| **ID del ticket** | **Mensaje de alerta** | **Gravedad** | **Descripción** | **Estado del ticket** |
| --- | --- | --- | --- | --- |
| A-2703 | SERVER-MAIL Intento de phishing, posible descarga de malware | Media | El usuario puede haber abierto un correo electrónico malicioso, archivos adjuntos o enlaces al hacer clic en ellos. | **Escalado** |

| **Comentarios sobre el ticket** |
| --- |
| La alerta detectó que un empleado descargó y abrió un archivo malicioso desde un correo electrónico de phishing. Hay 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 el asunto contenían errores gramaticales. El primero también contenía un archivo adjunto protegido con contraseña, “bfsvc.exe”, que se descargó y abrió en el equipo afectado. Habiendo investigado previamente el hash del archivo, se confirma que es un archivo malicioso conocido. Además, la gravedad de la alerta se reporta como media. Con estos hallazgos, elegí elevar este ticket a un analista de SOC de nivel 2 para tomar 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 a.m.

Para: <hr@inergy.com> <176.157.125.93>  
Asunto: Re: Puesto de ingenero de infraestructura

A la atención del Departamento de Recursos Humanos de Ingergy:  
  
Me dirijo a ustedes para por expresar mi interés por el puesto de ingeniero publicado en su sitio web.  
  
Se adjunta mi currículum y carta de presentación. Por motivos de privacidad, el archivo está protegido con contraseña. Utilice la contraseña paradise10789 para abrirlo.   
  
Gracias,  
  
Clyde West

Archivo adjunto: filename="bfsvc.exe"