Cat Box Phishing Playbook

Derek Mayen

INTRODUCTION

This document is to detail the SOP (Standard Operating Procedures) when dealing with an attacker trying to gain access to data or personal information, through a phishing scam.

Playbook Table of Contents

Contact Info For Escalated Situations

When an attack occurs the organization needs to have a good form of communication so any mitigation and countermeasures can be taken in a timely manner. This diagram will show who to contact in specific situations, and when they are available.

First to be Contacted

In case of an attack or data breach, the first responders to be notified are:

- **Cat**: To be contacted during the Day time after hours & weekends
  - Email: cat@soc.cat
  - Phone (902) 88-1234 or cell (902) 77-4321

- **Misha**: To be contacted Mon - Fri, 9AM - 5PM AST Weekdays
  - Email: mesha@box.cat
  - Phone (902) 66-9999

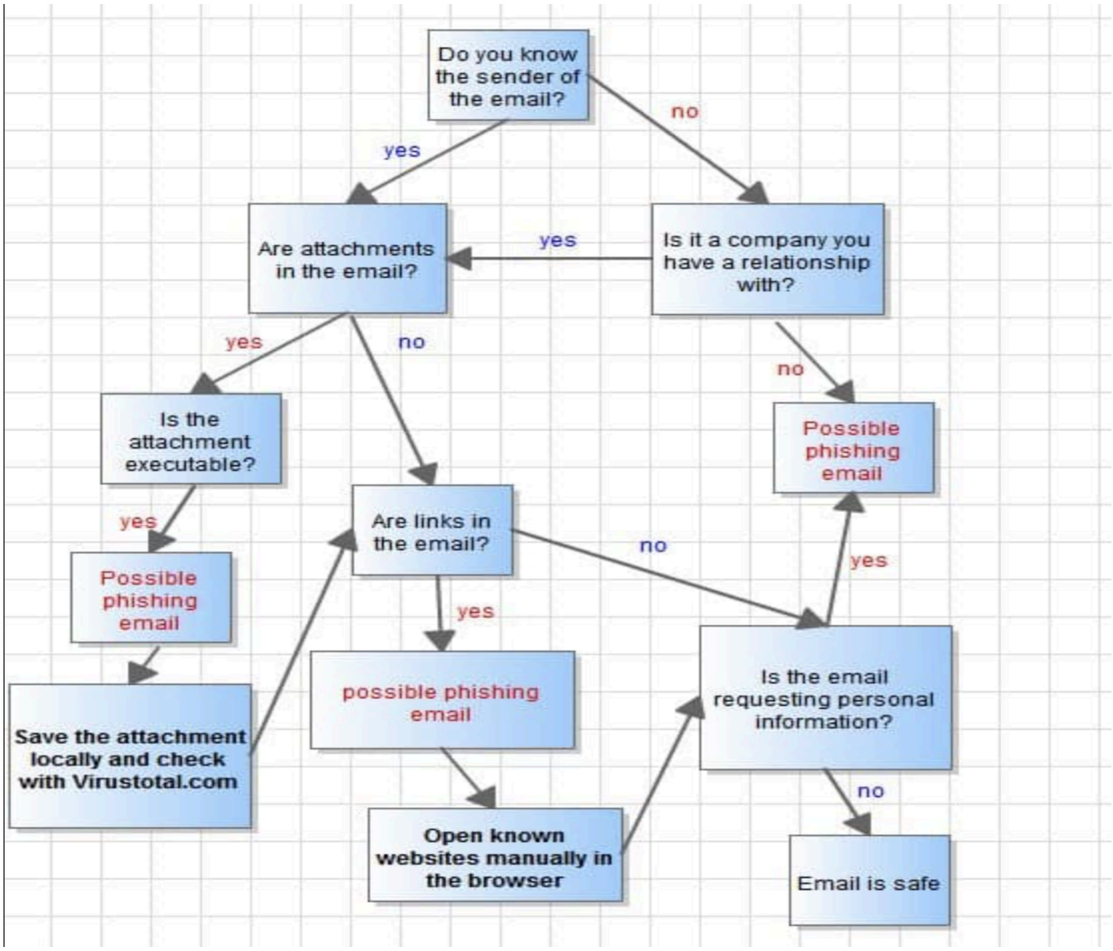
- **Minka**: To be Contacted in Alternation with Misha & Weekends
  - Email: minka@box.cat
  - Phone (902) 99-9999

To be Contacted After Escalation

If the situation is escalated or hasn’t been solved after 48 hours contact:

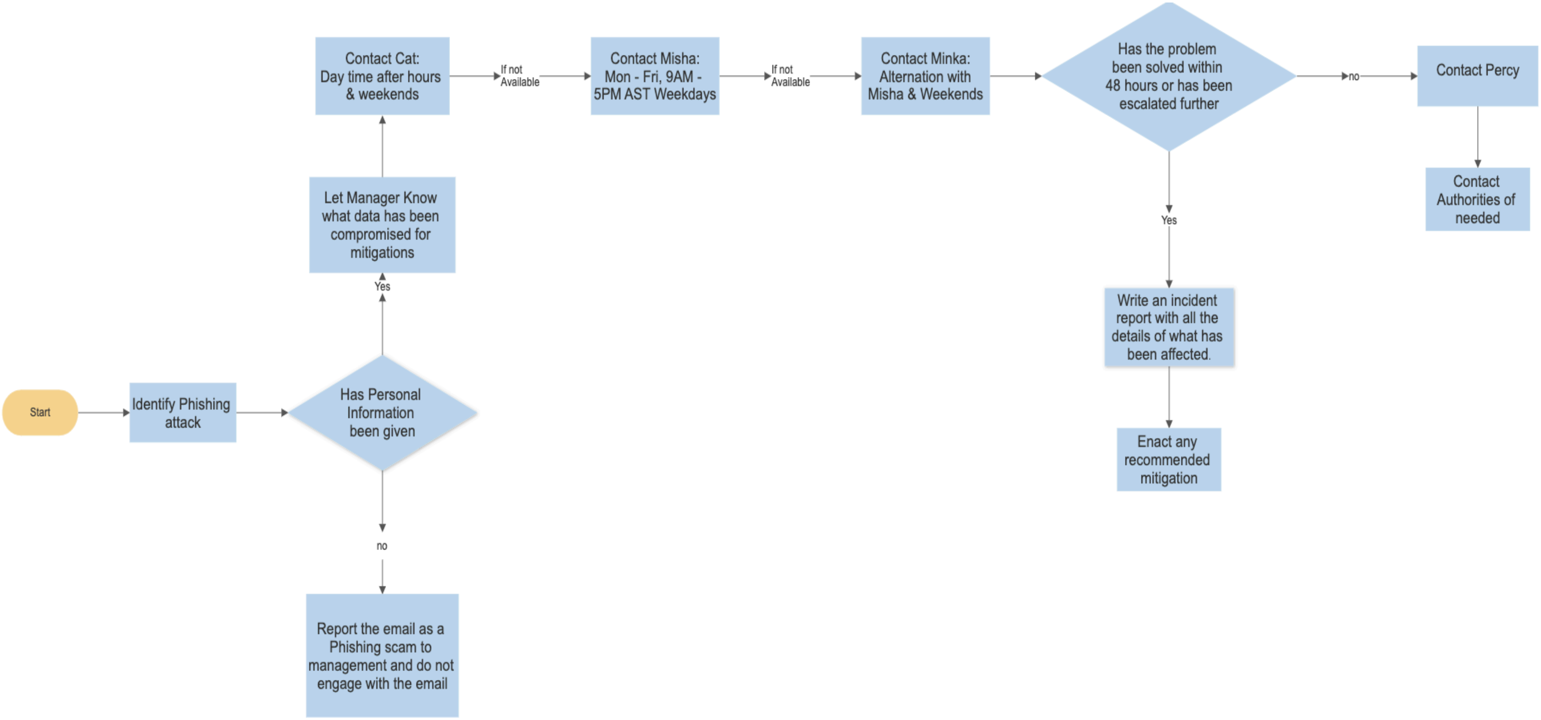
- **Percy**: percy@box.cat

Attack FlowChart


Do you know the sender of the email?
no
yes
Are attachments in the email?
yes
Is it a company you have a relationship with?
yes
no
no
Is the attachment executable?
Possible phishing email
Are links in the email?
no
yes
yes
Possible phishing email
yes
Save the attachment locally and check with Virustotal.com
possible phishing email
Is the email requesting personal information?
no
Open known websites manually in the browser
Email is safe

Note: This flowchart shows how the Standard Operating procedure when it comes to identifying whether or not emails or other forms of communication could contain a possible phishing scheme in order to gain private information, or access to the network to gain sensitive data.

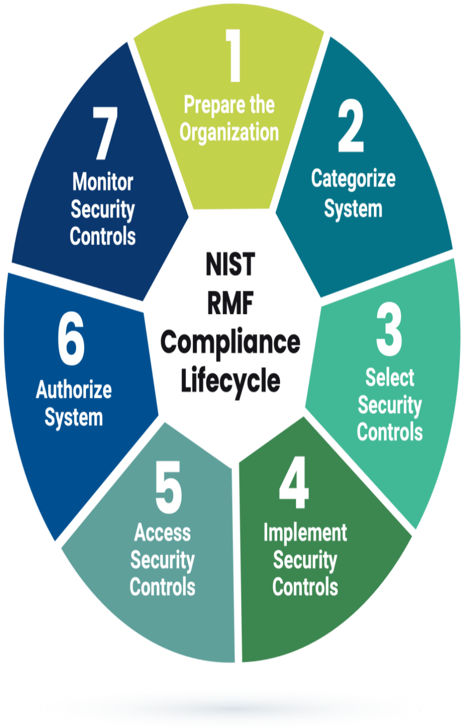
Contact & SOP Flowchart


Start
Identify Phishing attack
Has Personal Information been given
Yes
Let Manager Know what data has been compromised for mitigations
Contact Cat: Day time after hours & weekends
If not Available
Contact Misha: Mon - Fri, 9AM - 5PM AST Weekdays
If not Available
Contact Minka: Alternation with Misha & Weekends
Has the problem been solved within 48 hours or has been escalated further
no
Contact Percy
Contact Authorities of needed
Yes
Write an incident report with all the details of what has been affected.
Enact any recommended mitigation
no
Report the email as a Phishing scam to management and do not engage with the email

Note: This flowchart illustrates how management should be contacted when an attack is identified in accordance with contact section depicted above

Details of the Attack

There are many forms of attack that can plague the system(s) and network of Cat Box. For this example we shall take a look into an example of a threat called a ‘Phishing Attack’. A phishing attack can look many different ways, the one thing they all have in common is that they all ask for personal information or access to data through directly asking for it, or trying to get the victim to open a file or link. To take the necessary precautions, we will take a look at the NIST RMF (Risk Management Framework) cycle to prepare for this type of attack. The cycle goes as follows:



1. Identifying the network infrastructure.
2. Categorize systems - Based on importance and redundancy level.
3. Select the proper NIST RMF security controls (ie Configuration management).
4. Implementing security controls
5. Assessing the access of security controls & authorization.
6. Granting approval of an information system based on NIST. This may include risk assessment and determining vulnerabilities for operability.
7. Monitoring security controls for effectiveness, security breaches, performance metrics. This should help determine if the protocols implemented are suited for the network infrastructure and clients needs. (NIST 2023)

1. **Identifying the network infrastructure**: During this stage of the RMF (Risk Management Framework), we want to identify all the important data to the company. For Example, any important devices on the network that houses critical data, devices that manage the infrastructure of the network and have high levels of clearance to access the data, etc. This is where the preparation may begin.
2. **Categorize Systems**: At this stage categorizing the assets of the company in order of the level of importance and the level of affect the compromisation of the data would have against the company. Most valuable and vulnerable should be at the top of the priority list.
3. **Select Proper Security Control:** This stage involves choosing the best way to monitor the assets and their vulnerabilities in an effective way. Choosing the proper security control will allow the company to implement a monitoring system that allows an organization to understand the security state of the information over time and maintain the initial security authorization.
4. **Implementing Security Controls:** Implementing the selected security control involves setting the amount that the security will be monitoring the network. A security control that is more susceptible to change will need to monitor the network very frequently.
5. **Assessing the access of security controls & authorization:** Implementing security controls comes with its own set of risks, the main idea of this stage is for a senior official to make judgments based on the risks provided and to authorize the system being implemented.
6. **Monitoring security controls:** The final stage is to monitor the security controls and the possible risks to the network while the control is running.

Mitigation

Luckily Phishing attacks are easy to prepare for and train employees on how to identify when there could be a suspected phishing attempt. Ensuring employees are properly trained to be aware of emails, texts, or suspicious websites, asking for personal information. Conducting mock phishing scenarios where employees can raise their awareness of phishing scams. Preparation is key to preventing this type of attack, and to aid in that endeavor there are tools and programs that will also identify attempted phishing attacks. Finally, keeping all systems up to date and blocking untrusted or unsecure websites for devices that are a part of the infrastructure, will further protect the network from any other malicious attacks that include phishing attempts.

If an employee or user unfortunately provides sensitive information or data, then there are some mitigation processes that will help minimize any compromised data. Firstly following the SOP (Standard Operating Procedure), the employee who provided the information will need to update their user account information to deny further access from the attacker. Identifying any compromised data and isolating it from the system or infrastructure will help secure unaffected data from being compromised. After securing unaffected data and isolating compromised data, any further action would require management's authorization on how to handle the compromised data and how valuable/important the asset affected is.

Sample Letters

Dear Cat,

During the monitoring of the network activity of Box's servers, we have found some security concerns and some suspicious activity and believe it could use further escalation.

These are the samples of the activity amongst the network, as you can see there is an unusual amount of traffic heading into the network as well as unauthorized logs while checking the timestamp data.

Here are the proposed forms of mitigation used for this type of believed attack.

For further escalation and preventative measures, please advise on where to move forward, thank you for your time.

Sincerely,

SOC Analyst

Sample Letters (3rd Party)

Dear Misha or Minka F,

During the monitoring of the network activity of Box’s servers, we have found some security concerns and some suspicious activity and believe it could use further escalation.

These are the samples of the activity amongst the network, as you can see there is an unusual amount of traffic heading into the network as well as unauthorized logs while checking the timestamp data.

Here are the proposed forms of action for the believed type of attack.

For further escalation and preventative measures, please advise on where to move forward, thank you for your time.

Sincerely,

SOC Analyst

Work CIted

CISA Federal Government . (2021, November). Federal government cybersecurity incident and vulnerability ... - cisa. https://www.cisa.gov/sites/default/files/publications/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf

Computer Security Division, I. T. L. (n.d.-a). *About the RMF - NIST risk management framework: CSRC*. CSRC. https://csrc.nist.gov/Projects/risk-management/about-rmf

Brinkmann, M. (2019, September 7). *The Phishing Flow Chart - gHacks Tech News*. gHacks Technology News. https://www.ghacks.net/2010/02/11/the-phishing-flow-chart/

Quay-de la Vallee, H. (2022, March 16). *Prevention and Mitigation of Successful Phishing Attacks*. Center for Democracy and Technology. https://cdt.org/insights/prevention-and-mitigation-of-successful-phishing-attacks/