|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **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** |
| Insert your comments here.  Based on the notes and the scenario, the alert indicates that an employee downloaded and opened a malicious file received through a phishing email. The sender’s email address, “76tguy6hh6tgftrt7tg.su,” did not match the displayed sender name, “Def Communications,” or the name referenced in the email body, “Clyde West,” creating clear signs of impersonation. Both the subject line and message body contained multiple grammatical errors, further suggesting the email’s suspicious nature. The message included a password-protected attachment named “bfsvc.exe,” which the employee downloaded and executed on their workstation. Upon review, the file hash was confirmed to match known malware, validating the attachment's malicious nature. The alert was classified as medium severity, and based on the findings, the incident was escalated to a Level 2 SOC analyst for further investigation and remediation. |

### **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"