Phishing Incident Response

Project description

This simulation project puts the performer, **Maheswar Reddy Avula**, into the position of a Level 1 **SOC Analyst** for a financial services company. Responsibilities include using the Phishing Incident Response Playbook of the company to complete the investigation and take action on the SIEM Alert.

Review the phishing incident response playbook and alert

The Phishing Playbook instructions provide detailed, written instructions about each step represented in the flowchart.

The **Phishing Flowchart** provides a high-level overview and visual representation of the sequence of steps and substeps you'll take to respond to a phishing alert.

The **SIEM Aler**t is inserted below:

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.	**Open**

Ticket comments
Insert your comments here.

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"

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.	**Investigating**

Evaluating the alert

Following the 2nd step of the playbook, the alert is evaluated based on the following criteria and conclusions are drawn as follows:

1. Alert severity: The severity is medium. This means that the alert will probably require escalation to a level 2 analyst.

2. Sender details: The sender email is 76tguyhh6tgftrt7tg.su which originates from the su domain, which is a domain used commonly in cyber attacks due to its unregulated nature, because it was formerly used by the Soviet Union which was dissolved.

3. Receiver details: The attack seems to be a spear phishing attack that specifically targeted the HR department due to its nature of going through hiring emails.

4. Subject line: The subject is a reply, which is suspicious, the word engineer is misspelled as well.

5. Message body: The first line contains the company name misspelled. There are multiple grammatical errors present in the email body.

6. Attachments or links: The attachments are password protected with the password provided. The filename is bfsvc and the file extension is.exe which is an executable, not a document.

Determining whether the alert should be escalated

The **steps 3.1** and **3.2** of the playbook are followed and the email attachment is investigated through Virustotal. The following observations are made:

The sender's email address corresponds to a common domain used by threat actors. The multiple grammatical and spelling errors indicate that the email is not sent by a genuine applicant but a malicious actor.

The attachments are password protected, and the password is provided.

The file investigation proves the file to be a high severity trojan malware called Flagpro.

Based on the above, it is concluded that the email was indeed a malicious email sent with the intent of executing a spear phishing attack by a malicious actor.

Updating the alert ticket status

The email has been determined to be an attack after a thorough investigation, and hence, the ticket status of the alert is set to Escalated. Comments regarding the decision to escalate are also provided in the Ticket Comments.

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 sender's email address corresponds to a common domain used by threat actors (.su). ● The multiple grammatical and spelling errors indicate that the email is not sent ● by a genuine applicant but a malicious actor. ● The attachments are password protected, and the password is provided. ● The file investigation proves the file to be a high severity malware called Flagpro.

Summary

The email is investigated and acted upon as per the Phishing Incident Response Playbook. All tasks were successfully completed in accordance with the directions given by the organization.