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 security alert has identified an employee who downloaded and opened a malicious file from a phishing email. An inconsistency in the sender's details, such as the email address "76tguy6hh6tgftrt7tg.su," the mentioned name "Clyde West," and the declared sender's name "Def Communications," raises suspicions. Grammatical errors in the email body and subject line add to the concern. The email included a password-protected attachment, "bfsvc.exe," which, upon investigation, has been confirmed as a known malicious file based on its hash. Given these findings and a medium severity rating of the alert, I have opted to escalate this ticket to a level-two SOC analyst for further investigation and appropriate action.

Additional information

Known malicious file hash:
54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b

Email:
From: Def Communications <76tguyhh6tgftrt7tg.su> <114.114.114.114>
Sent: Wednesday, March 20, 2024 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"