COMPETIMEXTRA
inteligencia empresarial para tu negocio

COMPETIMEX
inteligencia empresarial

Ransomware, lo que debemos saber sobre estos ataques cibernéticos

Edición Número 42. Junio 2017

- Los hackers utilizan esta técnica para bloquear sus dispositivos y exigir un rescate a cambio de recuperar el acceso.
- El Ransomware lleva a los usuarios afectados a una difícil situación, por lo que es mejor saber cómo evitarlo.

En estos últimos meses tanto en los diarios, como en los noticieros se ha mencionado mucho sobre estos ataques cibernéticos basados en Ransomware y principalmente del último de ellos llamado WannaCry. Por tal razón es importante saber ¿qué es el Ransomware?, ¿cómo nos afecta?, ¿cómo eliminarlo? y principalmente ¿cómo prevenirlo?

¿Qué es el Ransomware?

El Ransomware es un software malicioso que al infectar nuestro equipo le da al ciber-delincuente la capacidad de bloquear un dispositivo **desde una ubicación remota y encriptar los archivos quitando el control de toda la información y datos almacenados.** El virus lanza una ventana emergente en la que solicita el pago de un rescate, dicho pago se hace generalmente en moneda virtual (bitcoins por ejemplo).

El Ransomware con mayor afectación publicado en las últimas semanas, es el llamado WannaCry y en las últimas horas se está dando a conocer uno nuevo llamado Petya del cual aún no se tiene mucha información.

Hay dos vías principales de infección a través de las cuales se puede ser víctimas del Ransomware. Por un lado, un usuario desprevenido puede acceder a un enlace inapropiado e iniciar la descarga del malware por medio de un link de una página de Internet o por un correo electrónico recibido. Por el otro, los atacantes pueden aprovechar las vulnerabilidades que aparecen cuando los sistemas no están actualizados.

¿Cómo nos afecta?

Este tipo de ataques han afectado a empresas de diferentes sectores y tamaños, dejando como resultado pérdidas millonarias.

Hoy en día la información es uno de los principales activos de las organizaciones y por ende cualquier afectación a la misma representa un riesgo importante que repercute en la operación de las organizaciones; así como el servicio a sus clientes.

En el ataque de WannaCry, México fue el país más afectado de América Latina y el quinto a nivel global después de Rusia, Ucrania, China e India, de acuerdo a los datos publicados por Kaspersky Lab.

Por lo anterior es importante tomar las medidas necesarias para prevenir este tipo de ataques y actuar de manera inmediata en caso de ser víctima de los mismos.

En un 90% de los equipos infectados no ha sido posible recuperar la información, por lo que estar prevenidos es la mejor estrategia para estos casos.

¿Cómo eliminarlo?

Aunque como se mencionó, las probabilidades de recuperar la información de un equipo infectado con Ransomware son muy pocas, es importante evitar su propagación en la red y por tal razón se debe tomar en cuenta lo siguiente:

- Aislar de la red el o los equipos afectados
- Actualizar el sistema operativo
- Actualizar antivirus con soporte para Ransomware
- Ejecutar escaneo y eliminación de Ransomware

La gran mayoría de las firmas de antivirus publican las actualizaciones que mantienen al día sus aplicaciones y ayudan a eliminar o detener la afectación de Ransomware y otros software's maliciosos. Por tal razón **es importante mantenerse al día en aplicaciones de antivirus y actualizaciones de sistemas operativos.**

¿Cómo prevenirlo?

La prevención es el mejor aliado en estos casos y tiene que ver con varios aspectos en la organización que van desde lo técnico, hasta una cultura de Seguridad de la Información de los colaboradores de la empresa.

Las organizaciones no pueden ser ajenas a estos eventos que cada vez son más frecuentes y la afectación pone en riesgo la operación de éstas.

Por lo anterior es importante tomar en cuenta las siguientes recomendaciones:

- **Contar con políticas y procedimientos de Seguridad de la Información**
- Generar una cultura de Seguridad de la Información en todos los colaboradores de la empresa
- Establecer mecanismos que permitan proteger los accesos a la información
- Evitar o cerrar las principales vías de infección
- **Implementar solución para administrar las actualizaciones de los sistemas operativos de los equipos de cómputo y servidores de la empresa**
- Resguardo de la información crítica
- **Mantener un esquema de respaldos y restauración de información**
- Contar con herramientas de antivirus actualizadas

La Seguridad de la Información es algo que compete a toda la organización y por tal razón es importante que las áreas de negocio estén en coordinación con las de TI (Tecnologías de la Información) para poder hacer frente a este y cualquier evento que atente contra ésta.

COMPETIMEXTRA es una publicación mensual emitida por Competimex, S.C. Julio Alejandro Millán, Socio Director.

COMPETIMEX
Iglesia No. 2, Torre E, Despacho 1203. Col. Tizapán San Ángel. México, 01090, D.F. Tel: (52) 55 56167283
www.competimex.com