| **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** |
| --- |
| * Initial evaluation indicates a medium severity alert. We received this alert due to a possible phishing attempt, and the user's interaction with the email is concerning. * The email received by the user, as detailed in the Additional Information, appears suspicious. The email comes from an unverified sender and contains a password-protected attachment. While the email itself may not exhibit typical red flags, the attachment's malicious nature is confirmed with a known malicious file hash. * The user interaction timeline indicates that the suspicious attachment was indeed opened, potentially leading to the execution of a malicious payload on the user's computer. * The known malicious file hash is "54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b," which has been verified as malicious. This information has led to the conclusion that the email attachment was indeed malicious. * Additionally, the sender's details and the password-protected attachment raise suspicions, indicating the need for further investigation. * 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"

### **Additional Notes:**

The evaluation of this alert suggests that it should be escalated for further investigation. The user's interaction with the email attachment, the suspicious sender's details, and the verified malicious file hash raise concerns about a potential security incident. Further analysis and containment are necessary to mitigate any potential risks.