|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **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 file attached is an executable (.exe) which is a program, email address seems suspicious, the ip address 114.114.114.114 is marked as suspicious on virustotal coming from china (see URL https://www.virustotal.com/gui/ip-address/114.114.114.114/detection). Furthermore, if you look at the email communication you will see spelling errors and grammatical mistakes.  Th exe file seems malicious when checking the hash (see URL <https://www.virustotal.com/gui/file/54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b/details>) you will see that it has a high score which means that many vendors identify this as malicious, this ticket should be escalated to SOC Level 2 to further investigate. |

### **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"