Phishing Incident Ticket 2024-12-18 #2

Globe Sistemas - Av. Libertador Jardin America

| Ticket ID | Alert Message | Gravity | Details | Ticket Status |
| --- | --- | --- | --- | --- |
| A-2703 | SERVER-MAIL Phishing attempt possible malware download | Half | The user may have opened a malicious email and opened attachments or clicked on links. | Escalado |

| Ticket Comments |
| --- |
| The alert detected that an employee downloaded and opened a malicious file from a phishing email.  There is an inconsistency between the sender's email address “76tguy6hh6tgftrt7tg.su'”, the name used in the body of the email “Clyde West”, and the sender's name, “Def Communications”.  The email body and subject line contained grammatical errors. The email body also contained a password-protected attachment, “bfsvc.exe,” which was downloaded and opened on the affected machine.  After having previously investigated the file hash, it was confirmed that this is a known malicious file. Additionally, the alert severity is reported as medium. With these findings, I decided to escalate this ticket to a level two SOC analyst for further action. |

### Additional information

Known Malicious Hash File:

54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b

Email :   
From: Def Communications <76tguyhh6tgftrt7tg.su> <114.114.114.114>

Sent: Wednesday, December 16, 2024 09:30:14 AM

To: <hr@sinergia.com> <176.157.125.93>   
Subject: Re: Infrastructure Egnieer role

Dear HR at Sinergy,   
  
I am writing 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"