Ticket ID	Alert Message	Severity	Details	Ticket status
A-2703	SERVER-MAIL Phishing attempt possible download of malware	High	The user may have opened a malicious email and opened attachments or clicked links.	Escalated

Ticket comments
After analyzing the ticket with caution and following the instructions of the phishing playbook, I decided to escalate the ticket. I noticed some incoherences in the email and after analyzing the attachment in VirusTotal I concluded that it was a malicious file and the email really was a phishing event. The phishing alert is legitimate because we can observe some critical points in the email. The sender email seems to be from a strange domain like a temporary email. The misspelling can be a second alert of fraud. Finally, if it's a resume in a spreadsheet file the attachment extension should not be from an executable.

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"