Ticket ID	Alert Message	Severity	Details	Ticket status
A-2703	SERVER-MAIL Phishing attempt possible download of malware	Medium	The user might have inadvertently accessed a malicious email and interacted with its attachments or clicked on embedded links.	Escalated

Ticket comments
The alert indicates that an employee has accessed and opened a malicious file from a phishing email. Several inconsistencies were observed within the email: the sender's email address "76tguy6hh6tgftrt7tg.su," the name used in the email body "Clyde West," and the sender's name "Def Communications" do not align. Additionally, grammatical errors were present in both the email body and subject line. Notably, the email contained a password-protected attachment named "bfsvc.exe," which was downloaded and opened on the affected machine. Previous investigations of the file hash confirmed its status as a known malicious file. The severity of the alert was assessed as medium. Considering these findings, I have chosen to escalate this ticket to a level-two SOC analyst for further investigation and 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"