|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **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 email is probably a phishing email sent to gain access to the company’s systems, since it has a known malware file attached to it, as confirmed by the hash value and name of the file ‘bfscv.exe’. Not only that, but the sender’s email also ‘76tguyhh6tgftrt7tg.su’ and IP are very suspicious, since the name ‘Clyde West’ is inconsistent with it, as well as the name ‘Def Communications’. Also suspicious are the grammatical mistakes, which usually are strong indicators of a phishing attempt. If the user opens the attachment is recommended to scan the network for malicious activity. Based on all this evidence, and the ‘medium’ severity of the incident, I proceed to escalate it. |

### **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"