| **Ticket ID** | **Alert Message** | **Severity** | **Details** | Escalated |
| --- | --- | --- | --- | --- |
| 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. | **Open** |

| Phishing alert identified from suspicious sender impersonating a legitimate entity.  The alert is escalated due to the following: - The attached file 'bfsvc.exe' was confirmed malicious via its SHA256 hash (54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b), flagged by 48/73 VirusTotal vendors. - The sender’s email address does not match the claimed name and domain. - The email contains grammatical errors and uses social engineering by including a password-protected file to evade detection. |
| --- |
| Insert your comments here. |

### **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"