Alert Ticket

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
I got a notification when the user opened up a malicious attachment from an email. I have evaluated the email and spelling mistakes and inconsistencies within the email indicate that this is a phishing email. In the email, the sender calls themself “Clyde West”, but the email belongs to Def Communication. Moreover, there is a spelling mistake in subject line where “Engineer” is spelt as “Egnieer”. I have also evaluated the file hash of the attachment using VirusTotal and I have found out that this is known malware. Due to this, I have chosen to escalate this ticket further to Level-2 SOC Analyst to take further actions.

Additional information

Known malicious file hash:
54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b

Email:
From: Def Communications <76tguyhh6tgftrt7tg.su> <114.114.114.114>
Sent: Monday, October 16, 2023 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"