Ticket de Incidente de Phishing 2024-12-18 #2

Globe Sistemas - Av. Libertador Jardin America

| ID Ticket | Mensaje de Alerta | Gravedad | Detalles | Estado del Ticket |
| --- | --- | --- | --- | --- |
| A-2703 | SERVER-MAIL Intento de phishing posible descarga de malware | Medio | Es posible que el usuario haya abierto un correo electrónico malicioso y haya abierto archivos adjuntos o hecho clic en enlaces. | Escalado |

| Comentarios del Ticket |
| --- |
| La alerta detectó que un empleado descargó y abrió un archivo malicioso de un correo electrónico de phishing.  Existe una inconsistencia entre la dirección de correo electrónico del remitente “76tguy6hh6tgftrt7tg.su’”, el nombre utilizado en el cuerpo del correo electrónico “Clyde West”, y el nombre del remitente, “Def Communications”.  El cuerpo del correo electrónico y la línea de asunto contenían errores gramaticales. El cuerpo del correo electrónico también contenía un archivo adjunto protegido con contraseña, “bfsvc.exe”, que se descargó y abrió en la máquina afectada.  Después de haber investigado previamente el hash del archivo, se confirmó que se trata de un archivo malicioso conocido. Además, la gravedad de la alerta se informa como media. Con estos hallazgos, decidí escalar este ticket a un analista de SOC de nivel dos para que tome más medidas. |

### Información Adicional

Archivo Hash malicioso conocido :

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 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"