| **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** |
| --- |
| **Brief description of the alert and what happened:**  An employee received an email from an external sender impersonating a job applicant. The email included a password-protected attachment (bfsvc.exe) and asked the recipient to use a specific password to open it. The file hash of the attachment matches a known malicious file per our threat intelligence check.  **2–3 reasons why this alert was escalated:**  **Confirmed Malicious File:** The attachment hash 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b is listed as malicious based on a VirusTotal hash check (confirmed prior to initiating this response).  **Phishing Indicators Present:** There are several hallmarks of phishing:   * + The sender email and domain 76tguyhh6tgftrt7tg.su are suspicious and unrelated to any known entity.   + The email body contains grammatical errors and awkward phrasing (e.g., "writing for to express," "from the website").   + The subject line “Infrastructure Egnieer role” contains a misspelling, which is commonly used in phishing.   **Malicious Attachment Methodology:** The attachment is an .exe file—an executable—which is highly unusual for a job application. Additionally, the file is password-protected, which is a known tactic used to bypass email security filters. |

| 5 W's Summary (For SOC Documentation/Journal Entry) | | | |
| --- | --- | --- | --- |
| **Who caused the incident?**  The external sender impersonating a job applicant: Clyde West (email: Def Communications <76tguyhh6tgftrt7tg.su>).  **What happened?**  A phishing email with a malicious executable file (bfsvc.exe) was sent and possibly opened by a user. The file was confirmed as malicious by hash.  **When did the incident take place?**  Wednesday, July 20, 2022, at 09:30:14 AM.  **Where did the incident occur?**  Email received by <hr@inergy.com> at IP 176.157.125.93.  **Why did it happen?**  An attacker attempted to distribute malware via a phishing email, possibly aiming to infect the system or steal credentials/data through the malicious .exe file. | | | |
|
|
|
|

### **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"