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 phishing alert has been escalated due to multiple indicators of compromise. The file hash (54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b) is confirmed as malicious on VirusTotal. The sender email (`76tgyuyhh6tgftr7tg.su`) does not match the display name, and the subject contains grammatical errors, which are consistent with phishing attempts. The employee may have downloaded and executed the file, posing a high risk to business operations.

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"