| **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** |
| --- |
| * Alert notice due to possible phishing attack by email with an attachment file has been downloaded by an employee with initial evaluation a medium severity alert. * The email received by the user, as detailed information, appears to be suspicious mail with an unverified sender. there is inconsistency between the email address and the name of the sender. * The email body has grammatical errors and there is a password to open a file called bfsvc.exe, needed for further investigation. * The know malicious file hash is “54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b” and an attachment file called “bfsvc.exe”. * The alert is being escalated to determine the extent of potential compromise and to take appropriate 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"