| **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 system alert has identified that an employee downloaded and accessed a harmful file from a phishing email. The email sender's name, "Def Communications," does not match the sender's email address, "76tguy6hh6tgftrt7tg.su," and the name used in the email body, "Clyde West." The email's subject line and body contained grammatical errors. Upon opening the email attachment, "bfsvc.exe," which was password-protected, the affected computer was compromised. The file hash has been previously investigated and confirmed to be malicious. The alert has been classified as medium severity, leading me to escalate the issue to a level-two SOC analyst for further investigation. |

### **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"