| **Identificación del billete** | **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. | **Escalated** |

| **Comentarios de entradas** |
| --- |
| 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**

**Hash de archivo malicioso conocido** : 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b

**Correo electrónico** :   
De: Def Communications <76tguyhh6tgftrt7tg.su> <114.114.114.114>

Enviado: miércoles, 20 de julio de 2022 09:30:14

Para: <hr@inergy.com> <176.157.125.93>   
Asunto: Re: Rol de Egnieer en Infraestructura

Estimado RR.HH. de Ingergy:   
  
Le escribo para expresar mi interés en el puesto de ingeniero publicado en el sitio web.   
  
Adjunto mi currículum y carta de presentación. Por cuestiones de privacidad, el archivo está protegido con contraseña. Utilice la contraseña paradise10789 para abrirlo.   
  
Gracias,   
  
Clyde West

Archivo adjunto: filename="bfsvc.exe"