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 identified that an employee accessed and opened a suspicious file from a phishing email. There are discrepancies between the sender's email address ("76tguy6hh6tgftrt7tg.su"), the name used in the email body ("Clyde West"), and the sender's claimed name ("Def Communications"). The email contained grammatical errors in both its body and subject line. Additionally, the email included an attachment named "bfsvc.exe," which was downloaded and opened on the affected device. Prior investigation of the file hash confirmed it as a known malicious file. The alert's severity was classified as medium. Based on these findings, I have escalated this issue 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 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"