QUÉ ES Y CÓMO FUNCIONA UN RANSOMWARE

El ataque perpetrado por **hackers** que está ocupando todos los titulares desde el viernes nos ha dejado un término que resulta novedoso para muchas personas. Dicho término es el **ransomware**. De repente ésta palabra se encuentra por todos lados. Todas las noticias en televisión e internet y todos los periódicos la mencionan de forma constante. Pero para muchos sigue existiendo la duda sobre lo que realmente significa.

Por ese motivo, a modo explicativo os diremos **qué es el ransomware** y también cómo funciona y su objetivo principal.

El **ransomware es un software malintencionado**. Es así de primeras, la definición más simple que podemos ofrecer sobre este concepto, aunque lógicamente hay mucho más detrás. Se trata de un **malware que busca encriptar los archivos** presentes en un ordenador. Dada la magnitud de algunos de estos ransomware, como el **WannaCry** que estamos viendo mucho estos días, pueden lograr **encriptar los archivos más sensibles** de cualquier ordenador.

Generalmente, se suelen centrar en **encriptar esos archivos sensibles** de nuestro ordenador. No importa del tipo que sean. Puede tratarse de documentos Word, o PDF aunque incluso hasta fotos o vídeos. Generalmente el tipo de archivos que va a tratar de encriptar **depende del objetivo de su creador**. El **desarrollador establece** qué archivos son el objetivo del ransomware.

Si el **ransomware logra entrar en tu ordenador y encriptar los archivos** que busca, lo más habitual es que te salga el **mensaje** de que has sido infectado. Al mismo tiempo te **piden un rescate** para poder liberar tu ordenador. Generalmente es **dinero real**, aunque en muchos casos también se han visto con **bitcoins**. Nos pedirán una transferencia. Si se realiza dicha transferencia de dinero lo que vamos a obtener es una **clave** con la que poder **desencriptar nuestro sistema** entero. De esa forma podemos liberar nuestro ordenador y volver a usarlo de forma normal.

Dado el aumento de la presencia de ransomware online, hay cada vez más **códigos genéricos** que nos ayudan a desbloquear el sistema. El problema es que no siempre funcionan, aunque en algunos casos pueden ser de enorme utilidad.

¿Hay que pagar?

Esta parte es una de las más controvertidas. En general, tanto las autoridades como los expertos en seguridad **recomiendan no pagar** y no ceder al chantaje de los hackers. Muchos usuarios pagan, en general por miedo. Es una reacción lógica, ya que al tener tu ordenador bloqueado tu único objetivo es volver a poder disponer del mismo y de todos tus archivos.

Es una situación complicada. Hay **empresas que se han visto obligadas a pagar cifras enormes** para poder liberar sus sistemas del ataque de ransomware. El principal problema de estos casos, es que **pagar no es ninguna garantía**.

Hay casos en los que a pesar de que se realice el pago del rescate solicitado por los

atacantes el ordenador **no ha sido liberado**. Por tanto, pese a hacer el pago no hay garantía alguna. Es por eso que muchos recomiendan no pagar. Pero el principal problema ante esa situación es que **apenas hay soluciones posibles**. Sin pago el ordenador no será liberado. Un callejón sin salida.

¿Cómo prevenir el ransomware?

Para evitar ser infectado por el **ransomware**, los consejos ofrecidos son los habituales para cualquier tipo de malware. La principal forma de **expansión del ransomware suele ser a través de correo electrónico**, por tanto se recomienda evitar abrir correos electrónicos desconocidos, y especialmente nunca descargar **archivos adjuntos** en los mismos. También hay que ser cuidadoso con las descargas, por tanto siempre de sitios de confianza.

Instaladores APK pueden ser más problemáticos, por lo que se recomienda especial cuidado con este tipo. Tampoco hay que instalar **complementos extraños** que alguna página web nos recomiende.