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.	**Escálado**

Comentarios sobre el ticket
Inserta tus co Who? Un hacker a enviado un correo phishing. What? El empleado a descargado el archivo y se instaló. When? miércoles, 20 de julio de 2022 09:30:14 a.m Were? En la oficina Why? Descargó el fichero de nombre bfsvc.exe El correo electrónica contenía un fichero malicioso. Se decide elevar el ticket al analista Soc del nivel 2

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"