|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **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** |
| An employee downloaded and opened a dangerous file from a phishing email, according to the alert. The email content and subject line featured grammatical problems, and the sender's name, "Def Communications," was inconsistent with the email address, "76tguy6hh6tgftrt7tg.su," and the name used in the body, "Clyde West." The password-protected attachment "bfsvc.exe," which was included in the email's body, was also downloaded and run on the compromised computer. The file hash has been examined previously, and it has been determined to be a known harmful file. Additionally, a medium alert severity rating has been reported. I decided to elevate this ticket to a level-two SOC analyst in order to take additional action in light of these findings. |

### **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"