|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **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** |
| * Initial evaluation indicates a medium severity alert. It happened due to a possible phishing attempt email. * The email is received by HR department IP: 176.157.125.93, and sent by unknown user with IP address: 114.114.114.114 * The email itself doesn’t look suspicious, but the file that attached to the email has malicious file hash: 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b. * It seems the user may have opened the attachment. * Additionally, the sender’s details and the password protected attachment raise suspicions. * This alert is being escalated to determine the extent of the potential compromise and to take appropriate 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"