|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Ticket ID** | **Alert Message** | **Severity** | **Details** | **Ticket status** |
| A-2703 | Malware Download Attempt | High | User might’ve opened a phishing email and clicked or downloaded a file. The email had a weird sender and a password-protected attachment that ended up being malicious. | **Escalated** |

|  |
| --- |
| **Ticket comments** |
| The alert showed that an employee downloaded and opened a sketchy file from a phishing email. The sender’s info didn’t match, the email address was “76tguy6hh6tgftrt7tg.su,” but it said it was from “Def Communications” and signed “Clyde West.” The message had a bunch of grammar issues and included a password-protected attachment named bfsvc.exe. After checking the file hash, it was confirmed to be a known malicious file. Since it’s verified bad, I escalated this to a Level-2 SOC analyst to handle containment and 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"