|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **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 message detected a phishing attempt and possible download of malware. The investigation of the email shows that there is an inconsistency about the sender. Sender named as “Def Communication” uses an email address without the company’s extension “76tguyhh6tgftrt7tg.su” with an IP address “114.114.114.114”, and senders name was written in the end of email as “Clyde West”. The email and subject contains grammatical errors. The email contains a password-protected file named “bfsvc.exe” which was downloaded and opened on the affected machine. Following an earlier investigation of the file hash, it is confirmed to be the known malicious file. The severity of the alert is indicated as medium. As a result of all the findings, I decided to escalate this ticket to an L2 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"