TLP:CLEAR

INCIDENT RESPONSE METHODOLOGY

IRM #22
BUSINESS EMAIL COMPROMISE

Guidelines to handle Business Email Compromise Incidents

IRM Author: Alex Kouzmine / CERT SG
Contributor: CERT aDvens
IRM version: 1.0
E-Mail: cert.sg@socgen.com
Web: https://cert.societegenerale.com
Twitter: @CertSG

C'EST VOUS L'AVENIR

SOCIETE GENERALE

TLP:CLEAR

ABSTRACT

This Incident Response Methodology is a cheat sheet dedicated to handlers investigating on a precise security issue.

WHO SHOULD USE IRM SHEETS?

- Administrators
- Security Operation Center
- CISOs and deputies
- CERTs (Computer Emergency Response Team)

Remember: If you face an incident, follow IRM, take notes. Keep calm and contact your business line's Incident Response team or CERT immediately if needed.

→ IRM CERT SG: https://github.com/certsocietegenerale/IRM

→ IRM CERT aDvens (French version): https://github.com/cert-advens/IRM

INCIDENT HANDLING STEPS

6 STEPS ARE DEFINED TO HANDLE SECURITY INCIDENTS

1. Preparation: get ready to handle the incident
2. Identification: detect the incident
3. Containment: limit the impact of the incident
4. Remediation: remove the threat
5. Recovery: recover to a normal stage
6. Lessons learned: draw up and improve the process

IRM provides detailed information for each step of the incident response process. The steps come from NIST Computer Security Incident Handling Guide.

PREPARATION

OBJECTIVE: ESTABLISH CONTACTS, DEFINE PROCEDURES, GATHER INFORMATION TO SAVE TIME DURING AN INCIDENT.

- Develop and enforce policies addressing email security, authentication protocols (e.g. SPF, DKIM, DMARC), and acceptable use.
- Integrate BEC scenarios into the broader Incident Response Plans, Playbooks, Procedures outlining roles, responsibilities, and procedures.
- Prepare a communication plan to warn collaborators, clients or partners about ongoing BEC attacks.
- Establish and maintain a list of takedown contacts at hosting providers, domain registrars, and email service providers.
- Run periodic awareness campaigns covering BEC, social engineering, scam and phishing incidents.
- Deploy a technical solution allowing collaborators to easily report suspicious emails to security teams or a perimetric security collaborator.
- Create dedicqted channels, such as email addresses, social media profiles, and phone lines to enable external reporting of suspicious emails, phone calls, fraudulent wires and other signs of BEC incidents.
- Establish specific procedures for attachments and URL link analysis in a sandboxed or otherwise secured environment inhibiting infection propagation.
- Maintain a list of contacts involved in financial transactions and wire transfers, including the validators.
- Implement strict verification procedures for wire transfers and changes in vendor payment information.
- Establish a cross-functional incident response and/or crisis teams with representatives from IT, security, antifraud, communication, legal, business units (add or exclude in regards to your organization's specific industry and needs).

Automated Monitoring and Detection

- Implement automated monitoring across all relevant systems, including email servers, network access logs, and authentication systems, to continuously detect BEC indicators.
- Make sure that any detection event triggers an immediate notification to the incident response team for rapid investigation and action.
- Utilize Security Information and Event Management tools to correlate events and identify potential BEC patterns effectively.

DEFINITION: Business Email Compromise is a type of advanced financial scam in which criminals use compromised email access to trick employees into transferring large amounts of money or sensitive information. BEC incidents can result in significant financial losses and reputational damage.

IDENTIFICATION

OBJECTIVE: DETECT THE INCIDENT, DETERMINE ITS SCOPE, AND INVOLVE APPROPRIATE PARTIES.

Identifying BEC Indicators

- Identify emails requesting wire transfers, sensitive information, or changes to payment details, especially those with urgent tones.
- Assess the potential impact and severity of the incident based on the nature of the compromise.
- Determine the extent of the compromised accounts and the breadth of the attack.
- Opt for using a centralized monitoring systems on all these sources, so that every detection triggers an alarm for instant reaction.
- Spot emails that convey a sense of urgency, secrecy, or high-stakes scenarios to pressure recipients into quick actions bypassing thorough verification.
- Notice deviations in the tone, language or formatting of emails from known contacts or executives.
- Make sure that alerts are delivered instantly to the incident response team and relevant stakeholders to facilitate swift action.
- Assess the potential financial, reputational, and operational impacts based on the nature and extent of the BEC incident.
- Define severity levels as per maximum potential impact in terms of financial losses, data compromise, operation disruption to prioritize response efforts and allocate resources effectively.

Scoping up

- Identify all email accounts that have been compromised and assess the level of access each account had within the organization.
- Determine how the BEC incident was executed, whether through phishing, account takeover, or leveraging business logic vulnerabilities.
- Identify which departments or business units are impacted by the BEC incident.
- Assess whether the attack originated from a single source or a threat actor group.

Involving Appropriate Parties

- Upon detection of a BEC incident, promptly notify designated company personnel authorized to make critical decisions, such as senior management, IT security leads, and finance executives.
- Ensure that decisions to act on fraudulent emails or transactions are made swiftly, preferably within minutes, to minimize potential damage.
- Engage relevant departments, including IT, legal, public relations, and finance, to ensure a coordinated response.
- If necessary, involve external partners such as email service providers, cybersecurity firms, and law enforcement agencies to support the investigation and mitigation efforts.

Evidence Collection

- Gather samples of the fraudulent emails, ensuring that both the email headers and content are preserved for analysis. Analyze collected fraudulent emails to identify patterns, such as recurring sender IP addresses or common malicious links.
- Make sure that email headers are intact to analyze the origin, routing, and authenticity of the emails.

CONTAINMENT

OBJECTIVE: MINIMIZE THE DAMAGE CAUSED BY THE INCIDENT, PREVENT FURTHER UNAUTHORIZED ACTIVITIES, AND SECURE COMPROMISED SYSTEMS AND ACCOUNTS TO HALT THE ATTACKER'S PROGRESS.

Isolate Compromised Accounts

- Temporarily suspend or disable email accounts identified as compromised to prevent further unauthorized access and malicious activities.
- Enforce immediate password changes for compromised accounts and any other accounts that may share similar credentials. Check the administrator account's integrity.
- Ensure MFA is enabled on all critical accounts to add an extra layer of security.
- Audit newly created mailbox rules, which may contain redirections to external mailboxes. Remove all rogue rules.

Block Malicious IPs and Domains

- Identify and block IP addresses associated with the unauthorized access or malicious activities using firewall rules and email security gateways.
- Add suspicious domains used in phishing or fraudulent emails to blacklist to prevent further communication from these sources.

Segregate Affected Systems

- Isolate affected systems from the main network to prevent lateral movement by the attackers. This includes segregating email servers, user endpoints, and any connected devices.
- Implement strict access controls; make sure that only authorized personnel have access to critical systems during the containment process.

Restrict External Communications

- Temporarily restrict or closely monitor outbound email traffic to detect and block any fraudulent communication.
- Limit or suspend remote access capabilities for affected accounts and systems until they have been secured and verified as safe.

Review and Update Email Security Policies

- Enhance spam and phishing filters to detect and block malicious emails more effectively based on the indicators identified during the Identification phase.
- Ensure that email authentication protocols such as SPF, DKIM, and DMARC are correctly put in place and properly configured to prevent email spoofing.
- Implement stringent monitoring of outbound emails for sensitive information or unusual patterns that may indicate ongoing compromise attempts.
- Apply temporary restrictions on certain types of email attachments or hyperlinks until the threat is fully contained and mitigated.

If you encounter Business Email Compromise fraud multiple times per week, it may be prudent to implement an alert or warning across your whole organization. Additionally, consider creating an informational page that outlines the characteristics of this scam and provides strategies and best practices for prevention.

CONTAINMENT

OBJECTIVE: MINIMIZE THE DAMAGE CAUSED BY THE INCIDENT, PREVENT FURTHER UNAUTHORIZED ACTIVITIES, AND SECURE COMPROMISED SYSTEMS AND ACCOUNTS TO HALT THE ATTACKER'S PROGRESS.

Communication Management

- Coordinate with public relations and legal teams to prepare appropriate public statements or notifications to stakeholders, customers, and partners while containing sensitive information.
- Engage with law enforcement agencies early in the containment phase to assist with their investigation and to follow any guidance they provide.

Preserve Evidence for Investigation

- Make sure that all relevant logs (e.g. email server logs, network traffic logs, authentication logs) are preserved in their original format for analysis and evidence.
- Create forensic images of compromised systems to aid in detailed investigations without altering the original evidence or tempering with the original hardware.

Collaborate with Stakeholders

- Establish contacts with the associated banking or financial entity regarding the pathways of money flows to enable subsequent legal proceedings.
- Work closely with IT, security, and other relevant teams to implement containment measures effectively and ensure all aspects of the incident are addressed.
- Provide regular updates to key stakeholders on the containment status and any emerging issues.
- Coordinate with email service providers to block malicious emails and secure compromised accounts.
- Communicate the fraudulent nature of the compromised email campaigns to involved external parties such as partners, clients, financial institutions etc.

Implement Short-Term Mitigations

- Temporarily reduce the privileges of accounts that are not essential for containment efforts to minimize the risk of further compromise.
- Reinforce monitoring on critical systems and accounts to detect any suspicious activities during the containment phase.

Update Security Configurations

- Apply necessary patches and updates to systems and software that may have been exploited during the BEC incident.
- Adjust the configurations of security tools and systems to better defend against the specific tactics used in the current BEC scheme.

REMEDIATION (EXTERNAL)

OBJECTIVE: TAKE ACTIONS TO REMOVE THE THREAT AND AVOID FUTURE INCIDENTS.

If fraudulent content is associated with the identified scam and is hosted online:

- **Identify the Owner, Hosting Provider and Domain Registrar** of the scam site with complete documentation of malicious activity.
- **Reference the Fraudulent Website via Toolbars for Instant Blocking in Major Web Navigators**. Implement enterprise-wide blocking through security tools rather than relying solely on browser extensions.
- **Draft a detailed abuse request** clearly explaining the **nature of the identified fraud**, providing specific details and evidence. Include screenshots, email headers, IP addresses, timestamps, and transaction details to expedite effective response from the Registrar/Hosting provider.
- **Send an abuse request to the Hosting and Registrar company** using the established abuse@hostingcompany or abuse@registrar email address. Follow up with multiple communication channels including their dedicated security response teams when available.
- **Follow up with direct phone contact** to the abuse/security teams to expedite the process and establish a clear timeline for resolution.
- **Report the fraudulent email account to the email hosting company** with a formal request for immediate account freeze or suspension. Preserve email evidence in accordance with your organization's data retention policy for potential legal proceedings.
- **Submit comprehensive evidence packages** including copies of fraudulent emails with complete headers, timestamps of unauthorized access, and documentation of financial impact.
- **Investigate and document all social media platforms** being used by the threat actors, including specific accounts, posts, and messaging tactics.
- **Submit coordinated takedown requests** to all affected social media platforms with your organization's security team contact information for follow-up.
- Block all email communication to/from the fraudulent account to prevent malicious actions.
- If no response or action is taken, follow up regularly via email and phone.
- If the takedown process is laxist or slow, consider contacting a local CERT team of the the involved country. Explain the challenges you have been facing and request their assistance in resolving the issue. Provide applicable evidence.

REMEDIATION (INTERNAL)

OBJECTIVE: TAKE ACTIONS TO REMOVE THE THREAT AND AVOID FUTURE INCIDENTS.

Implement immediate account security measures aka 'quick wins'

- Forced password changes for all affected and potentially affected accounts.
- Deployment of multi-factor authentication for all business email accounts.
- Review and revocation of suspicious mail forwarding rules.
- Suspension of legacy email protocols that may bypass MFA requirements.

Conduct thorough email environment scanning to improve early BEC incident alerting

- Unauthorized mail forwarding rules
- Suspicious inbox rules that automatically move, delete or forward messages
- Unusual delegate access permissions
- Evidence of email exfiltration or mass-downloading

Deploy advanced email security solutions with enhanced capabilities

- Detecting anomalous login locations and times
- Identifying suspicious forwarding patterns
- Flagging unusual sending behavior
- Quarantining messages with BEC indicators

Implement strict email authentication protocols

- DMARC aka Domain-based Message Authentication, Reporting & Conformance
- SPF aka Sender Policy Framework
- DKIM aka DomainKeys Identified Mail
- Configure – if deemed acceptable - policies to reject, rather than merely quarantine, failing messages.

Establish emergency financial safeguards

- Implement temporary additional verification steps for all financial transactions.
- Place holds on any pending transactions until verification processes are complete.
- Implement out-of-band verification for all payment changes and wire transfers.
- Establish threshold-based approval workflows requiring multiple authenticators.

Deploy transaction monitoring systems for enhanced detection

- Unusual payment destinations or amounts.
- Changes to established vendor banking information.
- Urgent or high-pressure financial requests.
- Transactions deviating from established patterns.

RECOVERY

OBJECTIVE: RESTORE AFFECTED SYSTEMS AND SERVICES TO NORMAL OPERATION, ELIMINATE THE ROOT CAUSES OF THE INCIDENT, STRENGTHEN SECURITY MEASURES TO PREVENT FUTURE OCCURRENCES, AND ENSURE THE ORGANIZATION IS FULLY RECOVERED FROM THE COMPROMISE.

Root Cause Analysis

- Analyze all details from the Identification and Containment phases to understand how the BEC incident occurred.
- Determine the specific methods and vectors used by the attackers, such as phishing emails, malware, or compromised credentials.
- Identify any misconfigurations or security gaps that were exploited during the attack.

Financial Impact Analysis

- Assess the financial impact by determining the extent of the loss.
- Determine the impact on sensitive information, financial transactions, and operational integrity.
- Contact relevant financial institutions to report the fraud.
- Request reversals of any unauthorized transactions if deemed possible.
- Temporarily put in read only mode the affected accounts to prevent further unauthorized access.

Eradication of Threats

- Scan and clean all affected systems to eliminate malware, spyware, or other malicious software introduced during the attack.
- Identify and delete any unauthorized user accounts or services created by the attackers.
- Remove any backdoors, scripts, or automated processes installed to facilitate ongoing access.

Patch Vulnerabilities

- Apply patches and updates to all software, operating systems, and applications to close exploited vulnerabilities.
- Adjust system configurations to adhere to security best practices and minimize exploitable weaknesses.

Enhance Email Security

- Implement or upgrade email security solutions with advanced threat protection features such as sandboxing and advanced heuristics
- Enforce encryption for sensitive email communications to protect data in transit.

For more details on authentication and infrastructure recovery, check the Large-scale malware compromise IRM-18

RECOVERY

Implement Advanced Authentication Measures

- Expand MFA implementation across all user accounts, especially those with access to critical systems.
- Enforce strong password policies, including complexity requirements and regular password changes.

Network Security Enhancements

- Deploy or upgrade applicable security controls (WAF, IDS, IPS, etc.) to monitor and block malicious activities in real-time.
- Further segment networks to limit access between different organizational units and reduce the attack surface.

Data Protection and Backup Strategies

- Ensure that regular, secure backups of critical data are conducted and stored offline or in a secure cloud environment.
- Implement DLP solutions to monitor and protect sensitive data from unauthorized access or exfiltration.

Restore from Clean Backups

- Restore data and systems from backups verified to be free from compromise, ensuring that restored data is accurate and up-to-date.
- Confirm that all restored systems operate correctly and securely without residual threats.

Back to Normal Operations

- Test and validate all services and systems to ensure they are functioning as expected after restoration.
- Gradually reinstate user access to systems, ensuring that all accounts are secure and authorized.

Reporting to Stakeholders

- Provide detailed reports to relevant stakeholders on the remediation process and its effectiveness.
- Fulfil any legal or regulatory reporting requirements related to the BEC incident, ensuring transparency and compliance.

Communication and Awareness

- Develop targeted security awareness training focused on BEC prevention.
- Implement additional verification procedures for financial transactions and communications.
- Establish clear communication protocols for future security incidents.
- Conduct regular phishing simulation exercises focused on BEC scenarios.
- Provide dedicated training for finance and accounting personnel on fraud detection.

LESSONS LEARNED

OBJECTIVE: DOCUMENT THE INCIDENT'S DETAILS, DISCUSS LESSONS LEARNED, AND ADJUST PLANS AND DEFENSES.

Report

A crisis report should be written and made available to all of the actors of the crisis management cell.

The following themes should be described:

- Initial cause of the infection
- Actions and timelines of every important event
- What went right
- What went wrong
- Incident cost
- Indicators of compromise

Capitalize

- Consider what preparation steps you could have taken to respond to the incident faster or more efficiently.
- Update your contacts-lists and add notes as to what is the most effective way to contact each involved party.
- Consider what relationships inside and outside your organization could help you with future incidents.
- Improve DKIM, SPF and DMARC filters.
- Collaborate with legal teams if a legal action is required.