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 alert concerns a phishing email sent from Def Communications <76tguyhh6tgftrt7tg.su> with a confirmed malicious attachment (hash: 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b). The email was directed to hr@inergy.com and purported to be an application for an engineer role.

I chose to escalate this ticket for the following reasons:

1. The sender's email address and domain are suspicious and do not correspond to any known or trusted entities.
2. The email contains grammatical errors and unusual phrases typical of phishing attempts.
3. The attachment is an executable file with a verified malicious hash, posing a significant threat to the recipient's system.

Next Steps:

1. Notify the affected user and advise them to avoid opening any further suspicious emails.
2. Isolate the affected machine to prevent further potential spread of malware.
3. Conduct a thorough scan and clean-up of the affected system.
4. Report the incident to senior SOC analysts for further investigation and potential reporting to external cybersecurity agencies.

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"