Playbook for Box

Playbook for Cat & Box Scenario

By Evelyn Wolfe

Table of Contents

Executive Summary

Mr Precy has requested our expertise in regards to his company. Box is a cardboard box maker for Cats of all sizes. Mr Percy is the CEO of this company, and the company is on a smaller size. He has delegated out the responsibilities for security solutions to a 3rd party Security Operations Center (SOC), however he came to Cat's Team for our playbook knowledge and services.

In this overview, we will be providing an example of a Phishing Attack Playbook, and the procedures from Standard Operating Procedures, to Playbook, and back to Standard Operating Procedures. This will also include email examples to the business, as well as to the Security Operation Center.

Playbook

With Box company vulnerabilities, I would like to recommend the following playbooks, Phishing Attacks, Suspicious Logins, and Brute Force. The following example of a playbook will be for Phishing Attacks and Suspicious Logins.

The reason why I would like to recommend these types of playbooks is due to the company being on the smaller size, limits to training, as well as the public facing information of Box's hierarchy, especially Mr Percy's information. No matter how much we train our employees regarding Phishing type attempts and attacks, today attackers are sophisticated in their trying to collect information, leverage that into breach. All it takes is that XYZ Store that may appear to look correct, but in all reality is the attack and the employee clicked on that link in the email, and the phishing breach has begun.

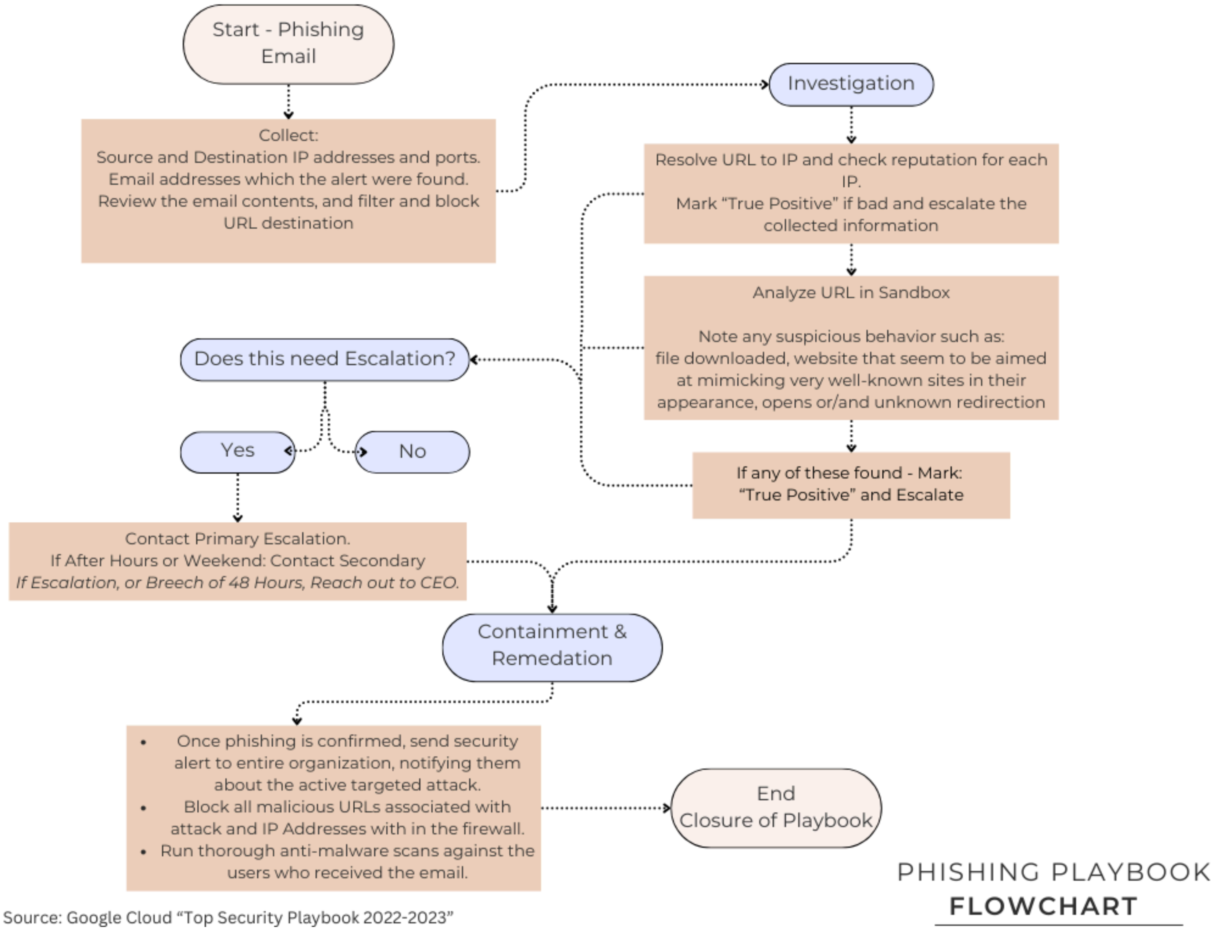
Standard Operating Procedures:

- Utilizing a tool like KnowBe4
  - This would allow the option for training and monitoring.
  - Training for awareness around social engineering and assistance with making better business practices overall.
    Resource: *PhishER Plus* | *How It Works* | *KnowBe4*
- Reviewing emails for potential errors, creating tickets for review when unsure if the ticket may not be from a reputable source.
- Continuous Monitoring of potential threats via SOC(Security Operations Center)

Phishing Playbook

- **Notice of Phishing Compromise**
  - Was there a suspicious email that a user clicked on?
  - Collect the following information
    - Collect Source and Destination IP addresses and Ports
    - Email addresses which the alerts were triggered from
    - Review the email contents, Filter and/or block URL destination with in the firewall
- **Investigate**
  - Resolve the URL to IP and check the reputation for each IP
    - Mark "True Positive" if bad and escalate the collected information
  - Analyze URL in a Sandbox
    - Note any suspicious behavior such as: file downloaded, website seems to be aimed at mimicking very well-known sites in their appearance, opens or/and unknown dedication.
  - If any of these are found - Mark: "True Positive" and escalate

- **Escalation**
    - If any marks noted “True Positive” and Escalate, the following is the chain of Escalation
    - Mr Percy is only to be contacted if an item is escalated or urgent, or has not been resolved within 48 hours.
        - Mr Percy Contact Info:
            - Email: percy@box.cat
        - Primary Contact: Misha F.
            - Business Hours: 9am to 5pm AST Weekdays(Monday through Friday.)
            - Email: mesha@box.cat
            - Phone: 902.66.9999
        - Secondary/Back Up Contact: Minka F.
            - After hours 5pm to 9am AST, and Weekends
            - Email: minka@box.cat
            - Phone: 902.99.9999
        - External MSSP & SOC Security Oversight (3rd Party)
        - Cat Security: cat@soc.cat
            - Phone: 902.88.1234
            - Cell: 902.77.4321
- **Containment and Remediation:**
    - Once phishing is confirmed, send security alerts to the entire organization, notifying them about the activities regarding the active attack. Example:
    - Block the following with in the firewall: URLs and IP Addresses
    - Run a thorough anti-malware scan against the users who received the alert.
- Once resolved, close the playbook along with the incidents tied to it.
- Return to Standard Operating Procedures (SOP)



Collect:
Source and Destination IP addresses and ports.
Email addresses which the alert were found.
Review the email contents, and filter and block URL destination

Resolve URL to IP and check reputation for each IP.
Mark "True Positive" if bad and escalate the collected information

Analyze URL in Sandbox

Note any suspicious behavior such as:
file downloaded, website that seem to be aimed at mimicking very well-known sites in their appearance, opens or/and unknown redirection

If any of these found - Mark: "True Positive" and Escalate

Contact Primary Escalation.
If After Hours or Weekend: Contact Secondary
If Escalation, or Breech of 48 Hours, Reach out to CEO.

- Once phishing is confirmed, send security alert to entire organization, notifying them about the active targeted attack.
- Block all malicious URLs associated with attack and IP Addresses with in the firewall.
- Run thorough anti-malware scans against the users who received the email.

PHISHING PLAYBOOK **FLOWCHART**

Source: Google Cloud "Top Security Playbook 2022-2023"

Source: Google Cloud: Top Security Playbooks pg 7

Example of the Letter to Box:

To Staff Members at Box,

It has been brought to our attention that a couple users have been compromised via a Phishing Email Attack on December 5th 2024. Even though the attack was isolated, the damages could have been more severe. If you believe that you may have been targeted by the Phishing Email, and/or clicked on any links from **Info@Boxx.com** please reach out to the IT Department and Security Operations Center for further assistance.

What is a Phishing Email Attack? This is an attack that targets a user to click on what may appear to be a credible source. This is a means of an attacker to socially engineer their attempt to collect data from anyone. Be sure to be using your KnowBe4 training to the best of your abilities.

Your Security is Our Solution.

Evelyn W.
Cat’s Security Team on Behalf of Box.

Example of the Letter to Box’s 3rd Party Security Operation Center

Cat’s Security Team was notified on December 5th of 2024, that two users in the accounting department, and one in supply chain fulfillment clicked on an email from **info@boxx.com** believing it to be from **Box**. We were notified after via alerts, and escalation that the compromise happened, and the Playbook for Phishing was open.

Our team assisted in the scans for any harmful contents that may have been downloaded, and changing of passwords due to the site prompting users to log in.

We tested the email and its link in a sandbox to confirm that this was a socially engineered attempt to gather top secret information regarding Box’s setup and design for the Cat Box, and even included a login page for the users to enter their username and password. Although one of our victims did enter their credentials, we did do the change of credentials for all three users.

We also performed scans for any known factors such as malware, ransomware, virus on any and every user within the departments associated with the three users, as well as the servers the three use. Other than the password attempt, and collection, there was not downloadable, or executable was triggered.

For anyone who may report that they clicked on the link from **info@boxx.com**, please reach out to Cat’s team immediately. We will want to perform credential resets, and a scan of their system.

Best Regards,

Evelyn W.
Cat’s Security Team on behalf of Box.

Citation: (Evelyn Wolfe, Personal Communication, December 2024)

Reference and Citations

Google Cloud. (2022). *Top security playbooks 2022: Preventing business disruptions caused by cyber threats*. Retrieved from https://services.google.com/fh/files/misc/top_security_playbooks_2022.pdf

Microsoft. (2024, November 6) *Incident response playbook: Phishing*. Microsoft Learn. Retrieved December 9, 2024, from https://learn.microsoft.com/en-us/security/operations/incident-response-playbook-phishing

Regarding the Letters: Evelyn Wolfe(2024.) While Senior IT Service Desk, used this layout for my company and suite communication while at GroupO.