# RANSOMWARE

*Ing. José Guillermo Rodríguez Ávila*

*Operador de Sistemas*

Edicion 04-01

El ransomware ha sido uno de los códigos maliciosos que más relevancia ha tenido en los últimos tiempos, afectando a usuarios y empresas de todo el mundo.

Dado que su explosión ha sido repentina y surgen muchas dudas sobre este malware.


## ¿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. Hoy en día los creadores de ransomware piden que el pago se efectúe mediante criptomonedas o tarjetas de crédito.

## ¿De qué forma puede infectarse un equipo con un ransomware? Posibles modos o vías de infección

La forma de infección más usual es a través de la apertura de archivos adjuntos de correos electrónicos no solicitados o al hacer clic en vínculos que aseguran provenir de entidades bancarias o de empresas de mensajería. También se encontraron versiones de Cryptolocker que se distribuyeron a través de redes peer-to-peer (P2P) para compartir archivos, haciéndose pasar por claves de activación para programas populares de software como Adobe Photoshop y Micro soft Office.

Si el equipo se infecta, Cryptolocker busca una amplia gama de tipos de archivos para cifrar y, una vez que terminó el trabajo sucio, muestra un mensaje donde exige una transferencia electrónica para descifrar los archivos.

En algunos casos, la pantalla de bloqueo también incluye la transmisión en vivo de lo que la cámara web del equipo está viendo en ese momento.

Esta maniobra se utiliza para que los usuarios con menos conocimientos técnicos piensen que realmente están siendo observados por las autoridades.

## ¿A QUIÉN ATACAN SUS CREADORES?

Cuando se introdujo (y posteriormente se reintrodujo) el ransomware, sus primeras víctimas fueron sistemas particulares (es decir, personas normales y corrientes). Sin embargo, los ciberdelincuentes empezaron a ser conscientes de todo su potencial cuando desplegaron el ransomware para las empresas. El ransomware tuvo tanto éxito contra las empresas, llegando incluso a detener la producción y provocar pérdidas de datos y de beneficios, que sus creadores dirigieron la mayoría de sus ataques contra ellas.

## ¿EL ANTIVIRUS NO PUEDE SIMPLEMENTE QUITAR LA INFECCIÓN DE RANSOMWARE?

En la mayoría de los casos, un buen software de seguridad tendría que ser capaz de quitar el ransomware del equipo. Pero ahí no se termina el problema, porque si se trata de un filecoder, los archivos seguirán cifrados. El software de seguridad puede llegar a descifrar la información confidencial si se utilizó un filecoder básico en el ataque, pero los archivos que fueron atacados por un tipo más sofisticado de ransomware como Cryptolocker son imposibles de descifrar sin la clave correcta. Por este motivo, la mejor medicina es la prevención.

## TIPOS DE RANSOMWARE

### 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

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.

### Ransomware de cifrado

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.

## FUENTES


http://www.eset-la.com/pdf/kit-anti-ransomware/Guia-Todo_Sobre_Ransomware.pdf

https://es.malwarebytes.com/ransomware/


## GLOSARIO

**Criptomonedas:** son monedas virtuales. Pueden ser intercambiadas y operadas como cualquier otra divisa tradicional, pero están fuera del control de los gobiernos e instituciones financieras.

**Cryptolocker:** es una familia reciente de ransoms cuyo modelo de se basa en la extorsión al usuario. Otro malware famoso que también se basa en la extorsión es el Virus de la Policía, con el que había que pagar para poder recuperar el equipo.

**FileCoder:** muestra un mensaje diseñado para parecerse a medida que sale del local de aplicación de la ley y, de nuevo exige un pago con el fin de recuperar el acceso a su computadora.