Activity: Use a playbook to respond to an attack

Scenario

You are a level-one security operations center (SOC) analyst at a financial services company. Previously, you received a phishing alert about a suspicious file being downloaded on an employee's computer. After investigating the email attachment file's hash, the attachment has already been verified malicious. Now that you have this information, you must follow your organization's process to complete your investigation and resolve the alert.

Your organization's security policies and procedures describe how to respond to specific alerts, including what to do when you receive a phishing alert.

In the playbook, there is a flowchart and written instructions to help you complete your investigation and resolve the alert. At the end of your investigation, you will update the alert ticket with your findings about the incident.

Ticket ID	Alert Message	Severity	Details	Ticket status
A-2703	SERVER-MAIL Phishing attempt possible download of malware	Medium	The user may have opened a malicious email and opened attachments or clicked links.	Escalated

Ticket comments
The alert detected that an employee has downloaded and opened a malicious file from a phishing email. There is an inconsistency between the sender's email address ("76tguy6hh6tgftrt7tg.su'"), the name used in the email body ("Clyde West"), and the sender's name ("Def Communications"). In addition, the email body and subject line contained grammatical errors. The email's body also contained a password-protected attachment, "bfsvc.exe," which had been downloaded and opened on the affected machine.

The attachment had been investigated previously and was proven to be malicious. Furthermore, the alert severity is reported as medium. This ticket has thus been escalated to a level-two SOC analyst for further action.

Additional information

Known malicious file hash:
54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b

Email:
From: Def Communications <76tguyhh6tgftrt7tg.su> <114.114.114.114>
Sent: Wednesday, July 20, 2022 09:30:14 AM
To: <hr@inergy.com> <176.157.125.93>
Subject: Re: Infrastructure Egnieer role

Dear HR at Ingergy,

I am writing for to express my interest in the engineer role posted from the website.

There is attached my resume and cover letter. For privacy, the file is password protected. Use the password paradise10789 to open.

Thank you,

Clyde West
Attachment: filename="bfsvc.exe"

- Sruthi Sathishkumar

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.)