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

|  |
| --- |
| **Comentarios sobre el ticket** |
| * **Who**: ¿Quién causó el incidente?: Grupo de hackers Eticamente Cuestionables. * **What**: ¿Qué sucedió?: Un incidente de seguridad “Ransomware”   **When:** ¿Cuándo ocurrió el incidente?: miércoles, 20 de julio de 2022 09:30:14 a.m.   * **Where:** ¿Dónde ocurrió el incidente? : En la plantilla de **ticket Alerta**   **Why:** ¿Por qué ocurrió el incidente?: El incidente ocurrió por que Hackers éticamente cuestionables, lograron acceder a los correos de la empresa mediante ataque phishing. Después de obtener acceso, los atacantes lanzaron un correo electrónico contra el usuario [hr@inergy.com](mailto:hr@inergy.com) ofreciendo interés por el puesto de la plaza “Ingenero de infraestructura”. La motivación de los atacantes se desconoce, ya envían solamente en el adjunto un archivo de nombre filename="bfsvc.exe" aparente Ransomware. |

**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 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"