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
This is a phishing attempt caused by <76tguyhh6tgftrt7tg.su> <114.114.114.114> on Wednesday, July 20,2022 09:30:14 AM. The sender's is from "Def Communications" and the sender's name is "Clyde West" The mail's subject contains spelling errors and the mail's body contains grammatical errors. The phishing attempt is carried out to one of the HR at Inergy as he in search for a candidate to Infrastructure Engineer role. Using this info, the attempt is done to drop a malware name "bfsvc.exe" which is password protected "paradise10789". Using the file hash which is confirmed previously as malicious. Now, confirming the file in the link provided is malicious and it may cause severe damage, I chose this ticket must be escalated to a level two SOC analyst.

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"