¿QUE ES UN ATAQUE DE RANSOMWARE?

¿Que es un ataque de RANSOMWARE?

El ransomware se encuentra entre las formas de malware más dañinas. Imagine tener que pagar para acceder a los archivos en su propio dispositivo. Así de malos son los ataques de ransomware. Descubra qué es el ransomware y cómo puede protegerse.

¿Cómo funcionan los ataques de RANSOMWARE?

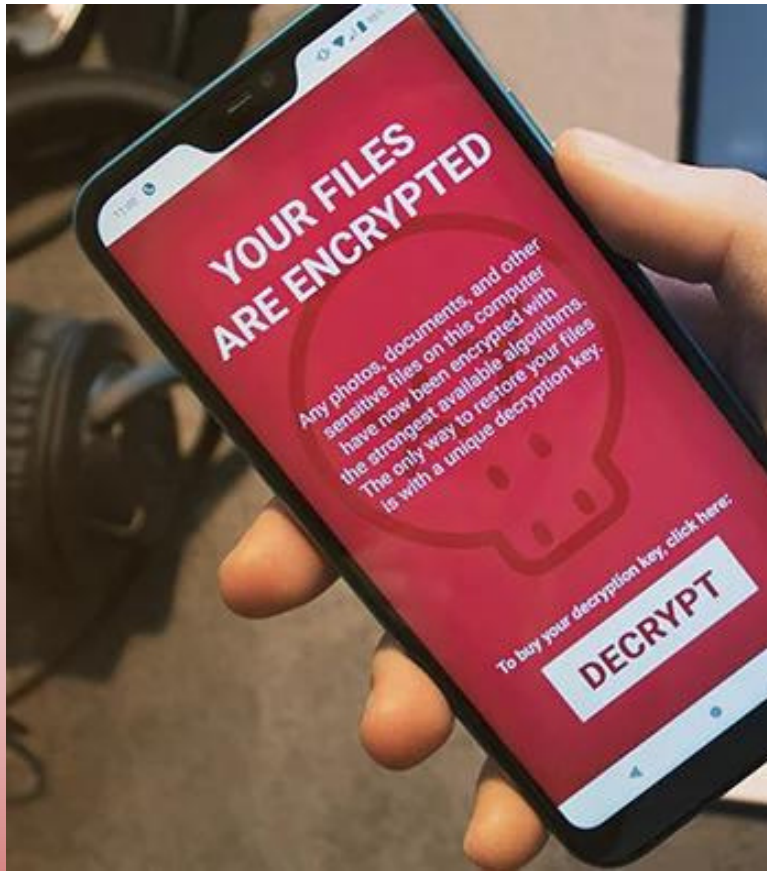
El ransomware cifra todos los archivos de su dispositivo para que no pueda acceder a ellos sin una clave de descifrado. También puede bloquear su dispositivo por completo. Debido a esto, estos diferentes tipos de ransomware se denominan crypto-ransomware y locker ransomware. Después de infectar sus archivos o dispositivo con ransomware, los delincuentes exigen un rescate de $300 a $500 en Bitcoin por dispositivo. El rescate se paga a cambio de la clave de descifrado del ransomware que devuelve los archivos o el dispositivo, o al menos eso es lo que los delincuentes les dicen a sus víctimas.

¿Cómo puede el Ransomware infectar mi dispositivo?

Los virus informáticos, los diferentes tipos de ransomware y troyanos , deben descargarse manualmente por accidente o automáticamente por otro malware. El ransomware se puede descargar de archivos adjuntos de correo electrónico, sitios web y anuncios comprometidos o maliciosos, o redes Wi-Fi inseguras. El phishing es un método común para infiltrar ransomware en el dispositivo de una víctima. Otro malware también puede descargar ransomware sin que usted lo sepa.

IMG

¿Puede el RANSOMWARE infectar mi TELÉFONO MÓVIL?



SÍ

El Ransomware móvil existe para dispositivos iOS y Android. Lo que es peor, es una amenaza creciente debido a la gran cantidad de personas que usan dispositivos inteligentes.

Afortunadamente, existen aplicaciones antivirus móviles que lo ayudan a proteger su dispositivo Android o iOS.

¿Debo PAGAR el rescate?

En caso de que haya sido víctima de un ataque de ransomware, pagar el rescate puede parecer la solución más fácil para recuperar sus archivos cifrados o controlar su dispositivo bloqueado.

Sin embargo, NO PUEDE ESTAR SEGURO de que los delincuentes detrás del ataque de Ransomware vayan a hacer lo que dicen una vez que se pague el rescate. Además de eso, pagar el rescate alienta a los delincuentes a buscar más objetivos que estén dispuestos a pagar el rescate y cumplir con las demandas de los delincuentes.

¿Cuáles son algunos ejemplos recientes de RANSOMWARE?

Desafortunadamente, la cantidad de ataques de ransomware y diferentes tipos de ransomware ha ido en aumento. Los más difundidos e impactantes a menudo también aparecen en las noticias nacionales y mundiales. Estos son algunos ejemplos de ataques de ransomware recientes.

WannaCry: Ataque de ransomware en el NHS

Un ataque de ransomware notable que tuvo lugar en el Reino Unido en 2017 fue el ataque de ransomware WannaCry en el Servicio Nacional de Salud (NHS).

El ransomware WannaCry cifró los datos en las computadoras que infectó. Luego, los atacantes del ransomware exigieron que se les pagara en bitcoins si la víctima quería que se le devolvieran sus datos. Como muestra el ejemplo de WannaCry, los ataques de ransomware a menudo se dirigen a grandes organizaciones, como servicios de atención médica o empresas importantes.

Otros ataques de RANSOMWARE conocidos

- CryptoLocker
- Ryuk
- Petya y No Petya
- Conejo malo
- Bloqueado
- Ojo dorado

5

SENCILLOS CONSEJOS CONTRA EL RANSOMWARE

- Asegúrese de ejecutar un programa de seguridad de Internet efectivo en todos sus dispositivos.
- Realice copias de seguridad periódicas de sus datos. Guárdelos sin conexión para que no se infecten.
- Mantenga su software y sistemas operativos actualizados. Activa las actualizaciones automáticas para tenerlas siempre actualizadas.
- Tenga mucho cuidado con los archivos adjuntos que le solicitan habilitar o permitir algo: macros, edición, contenido, etc.
- Deshabilite los complementos de navegador comúnmente explotados, como Flash Player y Silverlight, cuando no los esté utilizando.

PARA MÁS INFORMACIÓN CONTÁCTANOS EN NUESTRAS REDES SOCIALES

IMAGENTI

info@imagenti.mx

Tel. 55 55 12 73 37