| **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 a malicious file from a phishing email. There is an inconsistency between the sender's email address “76tguy6hh6tgftrt7tg.su’”, the name used in the email body “Clyde West”, and the sender’s name, “Def Communications.” The email body and subject line had grammar errors. The email body also contained a password-protected attachment, “bfsvc.exe,” which was downloaded and opened on the affected machine. After investigating the file hash, it is confirmed to be known as a malicious file. The alert severity is reported as medium, with these findings I chose to escalate this ticket to a level two SOC analyst to take further 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"