Playbook for Cat & Box Scenario

Fahad Shahzad

Project 4

The Scenario

We are hired as a specialist for the Box company, a small manufacturing organization that specializes in creating boxes for varying sizes of cats. Mr. Percy F. has hired a SOC and consultant to manage the company's network, systems, data, and security. Mr. Percy also requested that certain individuals be notified when and if any potential impacts occur and have there be transparent communication.

The SOP

Purpose:

The purpose of this SOP is to ensure the security of assets and information for the cardboard box manufacturing company.

Scope:

The scope of the SOP includes all assets, networks, and systems used by the company.

The assets used are laptops, desktops, printers, and scanners.

The networks used are webservers, data base servers, file servers, and email servers.

Roles and Responsibilities:

The key individuals are:

- Mr. Percy (CEO) needs to be informed about anything impacting his business.
- Cat (consultant) in charge of overseeing security needs.
- SOC (contractors) responsible for monitoring network, systems, and data.
- Miss Misha (production manager) informed about all highlights and potential impacts caused by breach of systems.

Security Policies:

- Document all relevant cybersecurity policies, including password policies, data encryption policies, access control policies, and acceptable use policies.
- Ensure that all employees are aware of and comply with these policies.

Network Security:

- Implement measures for securing the Box's network infrastructure, by applying firewalls, intrusion detection/prevention systems, and secure Wi-Fi networks.

Data Protection:

- Fail over and redundancy procedures for data backup and recovery to prevent data loss in case of cyberattacks or system failures.

Employee Training and Awareness:

- Implementing cybersecurity training programs for all employees in order to raise awareness of potential threats mainly phishing attacks, and some of the best practices for data protection.
- Conducting regular security awareness campaigns insure employees are informed about the latest cybersecurity trends and threats.

Documentation and Reporting:

- Maintain detailed documentation of all cybersecurity measures, incidents, and response activities.
- Establishing protocols for reporting cybersecurity incidents to relevant authorities and stakeholders.

Continuous Improvement:

- Regularly review and update the SOP to reflect evolving cybersecurity threats and technologies.

The Playbook

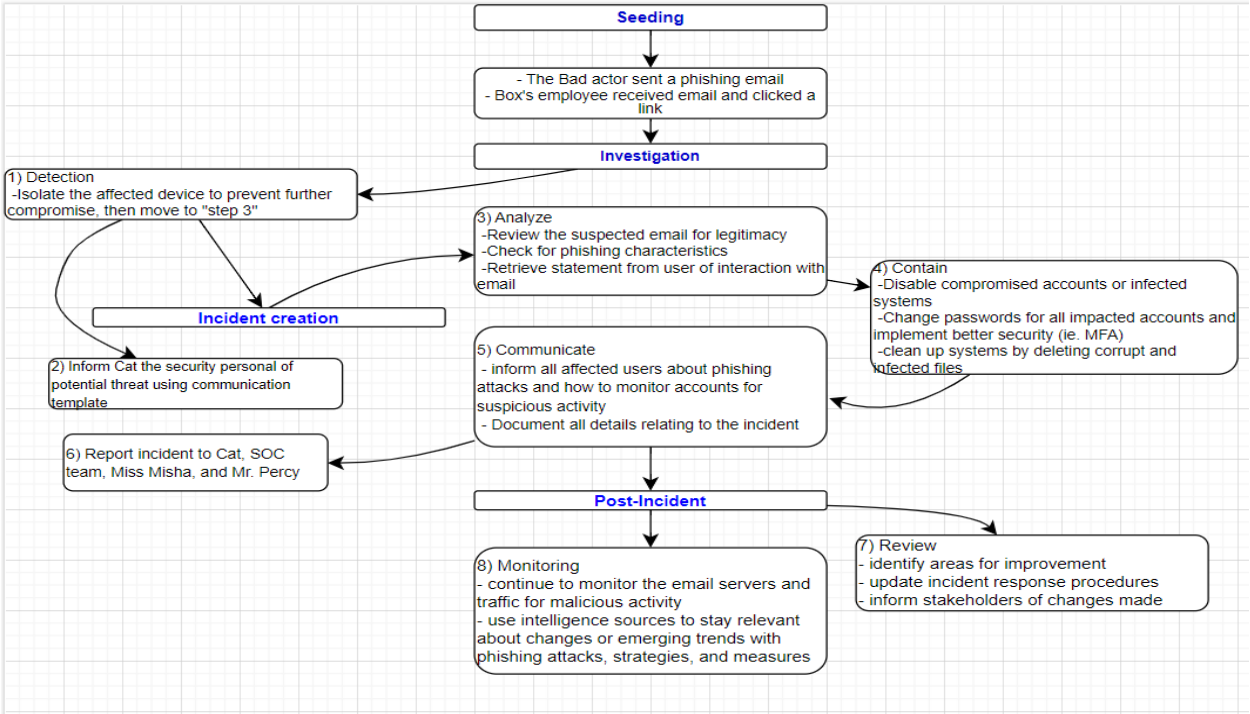
While there are many threats faced by any organization, we will be focusing on a simple yet a rudimentary threat, the phishing attacks. Before getting into the paybook and the flow chart, what is a phishing attack.

A phishing attack is a type of cyber attack where an attacker attempts to deceive individuals into revealing sensitive information such as login credentials, credit card numbers, or other personal information. This is typically done through fraudulent emails, messages, or websites that appear to be from legitimate sources. Phishing attacks often use social engineering techniques to manipulate and trick users into taking actions that benefit the attacker, such as clicking on malicious links, downloading malware-infected files, or providing confidential information.

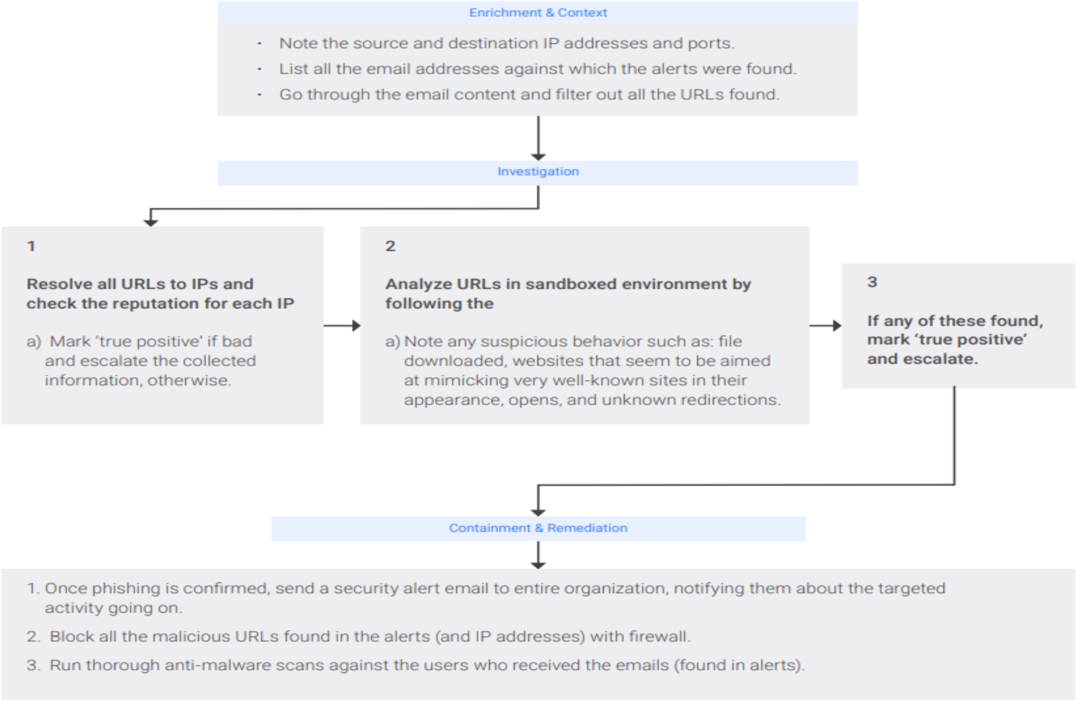
The following are some characteristics of phishing attacks:

- Spoofed emails
- Urgency or use of fear tactics
- Fake links

Now let us look at the flow for responding to a phishing attack as shown below.


Seeding
- The Bad actor sent a phishing email
- Box's employee received email and clicked a link
Investigation
1) Detection
-Isolate the affected device to prevent further compromise, then move to "step 3"
3) Analyze
-Review the suspected email for legitimacy
-Check for phishing characteristics
-Retrieve statement from user of interaction with email
4) Contain
-Disable compromised accounts or infected systems
-Change passwords for all impacted accounts and implement better security (ie. MFA)
-clean up systems by deleting corrupt and infected files
Incident creation
2) Inform Cat the security personal of potential threat using communication template
5) Communicate
- inform all affected users about phishing attacks and how to monitor accounts for suspicious activity
- Document all details relating to the incident
6) Report incident to Cat, SOC team, Miss Misha, and Mr. Percy
Post-Incident
7) Review
- identify areas for improvement
- update incident response procedures
- inform stakeholders of changes made
8) Monitoring
- continue to monitor the email servers and traffic for malicious activity
- use intelligence sources to stay relevant about changes or emerging trends with phishing attacks, strategies, and measures

Furthermore, we can also refer to the pre-defined playbook on phishing attacks by following Google's flow as shown below:


Enrichment & Context
Note the source and destination IP addresses and ports.
List all the email addresses against which the alerts were found.
Go through the email content and filter out all the URLs found.
Investigation
1
Resolve all URLs to IPs and check the reputation for each IP
a) Mark 'true positive' if bad and escalate the collected information, otherwise.
2
Analyze URLs in sandboxed environment by following the
a) Note any suspicious behavior such as: file downloaded, websites that seem to be aimed at mimicking very well-known sites in their appearance, opens, and unknown redirections.
3
If any of these found, mark 'true positive' and escalate.
Containment & Remediation
1. Once phishing is confirmed, send a security alert email to entire organization, notifying them about the targeted activity going on.
2. Block all the malicious URLs found in the alerts (and IP addresses) with firewall.
3. Run thorough anti-malware scans against the users who received the emails (found in alerts).

The Communication

The below are the two separate emails to be sent one mainly to Cat at step 2 of the playbook flow to inform her about the potential threat, and the second email to to all stakeholders to update them about the changes made to the flow or the completion of the incident.

The template are as follows:

To: mesha@box.cat, cat@soc.cat , SOC
CC: percy@box.cat
From: fromusemail@address.com

Subject: CS Incident Notification ***Alert*** completion

Hi All,

This is a notice on an incident creating.

As per our protocol, detailed information regarding the incident will be shared with all shareholders. Rest assured, we have taken all necessary steps to mitigate any potential risks and ensure the security of your systems and data.

You can view the documentation by either using the internal ticketing system referencing (incident#

or

clicking this link: http://documentedIncident_report.pdf

We will provide regular updates as our investigation progresses. Please do not hesitate to contact us if you have any questions or require additional information.

Regards,

Fahad Shahzad
Playbook specialist

To: cat@soc.cat

CC: percy@box.cat, mesha@box.cat

From: fromusemail@address.com

Subject: CS ***Potential*** Incident Alert

Hi Cat,

We have detected a suspected cybersecurity incident within Box Manufacturing's network and require your immediate assistance in analyzing and remedying the situation.

Please find attached detailed information regarding the incident for your review (insert incident#). Your expertise and guidance are crucial in resolving this matter efficiently and effectively.

Thank you for your prompt attention to this matter.

Thank you,

Fahad Shahzad

Playbook specialist

The References

Security, C. C. F. C. (2022, January 13). *Ransomware playbook (ITSM.00.099) - Canadian Centre for Cyber Security*. Canadian Centre for Cyber Security. https://www.cyber.gc.ca/en/guidance/ransomware-playbook-itsm00099

Chronicle. (2022). *Top Security Playbooks* (Third Edition) [Whitepaper]. https://learningimages.lighthouselabs.ca/Cyber+BC/Cyber+BC+C4/Top_Security_Playbooks_2022.pdf

What is phishing? - definition, types of attacks & more | ProofPoint US. (2024, May 9). Proofpoint. https://www.proofpoint.com/us/threat-reference/phishing