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.	**Investigating**

Ticket comments
There was an alert of a severe mail phishing attempt sent to multiple users. The possible cause of this issue was of a downloadable software that began to download as soon as the email user open the set attachment. The sender in this occasion has different email that is not consistent, having different numbers and letters,"76tguyhh6tgftrt7tg.su". The said user who sending this email has the name Clyde West. The grammar in the file indicates that it was not well written and misspelled. The given attachment,"bfsvc.exe", should be a regular text file; however, on this occasion, the file has an exe, meaning that it is an executable file. Having previously investigated this incident in the previous exercise, it was found to be malicious. Therefore, I'm updating the alert ticket and escalating the ticket from medium severity. And notify a level two SOC analyst for further investigation

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"