|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **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 alert was triggered due to a suspicious email received by a user in the HR department. * The email originated from an unknown sender with IP address 114.114.114.114 and was received by the target system with IP 176.157.125.93 * Although the body of the email appeared benign, the attached file was found to have a **known malicious hash**. 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b. * The attachment was password-protected, which is a common evasion tactic in phishing campaigns. * It appears that the user **may have opened** the attachment, though further validation is required. * Indicators of compromise and suspicious metadata warrant deeper investigation. |

### **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"

Actions Taken:

* Alert reviewed and categorized per SOC playbook.
* Attachment hash verified as malicious through internal threat intelligence sources.
* Case escalated to Tier 2 SOC / Incident Response for:
  + Full endpoint analysis
  + Assessment of user interaction
  + Investigation of potential lateral movement or data compromise

Next Steps:

* Await Tier 2 investigation results.
* If confirmed, initiate containment and remediation measures, including possible password resets, email purge, and IOC blocks.