|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **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. | Closed |

|  |
| --- |
| **Ticket comments** |
| Insert your comments herAfter a thorough investigation, this alert ticket has been escalated due to the following findings:   1. **Confirmed Malicious Attachment**: The file bfsvc.exe, attached to the phishing email, was verified as malicious based on its SHA256 hash (54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b). 2. **Suspicious Sender Details**: The email sender’s address (76tguyhh6tgftrt7tg.su) and IP address (114.114.114.114) indicate possible spoofing or impersonation, commonly associated with phishing attempts. 3. **Indicators of Phishing**: The email contains several red flags, including grammatical errors and a prompt to open a password-protected attachment, suggesting a social engineering attempt. |

### **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"