| **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** |
| --- |
| As per the playbook I have investigated the email and found it to be a Phishing email that includes malware. With a name of “Def Communications” and an address of “76tguyhh6tgftrt7tg.su” along with the name “Clyde West” indicating a fake email.  The email is also full of misspellings and grammar errors such as “I am writing for to express my” and claims to be a resume and cover letter but it is a .exe file named “bfsvc.exe”.  I investigated the file hash on VirusTotal and found it to be malware, given these factors, the severity rating and the fact the employee has downloaded and opened the malware, I have escalated this ticket. |

### **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"