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 indicated that an employee accessed a suspicious file from a phishing email. Discrepancies were noted between the sender's email address ("76tguy6hh6tgftrt7tg.su"), the name used in the email ("Clyde West"), and the sender's claimed name ("Def Communications"). Grammatical errors were observed in both the email body and subject line. Additionally, the email contained a password-protected attachment named "bfsvc.exe," which was downloaded and opened on the affected device. Prior analysis of the file hash confirmed its malicious nature. The severity of the alert was classified as medium. Consequently, I opted to escalate this matter to a level-two SOC analyst for further investigation and 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"