| **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** |
| --- |
| When investigating this information, it was revealed that this letter is a phishing attack, since the letter contains clear evidence of this, such as:  1. Mismatch between the name and mailing address of the sender  2. Fake sender IP address  3. Grammatical errors in the letter  4. Attached file in .  exe which is unsafe and incorrect from the point of view of the sender's letter.  Based on this, measures were taken to increase the danger level of the file, since this attachment may pose a great danger to the organization’s data. The IP address, name, and postal address of the sender were also recorded. The investigation also introduced network traffic analysis systems, such as tcpdump, to confirm that data was not being sent anywhere outside the organization. The system was also scanned by VirusTotal, as was the hash file provided by the threat detection system. |

### **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"