Phishing Process Flow

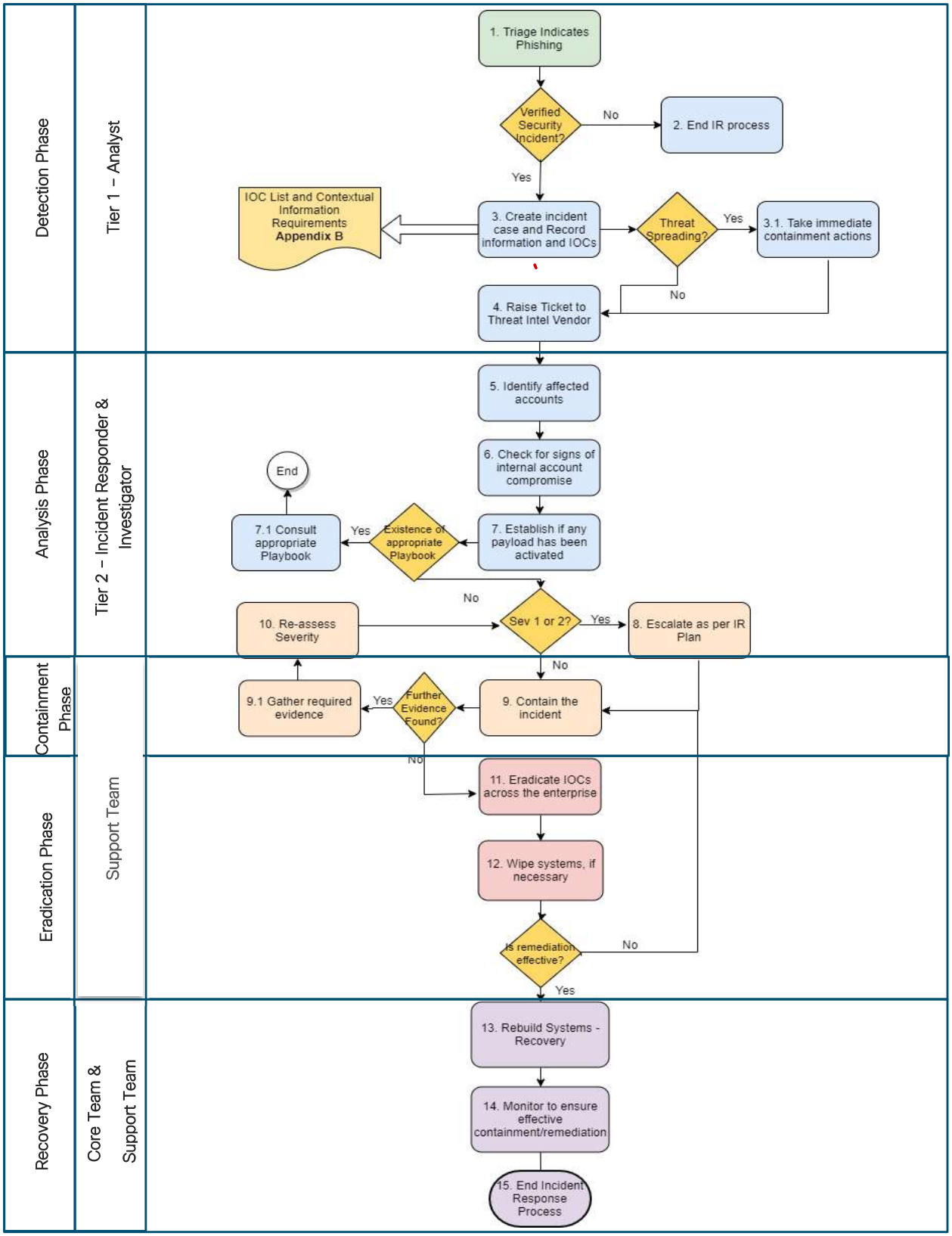
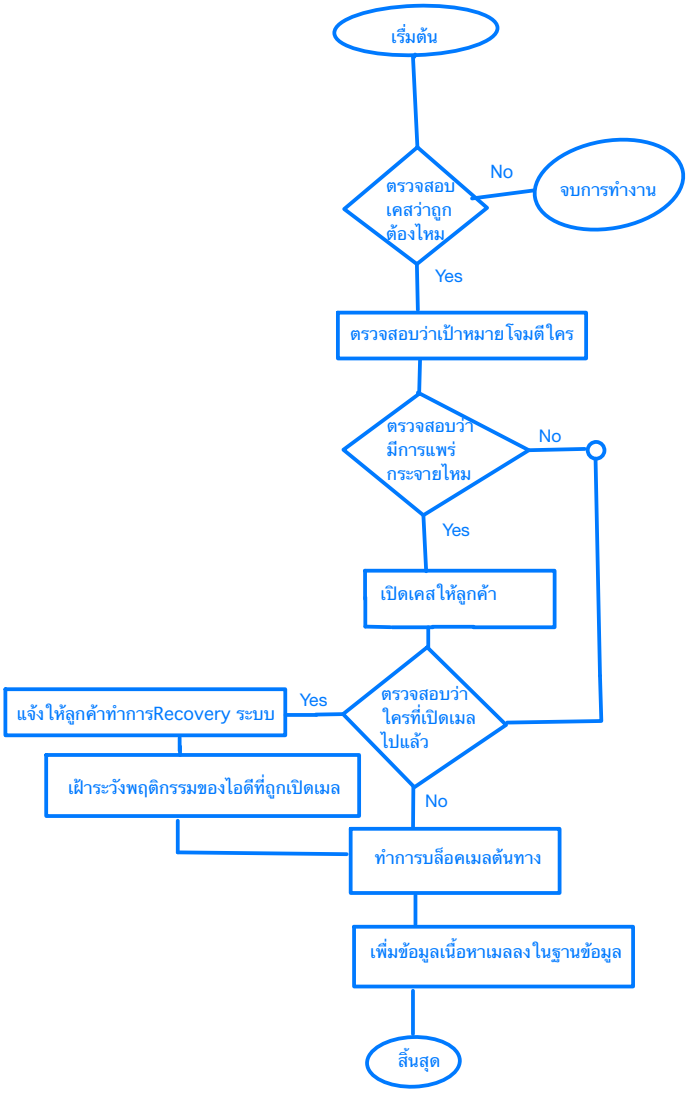


Figure 1: Phishing Process Flow


เริ่มต้น
ตรวจสอบเคสว่าถูกต้องไหม
No
จบการทำงาน
Yes
ตรวจสอบว่าเป้าหมายโจมตีใคร
ตรวจสอบว่ามีการแพร่กระจายไหม
No
Yes
เปิดเคสให้ลูกค้า
ตรวจสอบว่าใครที่เปิดเมลไปแล้ว
Yes
แจ้งให้ลูกค้าทำการRecovery ระบบ
เฝ้าระวังพฤติกรรมของไอดีที่ถูกเปิดเมล
No
ทำการบล็อคเมลต้นทาง
เพิ่มข้อมูลเนื้อหาเมลลงในฐานข้อมูล
สิ้นสุด

Step 1 ตรวจสอบว่า เคสที่เด้งเข้ามานั้นถูกต้องหรือไม่ หากใช่ให้ดำเนินการต่อใน Step 2 หากไม่ใช่ให้หยุดการทำงาน

Step 2 ตรวจสอบว่าการโจมตีนี้มุ่งเป้าไปที่ใคร เพื่อให้สามารถระบุ วัตถุประสงค์ของแฮกเกอร์ และ จะได้เตรียมแผนรับมือที่ถูกต้อง เช่น มุ่งเป้ามาที่ ผู้บริหาร ต้องเตรียมรับมือว่าผู้บริหาร มีสิทธิ์เข้าถึงอะไรได้บ้าง อะไรมีความเสี่ยงที่สุด

Step 3 ตรวจสอบว่าการโจมตีนี้ได้แพร่กระจายไปหรือไม่ เพื่อให้แน่ใจว่า จะไม่มีผู้อื่นในองค์กรนั้นได้รับผลกระทบของเมลนี้ และ เพื่อจำกัดขอบเขตไม่ให้แพร่ความเสี่ยงไปมากกว่านี้ เช่น อาจรีบปรับสิทธิ์การเข้าถึงผู้ใช้งานที่ถูกโจมตีอยู่ในเวลานี้

Step 4 ทำการแจ้งลูกค้า ขั้นตอนจะต้องรีบแจ้งลูกค้า เกี่ยวกับเมลที่ได้เจอ และคำแนะนำในการรับมือและป้องกันเพื่อให้ลูกค้านั้นได้นำไปใช้ให้เร็วที่สุด โดยขั้นตอนการรับมือนั้นให้ถาม L2 และ L3

Step 6 แจ้งให้ลูกค้าทำการ กู้คืนระบบเก่า และ รีเซ็ตรหัสผ่านระบบตัวเอง และ ค่อยตรวจสอบพฤติกรรมต่างๆอย่างใกล้ชิดเพื่อให้แน่ใจว่า แฮกเกอร์จะไม่สามารถเข้าถึงคอมพิวเตอร์ของบริษัทได้ และ ไม่สามารถทำอะไรที่เป็นความเสียหายต่อบริษัทได้ โดยขั้นตอนนี้เป็นสิ่งที่สำคัญอย่างมากในการให้ลูกค้าทำให้เร็วที่สุด

Step 7 ทำการบล็อคเมลต้นทาง เพื่อไม่ให้กระจายไปหาใครอีกหรือบริษัทที่อยู่เครือของลูกค้าเอง

Step 8 เพิ่มข้อมูลเกี่ยวกับเมลไว้ในฐานข้อมูลของ Soc เพื่อเป็นข้อมูลไว้ค่อยเฝ้าระวังให้ลูกค้าไม่ให้เกิดเหตุการ์ณนี้อีกในอนาคต

Phishing Process Detail

Step	Action	Performer	Actions	Notes
1	Triage Indicates Phishing	Tier 1 - Analyst	☐ Become familiar with the background and context of the incident by ingesting the detail within the triage report ☐ Ensure access to incident ticket and incident log are granted ☐ (Optional) Engage with Corporate Branding and Communications for external communications ☐ Ensure that all the relevant information regarding the email has been gathered: ○ Affected user information ○ Device name ○ Email Sender ○ Email Subject ○ Data & Time email received ○ Name of any attachments or URLs ○ Action taken on the email so far (if opened, clicked on a link/attachment, etc.) ☐ USE CASE: WEB PHISHING /RANSOM DEMAND ○ Consult Appendix A for above use cases. ☐ Update Incident Log	
2	End IR Process	Tier1 - Analyst	☐ In the case that the incident is determined to not be a security incident end the IR process.	

3	Create incident case and Record information and IOCs	Tier 1 - Analyst	☐ Create a security incident case and record contextual data and IOCs. ☐ Log any of the IOCs that have previously been identified (or analysis has provided) into the Incident case ☐ Examine the email in question and record any further relevant IOCs o This may done by retrieving the email through the email management system in use or by requesting a copy to be sent as an attachment ☐ Check reputation of sender IP address in VirusTotal ☐ Scan any attachments with anti-virus software	IOC List at Appendix B
3.1	Take immediate containment actions	Tier 1 - Analyst	☐ In the case that the attack is spreading or has a high potential of spreading, block any malicious URLs in the email ☐ Consider blocking the sender's IP address ☐ Log details in incident log	
4	Raise Ticket to Threat Intel Vendor	Tier 1 - Analyst	☐ Raise Ticket to threat intelligence vendor (Group-IB) to get additional information ☐ Add Ticket number to the incident log ☐ Monitor Ticket for updates to be included in the incident log	
5	Identify affected accounts	Tier 2 – Incident Responder & Investigator	☐ Using the IOCs gathered so far, search the enterprise to determine which users have been subject to (web and/or email) Phishing	Depending on the number of users affected, consider escalating the incident to CSIRT

6	Check for signs of internal account compromise	Tier 2 – Incident Responder & Investigator	☐ Continuously examine for any signs of internal account compromise ○ Watch for alerts from security solutions (e.g. SIEM) or suspicious activity reported by users ○ Examine shared mailboxes ○ Check affected mail accounts for large volumes of sent mail ○ Monitor for account logins from suspicious IP addresses ○ Monitor for the creation of automatic mail forwarding rules	
7	Establish if any malicious payload has been activated	Tier 2 – Incident Responder & Investigator	☐ Check email logs (if available) for replies to the sender ☐ Check for evidence of access to malicious URLs ☐ Confirm from the user how they interacted with the email ☐ Monitor for attack morphing if the payload is not being activated	Examples of a payload being activated include the opening of an attachment, a URL being clicked, or sensitive information being provided
7.1	Consult appropriate Playbook	Tier 2 – Incident Responder & Investigator	☐ In the case that more suitable playbooks exist, they can be consulted (e.g. signs of Unauthorised Access, Malicious Code, or Data Leakage)	
8	Escalate as Per IR Plan	Tier 2 – Incident Responder & Investigator	☐ In the case of a severity 1 or severity 2 incident, escalate the incident to the appropriate stakeholders for action according to the IR Plan escalation procedure.	
9	Contain the Incident	☐ TM ☐ Networks & Datacentre Team	☐ Disable user accounts/access as appropriate ○ User/device AD account ○ System Accounts	

		☐ Others as deemed appropriate	☐ Ensure that all malicious URLs have been blocked ☐ Remove the machine from the network if necessary ☐ Log all actions to incident log	
9.1	Gather required evidence	☐ Tier 2 – Incident Responder & Investigator ☐ CSIRT Forensic Investigators (if needed) ☐ TM ☐ Networks & Datacentre Team ☐ Others as deemed appropriate	☐ It is common to identify further artefacts, IOCs and/or IOAs during containment. If such evidence is found they need to be recorded as they can further drive the IR efforts. ☐ Where specialist assistance is required consider invoking the CSIRT team or any Incident Response providers via the Incident Manager. Can be assisted by the appropriate IT department (e.g. TM, Networks & Datacentre team, etc.) ☐ Where appropriate preserve network log information ☐ Gather relevant files and artefacts that could assist the investigation ☐ Store artefacts securely within Incident Folder. Make sure that the appropriate file hashes are compiled. ☐ Log actions in incident log	
10	Re-assess Severity	☐ Tier 2 – Incident Responder & Investigator	☐ Depending on the new artefacts, IOCs, IOAs found the severity of an incident might change and according actions shall be taken.	
11	Eradicate IOCs across the enterprise	☐ TM ☐ Networks & Datacentre Team ☐ Others as deemed appropriate	☐ Confirm from the relevant team(s) that all IOCs (e.g. phishing emails) have been deleted across the enterprise.	

12	Wipe systems, if necessary	▯ On-site team ▯ Networks & Datacentre Team	▯ If there is evidence that systems have been compromised through unauthorised access or malicious code, then consider eradicating all malicious artefacts (DLLs, registry entries, drivers, etc.) o Inform resolver group that systems are required take the appropriate actions ▯ Log notification in incident log	
13	Rebuild Systems-Recovery	▯ TM ▯ Networks & Datacentre Team	▯ In the case that is believed that the remediation steps (containment and eradication) were effective proceed with this step, otherwise go to step 9 for further containment actions. ▯ If there is evidence that systems have been compromised through unauthorised access or malicious code, then consider rebuilding from trusted media o Inform resolver group that systems are required to be rebuilt o (Optional) Confirm to resolver group if rebuilt devices can be immediately re-introduced into the environment ▯ Once the threat has been eradicated, re-enable any access that was revoked during the incident, ensuring any compromised credentials have been changed o User/device AD accounts o SYSTEM accounts ▯ Utilise resolver groups to implement the rebuilds / replacement systems	

			○ Control deployment via SOC team to ensure effective monitoring can occur	
14	Monitor to ensure effective containment / remediation	SOC Team	Monitor systems that were involved in the incident for an appropriate period to confirm that the containment has been successful. Alert resolver group(s) upon identifying further suspicious activity in order to implement further containment and remediation Log all actions in incident log	
15	End Incident Response Process	Tier 2 – Incident Responder & Investigator	Notify Incident Manager of completion of Incident Response process If Post Incident Review (PIR) is required refer to PIR Playbook ○ PIR is required where an incident is a Severity 1 or Severity 2	

Appendix A - Specific Use Case

Web Phishing

External

C-level executives from the customers of K received an email informing them there is going to be an event to celebrate the end of the year. In order to reserve a seat and get further information they would have to login with their internal credentials to the website to include in the email. Once the victims/ customers use their credentials to log in the provided Phishing website the attackers gather the data to further escalate their attack in the clients.

Internal

Monday morning an internal email is sent to employees for checking their bonuses. To see the amount that is going to be paid to each of them they have to click on the link provided and log in with their credentials.

Special Considerations

1. Phishing attacks can be extremely accurate and well researched (Spear-phishing)
2. The goal of the attackers is to lure a victim to navigate to a web page they control and trick the users to use their credentials.
3. Inform the security team or the designated entity according to policies.
4. If an email is suspicious it should be brought to the attention of the security team.
5. For external web phishing cases make sure that the clients receive regular emails raising awareness for phishing stating the official channels of communications (websites, phone numbers, etc.)

Ransom Demands

Ransom demands may be directed at your organisation. A common example is ransomware – asking for a sum of money to give access back to files. Although it may not seem beneficial to pay the ransom, the advantages and disadvantages of doing so should be considered before any decisions are made. It may be cheaper to pay the ransom and then bolster defences than spend time and money attempting to decrypt the files or recover the data; however, it is not guaranteed that the attacker will decrypt any files.

Ransom demands may not just be in the form of ransomware. KTB may receive emails threatening to leak customer data or other physical or digital threats. These threats should be investigated for their credibility and the benefits of paying any ransom thoroughly assessed.

Special Considerations

1. Ransom demands usually come with an associated threat if the ransom is not paid. Assess the credibility of the threat before making any decisions, for example:
    a) If an attacker is threatening to leak data, try to obtain a sample of the data to determine if it is actually of concern.
    b) If an attacker has encrypted files, try to get a sample of them decrypted to see if the functionality exists.
2. Save a copy of the ransom email as it may be examined by the authorities.
3. Be aware that the attacker may not necessarily hold up their end of the ransom once the money is received.
4. Inform the Incident Coordinator of any credible ransom demands.

Appendix B - IOC List, Typical Forensic Artefacts and Contextual Information Requirements

Indicators of Compromise

Indicators convey specific observable patterns combined with contextual information intended to represent artefacts and/or behaviours of interest within a cyber-security context. They consist of one or more observable patterns potentially mapped to a related Tactic, Technique or Procedure (TTP).

The following is a non-exhaustive list of Indicators of Compromise (IOCs) to be leveraged during Incident Response (IR) investigations:

- IP Addresses
- File Hashes (MD5, SHA1, SHA256 etc.)
- URLs
- URIs
- Domain Name
- Domain Registrant Information
- Virus Signatures
- File Name
- Autonomous System Number (ASN)
- User Defined Input (usernames, passwords etc.)
- User Agents (UAs)
- Unique / Identifiable Strings
- Network Traffic patterns
- Any item of intelligence that can directly indicate suspicious activity

Typical Forensic Artefacts

The following list details typical forensic artefacts that may be of interest during an investigation:

- Operating System Logs (Windows Event Logs, syslog, etc.)
- Application Specific Logs
- Application Configuration Files
- Operating System configuration files
- Windows Registry Files
- Deleted Files / Recycle Bin Contents

- User Specific folder files
- Internet History Databases
- Email storage files (ost, mbox etc.)
- Application Data folder
- Temporary folders
- Hibernation files
- Page files
- Crash Dumps
- Server Management Logs
- Networking Details

Contextual Information Requirements

During any incident, analysts should aim to identify the following background information. This will assist with ongoing investigation, analysis, timelining, containment and remediation:

- Dates and Times of reported suspicious activity
- Affected persons views on the suspicious behaviour
- Actions taken immediately prior to the initial incident
- Actions taken immediately after the initial incident
- Affected systems roles
- Critical business data stored on or associated with affected systems
- Normal working behaviour of affected systems
- Normal working behaviour or affected business unit and personnel
- Other recent incidents affecting the same or similar systems
- Historical incidents similar to ongoing issue
- Time sensitivity / downtime issues likely to impact decision making