|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **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. | **Elevado** |

|  |
| --- |
| **Comentarios sobre el ticket** |
| El Archivo se clasifico como malisioso ya que se comprobo su hash, la direccion de correo electronico, la IP y el archivo adjunto.  Se observo errores gramaticales en el correo electronico.   El Hash se comprobo con Virus Total, una pagina web que ayuda a recopilar informacion de la comunidad y determino que aproximadamente el 90% de los provedores lo calificaron como malware.  La dirección de correo electronico parece ser absurdo o inclusive inventado.  La direccion IP se comprobo con virus total y solo 2 proveedores lo calificaron como peligroso, esto puede ser a que es un VPN para evitar que rastreen de donde se origina el ataque.  Como el Archivo se abrio en un equipo afectado y es una amenza clasificado como nivel medio, decidi elevar el ticket a un analista SOC de nivel 2 para que continue con la investigación. |

**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"