Actividad practica integradora

Fecha: 09/12/2022

Integrantes:
Isabel Palacios
Bryan Bermudez
Alejandro Hernández
Carlos Zelada

Actividad

Deberán leer cada una de las noticias asignadas y responder en un documento de Google, las siguientes consignas:

Noticia:

https://www.welivesecurity.com/la-es/2021/05/11/ataque-ransomware-compania-oleoducto-colonia-pipeline-afecta-suministro-combustible-estados-unidos/

Respuestas:

- ¿Qué tipo de amenaza es?

Ransomware

- ¿Cómo comienza y cómo se propaga esta amenaza?

El Ransomware es un software malicioso que al infectar nuestro equipo le da al ciberdelincuente la capacidad de bloquear un dispositivo desde una ubicación remota y encriptar nuestros archivos quitándonos el control de toda la información y datos almacenados, El virus lanza una ventana emergente en la que nos pide el pago de un rescate, dicho pago se hace generalmente en moneda virtual (bitcoins por ejemplo). Se camufla dentro de otro archivo o programa apetecible para el usuario que invite a hacer click: archivos adjuntos en correos electrónicos, vídeos de páginas de dudoso origen o incluso en actualizaciones de sistemas y programas en principio fiables como Windows o Adobe Flash.

Una vez que ha penetrado en el ordenador, el malware se activa y provoca el bloqueo de todo el sistema operativo y lanza el mensaje de advertencia con la amenaza y el importe del “rescate”

que se ha de pagar para recuperar toda la información. El mensaje puede variar en función del tipo de ransomware al que nos enfrentemos

- ¿Hay más de una amenaza aplicada?

Si, alteró el normal funcionamiento de la estación de combustible y encripto archivos para poder cobrar rescate.

- ¿Qué solución o medida recomendarían?

Las prácticas para evitar ser infectado por este malware son comunes a las que debemos seguir para evitar otros virus:

  - Mantener nuestro sistema operativo actualizado para evitar fallos de seguridad.
  - Tener instalado un buen producto antivirus y mantenerlo siempre actualizado.
  - No abrir correos electrónicos o archivos con remitentes desconocidos.
  - Evitar navegar por páginas no seguras o con contenido no verificado.
  - Ten siempre una copia de seguridad actualizada, es la mejor forma de evitar pérdida de información