|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **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. | **Open** |

|  |
| --- |
| **Ticket comments** |
| **Incident Summary:**   * The phishing email was designed to impersonate a job applicant. * It contained a password-protected malicious attachment (bfsvc.exe). * The sender’s email address (76tguyhh6tgftrt7tg.su) appears suspicious and does not align with legitimate applicants.   **Reason for Escalation/Closure:**   * The file hash has been verified as **malicious** using VirusTotal. * The email originated from an untrusted domain (.su), often linked to phishing attempts. * The message body contains **grammatical inconsistencies**, a common trait in phishing campaigns. * Given the **medium severity**, the phishing attempt has been mitigated by blocking the sender and attachment. * No further escalation required, updating the ticket to **Closed**. |

### **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"