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 alert advised us that an employee downloaded a malicious file attachment from a phishing email. The sender is listed as “Clyde West” and the sender’s email as “76tguyhh6tgftrt7tg.su” with IP 114.114.114.114. The sender is listed as “Def Communications”. The employee who received the email was Inergy HR team. Many grammatical errors were found in the email and the email signature mentioned the following, Attachment: filename="bfsvc.exe". After entering the malicious file hash into VirusTotal, it has been deemed malicious and therefore, escalating this alert to SOC L2.

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"