|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **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 phishing email contained grammar errors ("writing for to express"), which is a common indicator of phishing attempts. * The mismatch between the sender's email address ("76tguyhh6tgftrt7tg.su") and the displayed name ("Def Communications") is suspicious. * The attachment "bfsvc.exe" is an executable file, which is uncommon for resume submissions and is a red flag for potential malware. * The malicious file hash provided in the additional information matches the hash of the attachment, confirming the malicious nature of the file.   Given the high severity of the alert, the suspicious nature of the email, and the confirmed malicious attachment, immediate escalation and further investigation are warranted. |

### **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"