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
Alert ticket has been generated which severity is Medium. Based on the details, employee may have opened a malicious file which might contain Malware. The sender’s email address, "76tguy6hh6tgftrt7tg.su," conflicts with the name provided in the email body, "Clyde West," as well as the sender’s identified name, "Def Communications." Additionally, the email's subject line and body displayed grammatical mistakes. Within the email's content, there was an attached file named "bfsvc.exe," protected by a password, which was subsequently downloaded and accessed on the impacted device. Prior analysis of the file hash confirms its classification as a recognized malicious file. Based on the playbook, I decided to escalate the ticket to SOC L2 Analyst to handle this ticket.

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"