Ransomware, un peligro capaz de secuestrar tu equipo

El mundo cibernético no es ajeno al peligro de sufrir algún tipo de secuestro de nuestra información o nuestro equipo informático por el que tener que pagar un rescate para recuperar todos esos datos. Es lo que se conoce como Ransomware, un tipo de ataque cada vez más extendido y que nos puede impedir a cualquier información que tengamos almacenada en nuestro dispositivo. A la largo de este White Paper hablaremos más sobre esta amenaza.

¿Qué es el Ransomware?

Para aquellos que no hayan oído nunca hablar de los ransomware, decir que se trata de un malware o software malicioso que una vez que infecta nuestro equipo, le da al ciberdelincuente la posibilidad de bloquearlo desde una ubicación remota, impidiendo que el dueño pueda acceder a la información ahí almacenada.

Para evitar que el usuario pueda acceder a esos archivos, el atacante lo que suele hacer es encriptar los ficheros y datos almacenados. Para poder volver a tener el control sobre nuestra información, suele aparecer algún tipo de ventana emergente solicitando que se realice el pago de un rescate, de forma similar a lo que ocurre cuando una persona es secuestrada.

La necesidad de tener que recuperar la información, la vergüenza que se puede llegar a pasar por contener información comprometida o la presión ante un mensaje alarmante y desconocido, son los principales motivos que llevan al usuario a realizar el pago de ese rescate.

Forma de actuar del ransomware

La forma de actuar de la amenaza ransomware suele ser muy similar a cualquier otro tipo de ataque. Se suele presentar como un archivo comprimido, generalmente en formato ZIP, que al descomprimirlo muestra varios archivos en formato supuestamente "pdf". Decimos supuestamente porque en realidad suele tratarse de archivos ejecutables .EXE a los que se le agrega la extensión PDF aprovechando la

funcionalidad preactivada de Windows que oculta las extensiones. Una vez que la víctima ha ejecutado este falso archivo PDF, comienza todo el proceso de infección.

Lo primero que suele ocurrir, es la instalación del malware en el equipo o servidor infectado bajo un nombre aleatorio. A continuación crea una entrada en el registro del sistema operativo, asegurándose de esta forma poder ejecutarse aunque el equipo sea apagado.

Una vez hecho todo lo anterior, lo que intenta es conectarse al servidor donde se aloja su centro de control que suele ser el equipo de una tercera persona que ha sido infectado pero que no tiene conocimiento de ello. Este método le permite mantener el anonimato en caso de ser rastreados.

Tras conectarse se generan una clave pública y otra privada utilizando el algoritmo RSA de 20148 bits. Mediante el uso de la clave pública, se cifran los distintos archivos de la víctima, mientras que la clave privada es almacenada en el equipo de esa tercera persona que está bajo el control del atacante. Es precisamente esa clave privada la que se debería utilizar para poder descifrar la información.

Tipos de bloqueos llevados a cabo por el ransomware

Básicamente los ataques mediante ransomware utilizan dos tipos diferentes de bloqueos, sin encriptación o con encriptación.

a) Bloqueos sin encriptación

Son los menos dañinos y también los menos habituales. En este caso, lo que suele hacer el software atacante es tomar el control del sistema desactivando el administrador de tareas, blindando el acceso al registro y atacando al fichero "explorer.exe" para que no se muestre ningún icono en el escritorio. Al no estar la información encriptada, haciendo uso de un buen antivirus, podemos llegar a conseguir revertir la situación.

b) Bloqueos con encriptación

Se trata del sistema más utilizado en este tipo de ataques, encriptando los datos almacenados en el disco duro de tal forma que si no se tiene la clave adecuada, es prácticamente imposible acceder a ellos. Si la encriptación afecta a archivos del sistema, un antivirus puede ser suficiente para recuperar el control, pero si

los archivos encriptados son los datos del usuario, la única solución es pagar el rescate que piden o bien formatear el disco duro, lo que significa perder los datos.

Chantajes más habituales que se pueden dar

Aunque con anterioridad hemos hablado de que este tipo de amenazas suele encriptar la información hasta que el usuario paga por su rescate, también se pueden dar otro tipo de chantajes mediante avisos o contenidos embarazosos. Veamos a continuación algunos de los más habituales que nos podemos encontrar.

- **Contenido pirateado.** En la pantalla aparece un mensaje de una falsa agencia de copyright informando de que se ha analizado tu equipo y se ha encontrado material ilícito como películas, juegos o música. Si no pagas amenazan con denunciarte.
- **Falsos virus.** También hay casos en los que el mensaje informa de que el equipo ha sido infectado por un virus muy potente y que para solucionar esa situación, te debes descargar un determinado antivirus que tendrás que pagar.
- **Software caducado.** Hay otras versiones que se camuflan como algún programa de pago que tengas instalado, indicando que tu licencia ha expirado y que es necesario que pague para seguir utilizando dicho programa.
- **Contenido embarazoso.** Suele consistir en mostrar imágenes pornográficas en la pantalla que no desaparecen mientras que no se hace el pago solicitado.

Consejos para protegernos de las garras del ransomware

Ya hemos visto cómo funciona este tipo de ataques, pero ahora toca conocer qué medidas podemos llevar a cabo para evitar ser infectados. Algunas de ellas son de sentido común, pero nunca está de más recordarlas. Empecemos con este repaso.

Instalar revisiones y actualizaciones de nuestro software

Se trata de un consejo general que es aplicable para evitar cualquier tipo de ataque y que siempre deberíamos llevar a rajatabla. La idea es mantener actualizado todo el software que tengamos instalado en nuestra máquina para evitar que posibles agujeros de seguridad puedan ser utilizados por los hackers para infectarnos.

Asegúrate de que están activas las actualizaciones automáticas de Microsoft para poder recibir de esta forma sus últimos parches de seguridad.

Utilizar software que nos proteja de posibles ataques

Siempre es una buena idea tener un software antimalware y un firewall activados que nos ayuden a identificar amenazas o conductas sospechosas. También es muy recomendable utilizar algún bloqueador de ventanas emergentes.

Copia de seguridad de los datos

Se trata de la única herramienta y la más importante que tenemos para derrotar al ransomware. Es aconsejable realizar un backup periódico de toda nuestra información, o por lo menos de lo más importante, para que en caso de ser atacados, podamos recuperarla de forma sencilla y sin tener que pagar.

Es aconsejable que esta copia se realice en algún tipo de unidad de almacenamiento extraíble (memorias USB, discos externos, DVDs,...) que únicamente estén en contacto con el equipo mientras se lleva a cabo la copia de seguridad.

Mostrar las extensiones ocultas de los archivos

Ya hemos explicado que suelen hacerse pasar por otro tipo de archivos para que el usuario los ejecute beneficiándose de que Windows por defecto no muestra las extensiones. Es muy recomendable configurar nuestro sistema para que las muestre, de esta forma seremos capaces de detectar cualquier cosa extraña que veamos, descartando aquellos ficheros que cuenten con la extensión .EXE.

Para conseguir esto en Windows, deberemos acceder al "Panel de Control", luego en "Apariencia y personalización" y por último en "Opciones de Carpeta". Hacemos clic en la ficha "Ver" y a continuación en la zona de "Configuración Avanzada" desmarcamos la opción "Ocultar las extensiones de archivo para tipos de archivo conocidos"

Mucho cuidado con los correos electrónicos que se abren

El correo electrónico suele ser el medio más utilizado para infectar un equipo. Hay que tener mucho cuidado con los correos que abrimos y descartar aquellos que no conozcamos el remitente y sobre todo, no ejecutar ningún archivo que lleven adjunto.

Desconectarnos de la red si pensamos que hemos sido infectados

Si ejecutas un archivo y piensas que puede tratarse de un ransomware, si aún no ha aparecido el mensaje de aviso, si actúas de forma rápida, quizá puedas cortar la comunicación con el equipo que actúa como centro de datos y de esta forma evitar que pueda llevar a cabo la encriptación de la información.

Restaurar el sistema a un estado anterior sin infecciones

La opción "Restaurar sistema" en Windows, suele estar activada por defecto, por lo que si no la hemos desactivado, siempre podemos intentar volver a un estado anterior en el que no existiera la infección. Si puedes llevar a cabo esto, podrás vencer a este malware, aunque puede ser que tengas que sacrificar para ello parte de tu información, más concretamente, aquella que no exista en la copia que restaures.

¿Pagar o no pagar? He ahí la cuestión

Cuando hemos sufrido un ataque por medio de ransomware, siempre nos aparecerá la duda de pagar o no pagar. Tomar esta decisión dependerá del grado de importancia que tenga la información que haya sido encriptada, aunque se entiende que puede haber casos que se trate de datos cruciales y que se haga cualquier cosa para recuperarlo.

De todas formas hay que tener claro una cosa, aun pagando el rescate solicitado por el atacante, se puede dar el caso de que no se recupere la información.