNIARY LOSS)
        ARISING OUT OF THE USE OF OR INABILITY TO USE THE SAMPLE SCRIPTS OR DOCUMENTATION,
    EVEN IF MICROSOFT HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES

    ** THIS MODULE COLLECTS NON-PII INFORMATION TO INFORM THE DEVELOPERS OF ITS USEAGE.


Disclaimer
Do you agree with the above disclaimer?
[Y] Yes  [N] No  [?] Help (default is "Y"):
```

Figure 7 - Starting HAWK

2.2 Administrator Audit Log

The administrator audit log records specific actions based on Exchange Online PowerShell cmdlets that are performed by administrators and users who have been assigned administrative privileges. Entries in the administrator audit log provide information about what cmdlet was run, which parameters were used, who ran the cmdlet, and what objects were affected.[7]

Only extract the Administrator Audit Log when the UAL is unavailable because the UAL contains all the information in the Administrator Audit Log. Only in older environments, when UAL is not enabled, does the Administrator Audit Log contain useful information for the investigation.

2.2.1 Roles and Permissions

Microsoft has the following description on what roles are needed to extract the Administrator Audit Log: You have to be assigned the Audit Log role in Exchange Online to search the administrator audit log and view the results. By default, these roles are assigned to the ComplianceManagement, OrganizationManagement or SecurityAdministrator role groups on the Permission page in the Exchange Admin center.[8]

During our investigations we often ask for a Global Reader account with Audit Log roles assigned, which can be accomplished via the following steps:

1. Create a new user account in the Microsoft 365 admin center (admin.microsoft.com);
2. Assign the new user ‘Global Reader’ role;
3. Go to Exchange admin center (protect.microsoft.com);
4. Click on ‘+’ to create a new ‘Role Group’, pick a name, and add the Audit Log role; and
5. Add the user to the new group.

2.2.2 Collection Methods

The Administrator Audit Log can be extracted by running the following PowerShell command:

```
Search-AdminAuditLog -StartDate 09/17/2020 -EndDate 10/02/2020 |
epcsv output.csv -NoTypeInformation -Append
```

[7] ‘View the administrator audit log’, Micrsosoft, https://docs.microsoft.com/en-us/exchange/security-and-compliance/exchange-auditing-reports/view-administrator-audit-log (7 July 2020)

[8] ‘Permissions in standalone EOP’, Microsoft, https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/feature-permissions-in-eop?view=o365-worldwide

2.3 Message Trace Logs

Message trace follows email messages as they travel through your Exchange Online organization. You can determine if a message was received, rejected, deferred, or delivered by the service. It also shows what actions were taken on the message before it reached its final status.[9]

2.3.1 Roles and Permissions

Microsoft has the following description on what roles are needed to extract the Message Trace Logs:
To do a message trace, you need to be a member of the Organization Management, Compliance Management or Help Desk role groups.[10]

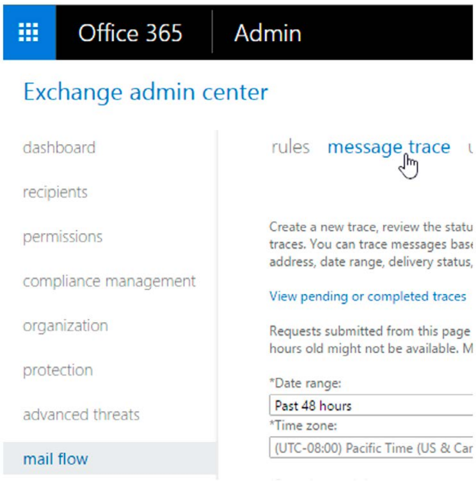
You can add a new user to one of the required roles by following the steps below:

1. Create a new user account in the **Microsoft 365 admin center**. (admin.microsoft.com)
2. Next, go to **Exchange admin center** (protect.microsoft.com).
3. Click on go to **Exchange admin center** and add the user to the required role(s).

2.3.2 Collection Methods

Extracting the Message Trace Logs is possible via the GUI or by running a PowerShell script. The following is an overview using the GUI method to extract the Message Trace Logs:

1. Go to the Exchange Admin center;
2. Go to Mail flow; and then
3. Message trace.



Create a new trace, review the statu traces. You can trace messages bas address, date range, delivery status,

Requests submitted from this page hours old might not be available. M

*Date range: Past 48 hours

*Time zone: (UTC-08:00) Pacific Time (US & Car

Figure 8 - Message Trace Logs

Depending on what information is needed from the message trace log, the fields mentioned below can help. None of these fields require values for messages that are less than 7 days old. The default search without providing any of the fields is 48 hours. If searching for data beyond 7 days, then a specific value is needed for one of the fields.

- Date range;
- Delivery status;
- Message ID;
- Sender; And
- Recipient.[11]

[9] ‘Message trace in the Security & Compliance Center’, Microsoft, https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/message-trace-scc?view=o365-worldwide (22 September 2020)

[10] ‘Message trace in the Security & Compliance Center’, Microsoft, https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/message-trace-scc?view=o365-worldwide (22 September 2020)

[11] ‘Run a message trace in the classic EAC’, Microsoft, https://docs.microsoft.com/en-us/exchange/monitoring/trace-an-email-message/run-a-message-trace-and-view-results (28 October 2020)

The following is an overview using the PowerShell method to extract the Message Trace Logs:

Extract the Message Trace logs by using a script provided by Microsoft,[12] which saves the results in a CSV file found in the C directory.

```
   do
    {
        Write-Host “Processing - Page $Page...”

        # by default it will just get the last 7 days, to get more change -7
below up to -30
        $Batchfile = Get-MessageTrace -StartDate (Get-Date).
AddDays(-7) -EndDate (Get-Date)  -PageSize 5000  -Page $Page| Select
Received,*Address,*IP,Subject,Status,Size

        $Batchfile | Export-Csv c:\FILE-$PAGE.csv -NoTypeInformation

        $Page++
    }
    until ($Batchfile -eq $null)
```

[12] ‘Export Mail logs to CSV for up to 30 days,regardless of the number of entries’, Microsoft, https://gallery.technet.microsoft.com/scriptcenter/Export-Mail-logs-to-CSV-d5b6c2d6 (19 June 2014)

Step 3

Forwarding Rules

BEC threat actors often create email forwarding rules to collect sensitive information and to maintain persistence in the environment; even when a compromised account's password is reset. The main TTP observed in our BEC investigations are malicious forwarding rules. Those rules allow the threat actor to continuously monitor activities of a victim and further gain information relating to the victim and their associates. Forwarding rules are commonly created by blind carbon copying all incoming and outgoing emails to an external email account. This tactic allows the threat actor to read all emails without leaving obvious signs of their presence.

3.1 Detect forwarding rules

Malicious forwarding rules can be identified by using the UAL. In the UAL look for the following operations to identify new forwarding rules, rules being modified or to detect active rules.

Operation	Description
New-InboxRule	Inbox rules process messages in the Inbox based on conditions and take actions such as moving a message to a specified folder or deleting a message. [1]
New-TransportRule	Transport rules (mail flow rules) in your organization. [2]

[1] 'Set-InboxRule, Microsoft, https://docs.microsoft.com/en-us/powershell/module/exchange/set-inboxrule?view=exchange-ps

[2] 'New-TransportRule', Microsoft, https://docs.microsoft.com/en-us/powershell/module/exchange/new-transportrule?view=exchange-ps

3.1.2 Rules Being Modified

Operation	Description
Set-Mailbox	Used to modify the settings of existing mailboxes. This is also applicable for forwarding settings of existing mailboxes.[3]
Set-InboxRule	Used to modify existing Inbox rules in mailboxes. Inbox rules process messages in the Inbox based on conditions specified and take actions such as moving a message to a specified folder or deleting a message. [4]
Set-TransportRule	Used to modify existing transport rules (mail flow rules) in an organization.[5]

3.1.3 Active Rules

Property	Description
DeliverToMailboxAndForward	Indicates messages sent to a mailbox are forwarded to another mailbox.
ForwardingSMTPAddress	A ProxyAddresses value that has lower priority than ForwardingAddress.
ForwardingAddress	A RecipientIdParameter and used to forward emails to a mail-enabled object.
SentTo	Indicates where the messages are being sent to.
BlindCopyTo	Indicates where the messages are being blind copied to.
ForwardTo	Indicates where the messages are being forwarded to.

[3] 'Set-Mailbox, Microsoft, https://docs.microsoft.com/en-us/powershell/module/exchange/set-mailbox?view=exchange-ps

[4] 'Set-InboxRule, Microsoft, https://docs.microsoft.com/en-us/powershell/module/exchange/set-inboxrule?view=exchange-ps

[5] 'Set-Transport rule', Microsoft, https://docs.microsoft.com/en-us/powershell/module/exchange/set-transportrule?view=exchange-ps

3.2 Determine if forwarding is malicious or expected

Investigations involving large organisations sometimes have an immense amount of forwarding rules. There are valid reasons for having forwarding and not all forwarding rules are malicious. It can be a challenge to identify the malicious rule(s) amongst a large data set. However, there are two areas to focus on that can help determine if a rule is malicious or not:

External Recipients

It is a red flag when an email is being forwarded to external recipients, especially when the rule hits on specific keywords such as payment and invoice. There are not many legitimate business reasons to forward emails with invoices to an external mail account. Upon finding such a rule, it is good practice to corroborate with both the IT administrator and mailbox account owner if the forwarding rule is likely legitimate or malicious.

Folders

Threat actors often hide their malicious forwarding rules. The following list provides common folders threat actors often place forwarding rules, which could be an indication of malicious activity:

- RSS;
- Archive;
- Junk Email; and
- Conversation History.

3.3 Tactics and Techniques

More detailed information on each of the tactics and techniques used by a threat actor in this section, along with mitigations, correspond to the following MITRE tactics and techniques:

ID	Tactic/Technique
T1114.002	Email Collection: Remote Email Collection
T1114.003	Email Collection: Email Forwarding Rule

Step 4

Login Activity

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. Evasion techniques that could be used to disguise login activity is discussed in Step 7.

4.1 Suspicious Logins

Each time a user logs into their account an event is created. This event will contain valuable information such as the IP address. An IP address can be used to conduct a geographic lookup and compare the results to expected geographic locations of an organization and its user. For example, if a company is located in the Netherlands and there is no business presence in Asia, or the company's VPN does not resolve to an IP address in Asia, then you would not expect any events recorded from Asia. So in this example, logins from Asia are suspicious and require attention. Detecting these types of suspicious logins is accomplished by searching keywords in the UAL.

Operation	Description
MailboxLogin	The user has just logged in.
UserLoggedIn	The user has just logged in.
UserLoginFailed	The login of a user has failed.

In addition to searching IP addresses, both UserAgent and Time of logins are strong indicators for suspicious logins. UserAgent can be used to detect suspicious logins, such as identifying a 'new' or non-corporate device login to an account. This behavior is a possible red flag that should be further reviewed. The time at which a login occurs can also be an indication of malicious activity. For example, logins occurring outside of the user's normal working hours is possibly a red flag that warrants further examination.

4.2 Multi-Factor Authentication (MFA) Errors

MFA errors are another red flag for possible malicious activity. In some cases, a threat actor manages to acquire the login credentials of a user and attempts to log into the account, but is stopped with MFA. If the attacker doesn't have access to the second factor then the authentication process fails and an event is generated.

Operation	Description
UserStrongAuthClientAuthNRequired	Due to a configuration change made by the admin, or because of moving to a new location, the user must use multi-factor authentication to access the resource. Retry with a new authorized request for the resource.[1]
UserStrongAuthClientAuthNRequiredInterrupt	Strong authentication is required and the user did not pass the MFA challenge.

4.3 Brute Force Attacks

Brute force attacks create a lot of noise; resulting in many events which are relatively easy to detect. Searching the UAL for the rules below can identify possible brute force attacks.

Operation	Description
IdsLocked	The account is locked because the user tried to sign in too many times with an incorrect user ID or password.
UserKey="Not Available"	When a threat actor is guessing user accounts and the account does not exist then the UserKey="Not Available" event will be created.
UserLoginFailed	The login of a user has failed.

After identifying a brute force attack, it is recommended to determine if the attack was successful. This is accomplished by observing a successful login preceded by an abnormal amount of failed attempts. Sync activity can generate events that mimic a brute force attack, but it is almost certainly a false positive.

[1] 'Azure AD Authentication and authorization error codes', Microsoft, https://docs.microsoft.com/en-us/azure/active-directory/develop/reference-aadsts-error-codes (9 November 2020)

4.4 Tactics and Techniques

More detailed information on each of the tactics and techniques used by a threat actor in this section, along with mitigations, correspond to the following MITRE tactics and techniques:

ID	Tactic/Technique
T1110.001	Brute Force: Password Guessing
T1110.002	Brute Force: Password Cracking
T1110.003	Brute Force: Password Spraying
T1110.004	Brute Force: Credential Stuffing
T1078.001	Valid Accounts: Default Accounts
T1078.002	Valid Accounts: Domain Accounts
T1078.003	Valid Accounts: Local Accounts
T1078.004	Valid Accounts: Cloud Accounts

Step 5

Permission changes

Permission changes are a commonly observed TTP that establish persistence and escalate privileges. Often when the threat actor accesses a victim's account, they do not possess sufficient privileges to reach their actions on objectives. In order to achieve those objectives the threat actor usually attempts to change permissions of existing or newly created accounts.

5.1 Identify Permission Changes

Events related to permission changes are identifiable by searching for the following keywords:

Operation	Description
Add-MailboxPermission	Used to add permissions to a mailbox or to an Exchange Server 2016, Exchange Server 2019, or Exchange Online mail user.[1]
Add-RecipientPermission	Used to add SendAs permission to users in a cloud-based organization.[2]
Add-MailboxFolderPermission	Used to add folder-level permissions for users in mailboxes.[3]
Set-MailboxFolderPermission	Used to modify folder-level permissions for users in mailboxes.[4]

[1] 'Add-MailboxPermission', Microsoft, https://docs.microsoft.com/en-us/powershell/module/exchange/add-mailboxpermission?view=exchange-ps

[2] 'Add-Recipient Permission', Microsoft, https://docs.microsoft.com/en-us/powershell/module/exchange/add-recipientpermission?view=exchange-ps

[3] 'Add-Mailbox Folder Permission', Microsoft, https://docs.microsoft.com/en-us/powershell/module/exchange/add-mailboxfolderpermission?view=exchange-ps

[4] 'Set-mailbox Folder Permission', Microsoft, https://docs.microsoft.com/en-us/powershell/module/exchange/set-mailboxfolderpermission?view=exchange-ps

Add member to role	This indicates a member being added to a role.
Add member to group	This indicates a member being added to a group.

We recommend having increased monitoring capabilities on the custom administrator groups. Any user being added to any of the administrator groups should be reviewed. It's important to keep in mind that it's possible to create custom groups with a high amount of privileges, such as those listed below:

- Billing administrator
- Conditional Access administrator
- Exchange administrator
- Global administrator
- Helpdesk (Password) administrator
- Password administrator
- Security administrator
- SharePoint administrator
- User administrator

5.2 Identify New User Account(s)

Threat actors may create an account to maintain access to an environment. Accounts may be created on the local system, within a domain or cloud tenant. In cloud environments, adversaries may create accounts that only have access to specific services, which can reduce the chance of detection.

To identify new user accounts search for the following operation in the UAL:

Operation	Description
Added user	New user has been added

The UAL often only shows a limited history of accounts. However, using https://admin.microsoft.com/AdminPortal/Home#/users and the Admin GUI, a complete list of users is available. Additionally, it is recommended to check all user accounts in the Office 365 environment against a list of users from the IT administrator and/or Human Resource department. This approach could potentially spot other previously unknown accounts.

Note: The UAL has limited history available depending on the type Office 365 license used, which can affect the ability to identify a specific account; especially if it occurs outside of the last captured event.

5.3 Tactics and Techniques

More detailed information on each of the tactics and techniques used by a threat actor in this section, along with mitigations, correspond to the following MITRE tactics and techniques:

Operation	Tactic/Technique
T1136.002	Create Account: Domain Account
T1136.003	Create Account: Cloud Account

Step 6

OAuth2 Abuse

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. The advantage of OAuth is that users don't have to reveal their password; instead, the third-party applications use a token for authentication. In an OAuth abuse attack, a victim authorizes a third-party application to access their account. Once authorized, the application accesses the user's data without the need for credentials. The user receives a message to accept the application with its requested API permissions. After the user selects accept, the threat actor has control of the user's account.

6.1 Detect Abuse of OAuth

Sometimes an organisation does not actively monitor application(s) of their users. In such cases it is easy for a malicious application or abuse of an application to occur. In order to detect this kind of behavior, there are at least three operations to check in the UAL that indicate an application is receiving API access to a user's account via OAuth.

Operation	Description
Add 0Auth2PermissionGrant	OAuth2PermissionGrant was created for an application in Azure AD.
Consent to application	Admin consent was granted to an enterprise app in Azure AD.
Add app role Assignment grant to user	An app role was assigned to a user in Azure AD.

The name of the application can be found in either of the two events in the UAL:

1. Consent to application; or
2. Add app role assignment grant to user.

When opening one of the above events you can identify the name under the ID field.

If the use of the application by the user is not expected, then the next step is to check the API permissions by the application. Those can be found by opening the Consent to application event and look for the field: ConsentAction.Permissions. All new assigned permissions to the application will be listed after. For example, the operation Contacts.Read User.Read Mail.Read Notes.Read.All MailboxSettings.ReadWrite Files.ReadWrite.All openid profile shows the application is able to read the following:

- Contacts;
- Mail;
- Notes;
- MailboxSettings; and
- Files.

6.1.1 Review Applications Assigned

Reviewing a user's application access is possible via https://myapps.microsoft.com. On the webpage are all the apps with access, including details for each of them. The following apps are shown by default in an environment:

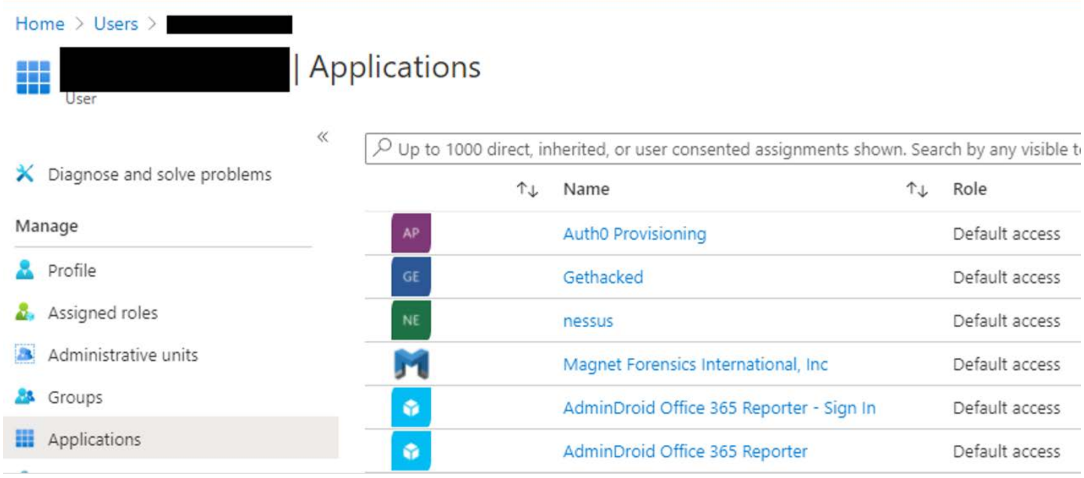
Add-ins	Admin	Calendar
Compliance	Dynamics 365	Excel
Forms	Kaizala	Myanalytics
OneDrive	OneNote	Outlook
People	Planner	Power Apps
Power Automation	Powerpoint	Security
Sharepoint	Stream	Sway
Task	Teams	To Do
Whiteboard	Word	

Any additional applications than those listed above, likely requires reviewing the application.

A second method to detect malicious applications is by using the Azure portal:

3. Go to the Azure portal and the Azure directory;
4. Select user; and
5. Select Applications.

The dashboard (see image below) shows all applications assigned to the user, and if a suspicious application identified then a user can view the permissions setting by selecting the application and then View Granted Permissions.



Home > Users > [redacted]

[redacted] | Applications

User

«

Diagnose and solve problems

Manage

Profile

Assigned roles

Administrative units

Groups

Applications

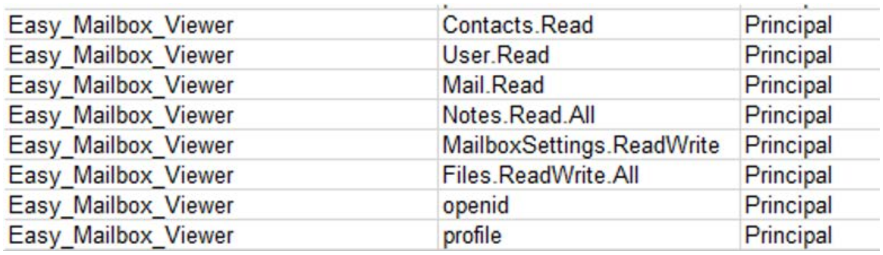
Up to 1000 direct, inherited, or user consented assignments shown. Search by any visible t

	Name	Role
AP	Auth0 Provisioning	Default access
GE	Gethacked	Default access
NE	nessus	Default access
	Magnet Forensics International, Inc	Default access
	AdminDroid Office 365 Reporter - Sign In	Default access
	AdminDroid Office 365 Reporter	Default access

Figure 9 - Applications assigned to user

6.1.2 Overview of All Applications in PowerShell

There is a script called Get-AzureADPSPermissions.ps1[1] that lists all delegated permissions (0Auth2PermissionsGrants) and application permissions (AppRoleAssignments) in Azure Active Directory. The results can be exported to a CSV file and used to identify unexpected applications.



Easy_Mailbox_Viewer	Contacts.Read	Principal
Easy_Mailbox_Viewer	User.Read	Principal
Easy_Mailbox_Viewer	Mail.Read	Principal
Easy_Mailbox_Viewer	Notes.Read.All	Principal
Easy_Mailbox_Viewer	MailboxSettings.ReadWrite	Principal
Easy_Mailbox_Viewer	Files.ReadWrite.All	Principal
Easy_Mailbox_Viewer	openid	Principal
Easy_Mailbox_Viewer	profile	Principal

Figure 10 - Application permissions of a suspicious application

6.2 Tactics and Techniques

More detailed information on each of the tactics and techniques used by a threat actor in this section, along with mitigations, correspond to the following MITRE tactics and techniques:

ID	Tactic/Technique
T1550.001	Use Alternate Authentication Material: Application Access Token

[1] Psignoret, GitHub, https://gist.github.com/psignoret/41793f8c6211d2df5051d77ca3728c09

Step 7

Evasion Techniques

It is common for BEC threat actors to use evasion techniques to avoid detection. The evasion techniques described below could be helpful in furthering an investigation.

7.1 Purge or Delete Rules for Forwarded Emails

As previously mentioned, a common tactic is to create a new forwarding rule once an account has been compromised. Additionally, threat actors often create a purging rule, which deletes or moves emails with specific terms to the trash. For example, the threat actor sends an email from a compromised account, but the email is subsequently deleted along with any replies. This allows the threat actor to carry on a conversation undetected from the compromised account.

7.2 Audit Log Disabled by User

Threat actors might disable the Audit Log to try and hide their tracks. However, disabling the Audit Log creates an event that is searchable using the operation below.

Operation	Description
Set-AdminAuditLogConfig	To configure the administrator audit logging configuration settings.[1]

7.3 eDiscovery: Compliance Search and Deletion of Items

eDiscovery is a legitimate tool available within Office 365. The tool is intended for legal and eDiscovery teams to search or acquire evidence in legal cases, such as mailbox contents. The compliance search feature of the tool can delete items, which could be used to remove evidence of an intrusion, such as phishing emails.

[1] 'Set-AdminAuditLogConfig', Microsoft, https://docs.microsoft.com/en-us/powershell/module/exchange/set-adminauditlog-config?view=exchange-ps

Operation	Description
New-ComplianceSearchAction + -Purge	Can be used to create actions for content searches in Office 365.[2]

7.4 Alternate Authentication Methods

Threat actors could use alternative authentication methods, such as application access tokens to bypass access controls. For further information see Step 5: OAuth Abuse.

7.5 Tactic and Techniques

More detailed information on each of the tactics and techniques used by a threat actor in this section, along with mitigations, correspond to the following MITRE tactics and techniques:

ID	Tactic/Technique
T1562.001	Impair Defenses: Disable or Modify Tools
T1550.001	Use Alternate Authentication Material: Application Access Token

[2] 'Content Search', Microsoft, https://docs.microsoft.com/en-us/microsoft-365/compliance/content-search?view=o365-worldwide (8 May 2020)

Step 8

Assess Data Accessed or Exfiltrated

One of the biggest challenges during a BEC investigation is determining which emails or data has been accessed by a threat actor. There are several specific actions that can help assess data accessed. However, it is good practice to assume that a threat actor accessed all emails within a compromised account. Logs may be missing or unavailable which are needed to determine more specifically which emails were accessed, copied and/or exfiltrated.

8.1 Determining Data Accessed

8.1.1 MailItemsAccessed

MailItemsAccessed is captured in the UAL under two similar yet different record types called Sync access and Bind access. Sync access is recorded when a mailbox is accessed by a desktop version of the Outlook client for Windows or Mac. More information on sync events can be found here [1]. Bind access is recorded when an individual message is accessed, the UAL also contains the message id of an email, required to determine which email was accessed. More info on bind events can be found here[2].

There are multiple ways of accessing this information. The audit logs can be investigated with any of three previously mentioned methods using the Security and Compliance Center, the Microsoft API or the Powershell cmdlets. Similar to the Office365 Extractor, we developed another tool to access MailItemsAccessed which we call MIA.[3] MIA relies on the UAL and the Message Trace log. An account with sufficient permissions is needed to use the tool, and more information on setting up MIA can be found on our Github page.[4]

[1] 'Auditing sync access', Microsoft, https://docs.microsoft.com/en-us/microsoft-365/compliance/mailitemsaccessed-forensics-investigations?view=o365-worldwide#auditing-sync-access (12 September 2020)

[2] 'Auditing bind access', Microsoft, https://docs.microsoft.com/en-us/microsoft-365/compliance/mailitemsaccessed-forensics-investigations?view=o365-worldwide#auditing-bind-access (12 September 2020)

[3] https://github.com/PwC-IR/MIA-MailItemsAccessed-

[4] PwC-IR, GitHub, https://github.com/PwC-IR/MIA-MailItemsAccessed-

8.1.2 Using MailItemsAccessed for an investigation

The following workflow is used to help identify what email data was accessed by the threat actor:

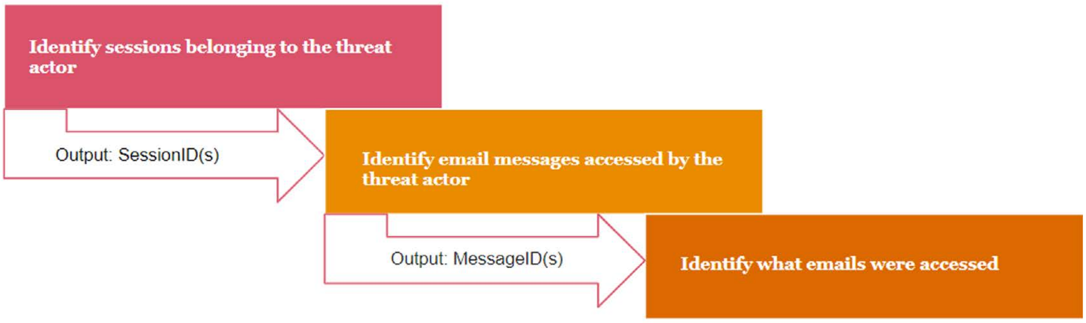

Identify sessions belonging to the threat actor
Output: SessionID(s)
Identify email messages accessed by the threat actor
Output: MessageID(s)
Identify what emails were accessed

Figure 11 - Workflow to identify accessed data

1. **Identify sessions belonging to the threat actor**
   The first step is to determine sessions belonging to the threat actor, which assumes that the account(s) compromised or the IP address of the threat actor is already identified. Identifying either pieces of information is possible by searching for the MailItemsAccessed operation in the UAL and filtering on the victim email account or the malicious IP address. The output displays multiple SessionIds and IP addresses for one user account. Based on indicators of compromise (IOCs) identified in previous steps it is possible to determine which sessions are likely legitimate or valid. Some sessions do not have a SessionId because legacy authentication was used to login. More information on sessions can be found on Microsoft's blog.[5]

   Another field is the 'OperationCount' which shows the count of messages that were accessed in a bind operation. All bind operations that occur within a 2-minute interval are aggregated, and the number of bind operations that are aggregated in the record is displayed in the OperationCount field.

2. **Identify InternetMessageID**
   The second step is using the SessionId to gather the InternetMessageID(s) of the accessed messages. The InternetMessageId is a unique identifier for email messages, which is used to identify individual emails. Locating the InternetMessageID is possible via the events found belonging to the sessions of the threat actor. Each event contains both multiple MessageID(s). You can use those MessageID(s) to identify the emails accessed by the threat actor.

3. **Identify Emails were accessed**
   The final step is using the Message Trace Log to determine the metadata of the exposed emails. Searching the Message Trace Log for the InternetMessageID shows metadata of the email accessed by the threat actor. This process is repeated for all the InternetMessageIDs to obtain an overview of all emails accessed within the incident period. In some cases, the threat actor could have accessed the environment before the earliest log entry, which would not show in the search. Emails identified via the metadata can be further analysed using the ComplianceSearch option in the Compliance center or by using PowerShell.

Limitations

Our testing of the sync access operation sometimes did not work properly. Several tests attempting to complete a full sync of a mailbox with a local installation of Outlook or Thunderbird did not record any sync events. This limitation could improve in the future.

Another limitation observed is identifying email metadata using the InternetMessageID. The available options are not ideal as the Get-MessageTrace cmdlet only has a history of 10 days, while Start-HistoricalSearch is too slow. The use of the InternetMessageID in the eDiscovery module would be ideal to quickly identify the email contents. At the time of writing this it's not possible to to use the eDiscovery module to identify email contents.

[5] 'Contextualizing Attacker Activity within Sessions in Exchange Online', Microsoft, https://techcommunity.microsoft.com/t5/exchange-team-blog/contextualizing-attacker-activity-within-sessions-in-exchange/ba-p/608801 (4 January 2019)

The MailItemsAccessed is only available via the Office 365 E5 license, and therefore, this subsection may not be applicable for some investigations. It is plausible that this functionality is expanded to E3 licenses in the future.

8.2 Identify Data Exfiltrated

8.2.1 Active Forwarding Rules

As previously mentioned, most BEC cases include email forwarding rules, which can help determine what data was exfiltrated. The table below contains operations to identify active forwarding rules.

Property	Description
DeliverToMailboxAndForward	Indicates messages sent to a mailbox are forwarded to another mailbox.
ForwardingSMTPAddress	A ProxyAddresses value that has lower priority than ForwardingAddress.
ForwardingAddress	A RecipientIdParameter and used to forward emails to a mail-enabled object.
SentTo	Indicates where the messages are being sent to.
BlindCopyTo	Indicates where the messages are being blind copied to.
ForwardTo	Indicates where the messages are being forwarded to.

It is possible to search on forwarding rule(s) to obtain all the events for emails being forwarded. The list of events contains all InternetMessageID(s) belonging to those events and can be searched in the Message Trace Log to find the metadata for the emails. This action can support a data impact assessment.

8.3 Sharing items with individuals outside of an organization

Searching for the AddedToSecureLink keyword in the UAL shows documents being shared with internal or external users. We recommend filtering out all internal email accounts, and only focus on the external accounts.

Operation	Description
AddedToSecureLink	A link that only works for specific people was secured to a user. The value in the Detail column for this activity identifies the name or email of the user the link was secured to and whether this user is an external user. The value also has a UniqueSharingId column that identifies the link they were secured to.[6]

[6] 'Secure external sharing recipient experience', Microsoft, https://docs.microsoft.com/en-us/sharepoint/what-s-new-in-sharing-in-targeted-release (17 June 2020)

8.4 eDiscovery alerts: Compliance search started or exported

As mentioned previously, eDiscovery is a legitimate tool intended for use by legal and eDiscovery teams to search or acquire evidence in legal cases. Typically, suspicious queries using this function should be reported and validated by another party responsible for overseeing legal and compliance functions.

Operation	Description
eDiscovery search started or exported	Generates an alert when someone uses the Content search tool in the Security and compliance center.[7]

[7] 'Alert policies in the security and compliance center', Microsoft, https://docs.microsoft.com/en-us/microsoft-365/compliance/alert-policies?view=o365-worldwide (20 November 2020)

Step 9

Threat Intelligence, Phishing Emails and Malware

Threat intelligence helps in a variety of stages of the investigation and is used extensively in our investigations. This section sets out to provide details useful for finding common BEC phishing emails, including subject lines, themes, contents, and fake domains. We also provide a non-exhaustive list of some of the common malware used by BEC focused threat actors, along with how the malware is used in an attack. We also briefly discuss victimology and attribution to round out practical uses of threat intelligence in a BEC investigation.

9.1 Initial Access

It might seem counterintuitive to hunt for artefacts relating to the start of an intrusion at the later stage of your BEC investigation. It is best practice within intrusion analysis to begin where detection first occurred and move forward in the investigation until the threat actor was stopped or succeeded in achieving their action on objectives. This procedure allows an analyst to know the worst first, such as whether confidential information was accessed by a threat actor, before identifying less important pieces of information such as phishing emails. Once the worst is taken care of, analysts work backwards in identifying the other tactics used or completing the earlier stages of the kill chain.

The initial access stage within an investigation can broadly be categorized into phishing, exploitation of a trusted relationship, valid account, and bypassing of applications. Several of these techniques are not exclusive to gaining initial access and can be used to establish persistence or move laterally within a victim’s environment.

9.1.1 Phishing

In some cases, there is no link or file included in the phishing email, and only social engineering techniques are relied on to manipulate the victim. This type of BEC attack could use spoofing domains and/or altered email headers, but typically it begins with a seemingly benign email requesting a meeting or checking if the victim is in the office. The conversation evolves over time with multiple email replies, until the victim receives banking details and is scammed into wiring money to the threat actor.

Email content and subject line searches are likely the best approach to finding the initial malicious email. The subject lines for these are usually a simple ‘hello’ or ‘hello [Name]’ or possibly something more striking such as ‘Urgent Request’. See section Email contents for more tips to use in an investigation.

9.1.2 Spearphishing Attachment

Spearphishing attachments pose a connotation of being the initial infection point for malware. However, often attachments in BEC attacks consist of fake invoices that do not contain malware but are simply used for social engineering. Attachments often use a lure related to one of the previously discussed email themes but can also be a fake invoice containing malware. In 2019, approximately 58% malware samples observed in BEC cases could easily be identified by public online multi-virus scanners.[1] The other 42% likely need to be reversed engineered or at least uploaded to a sandbox for further analysis. This high number indicates that incident response teams need to have access to specialised tools and knowledge to successfully analyse BEC related spearphishing attachments.

9.1.3 Spearphishing Link

Spearphishing links are one of the most common observed techniques by BEC threat actors. Often the link is disguised as a button or phrase such as "Click to View Document' which redirects a user to a phishing page. Hovering over the button or hyperlink typically allows collection of the URL, which can be further analysed. Other phishing links observed in BEC cases can be used to download malware. Additional details that can be obtained from phishing include the C2 of the malware or domain hosting the phishing page. Passive DNS records can be used to observe resolution dates and assess how long the campaign has occurred. Pivoting on IP addresses hosting phishing pages could produce related infrastructure used in the campaign.

9.1.4 Trusted Relationship

Exploitation of a trusted relationship is another common method for initial access. Often threat actors compromise an organisation, review emails to understand who the organization's clients are and attempt to find out when upcoming payments are due. The threat actor uses the compromised yet legitimate email account to contact real clients and request fake payments. Since everything appears to be coming from a trusted party, the email is not flagged as suspicious, perhaps other than requested changes to bank details. Email content searches are likely the best approach to detect the malicious email. Any reference to 'new' or 'switching' bank accounts could be a sign of a BEC attack. See section 9.2 for more tips to use in an investigation.

9.1.5 Valid Account

Valid accounts are also often abused by BEC threat actors. Techniques used to access valid accounts include password spraying, brute force and credential stuffing. Password spraying is typically defined as an attack using a large dictionary of passwords against an account of interest. Similarly, credential stuffing is the attempt to use credentials exposed online from previous compromises. The success rate of these types of attacks are usually determined by a weak or absent password policy.

9.1.6 Abusing OAuth

As previously mentioned, Microsoft OAuth API is abused by BEC threat actors.[2] OAuth is an open authentication and permission standard that is often used by services to allow third party access of a user's account. BEC threat actors use this legitimate tool for malicious purposes by sending links via email that display permission requests for OAuth apps. The URLs in the links are legitimate, along with the displayed requests asking the user to allow the app to be used. Once the user accepts this request the threat actor gains access to the user's account.

[1] 'SilverTerrier: 2018 Nigerian Business Email Compromise Update', PaloAlto Networks, https://unit42.paloaltonetworks.com/silverterrier-2018-nigerian-business-email-compromise/ (9 May 2019)

[2] 'Phishing Attack Hijacks Office 365 Accounts Using OAuth Apps', BleepingComputer, https://www.bleepingcomputer.com/news/security/phishing-attack-hijacks-office-365-accounts-using-oauth-apps/ (10 December 2019)

9.2 Hunting BEC Phishing Emails

This section covers common characteristics used to find BEC phishing emails. As previously mentioned, phishing emails are not exclusive to gaining initial access and are often used to establish persistence or move laterally. It is important to note that what works today may become obsolete tomorrow. Threat intelligence has a shelf life, which dictates analysts need to constantly collect, process and analyse a threat actor's TTPs.

9.2.1 Subject Lines

Phishing emails observed in BEC attacks often contain generic subject lines that create a sense of urgency.[3] In an attempt to compile some of the more popular and commonly observed subject lines we created a list of words and phrases used by BEC threat actors. This list is non exhaustive and different permutations of the following words and phrases are likely necessary to identify potential BEC related phishing emails:

Request	Reconfirm Password
Overdue	Account Alert
Confirmation	Account Reset
Payments	Reminder
Confidential	You Recieved
[First Name]	Voice Messages
Hello	Voicemail from [Phone Number]
Immediate Response	Voic(e)Message
Urgent	VM from [Phone Number]
Action Required	Audio Message
Account Suspended	Voice Recording Available
Password Confirmation	Password Reset
Received Fax Document	Sign-in attempt
Bill	Invoice

There are likely going to be false positives returned in the queries, since the above terms are common words often found in non-malicious emails. Consider these queries as starting points to identify possible phishing emails, which should incorporate additional searches and analysis of a suspected email's language, theme and content.

[3] 'Quick, Urgent, Request: Agari Research Reveals Top Ten Subject Lines Used for BEC', Agari, https://www.agari.com/email-security-blog/subject-lines-used-bec/ (13 May 2019)

9.2.2 Language(s)

Subject lines mentioned above could appear in a non-English language. Translations or similar expressions commonly used in different languages and cultures should be included in a query if applicable. The notion of poor grammar or misspelled words in emails can be used in assessing the likelihood of a BEC phishing email. However, this is becoming less common, especially with some BEC threat actors showing native fluency and grammar in multiple languages.[4] BEC threat actors operate in networks across countries, making it likely that communicating with targets in the local language is not uncommon, however the majority use English.

9.2.3 Themes

Companies

BEC phishing emails often spoof famous companies that are well-known for service offerings related to daily businesses activities. Search queries using some of the popular names below can be combined with subject lines mentioned above. This list is non exhaustive and different permutations of the following brands or service are likely necessary to identify BEC phishing emails:[5]

- Microsoft
- OneDrive
- OneNote
- SharePoint
- Outlook
- DropBox
- DocuSign
- Apple
- PayPal
- Amazon
- DHL

Password and account resets, confirmations and expirations

A common theme in BEC phishing emails is using urgent requests related to a victim's account or password. These types of emails often build up urgency and fear by stating that a user's account is due to expire and needs to be logged into to avoid deactivation; or warning a user to reset their password because there has been suspicious activity detected. These emails often use popular brands for both business and recreational purposes, as seen in the list above.

File hosting and sharing

Another popular focus of BEC phishing emails is the use of file hosting and sharing platforms.[6] Often emails are crafted around services that businesses use to share content, including invoices and confidential information. The spoofing of popular companies that businesses use makes the emails appear legitimate. Furthermore, the emails typically report the contents as 'confidential' or 'redacted' which requires logging in to a phishing page to view the contents.

Voice message

In addition to masquerading as well-known brands or services, BEC phishing emails have begun to use fake voice messages as a lure.[7] The email is rather simplistic, stating only that a voice message is waiting to be received with an attached link. The phone numbers used by the threat actors are usually voice over IP (VoIP) and can include a variety of country codes in the prefix.

[4] 'Cosmic Lynx: A Russian Threat Hits the BEC Scene', Agari, https://www.agari.com/email-security-blog/cosmic-lynx-russian-bec/ (7 July 2020)

[5] 'The Rise of New Tactics in Business Email Compromise', FireEye, https://www.fireeye.com/blog/products-and-services/2019/09/the-rise-of-new-tactics-in-business-email-compromise.html (12 September 2019)

[6] 'New BEC Spam Campaign Targets Fortune 500 Businesses', ThreatPost, https://threatpost.com/new-bec-spam-campaign-target-fortune-500-businesses/130012/ (21 February 2018)

[7] 'Office 365 Users Targeted by Voicemail Scam Pages', McAfee https://www.mcafee.com/blogs/other-blogs/mcafee-labs/office-365-users-targeted-by-voicemail-scam-pages/ (30 October 2019)

Geopolitical or seasonal related campaigns
Geopolitical trends and seasonal periods are often incorporated into BEC phishing emails. For example, at the start of the COVID-19 pandemic, analysts observed a large influx of BEC cases mentioning payment changes due to the pandemic and remote working. Many of these phishing emails explicitly mention 'COVID-19' or 'Coronavirus'. Seasonal events can also be a theme, such tailoring emails with tax themes during tax season.

9.2.4 Attachments

Attachments used by BEC threat actors can be both malicious in the form of malware or part of an actor's social engineering tactics. Throughout our investigations, non-malware attachments have provided countless clues to help with attribution, constructing timelines, and supporting the recovery of stolen funds. Often attachments masquerade as fake invoices, and those invoices include details such as names, phone numbers, dates and bank details. Names and company names can be checked using simple open source intelligence (OSINT) techniques, including country specific business registries.

Phone numbers are often VOIP numbers that don't provide much valuable intelligence. However, the country code or international prefix following the country code could be useful in indicating the country of origin of the threat actor. For example, if the phone number on a fake invoice starts with +234 or 009 it could indicate the threat actors are Nigeria-based. This is not definitive but rather a singular piece of intelligence that must be assessed amongst all evidence.

The post date on the invoice could help in constructing a timeline of the threat actor's actions. Furthermore, metadata is often valuable for spotting operational security (OPSEC) mistakes and compilation times of the document, which support both attribution and timelining.

Banking details are another important piece of information identifiable in attachments. Typically BEC threat actors use banks in countries with varying regulations, including China, Turkey and Mexico. More importantly, the bank account numbers can be passed along to those Banks or local affiliated branches to flag the account and possibly recover stolen funds.

9.2.5 Domains

BEC threat actors register domains similar to client or vendor names of the targeted organisation. These domains spoof organisation names by including typos, such as doubling letters or using a different top-level domain (TLD). Often threat actors use spoofed domains to send a well crafted email requesting payment with no additional phishing links, attachments or malware. Other cases show the threat actors use a combination of spoofed domains and phishing links, etc. which indicates these tactics are not mutually exclusive. A generic example of typo-squatting domains is seen with ITcornpany[.]com. The domain is spoofing an 'IT company' by replacing the letter 'm' with the letters 'r + n'.

It is challenging to search for a spoofed domain, like the one above, without actually knowing how it is misspelled. This is a disadvantage at the beginning of an investigation, especially when trying to identify the initial email sent by the threat actor. A better approach for finding the initial malicious email is discussed below, but there is still value in understanding domain spoofing.

Spoofed domains are sometimes used to set up email accounts mimicking the general contact email for a company. The threat actor often finds the company's website contact details and uses that as a template to spoof. Email addresses purporting company employees is also common. For example, both info@ITcornpany[.]com and alice@ITcornpany[.]com spoof emails typically found on a company website, and increase the legitimacy of the malicious domains. These two types of email addresses are often used for persistence. Usually, one is cc'd on email chains after initial access is complete. It is best practice to review all recipients of emails suspected of being either sent or replied to by the threat actor for spoofed domains.

In some cases, spoofed company names are used alongside free and well respected email services without actually registering a domain name, such ITcornpany@gmail[.]com. At least one study found overwhelmingly that the most common used email service by BEC threat actors is Gmail.[8] Gmail accounts are likely used because they are free, easy to set up and often bypass mail security products or spam folders.

9.2.6 Security themes

BEC threat actors have also been observed registering domain names with security themes. Many of the domains contain words such as, "ssl", "secure", "server", "portal" in an attempt to make the spoofed email look legitimate. Examples include:[9]

- mails-offices-exec-ssl-secure-server-portal-executive[.]management
- office-mailserver-secure-portal-8d601780ced1c6719fe6[.]network
- office-secured-adminteam-clevel[.]com
- mx-secure-email-server[.]cc
- relay-secure-smtp[.]com
- secure-email-delivery[.]cc
- secure-email-gateway[.]cc

9.2.7 Header spoofing

Header Spoofing or Display Name Deception leverages a default function within some email service providers which displays a sender's name only, without the domain name being visible. For example; emails from john.smith@company[.]com and john.smith@company[.]co[.]za will both appear as From: John Smith as sender.[10] Around 19% of BEC emails have a different "Reply-To" address compared to the "From" address. Another 12%, use the target organization's domain as the "From" domain.[11]

9.3 Commodity Malware used by BEC threat actors

In the last decade there has been an increase in the use of commodity malware by threat actors specializing in BEC.[12] The malware used is typically commodity malware "that is widely available for purchase, or free download, which is not customised and is used by a wide range of different threat actors."[13] BEC threat actors typically use Remote Access Trojans (RATs) and Keyloggers with the intention of stealing credentials or maintaining persistence on a host.

RATs are pieces of malware which provide an external third party (external) access to a host machine. RATS are disguised as non/malicious software, which when installed, will allow a threat actor to access, manipulate and control the host. RATs allow a threat actor to take screenshots, log keystrokes, access files and documents and download other malicious files. A keylogger or keystroke logger is a piece of software that records and logs all keystrokes on a user's machine. Keyloggers are used to steal credentials, usernames, passwords, account information and other sensitive data. The following malware list is non exhaustive but are associated with BEC incidents:[14] [15]

[8] 'Threat Spotlight: Malicious accounts in business email compromise', Barracuda, https://blog.barracuda.com/2020/08/06/threat-spotlight-malicious-accounts-business-email-compromise/ (6 August 2020)

[9] 'Domains Associated with Csomic Lynx BEC Campaigns' Agari, https://www.agari.com/cyber-intelligence-research/whitepapers/acid-agari-cosmic-lynx.pdf

[10] 'Business Email Compromise: 54% of Email Attacks Use Display Name Deception', Agari, https://www.agari.com/email-security-blog/business-email-compromise-54-of-email-attacks-use-display-name-deception/ (31 October 2018)

[11] 'Advanced Deception with BEC Fraud Attacks', Trustwave, https://www.trustwave.com/en-us/resources/blogs/spider-labs-blog/advanced-deception-with-bec-fraud-attacks/ (6 September 2018)

[12] 'SilverTerrier: 2019 Nigerian Business Email Compromise Update', PaloAlto Networks, https://unit42.paloaltonetworks.com/silverterrier-2019-update/ (31 March 2020)

[13] 'SilverTerrier: 2019 Nigerian Business Email Compromise Update', PaloAlto Networks, https://unit42.paloaltonetworks.com/silverterrier-2019-update/ (31 March 2020)

[14] Silver Terrier: The rise of Nigerian business email compromise, Palo Alto Networks, Unit 42, May 2018 https://www.trendmicro.com/vinfo/de/security/news/cybercrime-and-digital-threats/olympic-vision-business-email-compromise-in-us-middle-east-and-asia

[15] 'Piercing the HawkEye: Nigerian Cybercriminals Use a Simple Keylogger to Prey on SMBs Worldwide', Trend Micro, https://documents.trendmicro.com/assets/wp/wp-piercing-hawkeye.pdf (2015)

NetWire;	Agent Tesla;	Adwind;
PredatorPain;	Atmos;	AZORult;
Limitless;	DarkComet;	HWorm;
BilalStealer (ISR Stealer);	ImminentMonitor;	NJRat;
ISpySoftware;	LokiBot;	Quasar;
KeyBase;	LuminosityLink;	Revenge;
Olympic Vision;	NanoCore;	WarZone RAT;
Pony;	Remcos;	WSHRat.

Threat actors might not change or hide the malicious .exe file extension, but simply give the file a name that would act as a lure or attempt to make the executable appear as another file type. For example, Purchase Order.rar or Purchase Order.rar.pdf.

9.4 Victimology

Target selection is opportunistic and typically determined by availability of personal or company details. The individuals targeted include the Chief Executive Officer (CEO), Chief Financial Officer (CFO), other executive or management, and accounts payable. Accounts payable can be considered any individuals within an organization that have the authority to modify payment details, request or approve payments. These targets are selected for their perceived rank and authority. For example, a direct request from the CEO to transfer a large amount of money to close a highly confidential deal is unlikely to be questioned by staff.

Organizations with large numbers of employees, high revenues, and those that conduct routine, large scale transactions are preferred by threat actors. However, these organizational characteristics are not prerequisites, and small-medium enterprises are just as likely to be targeted. Overall, BEC operations are executed indiscriminately against organizations, irrelevant of sector, industry or size.

9.5 Attribution

One of the most pressing questions received from a victim is; who did this? Such a question is difficult to answer and requires an assessment based on the available evidence. An assessment should always include estimative language to describe what is known, while addressing what is not precisely understood. Words of estimative probability are used to describe the assessment and can often include confidence levels of High, Moderate, and Low. Our words of estimative probability follow the UK Government's probability yardstick with five levels:

Qualitative term	Confidence level
Remote or highly unlikely	< 10%
Improbable or unlikely	10 – 25%
Realistic probability	26 – 50%

Probable or likely	51 – 75%
Highly probable or highly likely	76 – 90%
Almost certain	> 90%

It is important to note that attribution does not have to be assessed to a single entity. We discuss common BEC threat actors below, but preface that attributing a BEC intrusion is difficult. Often a generalised attribution assessment is enough to answer the 'whodunit' question. A generalized assessment could be the threat actor is highly likely financially motivated and opportunistic, which aligns with commonly observed BEC threat actors. Add to this assessment that the FBI reports total losses due to BEC is approximately USD 1.7 billion, and the 'whodunit' question is addressed based on what is known and not precisely understood.

9.5.1 BEC Threat actors

BEC focused threat actors are located in over 50 countries and 50% of all global BEC threat actors are Nigeria-based.[16] Investigations show that individuals suspected of engaging in BEC activities have been arrested in the US, France, Italy, Japan, Kenya, Malaysia, and the United Kingdom.[17] Geography is a singular element for tracking threat actors that should be considered in conjunction with a threat actor's capabilities, infrastructure and victims.

Telemetry or visibility of a threat actor's capabilities, infrastructure and victims often defines the ability and extent to which an organisation can track a BEC threat actor. This notion could cause organisations to track similar threat actors under different names or even track two separate threat actors as one single threat actor. For example, PwC tracks several Nigeria-based BEC threat actors as Bronze Dev 1 and Bronze Dev 2 according to our visibility and analysis of each set's use of malware, sector specific targeting, and infrastructure. Regardless of geography or visibility, BEC threat actors typically operate in loose networks, are financially motivated, and rely heavily on social engineering tactics. The threat actors listed below are publicly reported BEC threat actors:

- Gold Galleon[18]
- Gold Skyline[19]
- Silver Terrier[20]
- Silver Spaniel[21]
- London Blue[22]
- Scattered Canary[23]
- Scarlet Widow[24]
- Silent Starling[25]
- Exaggerated Lion[26]
- Curious Orca[27]

[16] The Geography of BEC: The Global Reach of the World's Top Cyber Threat, Agari, https://www.agari.com/cyber-intelligence-research/whitepapers/acid-agari-geography-of-bec.pdf (2020)

[17] '281 Arrested Worldwide in Coordinated International Enforcement Operation Targeting Hundreds of Individuals in Business Email Compromise Schemes', US Department of Justice, https://www.justice.gov/opa/pr/281-arrested-worldwide-coordinated-international-enforcement-operation-targeting-hundreds (10 September 2019)

[18] 'GOLD GALLEON: How a Nigerian Cyber Crew Plunders the Shipping Industry', Dell Secureworks, https://www.secureworks.com/research/gold-galleon-how-a-nigerian-cyber-crew-plunders-the-shipping-industry (18 April 2018)

[19] 'Wire Wire: A West African Cyber Threat', Dell Secureworks, https://www.secureworks.com/research/wire-wire-a-west-african-cyber-threat (4 August 2016)

[20] 'SilverTerrier: 2019 Nigerian Business Email Compromise Update', PaloAlto Networks, https://unit42.paloaltonetworks.com/silverterrier-2019-update/ (31 March 2020)

[21] '419 Evolution', PaloAlto Networks, https://www.paloaltonetworks.com/resources/research/419evolution (22 July 2014)

[22] 'London Blue', Agari, https://www.agari.com/cyber-intelligence-research/whitepapers/london-blue-report.pdf (2018)

[23] 'Scattered Canary', Agari, https://www.agari.com/cyber-intelligence-research/whitepapers/scattered-canary.pdf (2019)

[24] 'Scarlet Widow', Agari, https://www.agari.com/cyber-intelligence-research/whitepapers/scarlet-widow-bec-scams.pdf (2019)

[25] 'Silent Starling', Agari, agari.com/cyber-intelligence-research/whitepapers/silent-starling.pdf (2019)

[26] 'Exaggerated Lion, Agari, https://www.agari.com/cyber-intelligence-research/whitepapers/acid-agari-exaggerated-lion.pdf (2020)

[27] 'The "I's" Have It: How BEC Scammers Validate New Targets with Blank Emails', Agari, https://www.agari.com/email-security-blog/how-bec-scammers-validate-new-targets-blank-emails/ (13 August 2019)

- Ancient Tortoise[28]
- Anuanuanuoluwa group[29]
- Cosmic Lynx[30]

All of the mentioned threat actors rely on social engineering to some extent. Both Silver Terrier and Cosmic Lynx are observed using commodity malware alongside social engineering tactics to maintain persistence. The Anuanuanuoluwa group is a cluster of individuals operating in Nigeria and South Africa that rely on phishing to steal credentials of target organizations.[31] Business email compromise is highly attractive for financial motivated threat actors, since it requires relatively low investment and while promising high financial returns. As such, the nature of BEC focused threat actors is highly diverse.

9.5.2 Malicious Insider

One possible threat actor that should not be dismissed quickly at the investigation kickoff stage is the malicious insider. According to PwC's 2020 Global Economic and Crime Survey, 37% of fraud cases are committed by internal perpetrators, while 20% of cases are co-opted between internal and external perpetrators. Not all of the fraud described in the survey is related to BEC or general cybercrime, but it demonstrates that malicious insiders pose a valid and credible (fraud) risk. The steps taken up to this point in an investigation could be useful in assessing the involvement of a malicious insider, such as suspicious IP addresses, signs of brute force attacks, and observations of phishing emails.

9.6 Tactics and Techniques

More detailed information on each of the tactics and techniques used by a threat actor in this section, along with mitigations, correspond to the following MITRE tactics and techniques:

ID	Technique/Sub-Technique
T1566	Phishing
T1566.001	Phishing: Spearphishing Attachment
T1566.002	Phishing: Spearphishing Link
T1078.001	Valid Accounts: Default Accounts
T1078.002	Valid Accounts: Domain Accounts
T1078.003	Valid Accounts: Local Accounts
T1078.004	Valid Accounts: Cloud Accounts
T1199	Trusted Relationship
T1190	Exploit Public-Facing Application

[28] 'Ancient Tortoise: A Deeper Look at the Aging Report BEC Attack Chain', Agari, https://www.agari.com/email-security-blog/ancient-tortoise-bec-attack-chain/ (14 January 2020)

[29] 'PerSwaysion Campaign', Group IB, https://www.group-ib.com/blog/perswaysion (30 April 2020)

[30] 'Cosmic Lynx', Agari, https://www.agari.com/cyber-intelligence-research/whitepapers/acid-agari-cosmic-lynx.pdf (2020)

[31] 'PerSwaysion Campaign', Group IB, https://www.group-ib.com/blog/perswaysion (30 April 2020)

Step 10

Recommendations

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'. Recommendations are often specific to an organization and therefore, it is possible that some cannot be implemented due to internal policies, procedures or budget. The recommendations provided are technical but non-technical policies and procedures should not be overlooked, especially the four eyes principle.[1]

10.1 Enable Multi-Factor Authentication (MFA)

Accounts that are assigned administrative rights should implement MFA, as they are often targeted by threat actors. MFA reduces the risk of those accounts being compromised. Microsoft recommends requiring MFA for at least the following account types:[2]

- Billing administrator
- Conditional Access administrator
- Exchange administrator
- Global administrator
- Helpdesk (Password) administrator
- Password administrator
- Security administrator
- SharePoint administrator
- User administrator

10.2 Ensure mailbox audit logging enabled for all accounts

An administrator should enable the Unified Audit Log (UAL) in the Security and Compliance Center before queries can be run. The UAL is a critical piece of evidence in a BEC investigation because it is a centralized source for all Office 365 events.

[1] 'Four Eyes Principle, European Commision, https://ec.europa.eu/eurostat/cros/content/four-eyes-principle_en#:~:text=DEFINITION%3A,or%20the%20two%2Dperson%20rule. (8 March 2019)

[2] 'Conditional Access: Require MFA for administrators', Microsoft, https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-policy-admin-mfa (2020)

10.3 Enforce a strong password policy

The National Institute of Standards and Technology recommends the following password policy:

- A minimum of eight characters and maximum length of at least 64 characters;
- The ability to use all special characters but no special requirement to use them;
- Restrict sequential and repetitive characters (e.g. 12345 or aaaaaa);
- Restrict context specific passwords (e.g. the name of the site, etc.);
- Restrict commonly used passwords (e.g. p@ssw0rd, etc.) and dictionary words;
- Restrict passwords obtained from previous breach corpuses.[3]

10.4 Forward Office 365 logging to a centralized location

Centralizing logs increases the reliability and retention period. It is critical to integrate and correlate Office 365 logs with other log management and monitoring solutions. This will help ensure suspicious activity is detectable and make it possible to compare all data sets for further analysis.

10.5 Perform regular checks on (active) forwarding rules

It is recommended to perform regular checks on (active) forwarding rules configured in the environment. The acquisition of this information can be automated and reported on a structured interval for review.

10.6 Block mail forwarding to external domains

Blocking forwarding rules help prevent threat actors and internal users from forwarding emails to external mailboxes. This can prevent leakage of sensitive information, monitoring activities of a victim by a threat actor and further loss of intelligence.

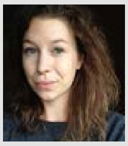
10.7 Disable legacy protocol authentication when appropriate

Legacy authentication refers to protocols that use basic authentication. Typically, these protocols can't enforce any type of second factor for MFA. These protocols include Post Office Protocol (POP3), Internet Message Access Protocol (IMAP), and Simple Mail Transport Protocol (SMTP). Single factor authentication (for example, username and password) no longer provides sufficient account protection. It is recommended to block all legacy protocols with a Conditional Access policy. However, should an organization require older email clients as a business necessity, these protocols will presumably not be disabled and only grant access to those protocols for the needed users.

10.8 Security awareness training

It is recommended to have recurring security awareness training that focuses on phishing attacks, including how to spot and avoid them. Phishing, and especially spearphishing are very difficult to stop, but training people to spot and avoid them decreases the likelihood of a successful attack.

About the Authors



Anna Laskai

Anna Laskai is a senior analyst at PwC Netherlands, who supports both Core Forensics and the Threat Intelligence teams. Her expertise lies in corporate and organized crime and she currently focuses on researching threat actors that specialise in BEC intrusions.

anna.laskai@pwc.com
https://www.linkedin.com/in/annalaskai/

Joey Rentenaar

Joey Rentenaar is a senior incident responder at PwC Netherlands. His main focus is applying incident response to cloud and office environments. He has developed open-source tooling to respond and analyse BEC intrusions.

joey.rentenaar@pwc.com
www.linkedin.com/in/joey-rentenaar

Korstiaan Stam

Korstiaan Stam leads the incident response team at PwC Netherlands. He supports technical investigations into engagements ranging from BEC to Advanced Persistent Threats (APT). He has also developed open-source tooling that is being used worldwide to respond and analyse BEC intrusions.

korstiaan.stam@pwc.com
https://www.linkedin.com/in/korstiaanstam//

Curtis Hanson

Curtis Hanson is a senior threat intelligence analyst at PwC Netherlands. He works alongside the incident response team, and helps clients understand advanced cyber threats. His area of focus and expertise is within the Middle East and Africa regions.

curtis.hanson@pwc.com
www.linkedin.com/in/curtis-34a394b7

Appendix A
List of RecordTypes

ExchangeAdmin

ExchangeItem

ExchangeItemGroup

SharePoint

SyntheticProbe

SharePointFileOperation

OneDrive

AzureActiveDirectory

AzureActiveDirectoryAccountLogon

DataCenterSecurityCmdlet

ComplianceDLPSharePoint

Sway

ComplianceDLPExchange

SharePointSharingOperation

AzureActiveDirectoryStsLogon

SkypeForBusinessPSTNUsage

SkypeForBusinessUsersBlocked

SecurityComplianceCenterEOPCmdlet

ExchangeAggregatedOperation

PowerBIAudit

CRM

Yammer

SkypeForBusinessCmdlets

Discovery

MicrosoftTeams

ThreatIntelligence

MailSubmission

MicrosoftFlow

AeD

MicrosoftStream

ComplianceDLPSharePointClassification

ThreatFinder

Project

SharePointListOperation

SharePointCommentOperation

DataGovernance

Kaizala

SecurityComplianceAlerts

ThreatIntelligenceUrl

SecurityComplianceInsights

MIPLabel

WorkplaceAnalytics

PowerAppsApp

PowerAppsPlan

ThreatIntelligenceAtpContent

TeamsHealthcare

ExchangeItemAggregated

HygieneEvent

DataInsightsRestApiAudit

InformationBarrierPolicyApplication

SharePointListItemOperation

SharePointContentTypeOperation

SharePointFieldOperation

MicrosoftTeamsAdmin

HRSignal

MicrosoftTeamsDevice

MicrosoftTeamsAnalytics

InformationWorkerProtection

Campaign

DLPEndpoint

AirInvestigation

Quarantine

MicrosoftForms

LabelContentExplorer

ApplicationAudit

ComplianceSupervisionExchange

CustomerKeyServiceEncryption

OfficeNative

MipAutoLabelSharePointItem

MipAutoLabelSharePointPolicyLocation

MicrosoftTeamsShifts

MipAutoLabelExchangeItem

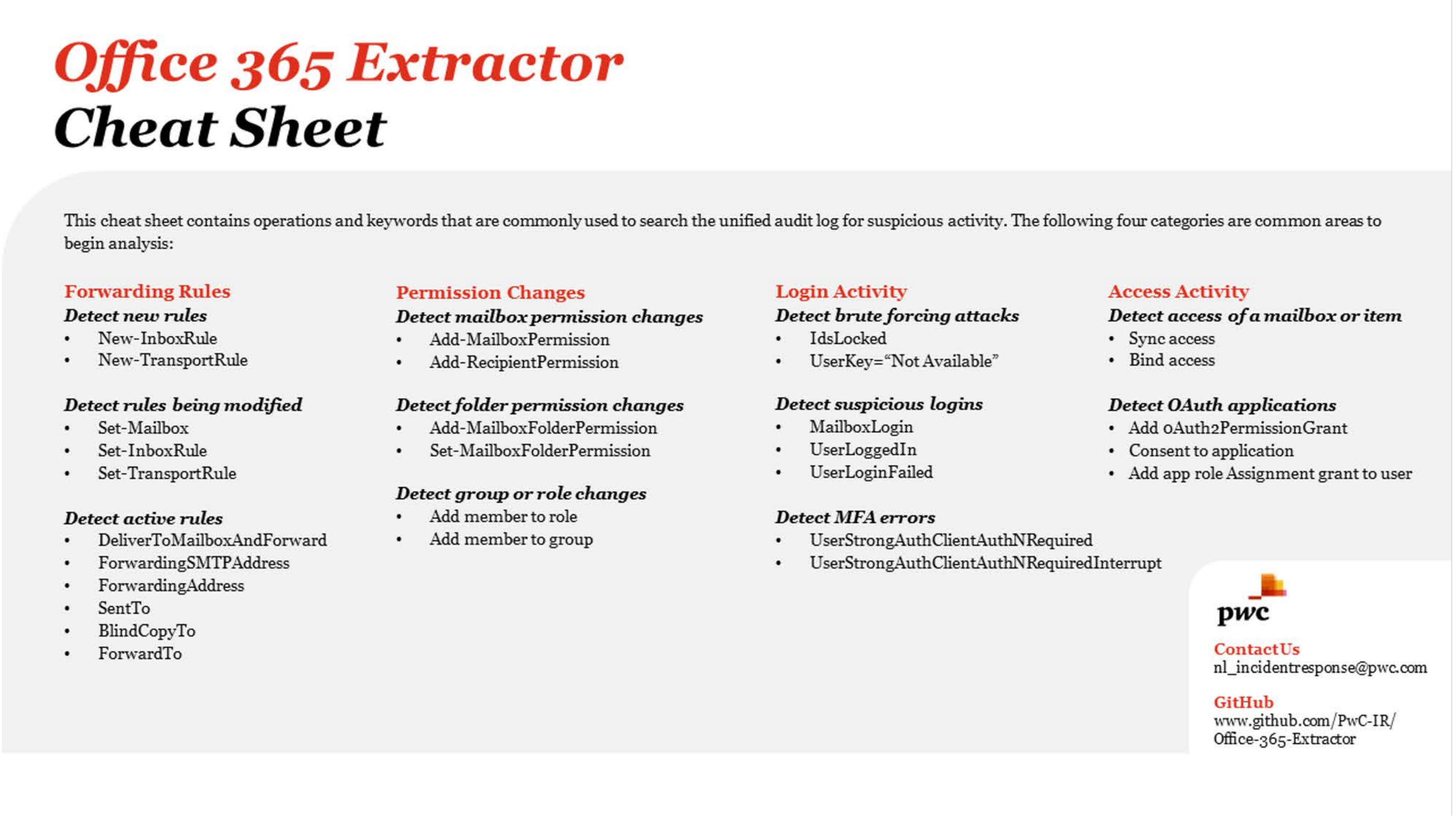
CortanaBriefing

Search

WDATPAlerts

MDATPAudit

Appendix B
Cheat Sheet



Office 365 Extractor
Cheat Sheet

This cheat sheet contains operations and keywords that are commonly used to search the unified audit log for suspicious activity. The following four categories are common areas to begin analysis:

Forwarding Rules

Detect new rules

- New-InboxRule
- New-TransportRule

Detect rules being modified

- Set-Mailbox
- Set-InboxRule
- Set-TransportRule

Detect active rules

- DeliverToMailboxAndForward
- ForwardingSMTPAddress
- ForwardingAddress
- SentTo
- BlindCopyTo
- ForwardTo

Permission Changes

Detect mailbox permission changes

- Add-MailboxPermission
- Add-RecipientPermission

Detect folder permission changes

- Add-MailboxFolderPermission
- Set-MailboxFolderPermission

Detect group or role changes

- Add member to role
- Add member to group

Login Activity

Detect brute forcing attacks

- IdsLocked
- UserKey=“Not Available”

Detect suspicious logins

- MailboxLogin
- UserLoggedIn
- UserLoginFailed

Detect MFA errors

- UserStrongAuthClientAuthNRequired
- UserStrongAuthClientAuthNRequiredInterrupt

Access Activity

Detect access of a mailbox or item

- Sync access
- Bind access

Detect OAuth applications

- Add oAuth2PermissionGrant
- Consent to application
- Add app role Assignment grant to user

pwc

Contact Us
nl_incidentresponse@pwc.com

GitHub
www.github.com/PwC-IR/
Office-365-Extractor

Thank you