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
Insert your comments here. A malicious file was downloaded and opened on an employee's device from a phishing email. This is seen by the differences between the sender's email address (76tguyhh6tgftrt7tg.su), the name used in the email body (Clyde West) and the sender's name (Def Communications). Both the email and subject line contain errors and there is a password-protected attachment - bfsvc.exe. This is the attachment that was downloaded and opened, compromising the machine. From further investigations, it is confirmed to be a known malicious file in the community. The alert severity is reported as a medium, therefore I choose to escalate this ticket to a L2 SOC analyst for further action.

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"