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
The alert was triggered by a phishing email sent to hr@inergy.com containing a malicious attachment (bfsvc.exe). The attachment's file hash (54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b) was verified as malicious using VirusTotal. The ticket is escalated due to the following reasons: 1. The attachment is confirmed malicious, posing a significant risk of malware infection or data breach. 2. The sender's email address (<76tguyhh6tgftrt7tg.su>) is suspicious and inconsistent with the claimed identity, indicating a phishing attempt. 3. The email's grammatical errors and the use of a password-protected executable file further suggest malicious intent. The ticket has been updated to "Escalated" and a level-two SOC analyst has been notified for further investigation.

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"