Manejo adecuado de Ransomware

El malware de rescate, o ransomware, es un tipo de malware que impide a los usuarios acceder a su sistema o a sus archivos personales y que exige el pago de un rescate para poder acceder de nuevo a ellos. Las primeras variantes de ransomware se crearon al final de la década de los 80, y el pago debía efectuarse por correo postal. Hoy en día los creadores de ransomware piden que el pago se efectúe mediante criptomonedas o tarjetas de crédito.

Este tipo específico de software malicioso se usa para extorsionar. Cuando un dispositivo logra ser atacado con éxito, el malware bloquea la pantalla o cifra la información almacenada en el disco y se solicita un rescate a la víctima con los detalles para efectuar el pago.

Cosas importantes que debemos saber de Ransomware

¿Cómo reconocer el ransomware?[1]

Si te han atacado, el ransomware te mostrará en la mayoría de casos un mensaje de rescate en la pantalla, o añadiendo un archivo de texto (mensaje) de las carpetas afectadas. Muchas familias de ransomware también cambian la extensión de los archivos cifrados.

- **Alertas del antivirus**. La aplicación antivirus del dispositivo (si nada ni nadie la ha deshabilitado) puede ser la primera en detectar una infección de ransomware.
- **Cambios en las extensiones de los archivos**. Una extensión típica para una imagen, por dar un ejemplo, es ".jpg". Si notas que esta extensión ha cambiado por otra (una combinación de letras que no reconoces), puede que hayas sufrido una infección de ransomware.
- **Cambios en los nombres de los archivos**. ¿Has notado que tus archivos ya no tienen el nombre que les diste originariamente? Cuando un programa malicioso cifra un archivo, no es atípico que le cambie el nombre. Si notas un cambio así, puede que haya un problema.
- **Mayor uso del procesador y del disco**. Si te percatas de que el procesador o el disco están trabajando más de lo usual, podría haber una aplicación maligna operando en segundo plano.
- **Tráfico de red dudoso**. Las comunicaciones entre una aplicación maligna y los servidores del atacante o delincuente pueden generar tráfico de red sospechoso.

[1] https://es.malwarebytes.com/ransomware/

- **Archivos cifrados**. Si la infección se encuentra en una etapa avanzada, descubrirás que ya no puedes abrir tus archivos.

¿Cómo llega el ransomware a infectar un equipo?

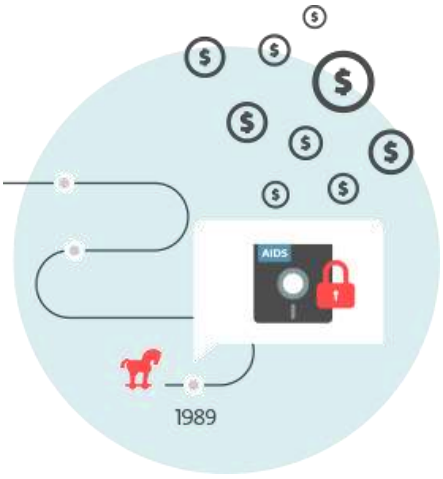
A grandes rasgos, en el mundo del cibercrimen encontramos tantas campañas de malware que buscan distribuir un malware de manera masiva y aleatoria, y también ataques dirigidos que emplean códigos maliciosos para afectar a empresas y organizaciones de todo tipo de industrias.

La forma de distribución más común del ransomware es a través de correos de phishing con archivos adjuntos o enlaces que intentan engañar a los usuarios mediante ingeniería social para convencerlos de descargar la amenaza. Otras formas de distribución son mediante ataques a conexiones remotas, como el Protocolo de Escritorio Remoto (RDP), aprovechando el uso de contraseñas débiles. También a través de la explotación vulnerabilidades —por ejemplo, mediante sitios web comprometidos utilizados para redirigir a sus visitantes a diferentes tipos de exploits—, así como también dispositivos USB, descarga de software pirata, entre otros.

Como podemos deducir de lo anterior, gran parte de los ataques comienza con el engaño de las personas que hacen uso del sistema, utilizando alguna de las numerosas técnicas que conforman a la Ingeniería Social, y también mediante ataques a conexiones remotas como el RDP. No obstante, los atacantes también pueden procurar hacerse del control remoto del sistema aprovechando vulnerabilidades en equipos desactualizados, mal configurados y/o sin ninguna solución de seguridad instalada.

¿Cómo funciona el ransomware?

Hay múltiples técnicas que los creadores de ransomware utilizan:



- **Ransomware diskcoder:** cifra todo el disco y evita que el usuario acceda al sistema operativo.
- **Screen locker:** bloquea el acceso a la pantalla del dispositivo.
- **Crypto-ransomware:** cifra la información almacenada en el disco de la víctima.
- **PIN locker:** ataca los dispositivos Android y cambia los códigos de acceso para dejar fuera a los usuarios.

Todos los tipos de ransomware antes mencionados solicitan un pago y la mayoría de ellos piden que se realice en bitcoins o alguna otra criptomoneda difícil de rastrear. A cambio, los operadores prometen descifrar la información o restaurar el acceso al dispositivo afectado.[2]

Debemos resaltar que no existe ninguna garantía de que los cibercriminales cumplirán con su parte del trato (y algunas veces no pueden hacerlo, a propósito, o debido a problemas de codificación). Por lo tanto, se recomienda NO pagar la suma solicitada.

[2] https://www.eset.com/es/caracteristicas/ransomware/