Ticket ID	Alert Message	Severity	Details	Ticket status
A-2703	SERVER-MAIL Phishing attempt possible download of malware	Medium	Possible phishing attempt and malware download by a user.	Escalated

Ticket comments
An alert was triggered when an employee downloaded and opened a suspicious file from an email. Suspicious Indicators: Sender's email address: "76tguyhh6tgftrt7tg.su." Inconsistency between sender's name in the email body ("Clyde West") and the sender's name ("Def Communications"). Grammatical errors in the email body and subject line. Email contained a password-protected attachment, "bfsvc.exe," which was opened. Severity: Medium Action: The ticket was escalated to a level-two SOC analyst for further investigation.

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"