| Ticket ID | Alert Message | Severity | Details | Ticket status |
|---|---|---|---|---|
| A-2703 | SERVER-MAIL Phishing attempts possible download of malware | Medium | The user may have opened a malicious email and opened attachments or clicked links. | Escalated |

| Ticket comments |
|---|
| The alert indicated that an employee had downloaded and opened a malicious file from a phishing email. There was an inconsistency noted between the sender's email address, "76tguy6hh6tgftrt7tg.su," the name used in the email body, "Clyde West," and the sender's stated name, "Def Communications." Additionally, the email body and subject line exhibited grammatical errors. The body of the email contained a password-protected attachment named "bfsvc.exe," which was both downloaded and opened on the affected machine. A prior investigation of the file hash confirmed its status as a known malicious file. The severity of the alert has been classified as medium. Based on these findings, I have decided to escalate this ticket to a level-two SOC analyst for further action. |

## 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"