

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
<p>Firstly, the file type of the attachment, as indicated by the suffix “.exe” is a sign that this file is not a resume document, rather it is an executable file. The sender made multiple spelling and grammatical errors in the e-mail, which was not carefully worded - as is the typical behavior of a job applicant. Upon searching VlrusTotal for the file’s hash value, it was determined that the file is of malicious nature, and this this should be further examined. Escalation will be sent to Level 2 SOC analyst tema for further investigation.</p>

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 Inergy,

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"