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
An alert of an employee who downloads a suspicious file with the hash(54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b) into the computer of the organisation.It was discovered that there is a mismatch between the sender email(Def Communications) and the name (Clyde West).Further Investigation revealed that the file is malicious because its hash has been flagged by 59 of 72 security vendors .It was also revealed that this file hash is known as the malware fragpro/fragtor. Which has been previously used by an advanced persistent threat actor agent.Oa!S1s However, The alert serenity is medium but with the above findings, i have escalated the ticket to level-two SOC analyst for further actions.

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"