| **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. | **Investigating** |

| **Ticket comments** |
| --- |
| The alert system detected a phishing attempt via a server email that may contain malware. The user opened the malicious email, accessed the attachments, and clicked on the embedded links. Upon reviewing the email, inconsistencies were observed in the sender's name, as well as grammatical and spelling errors in the subject line and body of the email. Additionally, the attached file had a suspicious extension.  This issue has been escalated due to its potential impact on the company's security, and its severity has been categorized as medium. As a first response, I immediately reported the incident to the Level 2 SOC analyst for further investigation and 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"