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
Based on the alert, it was detected that an employee downloaded and opened a malicious file from a phishing email. Upon evaluating the alert ticket, I noticed some key factors. Firstly, there is an inconsistency between the sender's email address, "76tguy6hh6tgftrt7tg.su," and the name used in the email body, "Clyde West," as well as the sender's name, "Def Communications." Moreover, the email body and subject line exhibited grammatical errors, which are often red flags for phishing attempts. Additionally, the email contained a password-protected attachment named "bfsvc.exe," which was successfully downloaded and opened on the affected machine. Considering these findings, along with the confirmed knowledge of the file hash being malicious and the medium severity of the alert, I have decided to escalate this ticket to a level-two SOC analyst for further investigation and necessary actions.

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"

Yazeed

In this lab, I learned how to effectively respond to a phishing incident by following a playbook.

I gained the following skills:

- Evaluating alert details: I learned to analyze various elements such as alert severity, sender details, message body, and attachments or links to assess the legitimacy of a phishing alert.

- Assessing maliciousness: I gained knowledge about checking the reputation of links or file attachments using threat intelligence tools like VirusTotal to determine if they are malicious.

- Escalation decision-making: I understood the importance of considering multiple factors to decide whether to escalate a phishing alert for further investigation or close the ticket based on the findings.

- Documentation: I learned the significance of maintaining an incident handler's journal to record incident details and gather thoughts during the investigation. Additionally, I gained experience in updating the alert ticket with relevant information and reasons for escalation or closure.

Overall, this activity enhanced my incident response capabilities, critical thinking skills, and familiarity with phishing incident handling procedures.