| 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 |
|---|
| Received a phishing alert about a suspicious file being downloaded on an employee's computer. As per my evaluation, sender's email address contains <76tguyhh6tgftrt7tg.su> that doesn't look like a valid mail ID and also the email body and subject line contain a lot of grammatical errors and the name mentioned after thank you statement is very different from sender's name in the email address. I have marked the severity as "Medium" and this alert may need further escalation. The email body includes a password protected attachment file name "bfsvc.exe" that was previously downloaded and opened on the affected machine. A malicious file has been detected. |

## 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"