O365 BUSINESS EMAIL COMPROMISE PLAYBOOK

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

Version 1.0

Released date:
June 2020

Written by:
Frankie Li
Ken Ma
Mika Devonshire

OVERVIEW

This Incident Response (IR) Playbook is created to address IR issues on the fast-expanding usage of O365 SaaS application.

CEO Scam or Business Email Compromise (BEC) has been around for many years and there has always been an impression that email spam is well-controlled. However, phishing and BEC attacks require special attention as an increasing number of organizations move their email service to software as a service (SaaS) platforms like Microsoft Office 365 (O365) or Google G Suite.[1]

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 trend of Man-in-the-Email scams 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 to the public and advise company managements to impose guidelines on verifying identities before making fund transfers. [2]

The Institute of Criminal Justice Studies examines the complex money laundering methodologies adopted by BEC cybercriminals similar to those methods used in financing the 9/11 terrorist attacks. Likewise, the Institute has also explored ways on how law enforcement agencies and the private sector can work together to disrupt organized criminal groups from conducting cybercrimes.[3] This paper employs the Attack Kill Chain model and Financial Fraud Kill Chain (FFKC), which are unique threat intelligence initiatives used to combat BEC.

In March 2020, the FBI Cyber Division published a Private Industry Notification (the Notification) to help cybersecurity professionals and system administrators guard against persistent malicious actions of cybercriminals.[4] The FBI disclosed that cybercriminals conduct BEC through the exploitation of cloud-based email services of O365 and G Suite, causing businesses to lose over 2 billion dollars.

BEC scams are initiated through phishing kits designed specifically to mimic cloud-based email services in order to collect credentials from victims. Based on similar findings in FFKC, the Notification described the Tactics, Techniques, and Procedures (TTP) used by BEC cybercriminals which are as follows *(See Figure 1 for an image representation).*

[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://dragonadvancetech.com/reports/Security-White-Paper-on-BEC.pdf
[4] https://www.bleepingcomputer.com/news/security/fbi-warns-of-bec-attacks-abusing-microsoft-office-365-google-g-suite/

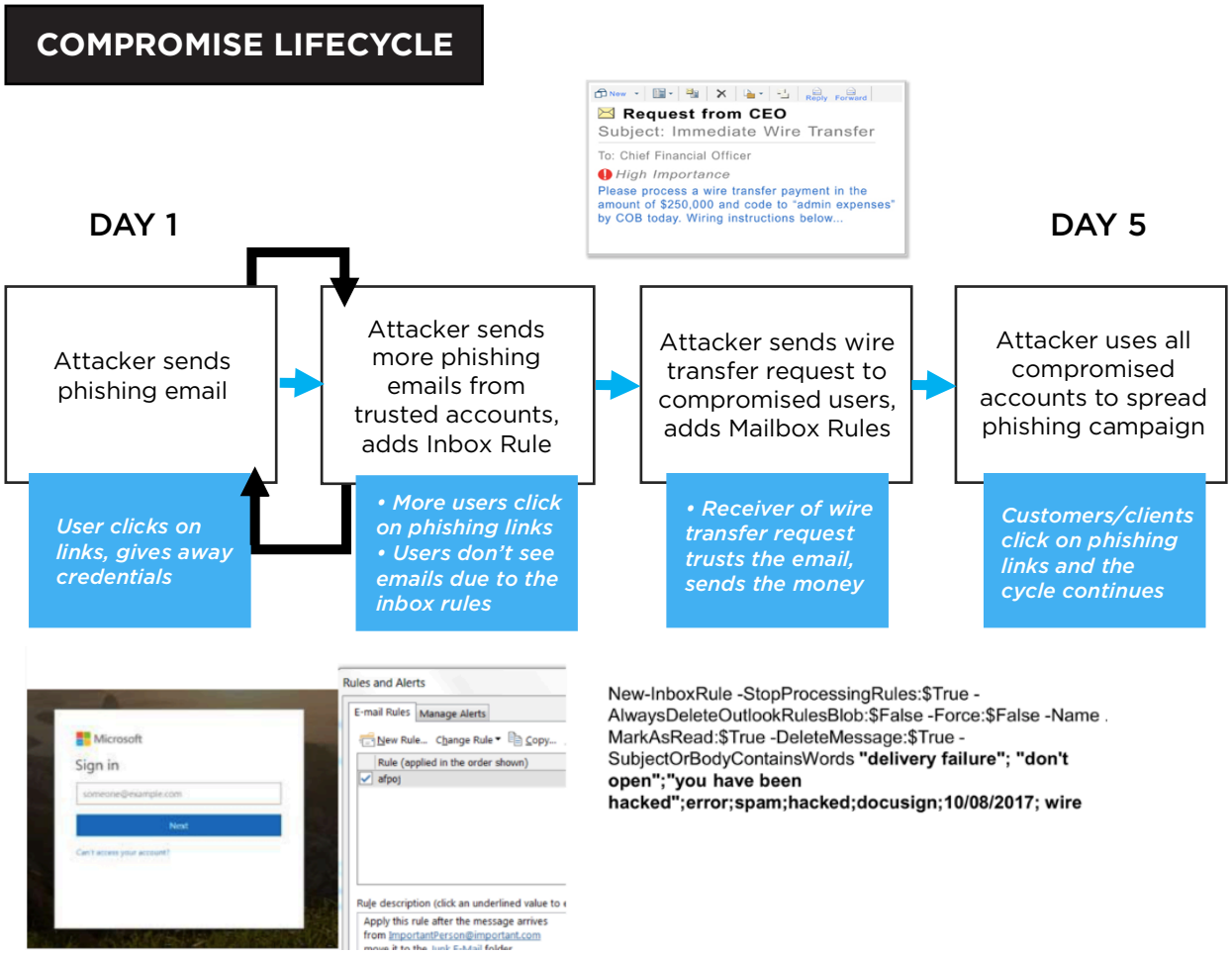


Figure 1. Tactics, Techniques, and Procedures (TTP) of the BEC cybercriminals.

First, cybercriminals deploy phishing kits to the target organization via large batches of emails. Upon compromising email accounts, cybercriminals will review the address books of the compromised accounts and search for more victims. Cybercriminals will also analyze the content of the compromised accounts to look for evidence of financial transactions. Then, they will 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 the persons involved in handling the company's financial transactions, cybercriminals would create lookalike domains of the targeted accounts, modify "From" and "Reply To" fields of the email message threads, and send impersonated email communications to targeted individuals requesting for pending or future payments.

Based on the cases Blackpanda has handled in the months prior to writing, we can confirm that the same TTP was applied to attack targeted business organizations–especially when they have not assigned designated security personnel to tune, configure, and monitor the O365 Security and Compliance settings *(See Figure 2).*

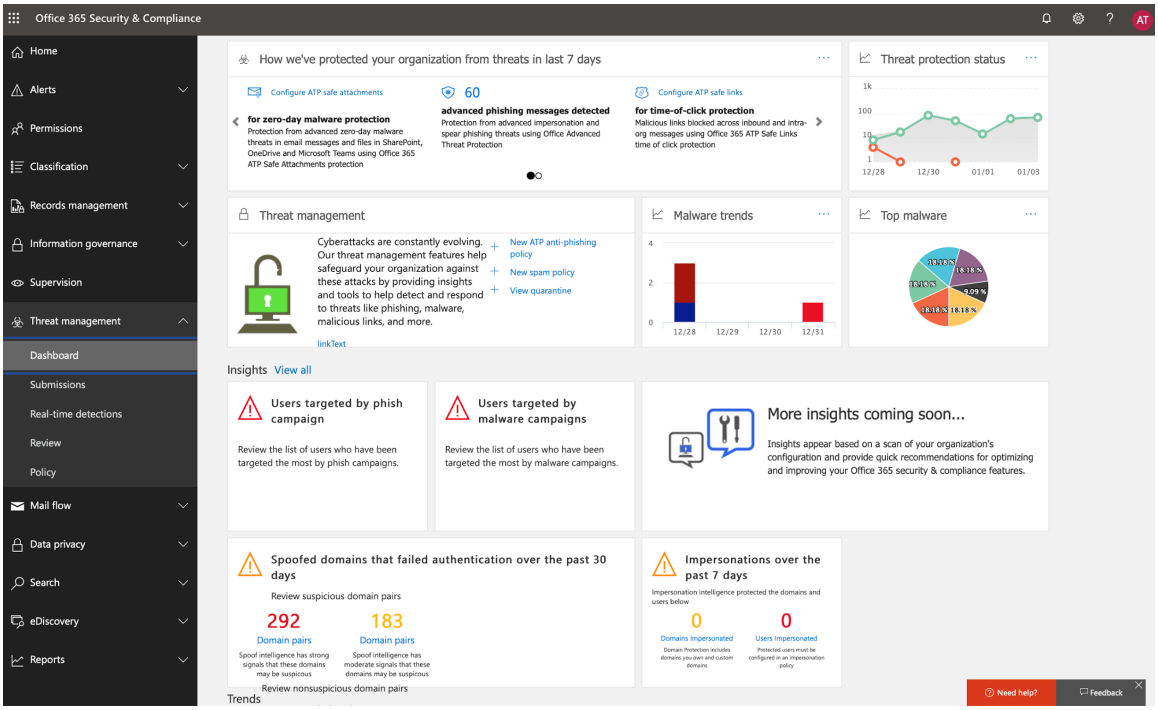


Figure 2. Office 365 Security and Compliance Portal as of May 2020

Blackpanda prepared this Phishing IR Playbook based on the recommendations described in the Notification and our experience on how to handle these kinds of incidents in order to help end-users or system and security administrators take the necessary mitigating actions when phishing emails or suspicious BEC activities are found.

INCIDENT LIFECYCLE

The incident response lifecycle is composed of many steps, including intrusion detection and intrusion response. The incident lifecycle (*See Figure 3*) can be classified into several phases, which are determined by the model designed by the National Institute of Standards and Technology (NIST) Computer Security Incident Handling Guide SP800-61. The initial phase, otherwise called as the Preparation phase, involves the identification of the security program's hygiene issues. Preparation also 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 (IR) team, and acquiring necessary tools and resources. During this phase, the organization should attempt to limit the number of incidents based on the results of their risk assessments.

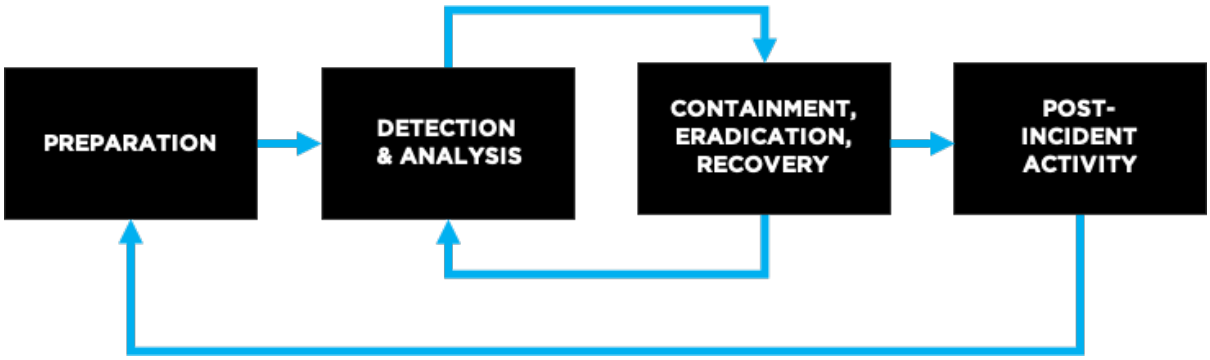


Figure 3. Incident Response Life Cycle.

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

Preparation is then followed by Detection. The detection of security breaches is heavily dependent on the deployed protection solutions, whether logging is enabled and O365 performance is tuned, configured, and monitored properly. Baseline threat protection policies need to be established to detect anomalies, and alerts must be monitored continuously. More importantly, the organization's senior management should be notified when an incident occurs.

The Analysis phase comes next, wherein the IR team analyzes the log data of O365 user and tenant configurations or even the mailbox of a compromised email account in an attempt to identify the root cause of the incident 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 impact of the incident by containing the threats and ultimately begin recovering all losses.

After the incident is managed appropriately, the organization should prepare a report that details all activities involved, a summary of the incident (including the actions of the attackers), procedures for remediation, and steps that the organization must take to prevent future incidents.

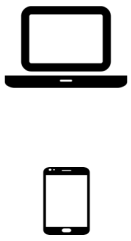
PREPARATION

Preparation refers to the initial phase where organizations perform preparatory measures, ensuring that they can respond effectively to incidents if and when they are discovered. Preparation involves all planning activities, such as developing policies and procedures, setting up a cyber incident response team (CIRT), establishing an incident reporting mechanism, implementing monitoring systems, understanding the O365 security roadmap and other protection subscriptions

(such as Microsoft Identity and Access Management and O365 Security Management), and enforcing threat protection.

The first responder who will perform the triage of O365 security incidents should be aware of Microsoft's Assume Breach Mindset and Zero-Trust Network Strategy. The IR responder should be provided with the organization's IR plan, which 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 used by the O365 tenant (*See Figure 4*) and the subscriptions acquired (ATP-plan 1, ATP-plan 2, E1, E3, E5 or A5)
- Confirmation on which Microsoft threat protection services are implemented (Defender ATP, Office 365 ATP, Azure ATP, or Cloud App Security)
- Confirmation on whether O365 threat management policies are tuned/configured properly and all logs are enabled in the Microsoft 365 Security Center
- Confirmation on whether the tenant is an O365 customer with mailboxes in the Exchange Online or is a Standalone Exchange Online Protection customer without Exchange Online mailboxes as email messages are protected automatically
  ***If ATP anti-phishing (a set of machine learning models trained to detect phishing messages) subscription is acquired, check whether the anti-phishing protection in O365 is tuned properly or not.

PROTECTION LEVEL	DEVICE TYPE	AZURE AD CONDITIONAL ACCESS POLICIES				AZURE AD IDENTITY PROTECTION USER RISK POLICY	INTUNE DEVICE COMPLIANCE POLICY	INTUNE APP PROTECTION POLICIES
BASELINE		Require Multi-factor Authentication (MFA) when sign-in risk is *medium or high*	Require approved apps (enforce mobile app protection for phones and tablets)	Block clients that do not support modern authentication (Clients that do not use modern authentication can bypass conditional access rules, so it is important to block these)	Require compliant PCs	High risk users must change password (Force users to change password when signing in if high risk activity is detected from their accounts)	Define compliance policies (one policy for each platform)	Define app protection policies (one policy per platform– iOS, Android)

SENSITIVE		Require MFA when sign-in risk is *low, medium or high*			Require compliant PCs and mobile devices (Enforce in-tune management for PCs and phones/tablets)			
HIGHLY REGULATED		Always require MFA						

PRODUCT KEY

- All Office 365 Enterprise plans
- Microsoft 365, E3, Enterprise Mobility + Security (EMS) E3, Azure AD P1
- Microsoft 365 E5, EMS E5, Azure AD P2

Figure 4. Table/Tier of Protection Policies of an Office 365 Tenant.

DETECTION, IDENTIFICATION & ANALYSIS

During the second phase, the organization should aim to detect and validate O365 security incidents rapidly. Thousands or even millions of phishing emails may come to an organization's mailboxes daily. If O365 protection policies are tuned or configured properly, phishing or BEC email attacks can be identified easily.[5]

Do not assume that your anti-phishing solutions, including O365 anti-phishing subscriptions, can filter out every phishing email, especially when these solutions are not tuned or configured appropriately. O365 audit logs should be the most reliable forensic artifact that allows the first responder to conduct the triage.[6]

Some secured email gateways place great emphasis on malware filtering or malicious URLs rewriting but overlook spoofed email validation and authentication detections by using SPF, DKIM, and DMARC.[7;8;9] If a secured email gateway is placed

[5] https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/tuning-anti-phishing
[6] https://docs.microsoft.com/en-us/microsoft-365/compliance/auditing-troubleshooting-scenarios
[7] https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/use-dkim-to-validate-outbound-email
[8] https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/use-dkim-to-validate-outbound-email
[9] https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/use-dmarc-to-validate-email

in front of O365, valuable phishing email threat intelligence (especially those metadata contained in the email headers) can sometimes be filtered out, making O365 protection policies less useful.

Adopting corrective actions, such as enabling Multi-Factor Authentication (MFA) on privileged email accounts, will immediately minimize the damage that the organization sustains as a result of the BEC incident. The organization can also follow guidelines from Microsoft O365. O365 Secure Score will soon provide a tenant-wide guideline on how an organization can use O365 Threat Protection to defend against 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 indicates that attacks spread out over time.[10] Attacks do not always happen as soon as the account is compromised. In one of our past investigations, attacks were launched more than five months after the email account was compromised.

From the alerts and logs, look for anomalies in login/logoff activities or unusual actions such as foreign success or failed logins. Review all setting changes of suspicious email accounts from O365 Security and Compliance Portal. All alerts, i.e., malware attachments, spikes on phishing emails received, spikes on email accounts sending out phishing emails, email account credential compromise, addition of rules to forward the email to an outside email address, other changes and types of attack, must be identified, categorized, and prioritized after triage.

Analysis includes the study of the indicators of compromise (IOCs) and the breadth and depth of the alerts that must be analyzed. The analysis of an incident, whether success or failure, will provide significant insights into the possible vulnerabilities of an organization.

Detection and Identification

IOCs of phishing or BEC attacks include a spike on the following alerts and messages:[11]

- Anti-spam or email filter
- Malware attachment
- An email account from the organization or a lookalike domain of the organization sending out a large volume of phishing emails to internal members
- A user from the financial department receives an email from a C-Suite level or high-ranking personnel (HP), ordering to immediately process an invoice, change the recipient of a payment, or provide sensitive documents
- A spoof email from an HP asking an employee to purchase gift cards for colleagues

[10] https://blog.barracuda.com/2020/02/06/threat-spotlight-email-account-takeover/
[11] https://bit.ly/2WkUQUh

- A legitimate email address from vendors or suppliers, which might send a malicious message as a result of an email compromise (vendor email compromise)
- Messages that are brief, urgent, and force receivers to bypass business protocols, policies and procedures
- Email titles usually 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 clauses or "I am currently unavailable"
- Sender seems to have good knowledge of the organization and refers to a sensitive situation, such as mergers and acquisitions
- Sender states that he or she is traveling, and his/her email address indicate the email originated from a lookalike or spoofed domain or a Gmail, Hotmail, Yahoo mail account rather than a legitimate organization account
- Sender provides instructions on how to proceed (this may be given later by a third party or be sent using another domain)
- A request for payment to a limited company in Hong Kong through a local bank, but the company incorporated less than six months prior to when the email was sent

Email Risk Assessment, Incident Categorization, & Triage

- For email spam or email that contains unwanted content:
    - Check junk mail and collect statistics of similar emails from the organizations' spam filters
    - Check logs and statistics of O365 email anti-spam protection[12]
    - Check ATP safe attachments policies[13]
- For phishing emails that may contain known or suspected attachment-based threats that deploy malware:
    - Filter known malware by using antivirus email plugin or secure email gateway
    - Check logs and statistics of anti-malware protection in O365[14]
    - Check ATP safe attachments policies[15]
    - Check quarantine email messages[16]
- For phishing emails that may contain suspected URL-based threats able to deploy malware or trick users to "click" in order to harvest users' credential:
    - Check spam filters and secure email gateway
    - Check ATP safe link policies[17]
    - Check quarantine email messages[18]
- For known or suspected email impersonation-based threats which attempt to establish trust and entice the recipient to take additional actions:

[12] https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/anti-spam-protection
[13] https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/atp-safe-attachments
[14] https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/anti-malware-protection
[15] https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/atp-safe-attachments
[16] https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/quarantine-email-messages
[17] https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/atp-safe-links
[18] https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/quarantine-email-messages

    - Be aware of attackers using the kill chain model to launch attacks to selected targets. These attackers persistently study their targets, paying close attention to details in order to mimic the victims' styles and mannerisms and reflect them in the email. Attackers can even create a lookalike domain before sending out their email messages.
    - Check spoofing emails with SPF, DKIM, and DMARC
    - Check ATP logs, campaign views, and threat analytics[19;20;21]
- For target phishing email, which may be in the form of BEC, Financial Fraud Kill Chain (FFKC), or espionage:
    - Beware as attackers first attack some email accounts of an organization using techniques described in the *"Detection and Identification" section*
    - Check ATP logs and campaign views and threat analytics[22;23]

Indicators of a Compromised O365 Account.[24]

- Large volumes of spam that originates from your account
- Sent or deleted folders contain common hacked-account messages
- Unusual profile changes
- Unusual credential changes
- Mail forwarding recently added
- Unusual signature recently added

Solution:

- Ensure that your computer is not compromised
- Enable MFA
- Remove forwarding rules

Incident Analysis

Check for the following artifacts or IOCs:

- Search, investigate, and select audit log search
- Find the IP address of the computer used to access a compromised account
- Determine who set up the email forwarding for mailbox
- Determine if users deleted email items in their mailboxes
- Determine if users created inbox rules
- Investigate how a successful login by a user outside your organization happened
- Investigate the timeline of foreign success (based on the IP addresses) and failed logins of a suspicious compromised email account
- Check tenant's Azure sign in logs

[19] https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/how-office-365-uses-spf-to-prevent-spoofing
[20] https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/campaigns
[21] https://docs.microsoft.com/en-us/microsoft-365/security/mtp/latest-attack-campaigns
[22] https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/campaigns
[23] https://docs.microsoft.com/en-us/microsoft-365/security/mtp/latest-attack-campaigns
[24] https://docs.microsoft.com/en-gb/office365/troubleshoot/sign-In/determine-account-is-compromised

- Export audit logs with HAWK or other Powershell tools. Place those logs in a data analytic platform, i.e., ElasticSearch and Splunk[25;26]

Incident Reporting
Escalate notification and reporting of the incident to appropriate parties. Do not hide or cover up any information.

- Designate a person to tune, configure, and monitor all kinds of email attacks by using functions provided by O365 subscriptions
- Extract relevant O365 threat and incident reports
- The report should answer the following questions based on the experiences of users and tenants:
    - What did the attacker access?
    - How long did the attacker have access?
    - Is there potential Personal Identifiable Information (PII) exposure?
    - Are there any compromised email accounts?
    - Are there any advanced malware deployed?
    - Is the tenant clean?
    - What is the motive of the attacker?

    *** Consider the possibility that more than one group of attackers compromised the network.

CONTAINMENT, ERADICATION, AND RECOVERY

The third phase, Containment, refers to the initial steps to mitigate the actions of the attacker. The Containment phase has two major components: stopping the spread of the attack and preventing further damage to systems. It is important for an organization 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 risk acceptable to the organization.

Containment includes the procedures listed below in order to stop the attackers from logging in using stolen credentials. 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 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 O365 Exchange server. The following procedures should be considered to fix a compromised O365 account:[27]

[25] https://www.powershellgallery.com/packages/HAWK/1.0.0
[26] https://github.com/PwC-IR/Office-365-Extractor-1
[27] https://docs.microsoft.com/en-us/archive/blogs/office365security/how-to-fix-a-compromised-hacked-microsoft-office-365-account

- Apply the PowerShell Script, *RemediateBreachedAccount.ps1*.[28]
- Reset your account 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 senior management in charge in order to determine the details of the containment and recovery procedures.

Next phase is Eradication, which consists of the longer-term mitigation efforts such as steps to tune, configure and monitor the threat protection policies at the O365 tenant. Once the attacker selects his/her target organization, he/she will persistently launch phishing attacks and figure out the vulnerabilities he/she can exploit to gain credential. An attacker will seek all possibilities he/she can use as bait in order to entice users to click and eventually download malware, allowing him/her to compromise the system or gain financial benefit.

Recovery often requires drastic actions in a BEC incident. Recovery includes steps to reset the password, enable MFA, remove foreign forward email rules, recreate email accounts, and notify law enforcement or the organizations' bank in order to recover the remitted money in case money was transferred to the attackers. Incident responders need to consider enabling O365 logs, or if resources are available, purchasing more ATP subscriptions for all unprotected O365 users. A qualified individual should be designated to use O365 threat hunting tools to handle continuous monitoring of the O365 tenant.

POST-INCIDENT ACTIVITY (LESSON LEARNED)

Handling a phishing email and BEC incident can be extremely expensive. Thus, organizations must conduct a robust assessment of lessons learned from the entire incident process to prevent reoccurrence of similar events.

Post-incident refers to the process of identifying lessons learned after action and review have been conducted following an incident. Other than upscaling the O365 Security Score, it is essential to implement the following Microsoft Office 365 security recommendations.

[28] https://github.com/OfficeDev/O365-InvestigationTooling/blob/master/RemediateBreachedAccount.ps1

Protect Privileged Accounts:

- Enforce MFA for all administrative accounts (E3 | E5*).
- Implement Azure Active Directory (AD) Privileged Identity Management (PIM) to apply just-in-time privileged access to Azure AD and Azure resources (E5).
- Implement PIM in O365 to manage granular access control over privileged access in (E5).
- Implement Privileged Access Workstations to administer services. Do not use the same workstations for browsing the internet and checking emails not related to your administrative account (E3 | E5).
- Ensure accounts that are synchronized from on-premises are not provided with administrative roles for cloud services.
- Ensure service accounts are not assigned administrative roles.
- Remove licenses from administrative accounts.

*E3 (Security):[29]

- Microsoft Security & Compliance Center
- Threat Management
- DLP for Exchange Online
- SharePoint Online
- OneDrive for Business & Information Governance
- eDiscovery
- Unified Audit, Retention policies

* E5 (Security):

- E3 + Microsoft Defender ATP
- Azure ATP
- O365 ATP Plan-2
- Microsoft Cloud App Security
- Azure AD Premium Plan-2
- 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).

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

- Raise malware protection for emails (E3 | E5).
- Implement ATP anti-phishing attacks (E5).
- Block connections from countries where you do not do business (E5).

Protect Against Advanced Persistent 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 O365 Security for sensitive data (E3 | E5).
- Configure data classification protection policies in O365 for sensitive data.
- Use Azure Information Protection labels for protection (E5).
- Protect data in third-party apps using Cloud App Security (E5).

Continuous Monitoring & Auditing *(APIs from Microsoft Security Graph30 – see Figure 5)**:***

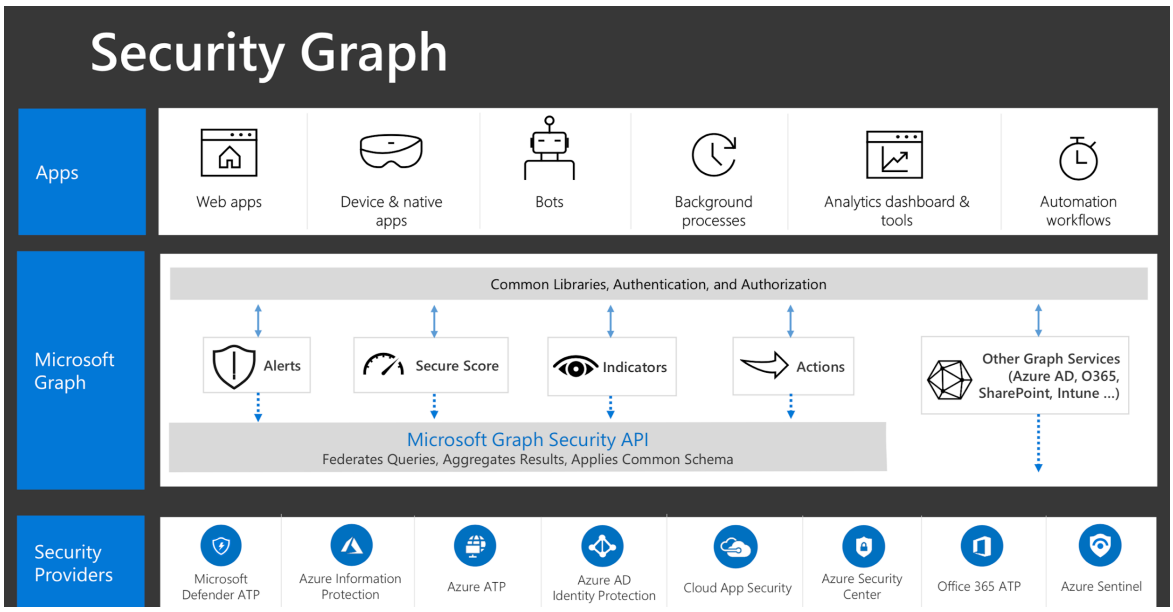


Figure 5. Security Provider and Microsoft Security Graph.

- Enable O365 audit log (E3 | E5).
- Review Secure Score weekly (E3 | E5).
- Use O365 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)
- Conduct advanced hunting (E5).

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

- Use Microsoft Cloud App Security to detect unusual behavior across cloud apps (E5).
- Use Microsoft Azure Sentinel or your current SIEM tool to monitor threats across your environment (E5).
- Deploy Azure ATP to monitor and protect against threats that target your on-premises AD environment (E5).
- Use the Azure Security Center to monitor threats across hybrid and cloud workloads.

Implement Email Threat Policies & Procedures:

- Set email usage guidelines and email account management policies.
- Arrange anti-phishing exercises 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 O365 threat protection policies.

Protect and secure your identity using Azure AD, which identifies the provider of many apps:

- Strengthen your credentials using MFA and 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 enabled password hash sync.
- Reduce your attack surface area.
    - Block legacy authentication.
    - Block invalid authentication entry points.
    - Restrict user consent operations.
    - Implement Azure AD PIM.
- Automate threat response.
    - Implement user risk security policy, which is 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.