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 employee had downloaded and opened a harmful file from a phishing email, according to the alert. The sender's email address, "76tguy6hh6tgftrt7tg.su," the name Clyde West used in the email body, and the sender's name, "Def Communications," are inconsistent. Grammatical problems were present in both the email's subject line and body. The password-protected attachment "bfsvc.exe," which was downloaded and run on the impacted PC, was also included in the email's body. It has been established after looking into the file hash that it is a known harmful file. Additionally, a medium alert severity is reported. I decided to elevate this ticket to a level-two SOC analyst to take further action in light of these findings.

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"