|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **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 alert detected that an employee had downloaded and opened a malicious file from a phishing email. There appears to be an inconsistency between the sender’s email address and the name used in the email body (“76tguyhh6tgftrt7tg.su” and “Clyde West”) and the sender’s name being “Def Communications.” Additionally, there seems to be grammatical errors in both the body of the email and the subject line. Furthermore, the email contained a password-protected attachment, “bfsvc.exe,” which was downloaded and opened on the affected machine. This file hash has been previously identified as a known malicious file, so the alert severity will be labeled as medium. In conclusion, I chose to escalate this ticket to a level-two SOC analyst for further review. |

### **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"