|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **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 the employee downloaded and opened malicious content from a phishing email. There are inconsistencies between the sender’s email address “76tguyhh6tgftrt7tg.su” and the name “Clyde West”. In the body and subject line there were many grammatical errors. The email contained a file that was password protected inside the body, “filename="bfsvc.exe"” which was downloaded and opened on the affected machine. Having investigated the file hash, it is confirmed to be a malicious file. The alert severity is medium with these findings I chose to escalate this ticket to level two SOC analyst to take further 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"