# Alert Ticket

| 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 |
|---|
| The file attachment was already identified as malicious using the VirusTotal website tool, known as a malicious file hash: 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b<br>Grammar errors detected at the Subject line as on the body text.<br>The sender's email address doesn't match with the name on the signature.<br>The IP address it is suspicious due to the sequence.<br><br>This incident must ESCALATED according to the playbook to further processing and actions. |

## Additional information

**Known malicious file hash**: 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b

**Email Template**:

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 Engineer 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"