| **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 is an alert generated from a phishing mail that contains a malicious file called "bfsvc.exe", we can categorize this as trojan. This event occurred due to an email received by the recruitment department from one of the supposed candidates interested in starting work as an engineer. We can see as well that the attacker has a strange domain mail and direct IP to contact de HR Recruiter; **From: Def Communications <76tguyhh6tgftrt7tg.su> <114.114.114.114>**  The main reasons we escalated the ticket are, first, the content within the link/email, and then the malicious files they contain. |

### **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"