|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **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** |
| * The attachment has been verified as malicious through its file hash. * The attachment's hash is 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b. * The sender's email address and IP address are not legitimate Ingergy addresses. |

### **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"

**Reasons for escalation**

* The attachment is known to be malicious.
* The sender is likely not a legitimate Ingergy employee.
* The user may have opened the attachment and is at risk of infection.

**Next Steps**

* The level-two SOC analyst will investigate the incident further and determine the appropriate next steps.
* The user will be notified of the phishing attempt and advised to not open any attachments or click on any links in emails from unknown senders.
* The user's computer will be scanned for malware.
* The organization's security awareness training will be updated to include information about phishing attempts.