| 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 |
|---|
| I am escalating this alert because I believe that the email sent from the subject header, the body of the email, and the attached file all show signs of this being a phishing email. There are grammatical errors in the body and subject header, as well as the email sent; it doesn't look like a normal email. I've confirmed that the file hash on VirusTotal indicates that the attachment sent and downloaded is indeed malicious. |

## 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"