

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>Alert was detected due to an employee downloading a malicious file from a phishing email. Email contained grammatical errors and inconsistent email address compared to name. IP address is suspicious. Instead of excel type/google spreadsheet file type, the link was sent as an executable. File was opened and has executed a malicious payload. Sourced information from VirusTotal as highly malicious.</p> <p>I have chosen to escalate the Ticket due to the nature of the file. This file could potentially compromise systems</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"