|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **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** |
| Here are the comments after following the Phishing Incident Response Playbook:   * Evaluating the alert as “Medium”, this incident may require escalation. * Sender details: the sender’s email address is 76tguyhh6tgftrt7tg.su, and the IP address is 114.114.114.114. * Message: the email has the indicators of a phishing attempt. The subject line and body contain grammatical errors. * Attachments: the email has an attachment that is protected by a password (paradise10789) to probably avoid being initially detected by any antivirus. The file is an executable (bfsvc.exe). * After investigating the suspicious file attached in the email, it’s confirmed that it’s a malicious file.   Here are the 5 W’s:   * Who: the email with the attached malicious file caused the incident. * What: after opening the attached file, the trojan was installed in the computer, compromising the security of the organization. * When: the incident occurred when the email was received. * Where: the incident occurred in the computer of the employee. * Why: it happened because the file attached was opened.   Since the file received is confirmed to be malicious, and it was opened, this ticket status will be changed to “Escalated” according to step 3.2 of the Phishing Incident Response Playbook. |

### **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"