| **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. | **Investigating** |

| **Ticket comments** |
| --- |
| An alert has been triggered indicating that an employee has downloaded and opened a malicious file from a phishing email. The email raises suspicions due to inconsistencies found within it. The sender's email address, "76tguy6hh6tgftrt7tg.su," differs from the name mentioned in the email body, "Clyde West," as well as the sender's name, "Def Communications." Additionally, the email contains grammatical errors in both the body and subject line. Notably, the email includes an attachment named "bfsvc.exe," which is password-protected and was successfully downloaded and opened on the affected machine. Our prior investigation of the file's hash confirms that it is a known malicious file. The alert severity has been classified as medium. Based on these findings, I have decided to escalate this matter to a level-two SOC analyst for further investigation and necessary action. |

### **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"