

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

Comentarios sobre el ticket
<p>La alerta mando que no es una pagina si no que es un archivo malisioso del tipo ejecutable , además que el usuario que lo envio viene de un host de correo bastante sospechoso "76tguyhh6tgftrt7tg.su" Habiendo investigado previamente el le hash, es una estafa rmed para ser un malicioso conocido le. Además, se informa de la gravedad de la alerta como medio. Con estos ndings, elegí escalar este boleto a un analista de SOC de nivel dos para tomar medidas adicionales.</p>

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 Inergy:

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"