Recuperar ficheros Encriptados

La conectividad por la web, si bien nos ha permitido vencer muchas barreras de comunicación, también ha permitido que los delincuentes informáticos se valgan de programar piratas, para robar información privada de nuestros computadores. Cuando un ataque de esos sucede, la ayuda de un perito informático puede ayudar a recuperar ficheros encriptados.

Si ya has pasado por esa situación tan delicada o conoces de un amigo o familiar en la misma situación**, en Perito Informático,** puedes encontrar el mejor soporte, a través del servicio profesional de sus peritos informáticos, altamente capacitados para resolver este tipo de ataques.

Recuperar ficheros encriptados

En el curso de la vida de una computadora, se recopilan numerosos datos personales, quizás también comerciales, pero definitivamente confidenciales en el disco duro.

¿Qué tienes en tu computadora? ¿Correos electrónicos importantes, archivos secretos de la oficina o incluso fotos antiguas de sus hijos?

Y eso es exactamente lo que te hace chantajeable. **Si en lugar de tu pantalla de inicio habitual, de repente, solo aparece una calavera o una nota de rescate en tu monitor, lo más probable es que estés tratando con ransomware.**

¿Qué es el ransomware?

La palabra "ramson" viene del inglés y significa "rescate" en español. De eso se trata exactamente el ransomware. **A veces, los expertos también hablan de troyanos de cifrado, porque el chantaje se basa en el hecho de que los datos están codificados indisolublemente para el usuario.**

Lo que emerge de estos títulos alternativos es cómo funciona el ransomware: se cuela en el sistema y el usuario se horroriza al descubrir que su computadora está bloqueada.

El ransomware es un malware que bloquea la computadora o encripta los datos que contiene. **Los perpetradores chantajean a sus víctimas al dejar en claro que la pantalla o los datos solo se vuelven a publicar después de un pago de rescate.** De esta manera, los ciberdelincuentes juegan con el miedo de las personas y se enriquecen a su costa.

Por esta razón, si no tienes muchos conocimientos en informática, para recuperar ficheros encriptados de tu computadora, **contar con el servicio profesional de un perito informático, te será de mucha ayuda.**

¿Cómo se hace sentir el ransomware?

Como regla general, la pantalla bloqueada o la nota de rescate, que ya no se puede cerrar, es lo primero que observaras sobre el ransomware. Algunas variantes de ransomware tienen un período de incubación. **Esto significa que el efecto dañino solo ocurre cuando ya no puedas recordar cuándo y dónde pudiste haber atrapado un troyano.**

Un programa de malware también puede ser detectado por un escáner de virus y volverse notorio como resultado positivo del análisis. **Desafortunadamente, si no tienes instalado ningún software antivirus, no notarás el ransomware hasta que sea demasiado tarde.**

Dado que muchos troyanos de extorsión se eliminan después de realizar su función maliciosa, es un verdadero desafío para el software de seguridad identificar el malware. Lo primero que como propietario de la computadora conocerás sobre el ransomware, es una ventana de notificación con una solicitud de pago que ya no se puede cerrar.

¿Cómo difieren las diferentes variantes de ransomware?

En principio, hay dos tipos diferentes de ransomware:

- Bloqueo de pantalla y encriptador de archivos. Los casilleros bloquean la pantalla.
- File-Encrypters, encripta los datos en la computadora y toma fotos de niños, archivos de texto y carpetas importantes como rehenes.

¿Cómo funciona el ransomware?

En el pasado, el ransomware bloqueaba principalmente el escritorio de PC individuales. **Mientras tanto, estos ataques bastantes pequeños con casilleros de pantalla se han vuelto bastante raros.**

Hoy, los programas de cifrado son mucho más comunes que los casilleros de pantalla. Los contenidos del disco duro están encriptados para que el usuario ya no pueda acceder a ellos.

Una dirección, un sitio web o una máscara de formulario que explica los reclamos y los métodos de pago generalmente aparecen en la pantalla de bloqueo. **Los extorsionistas prometen que descifraran los datos una vez que se haya recibido el pago.** Algunos perpetradores amenazan con hacer desaparecer los datos para siempre si la víctima habla con la policía.

Ahora incluso hay ransomware que elimina archivos cifrados por cada hora que aún no se ha pagado. **Para que el usuario no pueda evitar la amenaza apagando la PC, el software destruye la misma cantidad de archivos a la vez cuando se reinicia el sistema.**

El proceso de cifrado criptotroyano

Inicialmente, el malware se ingresa en casi todos los casos por dispositivos finales. **Esto se puede hacer, por ejemplo, a través de un correo electrónico infectado.**

Este correo electrónico puede haber sido personalizado para la industria, la empresa o para individuos. La mayoría de los archivos adjuntos que contienen código ejecutable son el comienzo de un ataque de ransomware.

Establecer una sesión de comunicación segura

Se utiliza una clave RSA asimétrica (pública) para establecer una conexión de red segura con el servidor del delincuente cibernético a través de Internet.

Debido a la conexión segura (similar a un sitio web https//) todos los datos intercambiados entre el sistema de la víctima y el servidor del atacante no pueden ser analizados en texto sin formato. **Por lo tanto, este paso no puede ser detectado por un cortafuego normal.**

Cifrado del sistema de la víctima

Una vez establecida la conexión de comunicación, se solicita otra clave RSA pública al Servidor de Mando y Control del atacante.

A partir de esta llave, el malware genera una llamada llave de sesión (256-bit). Esta clave se utiliza luego para cifrar los datos (el daño real a la víctima) utilizando el método AES de 256 bits. **La encriptación es simétrica, es decir, rápida y eficiente.**

Asegurando la clave del chantaje

Una vez que se completa la codificación de los datos, se realiza otra codificación, a saber, la de la clave secreta (local) AES de 256 bits. **Esta encriptación se hace de nuevo usando la clave pública asimétrica (del punto 1). La "clave cifrada" se almacena localmente junto con los archivos y carpetas cifrados.**

La tecla de sesión AES (la más importante para el usuario) se borra de la RAM, para que no haya más pistas sobre el procedimiento exacto.

Descifrado (teóricamente después de pagar el rescate)

Para volver a los datos normalmente legibles, es necesario desencriptarlos con la clave de sesión del AES.

El chantajista puede descifrar esta clave utilizando su clave privada (asimétrica) a partir de los datos almacenados previamente en el sistema de la víctima. **Tan pronto como la clave de sesión del AES esté disponible, los datos pueden ser descifrados de nuevo.**

Te invito a leer: [No seas Víctima de la estafa en Software a medida]

Información relevante si has sido afectado por un ramsonware

Nunca sigas las instrucciones directas de los extorsionistas. **Es preciso en primer lugar establecer la magnitud del daño causado al sistema de archivos de la computadora.** Incluso si a veces es posible un contacto telefónico, no puedes verificar los compromisos por adelantado.

Las direcciones de Bitcoin a menudo ya están huérfanas para que tu pago nunca llegue. Por razones técnicas, los pagos de Bitcoin no se pueden revertir.

Contáctanos lo antes posible, para que podamos analizar el cifrado. **Nuestros peritos informáticos cuentan con la preparación y los instrumentos tecnológicos para analizar tu caso y establecer un protocolo para proceder, incluso en el caso de que sea necesario negociar la clave del cifrado con los atacantes.**

Los virus, los troyanos y especialmente el ransomware ahora son comunes en el campo de los delitos informáticos. Las personas afectadas generalmente detectan un ataque de ransomware al encontrar datos cifrados.

Si no tienes experticia en informática, busca la asesoría de un perito informático para recuperar ficheros encriptados por los delincuentes cibernéticos.