PHISHING IR PLAYBOOK

A Special Incident Response Guide for Handling Office 365 Business Email Compromise

Version 1.0

Release date: March 2020

Frankie Li and Ken Ma
ir@dragonadvancetech.com

Overview

CEO Scam or ***Business Email Compromise (BEC)*** has been around for many years and we always have an impression that email spams are well controlled. However, phishing and BEC attacks require special attention as an increasing number of organizations move their email service to SaaS[1] services, such as Microsoft Office 365 or Google G Suite.

The BEC attackers make use of traditional social engineering techniques to trick highly educated executives (C-Suite level personnel) to authorize wire transfers to a foreign bank account controlled by the money mule. The increasing presence of Man-in-the-Email scams trend in Hong Kong has led the Anti-Deception Coordination Center (ADCC) of the Hong Kong Police Force to issue CEO Email Scam crime prevention tips[2] to the public and advise company management to impose guidelines on verifying identities before making fund transfers.

After publishing our cybersecurity alert on BEC in January 2019[3], we received more inquiries from our clients on how to deploy technological solutions to mitigate such attacks. In our previous white paper, we extended the research on this type of cybercrime threat and how Hong Kong is affected. We also reviewed several commercial solutions to defend against BEC threats. This IR playbook is created to address the IR issues on the fast-expanding usage of Office 365 SaaS application.

From the DATC previous research[4] mention that, the Institute of Criminal Justice Studies examines the complex money laundering methodologies adopted by BEC cybercriminals similar to those methods used to finance the 9/11 terrorist attacks and how law enforcement agencies and the private sector can work together to disrupt the organized criminal groups behind these cybercrimes. Similar to the Attack Kill Chain model, this paper also created a unique threat intelligence term for BEC, the ***Financial Fraud Kill Chain (FFKC).***

In March 2020, the FBI Cyber Division published a Private Industry Notification[5] (the Notification) to help cybersecurity professionals and system administrators guard against the ***persistent*** malicious actions of cybercriminals. They disclosed that cybercriminals conduct BEC through the exploitation of cloud-based email services of ***Microsoft Office 365*** and ***Google G Suite***, costing US business over 2 billion dollars.

The BEC scams are initiated through specifically developed ***phishing kits*** designed to mimic the cloud-based email services to collect credentials from victims.

---

[1] https://en.wikipedia.org/wiki/Software_as_a_service
[2] https://www.police.gov.hk/ppp_en/04_crime_matters/ccb/fst.php?msg_id=cct_30
[3] https://www.scmp.com/news/hong-kong/law-and-crime/article/2180879/more-us1953-million-defrauded-companies-hong-kong-and#comments
[4] https://dragonadvancetech.com/reports/Security-White-Paper-on-BEC.pdf
[5] https://www.bleepingcomputer.com/news/security/fbi-warns-of-bec-attacks-abusing-microsoft-office-365-google-g-suite/

Following similar findings in FFKC, the Notification also described the ***Tactics, Techniques, and Procedures (TTP)*** of BEC cyber-criminals (Fig. 1).

First, they deploy phishing kits to the organization with **large batches of emails**. Upon compromising victim email accounts, they review the address books of compromised accounts for the ***pivot to multiple victims*** and analyze the content to ***search for evidence*** of financial transactions. Then, they create ***mailbox forward rules*** to an outside email account and delete key messages from compromised accounts.

After ***collecting sufficient understanding*** of the targeted organization's corporate structure and persons involved in handling financial transactions, cyber-criminal ***creates lookalike domains*** of the targeted accounts, ***modify the "From" and "Reply-To" fields*** of the email message threads, and ***send impersonate email*** communications to the person to request pending or future payments.

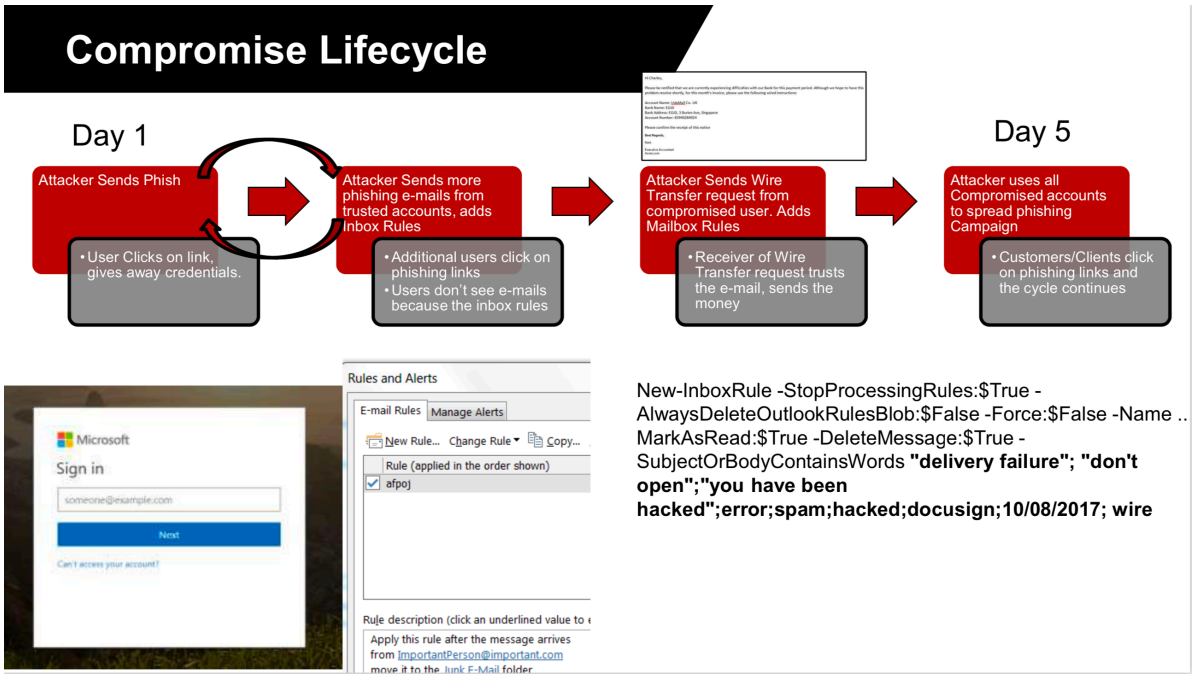
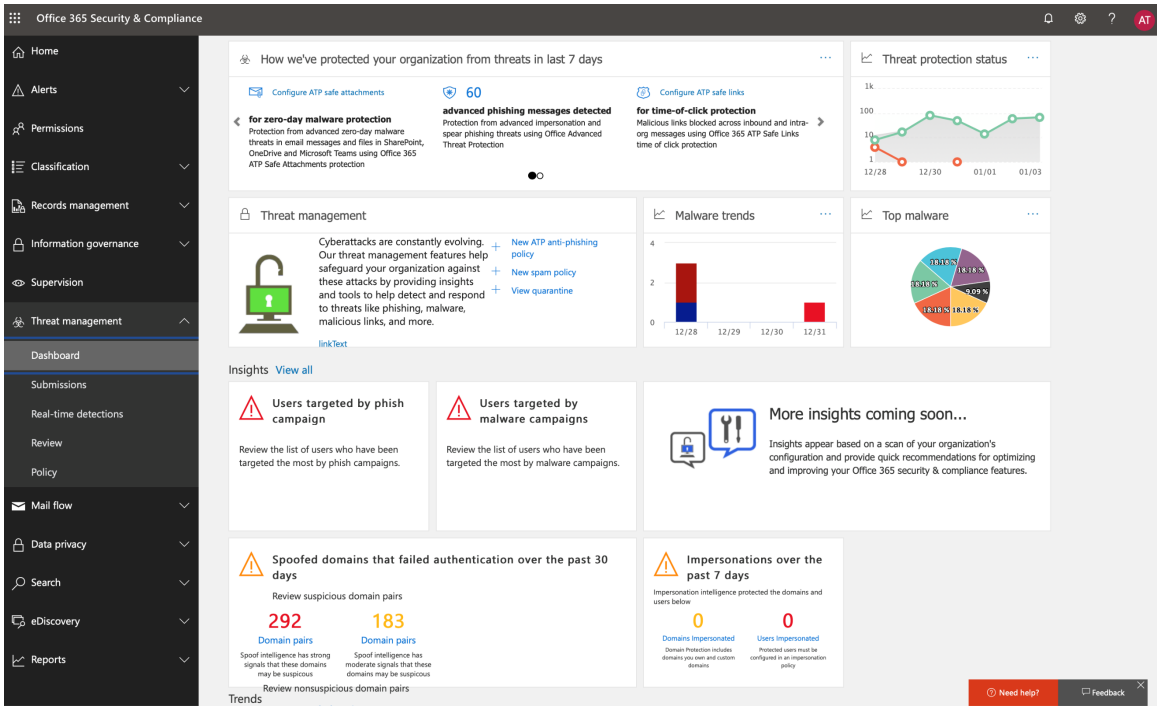


Fig. 1 – Tactics, Techniques, and Procedures (TTP) of the BEC cyber-criminals

In the few cases that we handled in the past months, we confirmed that the same ***TTP*** was applied to attack targeted victim business organizations especially if they have not assigned designated security personnel to tune, configure, and monitor the Office 365 Security and Compliance settings (Fig. 2).

Based on the recommendations described in the Notification and our experience on how to handle these kinds of incidents, we prepare this Phishing IR Playbook to help end-users or

system/security administrators to take the necessary migrations actions when phishing emails or suspicious BEC attacks activities are found.



(Fig. 2 – Office 365 Security and Compliance Portal as of the date of this Report)

Incident Lifecycle

The incident response cyber is composed of many steps, including intrusion detection and intrusion response. The incident lifecycle (Fig. 3) can be classified into several phases by referring to the model of the NIST SP800-61 Computer Security Incident Handling Guide. The initial phase involves the identification of the security program's hygiene issues, which includes a comprehensive analysis of the environment focused on finding evidence of ongoing or past compromises, assessment of systemic risks and exposures, establishing and training an incident response team, and acquiring necessary tools and resources. During preparation, the organization should attempt to limit the number of incidents based on the results of their risk assessments.

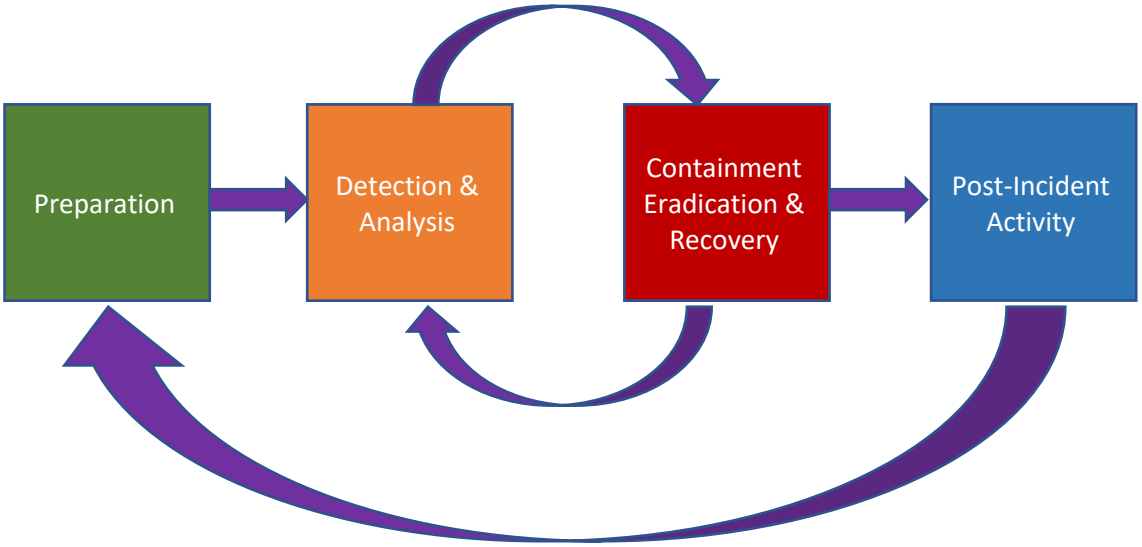


Fig. 3 – Incident Response Life Cycle

IR phase B and C may need to be performed iteratively and recursively.
Time window for the incident handling ***BEC is usually limited to 24–48 hours***

The detection of security breaches is heavily dependent on the protection solutions deployed, whether logging is enabled and whether Office 365 is tuned, configured, and monitored properly. Baseline threat protection policies need to be established to detect anomalies, and alerts need to be monitored continuously and the organization's senior management should be notified before an incident occurs. During the identification and analysis phase of an incident, the incident response team will analyze the log data of Office 365 user and tenant configurations or even the mailbox of a compromised email account to attempt to identify the root cause and pinpoint any additional compromised mailboxes. After analyzing the event and confirming the category and severity of the attack, the organization should perform the necessary actions to limit the effects of the incident by containing the threats and ultimately begin recovering from the attack.

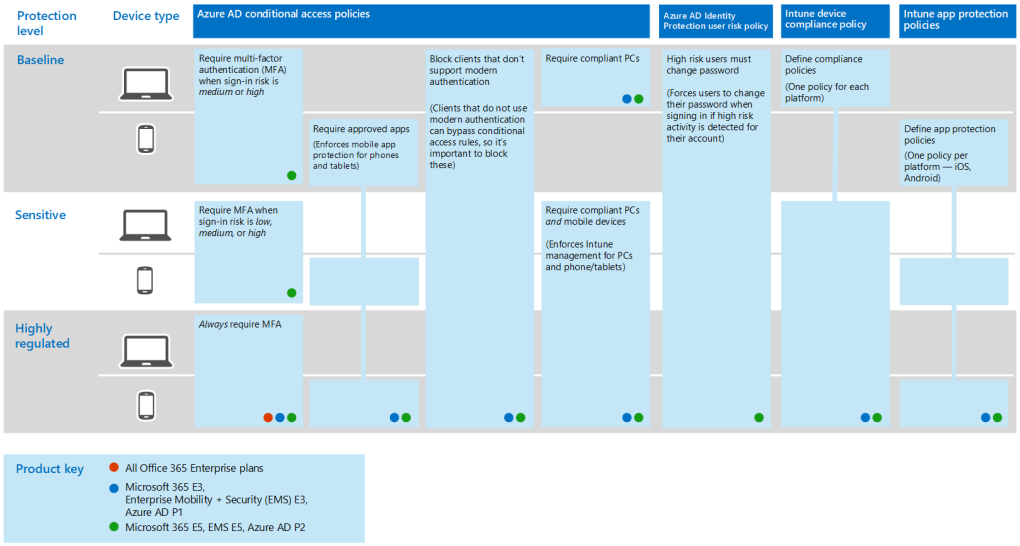
After the incident is handled adequately, the organization should prepare a report that details the attackers' activities, a summary of the incident, procedures for remediation, and the steps that the organization should take to prevent a future incident.

Preparation

This phase refers to the initial phase where organizations will perform preparatory measures to ensure they can respond effectively to the incidents if and when they are discovered. It involves all planning works such as develop policies and procedures, set up cyber incident response team (CIRT), set up incident reporting mechanism, implement monitoring system, understand the Office 365 security roadmap and other protection subscriptions, such as Microsoft identity and access management, Office 365 security management, and threat protection can be implemented by the tenant.

The first responder who performs the triage of Office 365 security incidents should aware of Microsoft's ***Assume Breach*** mindset and zero-trust network strategy. The IR responder should be provided with the organization's incident response (IR) plan. The IR plan and triage should contain the following documents:

- Contact information of the in-house IR team.
- Communication plan.
- Escalation and notification procedures and reporting mechanism.
- Architecture and policy applied (Fig. 4) of the Office 365 tenant and the kind of subscriptions acquired (ATP-plan 1, ATP-plan 2, E1, E3, E5 or A5).
- Confirm which Microsoft threat protection services are implemented (Defender ATP, Office 365 ATP, Azure ATP, or Cloud App Security).
- Confirm that the Office 365 threat management policies are tuned/configured properly and ensure all logs are enabled in the Microsoft 365 security center.
- If the tenant is an Office 365 customer with mailboxes in the Exchange online or a standalone Exchange Online Protection customer without Exchange Online mailboxes, the email messages are protected automatically. If ATP anti-phishing (a set of machine learning models trained to detect phishing messages) subscription is acquired, check if the anti-phishing protection in Office 365 is tuned properly.



(Fig. 4 – Tier of Protection Policies of an Office 365 Tenant)

Detection, Identification & Analysis

The second phase is where organizations should strive to detect and validate Office 365 security incidents quickly. Thousands or even millions of phishing emails may come to an organization's mailboxes daily and if the Office 365 protection policies are tuned[6] or configured properly, the phishing or BEC email attacks can be identified easily.

Please do not assume that your anti-phishing solutions including Office 365 anti-phishing subscriptions can filter out every phishing email, especially when these solutions are not tuned or configured properly. Office 365 audit logs[7] should be the most reliable forensic artifact to allow the first responder to perform the triage.

Some secured email gateways place high emphasis on malware filtering or malicious URLs rewriting but overlook spoofed email validation and authentication detections by using SPF[8], DKIM[9] , and DMARC[10]. If a secured email gateway is placed in front of Office 365, valuable phishing emails threat intel (especially those metadata contained in the email headers) can sometimes be filtered out, making the Office 365 protection policies less useful.

Taking corrective actions, such as enabling Multi-Factors Authentication (MFA) on privileged email accounts, will minimize immediately the magnitude of the damage to the organization sustains as a result of the BEC incident. The Office 365 Secure Score will provide a tenant-wide highlight on how an organization can use the Office 365 Threat Protection in defense of phishing and BEC attacks.

Detection includes review of the past 30 to 90 days alerts and logs or event notifications received from the organization's users. Research[11] indicates that attacks are spread out over time. The attacks do not always happen as soon as the account is compromised. In one of our past investigations, the attacks were launched more than five months after the email account was compromised.

From the alerts and logs, try looking for anomalies on login/logoff suspicious activity, such as foreign success or failed logins. Review all setting changes of suspicious email accounts from Office 365 Security and Compliance Portal. All alerts (such as malware attachments, a spike of phishing emails received, a spike of email accounts on sending out phishing emails, email account credential compromise, the addition of rules to forward the email to an outside email address or any changes and another kind of attack) need to be identified or categorized then prioritized after triage.

---

[6] https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/tuning-anti-phishing
[7] https://docs.microsoft.com/en-us/microsoft-365/compliance/auditing-troubleshooting-scenarios
[8] https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/how-office-365-uses-spf-to-prevent-spoofing
[9] https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/use-dkim-to-validate-outbound-email
[10] https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/use-dmarc-to-validate-email
[11] https://blog.barracuda.com/2020/02/06/threat-spotlight-email-account-takeover/

The analysis includes the study of the indicators of compromise (IoCs) and the breadth and depth of the alerts need to be analyzed. Analysis of an incident, either successful or failed, can provide significant insights into possible threats to an organization.

- Detection and identification (i.e. signs of the incidents) – Phishing or BEC attacks[12] can be discovered from the following:
    - A spike of anti-spam or email filters alerts
    - A spike malware attachment alerts
    - A spike of an email account from the organization or lookalike domain of the organization sending out a high volume of phishing emails to internal members
    - A user from the financial department receives an email from a C-Suite level or high ranking person, ordering him/her to process an invoice quickly, change the recipient of a payment, or provide sensitive documents.
    - A spoof email from a high ranking person asking an employee to purchase gift cards for colleagues.
    - Sometimes instruction may be received from a legitimate email address from vendors or suppliers because their email was compromised (vendor email compromise).
    - The messages are brief, urgent, and press the user to bypass normal policies and procedures.
    - The title of the email usually comes with simple payment requests, such as Payment Notice, Process Payment, Quick Request, Fund Payment Reminder, Wire Transfer Request, Bank Transfer Enquiry or even using confidentiality or I am currently unavailable.
    - The sender seems to have good knowledge of the organization and refer to a sensitive situation such as mergers and acquisitions.
    - The sender states that he or she is traveling and the senders' email addresses indicate the email originated from lookalike or spoofed domain or a Gmail or Hotmail or Yahoo mail account rather than a legitimate organization account.
    - Sometimes the sender will provide instructions on how to proceed may be given later by a third party or via later emails from another domain.
    - Often the request is for payment to a limited company in Hong Kong to a local bank, but the company just incorporated less than six months prior to sending the email.

- Email risk assessment, Incident categorization, and triage:
    - Email spam or contains unwanted content:
        - creates annoyance,
        - check junk mails and collect statistics of similar emails from the organizations' spam filters,
        - check logs and statistics of Office 365 email anti-spam protection, and[13]
        - check ATP safe attachments[14] policies.

[12] https://bit.ly/2WkUQUh
[13] https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/anti-spam-protection
[14] https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/atp-safe-attachments

- Phishing emails may contain known or suspected attachment-based threats:
  - deploys malware,
  - known malware can be filtered by anti-virus email plugin or filtered by the secure email gateway,
  - check logs and statistics of anti-malware protection[15] in Office 365,
  - check ATP safe attachments[16] policies, and
  - check quarantine[17] email messages.
- Phishing emails may contain suspected URL-based threats:
  - deploy malware or trick users to "click" for harvest users' credential,
  - spam filters and secure email gateway,
  - check ATP safe link[18] policies, and
  - check quarantine[19] email messages.
- Known or suspected email impersonation-based threats: to establish trust and entice the recipient to take additional actions:
  - attackers start using the kill chain model to launch attacks to selected targets. They are persistent and study the target organizations by paying close attention to details or even create a lookalike domain before sending out the messages,
  - check spoofing emails with SPF[20], DKIM, and DMARC, and
  - check ATP logs and campaign views[21] and threat analytics.[22]
- Target phishing email: BEC, Financial Fraud Kill Chain (FFKC) or espionage
  - attackers first compromise some email accounts of an organization using technique described in the "Detection and Identification" section and
  - check ATP logs and campaign views[23] and threat analytics.[24]

- How to identify whether your Office 365 account has been compromised:[25]
  - large amounts of spam that originates from your account,
  - Sent or Deleted Items folders contain common hacked-account messages,
  - Unusual profile changes,
  - Unusual credential changes,
  - Mail forwarding was added recently, and
  - An unusual signature was added recently.
  - Solution:
    - Ensure that your computer is not compromised,
    - Enable MFA, and

---

[15] https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/anti-malware-protection
[16] https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/atp-safe-attachments
[17] https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/quarantine-email-messages
[18] https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/atp-safe-links
[19] https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/quarantine-email-messages
[20] https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/how-office-365-uses-spf-to-prevent-spoofing
[21] https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/campaigns
[22] https://docs.microsoft.com/en-us/microsoft-365/security/mtp/latest-attack-campaigns
[23] https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/campaigns
[24] https://docs.microsoft.com/en-us/microsoft-365/security/mtp/latest-attack-campaigns
[25] https://docs.microsoft.com/en-gb/office365/troubleshoot/sign-In/determine-account-is-compromised

        - Remove forwarding rules.

- Incident analysis – Check for the artifacts or IOCs
    - Search and Investigation and select Audit log search.
    - Find the IP address of the computer used to access a compromised account.
    - Determine who set up email forwarding for a mailbox.
    - Determine if a user deleted email items in their mailbox.
    - Determine if a user created an inbox rule.
    - Investigate why there was a successful login by a user outside your organization.
    - Investigate the timeline of foreign success (based on the IP addresses) and fail logins of a suspicious compromised email account.
    - Check tenant's Azure sign-in logs.
    - Export audit logs (with HAWK[26] or other Powershell tools[27]) and place it in a data analytic platform, such as ElasticSearch or Splunk.
    - …

- Incident reporting – Escalation notification and reporting of the incident to appropriate parties *(smart recipe: do not hide)*
    - Designate a person to tune, configure, and monitor all kinds of email attacks by using functions provided by Office 365 subscriptions.
    - Implement extract relevant Office 365 threat and incident reports.
    - The report should contain answers on user-level and tenant-level, such as
        - What did the attacker access?
        - How long did the attacker have access?
        - Is there potential PII exposure?
        - Are there any compromised email accounts?
        - Any advanced malware deployed?
        - Consider the possibility that more than one group of attackers compromised the network
        - Is the tenant clean?
        - What is the motive of the attacker?

[26] https://www.powershellgallery.com/packages/HAWK/1.0.0
[27] https://github.com/PwC-IR/Office-365-Extractor-1

Containment, Eradication, and Recovery

The third phase, containment, which refers to the initial steps to mitigate the actions of the attacker, has two major components: stopping the spread of the attack and preventing further damage to systems. An organization needs to decide which methods of containment to employ early in the response. Organizations should have strategies and procedures in place to make containment-related decisions that reflect the level of acceptable risks.

Containment includes the following procedures to stop the attackers from logging in using stolen credentials. The MFA should be enabled for all privileged email accounts or even all user email accounts.

Containment can be performed concurrently with incident analysis as described in the above. Blocking emails from sending from a lookalike domain or blocking a foreign IP address to login for Azure AD may not be sufficient because attackers can use popular email services to send spoof emails and use many IP addresses to connect to the Office 365 Exchange server. The following procedures should be considered to fix[28] a compromised Office 365 account.

- Apply the PowerShell script RemediateBreachedAccount.ps1.[29]
- Reset the password (this step secures the account and kills active sessions).
- Remove mailbox delegates.
- Disable mail forwarding rules to external domains.
- Remove global mail forwarding property on the mailbox.
- Enable MFA on the user's account.
- Set password complexity on the account to be high.
- Enable mailbox auditing.
- Produce Audit Log for the admin to review.

Incident responders need to make quick and reliable recommendations to the responsible senior management to determine the details of the containment and recovery procedures.

Eradication consists of the longer-term mitigation efforts that include steps to tune, configure and monitor the threat protection policies at the Office 365 tenant. Once the attacker selects the organization as their target, it will keep trying to launch phishing attacks and finding the weakest link to exploit humans to gain credential or “click” to download malware to allow them to compromise the system or gain financial benefit.

Recovery often requires drastic actions in BEC incident. Recovery includes steps to reset the password, enable MFA, remove foreign forward email rules, re-create email accounts, and approach law enforcement or the organizations’ originating bank to recover the remitted money. Incident responders need to consider enabling Office 365 logs or if the resource is

[28] https://docs.microsoft.com/en-us/archive/blogs/office365security/how-to-fix-a-compromised-hacked-microsoft-office-365-account
[29] https://github.com/OfficeDev/O365-InvestigationTooling/blob/master/RemediateBreachedAccount.ps1

available, purchase more ATP subscriptions for all unprotected Office 365 users. An individual should be designated to use Office 365 threat hunting tools to handle continuous monitoring of the Office 365 tenant.

Post-Incident Activity (lesson learned)

Handling a phishing email and BEC incident can be extremely expensive and thus, organizations need to conduct a robust assessment of lessons learned after the incident to prevent reoccurrence of similar incidents.

Post-incident refers to the process of identifying lessons to be learned after actions and review. Other than upscaling of the Office 356 security score, we need to implement the following Microsoft Office 365 security recommendations.

Protect privileged accounts:

- Enforce MFA for all administrative accounts (E3 | E5*).
- Implement Azure AD Privileged Identity Management (PIM) to apply just-in-time privileged access to Azure AD and Azure resources (E5).
- Implement PIM in Office 365 to manage granular access control over privileged access in Office 365 (E5).
- Implement Privileged Access Workstations to administer services. Do not use the same workstations for browsing the Internet and checking email not related to your administrative account (E3 | E5).
- Ensure accounts synchronized from on-premises are not assigned administrative roles for cloud services.
- Ensure service accounts are not assigned administrative roles.
- Remove licenses from administrative accounts.

  * E3[30] (Security): Microsoft Security & Compliance Center, Threat Management, DLP for Exchange Online, SharePoint Online and OneDrive for Business & Information Governance, eDiscovery, Unified Audit, Retention policies

  * E5 (Security): E3 + Microsoft Defender ATP, Azure ATP, Office 365 ATP Plan-2, Microsoft Cloud App Security, Azure AD Premium Plan-2, and AIP Plan-2

Reduce the surface of attack:

- Disable legacy protocols, such as POP3, IMAP, and SMTP.
- Reduce Global Admins in the tenant.
- Retire servers and applications no longer used in your environment.
- Implement a process for disabling and deleting inactive accounts.

Protect against known threats:

- Setup MFA (E3 | E5).
- Set up sign-in risk policies through Enterprise Mobility + Security products (E5).
- Raise malware protection for emails (E3 | E5).
- Implement ATP–anti-phishing attacks (E5).
- Block connections from countries that you do not do business (E5).

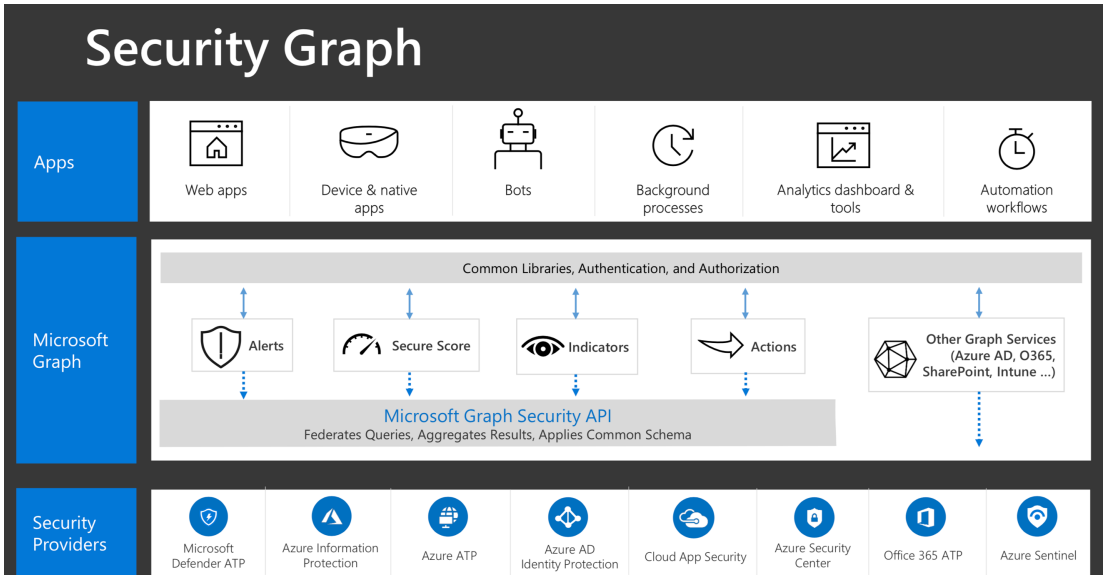
[30] https://docs.microsoft.com/en-us/office365/servicedescriptions/office-365-platform-service-description/office-365-securitycompliance-center

Protect against advance persistence threats:

- Implement conditional access for the zero-trust network. If Windows 10 is used, enable Windows Information Protection (E5).
- Disable external email forwarding (E3 | E5).
- Configure data loss prevention (DLP) policies in Office 365 Security for sensitive data (E3 | E5).
- Configure data classification protection policies in Office 365 for sensitive data.
- Use Azure Information Protection labels for protection (E5).
- Protect data in 3rd-party apps using Cloud App Security (E5).

Continuous monitoring and auditing (APIs from Microsoft Security Graph[31] - Fig. 5):

- Enable Office 365 audit log (E3 | E5).
- Review Secure Score weekly (E3 | E5).
- Use Office 365 ATP tools:
    - Threat investigation and response capabilities (E5).
    - Automated investigation and response (E5).
- Use Microsoft Defender ATP:
    - Endpoint detection and response (E5).
    - Automated investigation and remediation Secure score (E5).
- Advanced hunting (E5).
- Use Microsoft Cloud App Security to detect unusual behavior across cloud apps (E5).
- Use Microsoft Azure Sentinel or your current SIEM tool to monitor for threats across your environment (E5).
- Deploy Azure ATP to monitor and protect against threats targeted to your on-premises Active Directory environment (E5).
- Use the Azure Security Center to monitor for threats across hybrid and cloud workloads.



- Fig. 5 – Security Provider and Microsoft Security Graph

[31] https://www.microsoft.com/en-us/security/business/graph-security-api

Implement email threat policies and procedures:

- Email usage and email account management policies.
- Arrange anti-phishing exercise and user awareness training programs.
- Prepare phishing email and BEC attack statistics and alert reports.
- Designate a person to tune, configure, and monitor all available Office 365 threat protection policies.

Protect and secure your identity (Azure AD, identify the provider of many apps):

- Strengthen your credentials (MFA | Azure AD Security Defaults):
    - Start banning commonly attacked passwords and turn off traditional complexity and expiration rules (aka persistence mechanism).
    - Enable the dynamic banned password feature of Azure AD.
    - Protect against leaked credentials and add resilience against outages with enable password hash sync.
- Reduce your attack surface area:
    - Block legacy authentication.
    - Block invalid authentication entry points.
    - Restrict user consent operations.
    - Implement Azure AD Privileged Identity Management (PIM).
- Automate threat response:
    - Implement user risk security policy (a Conditional Access policy) using Azure AD Identity Protection.
    - Implement sign-in risk policy using Azure AD Identity Protection.
- Utilize cloud intelligence:
    - Monitor with Azure Logging and Auditing and check Audit activity reports.
    - Monitor Azure AD Connect Health in hybrid environments.
    - Monitor Azure AD Identity Protection events.
    - Audit apps and consented permissions.
- Enable end-user self-service:
    - Implement self-service password reset.
    - Implement self-service group and application access.
    - Implement Azure AD access reviews.

Other recommendations:

- Open Teams Federation only to Partners.
- Do not whitelist sender domains, individual senders, or source IPs.
- Enable outbound spam notifications.
- Disable Remote PowerShell for all users.
- Block access to the Microsoft Azure Management portal to all non-administrators.