Factureya®

RANSOMWARE

Factureya®

Objetivo

Crear en conciencia en todos los colaboradores de la Empresa para que tomen las medidas necesarias para evitar ser víctima de este ataque y siempre ser responsables de todo lo que hacemos en la red.

¿Qué es ransomware?

De la misma forma que existe el secuestro de personas con fines económicos, en el mundo IT el ransomware se ha convertido en un ataque secuestrador de datos ya que este ataque básicamente accede a nuestro equipo, encripta toda la información y exige una determinada suma de dinero para su recuperación, así de sencillo.

El origen del nombre "Ransomware" viene de la combinación de dos palabras:

- **Ransom** (Secuestro)
- **ware** (Software)

Factureya®

¿Cómo funciona? Ransomware

Ransomware hace uso de una serie de pasos donde lamentablemente el primero lo da la víctima al ejecutarlo, estos pasos son:

· Exploración del sistema a través de unidades USB, correos fraudulentos, etc.
· Instalación en el sistema al ejecutarse el archivo infectado.
· Selección de archivos a cifrar.
· Cifrado de los datos seleccionados
· Mensajes a la víctima
· Espera del pago
· Envío de las claves de cifrado a la víctima.

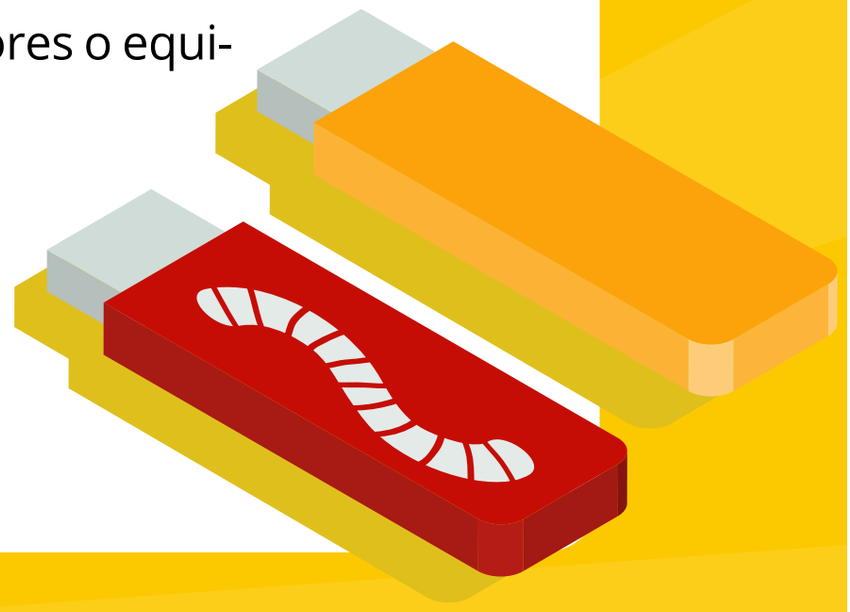
Como podemos observar, es una cadena que nosotros mismos podemos romper desde el principio

Factureya®

Técnicas para propagar Ransomware

Como hemos visto anteriormente existen diversos tipos de ataque ransomware y algunas de las técnicas empleadas para su propagación son:

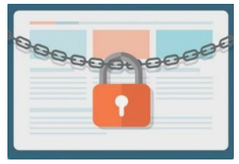
· Envío de correos electrónicos fraudulentos.
· Direccionamiento web a sitios falsos.
· Mensajes de texto.
· Vulnerabilidades encontradas a nivel de seguridad en servidores o equipos cliente.
· Campañas de publicidad maliciosa.
· Sitios web legales que poseen códigos maliciosos en su contenido.
· Auto propagación entre dispositivos.



Factureya®

1. Tipos de ataque de Ransomware

Lock screem
Pantalla de bloqueo



File coder
Codificador de archivos

Este es el Ransomware últimamente más conocido porque ha realizado ataques a muchos equipos de compañías y personas a nivel mundial.

Factureya®

2. Objetivo de Ransomware

Aunque muchos ataques de ransomware ocurren a nivel organizativo donde la información es mucho más delicada y confidencial, los atacantes que crean estos virus no ponen límite, también son un punto débil los usuarios de hogar por razones como:

· Pocos o nulos conocimientos de seguridad informática.

· No contar con aplicaciones de antivirus en sus sistemas operativos.

· Contar con redes abiertas e inseguras.

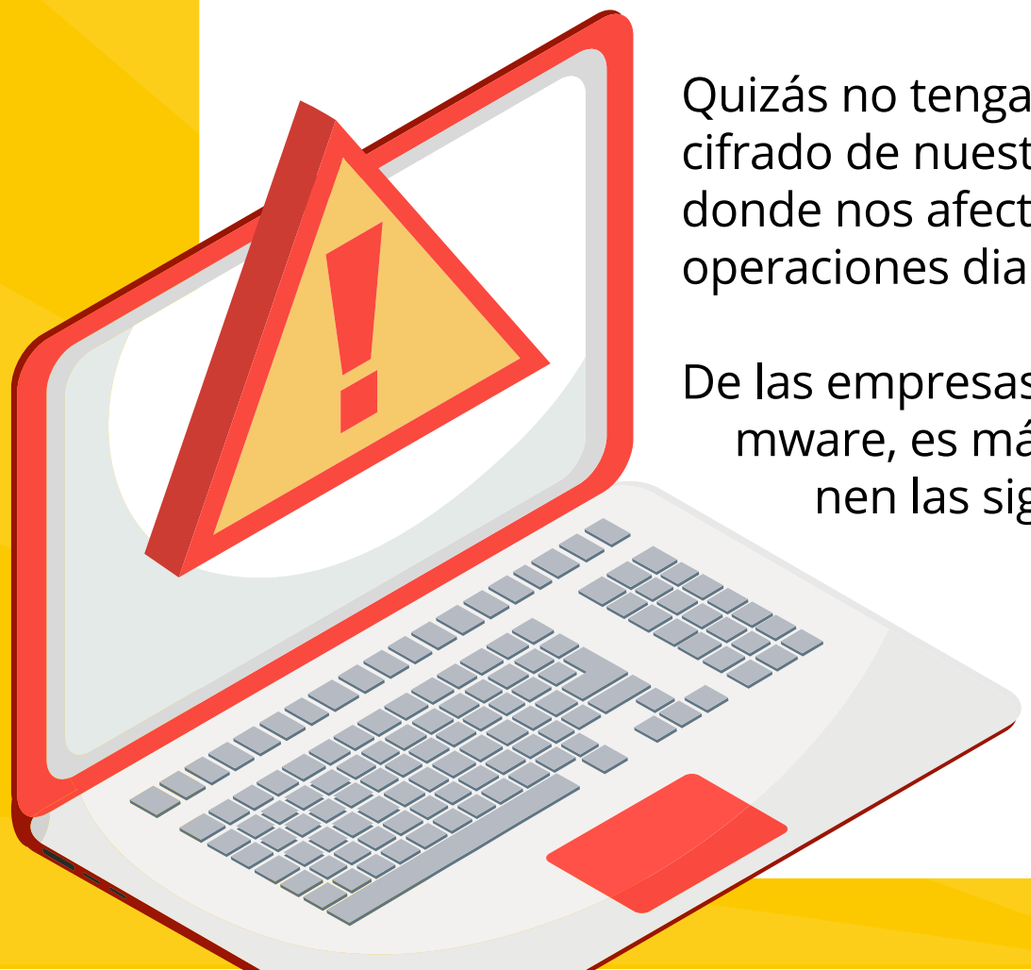
· No crear respaldos constantes de la información.

· No actualizar el sistema operativo y las aplicaciones de seguridad de forma periódica.

· Por el uso indebido de los servicios de internet.

Factureya®

2. Objetivo de Ransomware



Quizás no tengamos información valiosa, pero si somos víctimas del cifrado de nuestra información sin lugar a dudas seremos víctimas donde nos afectará para poder seguir de forma normal nuestras operaciones diarias como a nivel educativo, personal o empresarial.

De las empresas tampoco se han olvidado los creadores de ransomware, es más, son el objetivo número 1, ya que con ellas obtienen las siguientes ventajas:

Factureya®

2. Objetivo de Ransomware

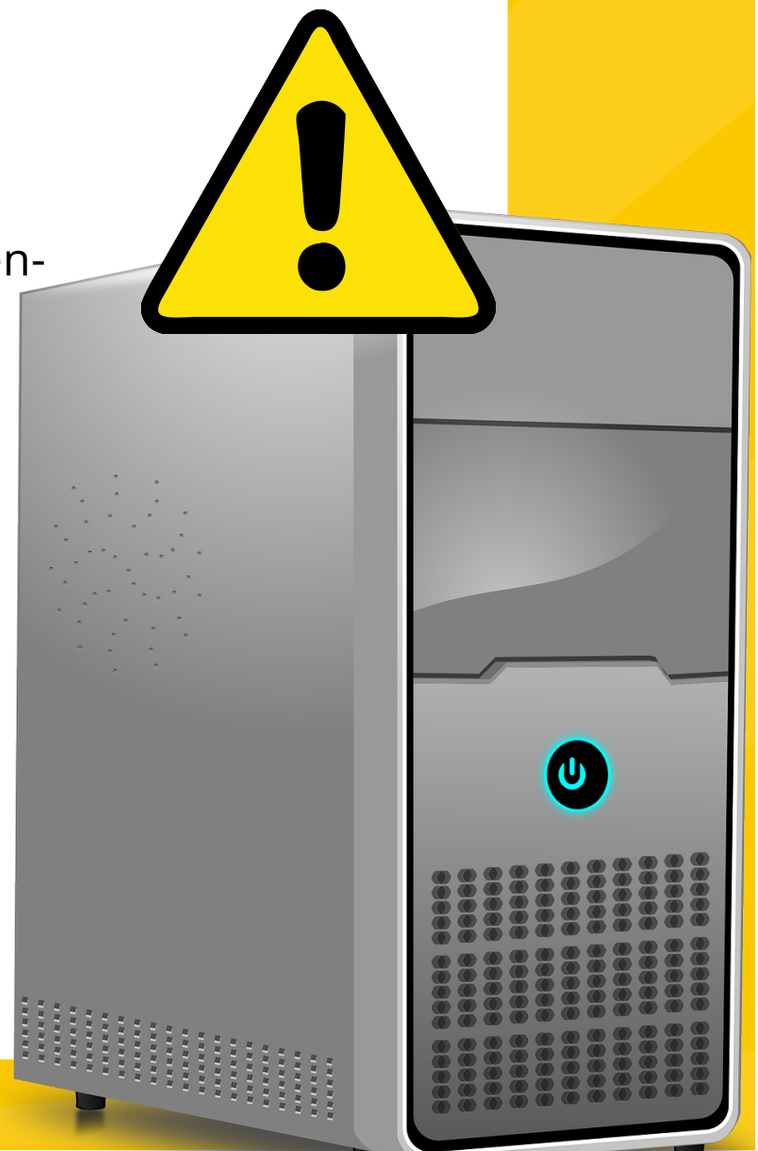
· Son donde más daño pueden hacer, con jugoso potencial económico para que paguen rescate.

· Mayor desestabilidad al cifrar datos delicados de nómina, finanzas, RRHH, etc.

· Posibilidad de afectar un mayor número de equipos y servicios.

· Vulnerabilidades presentadas en los servidores o equipos cliente.

· Desestabilizar puntos importantes de países, y sino creés esto, mirar las últimas noticias donde han sido afectados Hospitales de Londres, empresas cómo Telefónica en España etc.



Factureya®

3. Recomendaciones para protegernos contra malware Ransomware

En vista que ransomware está tomando tanta fuerza y es muy sencillo ser victimas, existen una serie de opciones que nos ayudarán a estar atentos ante este tipo de ataques y evitar ser una víctima más. Algunos consejos son:

Realizar copias de seguridad

Visualizar extensiones de los archivos

Es un aspecto fundamental ya que los archivos infectados son ejecutables,.exe, y están camuflados como archivos PDF, DOC, XLS, etc,

No abrir correos sospechosos o no conocidos

Muchas veces recibimos mensajes de entidades oficiales indicando que tenemos problemas jurídicos, o de la entidad bancaria solicitando el ingreso de la información, otros indicando que tenemos mensajes de voz, etc, pero todo ellos poseen un adjunto que esperan demos clic para, en segundo plano, infectar el equipo.

3. Recomendaciones para protegernos contra malware Ransomware

Repetimos, mucho cuidado en los adjuntos que abrimos, por defecto siempre debéis desconfiar. A la más mínima duda, os recomendamos no abrirlo o bien comprobar esto antes de hacerlo:

· Ver bien la dirección de correo del envío de forma completa del remitente (no sólo el nombre falso que ponen).

· Ver el tipo y extensión de archivo adjunto. Aunque sea conocido el remitente puede haber sido infectado y lo reenvía el malware o virus de forma automática con su cuenta a toda su lista de contactos. (tú una posible víctima).

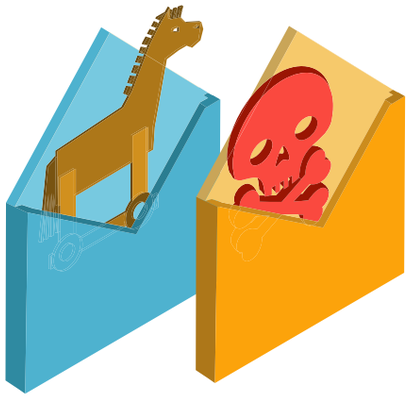
· Ver bien el texto y asunto del mensaje antes de abrir.

· Comprobar dirección IP de remitente y comprobar país de origen de esa dirección, introduciendo la dirección IP desde una web que geo-localiza de forma rápida y cómoda.

Factureya®

Si desconfías lo más mínimo no lo abras, mejor fallar de precavido y borrarlo que infectarse.

Factureya®



Filtrar las extensiones .exe en el correo electrónico

En caso de contar con servidores de correo que permitan filtrar tipo de archivos es ideal que filtremos todos los correos que contengan extensión .exe ya que estas pueden ser archivos infectados para robar nuestra información personal.

Deshabilitar archivos ejecutados desde la ruta AppData o LocalAppData

Si usamos sistemas operativos Windows podemos crear reglas en el firewall y abrir o cerrar puertos que impidan la ejecución de programas desde la ruta AppData o LocalAppData ya que desde allí es uno de los sitios donde Cryptolocker, entre otros tipos de Ransomware, realizan la instalación de sus infecciones

Factureya®

Actualización constante del sistema

Los desarrolladores de sistemas operativos y de los programas antivirus, antimalware y en general de seguridad, lanzan periódicamente nuevas actualizaciones que incluyen mejoras en fallas de seguridad y esto puede ayudarnos a evitar ser víctimas de ransomware.

Desconectarnos de la red en caso de detectar algún tipo de instalación

En caso de ejecución de algún archivo sospechoso, no debemos esperar hasta que concluya el proceso de instalación ya que no sabemos que finalidad tendrá, en este caso lo más prudente y responsable es desconectarnos inmediatamente de la red, Wi-Fi o Ethernet, con el objetivo de impedir la comunicación con el servidor que puede introducir el virus.

Factureya®

GRACIAS