Project

As a level-one Security Operations Center (SOC) analyst at a financial services company, I am investigating a phishing alert related to a malicious file downloaded on an employee's computer. After confirming the attachment's hash is malicious, I will follow our organization's playbook, which provides steps for handling such incidents. My investigation will include assessing the email details, documenting my findings, and updating the alert ticket with information about the phishing attempt and the actions taken.

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
An alert was triggered when an employee downloaded and opened a malicious file from a phishing email. The email showed inconsistencies: the sender's address, "76tguy6hh6tg@rt7tg.su," did not match the name "Clyde West" in the body, nor the sender name "Def Communications." It also contained grammatical errors and included a password-protected attachment, "bfsvc.exe," which is confirmed as malicious. With the alert severity rated as medium, I have escalated this ticket 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"