| 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 |
|---|
| -HR employee receive a job inquisition email with an attachment protected with the password **paradise10789**<br>-Said attachment triggered the IDS when several unauthorized files were downloaded.<br>-Email appears to be safe on the surface but several spelling errors and a suspicious email address mark it as a potential phishing email.<br>-The body of the email claims their name is **Clyde West**, however the email is from the domain **'Def Communications'** from the actual email address **76tguyhh6tgftrt7tg.su.**<br>-The SHA256 file hash is a match for a known trojan virus.<br>-According to the playbook given, this ticket will be escalated and sent to a SOC L2 analyst for further inspection. |

## 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"