|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **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** |
| A phishing attack lead to malicious files being downloaded and executed on an employee's computer and an alert being triggered.  The email used in this attack has some red flags. There are inconsitencies between the sender name, sender email address, and sender signed name. There are also grammatical errors in the email.  I have determined that the file used in this attack was malicious and the details for this evaluation is in my incident handler's journal. The file hash matches a known malcious file using the tool VirusTotal. The phishing playbook says to escalate the ticket in the event of a phishing attack so I have done so. |

### **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"