

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>The email contains an attachment .exe, which is an app that executes a trojan as the information we can see at virustotal using the hash.</p> <p>The email has some grammatical errors which makes us think about how reliable it is. Def communications looks anormal, because of “76tguyhh6tgftrt7tg.su” i dont think a document for an interview should have a pass or being encrypted.</p> <p>With these findings, I chose to escalate this ticket to a level-two SOC analyst to take further action.</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"