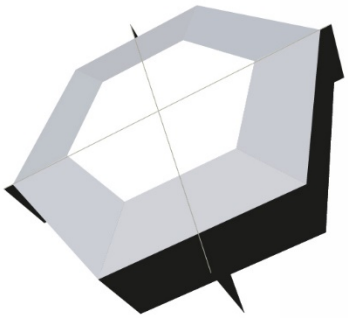

SoftGuard

TEC: 255

Qué es y cómo combatir el Ransomware

Ransomware

Cada día son mayores las amenazas cibernéticas o como comúnmente se conoce “Ciberataques”, por eso SoftGuard presenta una guía rápida en la cual le mostrará todo lo que necesita saber sobre el Ransomware, cómo protegerse de esos ataques y a su vez como eliminarlos en caso de ser infectado.

¿Qué es el Ransomware?

El ransomware es un tipo de malware que es como se conocen a los softwares maliciosos diseñados para infiltrarse o dañar una computadora o sistema de información sin el consentimiento de su propietario. El malware puede tomar varias formas, como la de un virus informático, un troyano, un spyware o un ransomware.

El nombre de ransomware es compuesto, y es la unión de las palabras Ransom y software. *Ransom* quiere decir rescate en inglés, y de hecho lo que hace este tipo de malware es secuestrar los datos de un ordenador y pedir un rescate económico a cambio de liberarlo. Normalmente lo que hace es cifrar tus datos, y lo que te ofrecen a cambio del rescate económico es la clave para poder descifrarlos.

Este tipo de programas puede acceder a tu ordenador por medio de un gusano informático u otro tipo de malware y una vez cifre tus datos bloqueará tu ordenador mostrándote una pantalla de advertencia en la que se te informa que has sido víctima del ataque. En esa pantalla se te muestra también la cantidad a pagar y el método de pago, que puede ser por SMS, Paypal o mediante bitcoins.

Se trata de una de las amenazas que más está creciendo en los últimos años, por lo que es importante tener tu ordenador siempre actualizado y seguir una serie de precauciones a la hora de enfrentarte a correos electrónicos o mensajes sospechosos, evitando siempre instalar nada que te manden por correo personas que no conozcas.

Otro consejo muy importante en el que coinciden casi todos los expertos en seguridad informática es que hay que tratar de no pagar nunca el rescate que se le pide. Haciéndolo permite que los criminales se salgan con la suya, y fomenta a los mismos a seguir recurriendo a este tipo de programa. El método más fácil de combatirlo es tener siempre copias de seguridad actualizadas de sus bases de datos y formatear los equipos afectados recuperándolos después con estas copias.

Tipos de Ransomware

El ransomware puede adoptar diversas formas. En todas ellas, el denominador común es la solicitud de un rescate. En 2017, se registraron algunos casos de ataques a instituciones con un software parecido al ransomware, pero no parecía que hubiese un móvil económico. Es posible que se usara el ransomware para ocultar actividades de espionaje o algún otro tipo de ciberataque.

- **Malware criptográfico**

El tipo más habitual de ransomware es el criptográfico o de cifrado: este ransomware cifra los archivos. Se puede iniciar sesión en el equipo, pero los archivos no se pueden abrir. WannaCry es un excelente ejemplo de este tipo de ransomware.

- **Bloqueador**

El ransomware bloqueador bloquea totalmente su acceso al equipo y le impide hasta iniciar sesión.
El ransomware Petya, que surgió en 2016 y regresó en 2017 con más sofisticación, cifra la tabla maestra de archivos del disco duro con el objeto de bloquear el equipo.

- **Doxware**

Doxware descarga una copia de sus archivos confidenciales en el equipo del atacante, que luego amenaza con publicarlos en Internet si no se paga el rescate. Alguien amenaza con publicar sus fotos o vídeos más personales en un sitio web público donde todo el mundo los pueda ver. El ransomware Ransoc usaba este método.

- **Scareware**

Scareware es un programa de software falso que asegura haber encontrado problemas en el equipo y solicita dinero para solucionarlos. Este tipo de ransomware puede llegar a inundar la pantalla con ventanas y mensajes de alerta o bloquear el equipo hasta que se pague.

Uno de los factores que más han contribuido a la popularización del ransomware es que es un tipo de malware que se encuentra fácilmente en la red y cualquiera que tenga malas intenciones lo puede usar. Se ha observado que alrededor de un tercio de todos los nuevos ransomware proceden de una variedad existente de código abierto. Además, los hackers están actualizando continuamente el código para perfeccionar el ransomware y mejorar el cifrado, de modo que una variedad de ransomware puede resurgir varias veces, como es el caso de Petna.

Como el objetivo final del atacante es propagar el ransomware en el mayor número posible de ordenadores para conseguir más dinero, ha aparecido una táctica alternativa para pedir el rescate.

En el caso del ransomware Popcorn Time, el delincuente le pide a la víctima que infecte a otros dos usuarios. Si esos dos usuarios pagan el rescate, la primera víctima podrá recuperar sus archivos sin tener que pagar nada.

Cómo se infectan los dispositivos

Lo más preocupante del ransomware es que, a diferencia de los virus, puede atacar los dispositivos sin que los usuarios hagan nada. En el caso de los virus, el usuario tiene que descargar un archivo infectado o hacer clic en un vínculo infectado, pero el ransomware puede infectar un equipo vulnerable por sí solo.

- **Kits de exploits**

Los atacantes maliciosos desarrollan kits de exploits que contienen código ya escrito diseñado para aprovechar vulnerabilidades como EternalBlue. Este tipo de ransomware puede infectar cualquier equipo conectado en red que tenga un software desactualizado.

- **Ingeniería social**

Otras formas de ransomware utilizan métodos ya comprobados para infectar los equipos. La ingeniería social (o phishing) hace referencia al acto de persuadir a alguien para que descargue malware desde un archivo adjunto o un vínculo web. Estos archivos suelen llegar en un correo electrónico que parece proceder de una fuente fiable, y el archivo adjunto o el vínculo se asemejan a un formulario de pedido, un comprobante, una factura o un aviso importante. Por su extensión, el archivo parece un PDF o un archivo de Excel o Word, pero, en realidad, es un archivo ejecutable enmascarado. El usuario lo descarga, hace clic en él y comienza la debacle. (Puede que no sea algo instantáneo. Algunos tipos de ransomware se diseñan para que se oculten en el equipo durante un tiempo determinado; de esta forma, es más difícil averiguar exactamente su origen).

- **Malvertising**

El malvertising es otro método de infección por el cual el atacante utiliza una red publicitaria para distribuir el malware. El anuncio falso podría aparecer incluso en sitios web de confianza. Si el usuario hace clic en el vínculo del anuncio, el ransomware se descarga en su equipo.

Las descargas silenciosas guardan archivos maliciosos en el equipo sin ninguna acción directa por parte del usuario. Algunos sitios poco fiables aprovechan los navegadores y las aplicaciones desactualizados para descargar, de manera subrepticia, malware en su equipo cuando está navegando por Internet inocentemente. Sea cual sea el método por el que ransomware haya llegado al equipo, cuando el programa se ejecuta suele funcionar del modo siguiente: empieza a modificar archivos (o estructuras de archivos) de modo que solo se puedan volver a leer o usar restaurándolos a su estado original. Para proteger la comunicación entre el malware y el equipo de control (el que emplea el delincuente para manipular el PC de la víctima), se utiliza el cifrado. El cifrado alberga la clave capaz de descifrar los datos o recuperar la clave de descifrado necesaria para restablecer la forma original de los archivos o el sistema de archivos. Cuando todos los archivos están bloqueados, en la pantalla aparece una nota de rescate en la que se indica el importe que debe abonar para descifrar los archivos, adónde o cómo transferir los fondos y cuánto tiempo tiene para hacerlo. Si no cumple el plazo, la suma aumenta. Si intenta abrir alguno de los archivos cifrados, aparece un mensaje de error donde pone que el archivo está dañado, no es válido o no se encuentra.

Cómo protegerte de un Ransomware

Desafortunadamente, cuando un ransomware ya ha infectado y bloqueado su ordenador no hay casi nada que puedas hacer, por lo que todo el trabajo para protegerte tiene que ser preventivo. En estas acciones que puedes realizar podemos distinguir dos tipos, por una parte, están los consejos para evitar verte afectado por estas amenazas, y por otra los consejos para que si te ves afectado por un ransomware el daño sufrido sea el mínimo posible.

Uno de los principales métodos para infectar tu ordenador con ransomware suele ser el envío de correos electrónicos con el malware adjunto y camuflado, el clásico “phishing”. Por ello, es importante no fiarte nunca de adjuntos no solicitados en los correos electrónicos. Si recibes un email inesperado de un desconocido y un fichero adjunto, jamás abras el adjunto y borra el correo intentando no abrirlo nunca. Si el correo que recibes es de algún contacto que conoces, pero te extraña que te haya enviado un adjunto o no le has pedido que te envíe nada, lo mejor es que te asegures preguntándole a esa persona antes de abrir el adjunto.

También, es importante no prestarles atención a correos falsos de empresas. A veces son difíciles de detectar porque están bien diseñados, pero desde hace años viene habiendo muchos ataques mediante correos falsos. Para evitarlo, si recibe el mensaje de una empresa o institución que no esperaba, o un correo que tengan una redacción extraña y un adjunto o enlace que le piden que abra, no haga caso al mensaje y bórrelo inmediatamente. Normalmente las instituciones tienen otras vías para comunicarse con usted sin añadir adjuntos.

Ya que se habla de enlaces, los mismos, son otro método clásico para infectar ordenadores, ya sea a través de correos electrónicos o mensajes en redes sociales. Por ello, se recomienda nunca hacer clic en enlaces de direcciones desconocidas o cuya procedencia no quede clara y preste especial cuidado con los enlaces que vienen de páginas que acortan direcciones.

Otra forma de distribución de ransomware son los archivos de Microsoft Office, como DOC, XLS y similares. Son archivos que comúnmente todos usan y se cree que son inofensivos, pero no siempre lo son. Por ello, es mejor es desactivar los macros de Word o tu aplicación ofimática de cabecera para evitar que en ellos se pueda introducir malware.

Por último, repase las opciones de seguridad y privacidad de su navegador. Desactive plug-ins como Flash o Java, o por lo menos configúrelos para que se pida permiso para utilizarlos cada vez que una página lo solicite para de esta forma poder evitar problemas. También revise las extensiones que tenga instaladas u así quitar todas las que no utilice o no conozca.

Además, también es importante tener bien asegurado su ordenador, con protecciones nativas contra ransomware como la incluida en Windows 10, y sin descargar utilizar aplicaciones de terceros como antivirus que incluyan protecciones contra el ransomware. De igual forma siempre habrá algunos ransomware diseñados para evitar ser detectados. Por esta razón, también puede analizar cualquier fichero sospechoso con algunos de los servicios de análisis o antivirus online para analizar los archivos individuales de los que no termine de fiarse. Sobre todo, si es algo que ha descargado y está tentado de instalar.

Si pese a todas las precauciones antes descritas acaba infectado, lo más importante es no pagar nunca el dinero que le piden para liberar sus archivos, ya que esto no le asegura recuperar sus datos o el acceso a su ordenador y estará dándole medios a los ciberdelincuentes para seguir estafando a más gente.

Si fue infectado, también se recomienda desconectar el PC de Internet y de su red local para evitar que se propague por otros equipos. Recuerde empezar a realizar la copia de seguridad para hacer una instalación limpia desde cero de su sistema operativo y volver a cargar los archivos de su copia de seguridad.

Hábitos para que un Ransomware no le haga daño

Existen una serie de buenos hábitos con los que puede evitar el impacto negativo que un ransomware tiene en su ordenador. El más importante es hacer copias de seguridad periódicas de todos sus archivos y especialmente los más importantes. Nunca dejes que los documentos y archivos importantes tengan sólo una copia en tu ordenador, mantén actualizadas las copias de seguridad para que, en caso de avería o ataque, pueda recuperar toda la información posible.

El lugar para guardar las copias de seguridad es a su elección, puede usar un disco duro portátil conectado al ordenador, un NAS, un servicio de alojamiento en la nube, o incluso un soporte óptico. Algunos expertos aconsejan desactivar la función de sincronización con servicios online tipo Dropbox, y sincronizar manualmente al menos una vez al día. Así se evita que un posible ataque con ransomware pueda alcanzar también a su copia en la nube.

Es importante que tenga el sistema operativo siempre actualizado y actualice también todas las aplicaciones o los antivirus que puedas tener en su ordenador. Las actualizaciones no sólo añaden nuevas funciones, sino que también corrigen problemas de seguridad y errores de los que un atacante se podría aprovechar para infectarle. De ahí la importancia de tener siempre actualizado su software.

por último, intente también mantenerse informado sobre nuevas amenazas que pueda haber en la red, para así saber cuándo debe prestar especial atención.