Ransomware: qué es y cómo protegerse de esta amenaza

Fotos, hojas de cálculo, videos, archivos PDF, son documentos que se almacenan en los dispositivos y se usan a diario, pero ¿qué sucedería si tu ordenador o tu móvil y todos los archivos que contienen fueran "secuestrados" y no se pudiera acceder a ellos? ¿Estás dispuesto a perder horas de trabajo y recuerdos personales? La mala noticia es que esto es cada vez más frecuente. La buena, es que si sigues leyendo te vamos a dar algunos consejos para evitar caer en la trampa de las bandas organizadas que se dedican a cometer este delito.

¿Qué es un ransomware y cuál es su objetivo?

Es un tipo de programa malicioso (malware) desarrollado para bloquear el acceso al equipo o a los archivos que contiene para, posteriormente, pedir un rescate a cambio de recuperarlos. Por desgracia es una amenaza cada vez más frecuente que afecta por igual tanto a personas como a empresas.

Existen distintas variantes de ransomware: las menos agresivas sólo impiden el funcionamiento normal del equipo, pero las más agresivas cifran todos los archivos del dispositivo (ordenador o teléfono móvil) impidiendo que se puedan abrir. En la mayoría de los casos la única solución es restaurar los archivos desde una copia de seguridad... siempre que la tengas, claro.

¿Cómo se infecta un dispositivo?

Los ciberdelincuentes tienen distintas maneras de infectar los dispositivos. La forma más común es mediante el correo electrónico con un fichero adjunto malicioso, pero hay otras. Aquí te las contamos:

Correo electrónico

Los ciberdelincuentes seleccionan una organización a la que suplantar y utilizan un mensaje alarmante o muy atractivo que deje poca capacidad de maniobra. Suele contener un fichero adjunto o un enlace para descargarlo. Si se trata de un correo que no estás esperando, lo mejor es que lo borres, ya que estos ficheros no son el malware, sino que son el programa que lo descarga. Y esta es la razón principal por la que los antivirus tienen problemas para detectarlo.

SMS/MMS y WhatsApp

El modus operandi seguido por los ciberdelincuentes es muy similar al utilizado con el correo electrónico. Tampoco debes fiarte de los mensajes que lleven enlace, de cuya procedencia no tengas una absoluta certeza: utilizan la ingeniería social para conseguir que hagas clic en el enlace, consiguiendo así que descargues el programa malicioso.

Redes sociales

En ocasiones las redes sociales se utilizan también para distribuir el ransomware: los ciberdelincuentes usan perfiles falsos o robados a otros usuarios para resultar menos sospechosos. No te fíes de aplicaciones milagrosas que prometen cosas increíbles o aquellas que se publicitan con muchas funcionalidades de forma gratuita: detrás puede esconderse un malware. Descarga siempre las aplicaciones de los sitos oficiales.

Archivos descargados desde Internet

Los archivos cuyo origen no es la fuente oficial, páginas de los fabricantes, mercados de aplicaciones, etc. pueden haber sido modificados por los ciberdelincuentes. Este tipo de archivos son generalmente software no oficial o «cracks» para hacer que la copia no original funcione. Al descargar y posteriormente instalar este tipo de archivos es posible que estés infectando tu ordenador o dispositivo móvil con ransomware u otro tipo de software malicioso.

Otras formas de infección

Esta es la forma de infección más peligrosa, porque es la más difícil de detectar. Se aprovecha de alguna vulnerabilidad sin "parchear" del sistema operativo, aplicación, navegador o plugin del dispositivo: si navegas con una aplicación sin actualizar te estás exponiendo a infectarte simplemente entrando a una página web maliciosa. Las páginas con contenido pornográfico son una fuente habitual de infección, pero ya no son el único entorno donde se esconden los virus. ¿La forma más fácil de evitarlo? Tener siempre el software actualizado con su última versión.

¿Cuáles son las principales organizaciones que suplantan los ciberdelincuentes?

Los cibercriminales usan a organizaciones reconocidas para engañarte, aprovechándose de la confianza que los usuarios tenemos en estas entidades. En Colombia suelen utilizar a instituciones públicas como la DIAN, Policía Nacional, Secretarías de Movilidad y Transporte.

¿Cómo evitar y mitigar esta amenaza?

Te recomendamos seguir estos consejos para protegerte de la amenaza del ransomware:

- *Mantén el sistema operativo, las aplicaciones y el antivirus siempre actualizados. Así los ciberdelincuentes no conseguirán infectar tu dispositivo mientras navegas por Internet.*

- *Evita abrir archivos adjuntos o acceder a enlaces en correos electrónicos no esperados, tanto si conoces el remitente como si no.*

- *Ten cuidado con los enlaces que te lleguen a través de SMS o de otros servicios de mensajería instantánea como WhatsApp y redes sociales.*

- *Evita aceptar solicitudes de amistad de personas que no conoces en las redes sociales.*

- *Ten cuidado cuando descargues e instales aplicaciones: procura evitar los repositorios no oficiales, sobre todo evita aquellas aplicaciones en las que el desarrollador no sea conocido y los comentarios y valoración de la app sean negativos. Y evita la descarga de aplicaciones o programas pirateados, debido a que son una fuente habitual de infección. Además de las recomendaciones anteriores es importante que también sigas todas las descritas en el artículo*

*de **phishing**, ya que el correo electrónico es la principal vía de difusión de este tipo de amenaza.*

Fuentes:

- Phishing – www.segu-info.com.ar
- Ransomware - https://www.bancosantander.es
- Contraseñas seguras - https://www.bancosantander.es