# Alert Ticket

## Step 1: Receive Phishing Alert

We’ve received the alert:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **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. | Investigating |

|  |
| --- |
| **Ticket comments** |
| Insert your comments here. |

### **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"

## Step 2: Evaluate the alert

1. **Alert Severity: High – requires immediate escalation**
2. **Receiver details:** [hr@inergy.com](mailto:hr@inergy.com) 176.157.125.93
3. **Sender details:** 76tguyhh6tgftrt7tg.su 114.114.114.114
4. **Subject Line:** Re: Infrastructure Egnieer role
5. **Message Body:** 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
6. **Attachments/links:** filename=”bfsvc.exe” KNOWN MALICIOUS FILE

## Step 3.0: Does the email contain any links or attachments?

Yes -> Proceed to step 3.1

## Step 3.1: Are the links or attachments malicious?

Yes, VirusTotal confirms this, also spyshelter.com states that bfsvc.exe is the Boot File Servicing Utility in Windows Operating Systems, however sender should not be sending an exe file.

## Step 3.2: Update the alert ticket and escalate

The Sender is sending an email to HR to supposedly apply for a position within the company. Generally when people are sending resumes, they would send a pdf or a docx file, not an executable which would install a program. Since this file is not a .docx or .pdf file, it is masquerading as a legitimate Boot File, but it is most likely a Trojan, according to spyshelter. Legitimate Boot Files already exist on a user’s system and should never be updated by a third party, but rather by a verified vendor such as Microsoft for Windows.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Ticket ID** | **Alert Message** | **Severity** | **Details** | **Ticket status** |
| A-2703 | SERVER-MAIL Phishing attempt possible download of malware | High | The user may have opened a malicious email and opened attachments or clicked links. Attachment is a malicious file (Trojan). Must confirm whether user downloaded this file and attempted to open it as their workstation would now be infected (and possibly others within the network). | Escalated |

## Step 4: Close the alert ticket

This email should be escalated until we either determine that no file was downloaded and executed; or that the user’s machine was quarantined/isolated, no other systems infected via lateral movement, we perform a RAM dump to keep the evidence, and then we restore the workstation to a previous snapshot before the user downloaded the file.