HABLEMOS DE RANSOMWARE-

Todo acerca del ransomware

¿Alguna vez se ha preguntado qué es todo este revuelo con el ransomware? Ha oído hablar de él en la oficina o leído sobre él en las noticias. Incluso puede que haya aparecido ahora mismo un mensaje emergente en la pantalla de su ordenador que le avisa de una infección con ransomware. Bueno, si tiene curiosidad por aprender todo lo que hay que saber sobre el ransomware, ha venido al lugar adecuado. Le hablaremos de las diferentes formas de ransomware, cómo

puede infectarse, de dónde procede, contra quién atenta y qué puede hacer para protegerse.

¿Qué es 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.

¿Cómo puede infectarse?

El ransomware puede infectar su ordenador de varias formas. Uno de los métodos más habituales actualmente es a través de spam malicioso, o malspam, que son mensajes no solicitados que se utilizan para enviar malware por correo electrónico. El mensaje de correo electrónico puede incluir archivos adjuntos trampa, como PDF o documentos de Word. También puede contener enlaces a sitios web maliciosos.

El malspam usa ingeniería social para engañar a la gente con el fin de que abra archivos adjuntos o haga clic en vínculos que parecen legítimos, aparentando que proceden de una institución de confianza o de un amigo. Los ciberdelincuentes emplean la ingeniería social en otros tipos de ataques de ransomware, por ejemplo, presentarse como el FBI para asustar a los usuarios y obligarles a pagar una suma de dinero por desbloquear los archivos.

Otro método de infección habitual, que alcanzó su pico en 2016, es la publicidad maliciosa. La publicidad maliciosa consiste en el uso de publicidad en línea para distribuir malware con poca interacción por parte del usuario o incluso ninguna. Mientras navegan por la web, incluso por sitios legítimos, los usuarios pueden ser conducidos a servidores delictivos sin necesidad de hacer clic en un anuncio. Estos servidores clasifican los detalles de los ordenadores de las víctimas y sus ubicaciones y, a continuación, seleccionan el malware más adecuado para enviarlo. Frecuentemente, ese malware es ransomware.

La publicidad maliciosa a menudo usa un iframe infectado, o elemento invisible de una página web, para hacer su trabajo. El iframe redirige a una página de aterrizaje de un exploit y el código malicioso ataca el sistema desde esta mediante un kit de

exploits. Todo esto sucede sin el conocimiento del usuario, por lo que a menudo se conoce como ataque drive-by-download (por descarga oculta).

Tipos de ransomware

Hay tres tipos principales de ransomware, cuya gravedad va desde «algo molesto» a peligro del nivel de «crisis de los misiles de Cuba». Son los siguientes: Scareware

Scareware

El scareware no resulta tan temible. Incluye programas de seguridad falsos y ofertas falsas de soporte técnico. Podría recibir un mensaje emergente que le informa de que se ha detectado malware y que la única forma de librarse de él es pagar. Si no lo hace, seguramente continuará siendo bombardeado con mensajes emergentes, pero sus archivos están básicamente a salvo.

Un programa de software legítimo de seguridad informática no se dirigiría a los clientes en esos términos. Además, si no tiene instalado un programa de esa compañía en el ordenador, esta no tiene por qué estar supervisándole para detectar una infección por ransomware. Y en caso de que tuviera ese software de seguridad, no tendría que pagar por la eliminación de la infección, puesto que ya pagó el precio del software para que este haga precisamente ese trabajo.

Bloqueadores de pantalla

Con estos la alerta pasa a naranja. Si un ransomware que bloquea la pantalla llega a su ordenador, le impedirá el uso de su PC por completo. Al encender el ordenador aparece una ventana que ocupa toda la pantalla, a menudo acompañada de un emblema de aspecto oficial del FBI o del Departamento de Justicia de los Estados Unidos, que le indica que se han detectado actividades ilegales en su ordenador y que debe pagar una multa. Sin embargo, el FBI no actuaría nunca así ni le exigiría ningún pago por la realización de una actividad ilegal. En caso de que sospecharan que usted comete piratería, o que está en posesión de pornografía infantil o por cualquier otro delito informático, el FBI seguiría los canales legales adecuados.

Ransomware de cifrado

Este es el peor de todos. Este es el que le secuestra los archivos y los cifra, exigiendo un pago para volver a descifrarlos y devolvérselos. La razón por la que este tipo de ransomware es tan peligroso es porque una vez que los ciberdelincuentes se apoderan de los archivos, no hay ningún software de seguridad ni restauración del sistema capaz de devolvérselos. A menos que pague el rescate, puede despedirse de sus archivos. E incluso si lo paga, no hay ninguna garantía de que los ciberdelincuentes le devuelvan los archivos.

Últimos ataques de ransomware

1. Europol: El ransomware se mantiene como la principal amenaza en el informe IOCTA
2. El ransomware continúa atacando a ciudades y empresas
3. Los troyanos y el ransomware dominan el panorama de las amenazas a centros educativos en 2018-2019

Cómo protegerse del ransomware

Los expertos en seguridad están de acuerdo en que el mejor modo de protegerse frente al ransomware es evitar la infección.

Aunque hay métodos para tratar una infección con ransomware, en el mejor de los casos son soluciones imperfectas, y a menudo requieren unos conocimientos técnicos que el usuario de a pie no posee. Por tanto, esto es lo que recomendamos a los usuarios para evitar las consecuencias de los ataques por ransomware.

El primer paso en la prevención del ransomware es invertir en un excelente programa de seguridad informática, algún programa con protección en tiempo real diseñado para frustrar los ataques con malware avanzado, como pueda ser el ransomware. También debe buscar características que protejan los programas más vulnerables frente a las amenazas (una tecnología anti-exploits) y al mismo tiempo impidan que el ransomware secuestre sus archivos (un componente anti-ransomware). Los clientes que utilizaron la versión Premium de Malwarebytes for Windows, por ejemplo, estuvieron protegidos de los principales ataques de ransomware de 2017.

A continuación, y aunque sea algo fastidioso, debe crear copias de seguridad de los datos regularmente. Nuestra recomendación es emplear un almacenamiento en la nube que incluya cifrado de alto nivel y autenticación multifactor. Sin embargo,

también puede comprar unidades USB o discos duros externos en los que puede guardar archivos nuevos o actualizados, pero no olvide desconectar físicamente estos dispositivos del ordenador después de realizar la copia de seguridad ya que, en caso contrario, se podrían infectar también con el ransomware.

Después asegúrese de que sus sistemas y el software estén siempre actualizados. El brote de ransomware del WannaCry se aprovechó de una vulnerabilidad en el software de Microsoft. Aunque la compañía había publicado un parche para solucionar el problema en marzo de 2017, muchos no instalaron la actualización y quedaron indefensos frente al ataque. Sabemos que es difícil mantener siempre al día una lista creciente de actualizaciones para el conjunto cada vez mayor de programas de software y aplicaciones que utiliza en su vida diaria. Por eso, le recomendamos que habilite las actualizaciones automáticas.

Finalmente, esté siempre informado. Una de las formas más habituales en la que se infectan los ordenadores con ransomware es a través de ingeniería social. Reciba formación (y proporciónesela a sus empleados si es el propietario de la empresa) sobre cómo detectar malspam, sitios web sospechosos y otras estafas. Y, sobre todo, utilice el sentido común. Si algo parece sospechoso, probablemente lo sea.