Generic Phishing Playbook

Version 1.0

Purpose

To help level-one SOC analysts provide an appropriate and timely response to a phishing incident

Using this playbook

Follow the steps in this playbook in the order in which they are listed. Note that steps may overlap.

Step 1: Receive phishing alert

The process begins when you receive an alert ticket indicating that a phishing attempt has been detected.

Step 2: Evaluate the alert

Upon receiving the alert, investigate the alert details and any relevant log information. Here is a list of some of the information you should be evaluating:

1. **Alert severity**
    - **Low**: Does not require escalation
    - **Medium**: May require escalation
      High: Requires immediate escalation to the appropriate security personnel
2. **Receiver details**
    - The receiver's email address
    - The receiver's IP address
3. **Sender details**
    - The sender's email address
    - The sender's IP address
4. **Subject line**
5. **Message body**
6. **Attachments or links**.

Note: **Do not** open links or attachments on your device unless you are using an authorized and isolated environment.

Step 3.0: Does the email contain any links or attachments?

Phishing emails can contain malicious attachments or links that are attempting to gain access to systems. After examining the details of the alert, determine whether the email contains any links or attachments. If it does, **do not** open the attachments or links and proceed to **Step 3.1**. If the email does not contain any links or attachments, proceed to **Step 4**.

Step 3.1: Are the links or attachments malicious?

Once you've identified that the email contains attachments or links, determine whether the links or attachments are malicious. Check the reputation of the link or file attachment through its hash values using threat intelligence tools such as VirusTotal. If you've confirmed that the link or attachment is **not malicious,** proceed to **Step 4**.

Step 3.2: Update the alert ticket and escalate

If you've confirmed that the link or attachment is **malicious**, provide a summary of your findings and the reason you are escalating the ticket. Update the ticket status to **Escalated** and notify a level-two SOC analyst of the ticket escalation.

Step 4: Close the alert ticket

Update the ticket status to **Closed** if:

- You've confirmed that the email does not contain any links or attachments
  or
- You've confirmed that the link or attachment **is not malicious.**

Include a brief summary of your investigation findings and the reason why you've closed the ticket.

Phishing Flowchart (Version 1.0)