| **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** |
| --- |
| The IDS triggered an alert to a possible phishing email attempt containing a file download. Review of the suspected email showed multiple discrepancies in it’s format such as the email address “76tguyhh6tgftrt7tg.su” not matching neither the sender of the email “Def Communications” or the name listed in the email body “Clyde West”. Other discrepancies include typos, misspellings and grammatical mistakes in both the subject line and email body. The file format of the attached file is also not one traditionally used for a resume or cover letter (“.exe” extension on the file versus the common “.doc” or “.pdf” extensions). The attached file was opened and downloaded to the user’s machine. Previous investigation of the file hash confirms it is malicious (trojan malware). With the severity alert listed as medium and a known malicious file having been downloaded and opened this ticket is being escalated to a level-two SOC analyst for further investigation. |

### **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"