| **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** |
| --- |
| This email is suspicious and contains a malware executable file. The email claims it is a resume, but it is an executable file. The sender’s email is suspicious and the grammatical errors indicate this could be phishing. Virustotal confirms the attachment is a malware file. The employee has downloaded this file and steps need to be taken to erase the malware and rectify any damage. |

### **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"

Who caused the incident?

* A “Clyde West” sending a phishing email

What happened?

* A suspicious email was received with a suspicious attachment, .exe file

When did the incident take place?

* Wed. July 20, 2022 at 9:30:14 AM

Where did the incident occur?

* Via email

Why did it happen?

* A malicious phishing email, we are unclear why but likely to infiltrate our computers / network.