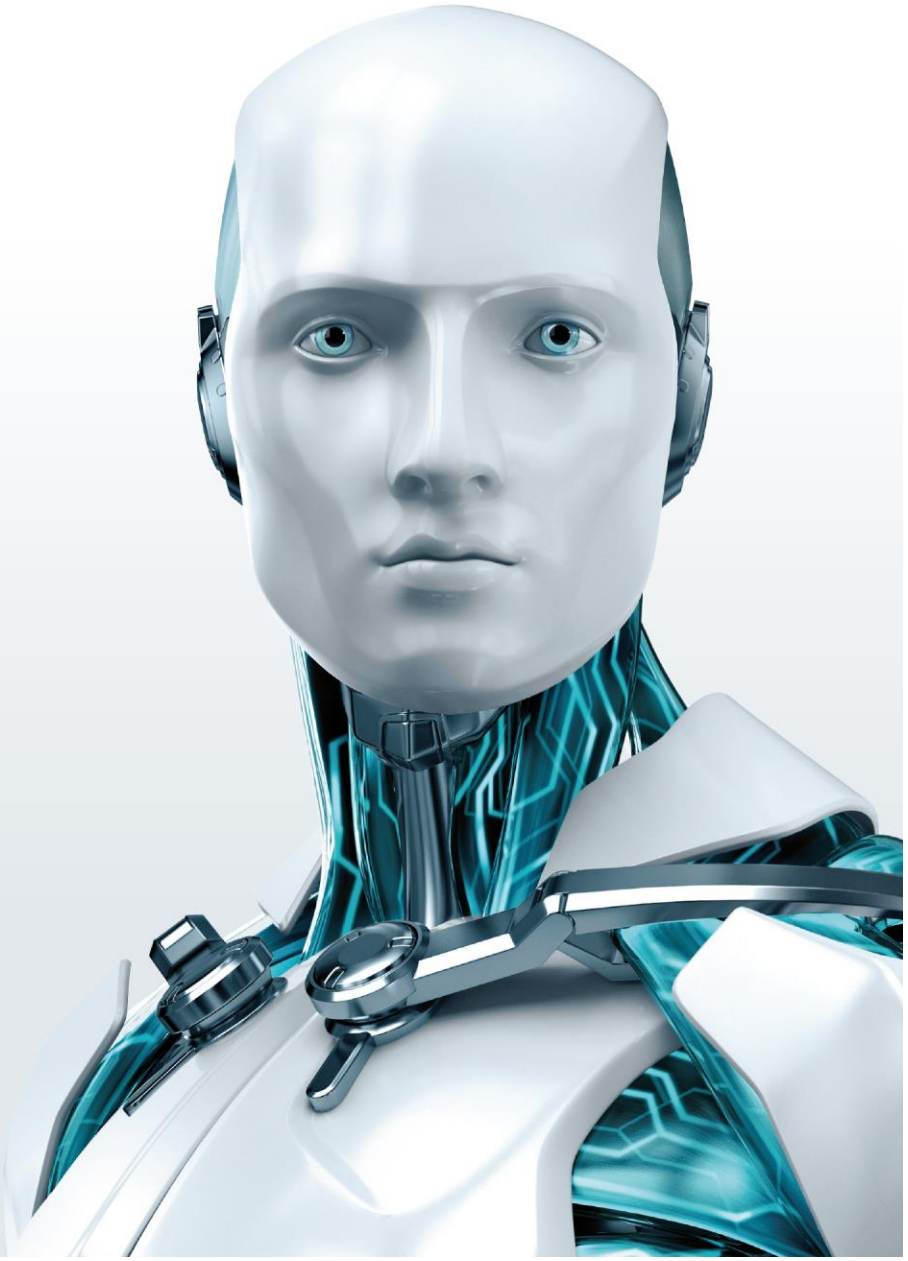
TODO SOBRE EL RANSOMWARE:

Guía básica y preguntas frecuentes



Octubre de 2016

ESET
ENJOY SAFER TECHNOLOGY™

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, desde ESET Latinoamérica hemos decidido responder algunas preguntas básicas y repasar algunos ataques para simplificar la comprensión de los mismos y brindar una explicación completa sobre el *ransomware.*

¿Qué es el *ransomware*?

El *ransomware* (secuestro de información) es el término genérico para referirse a todo tipo de software malicioso que le exige al usuario del equipo el pago de un rescate.

¿Por qué se accedería a pagar un rescate? ¿Cuál es el riesgo de no pagarlo?

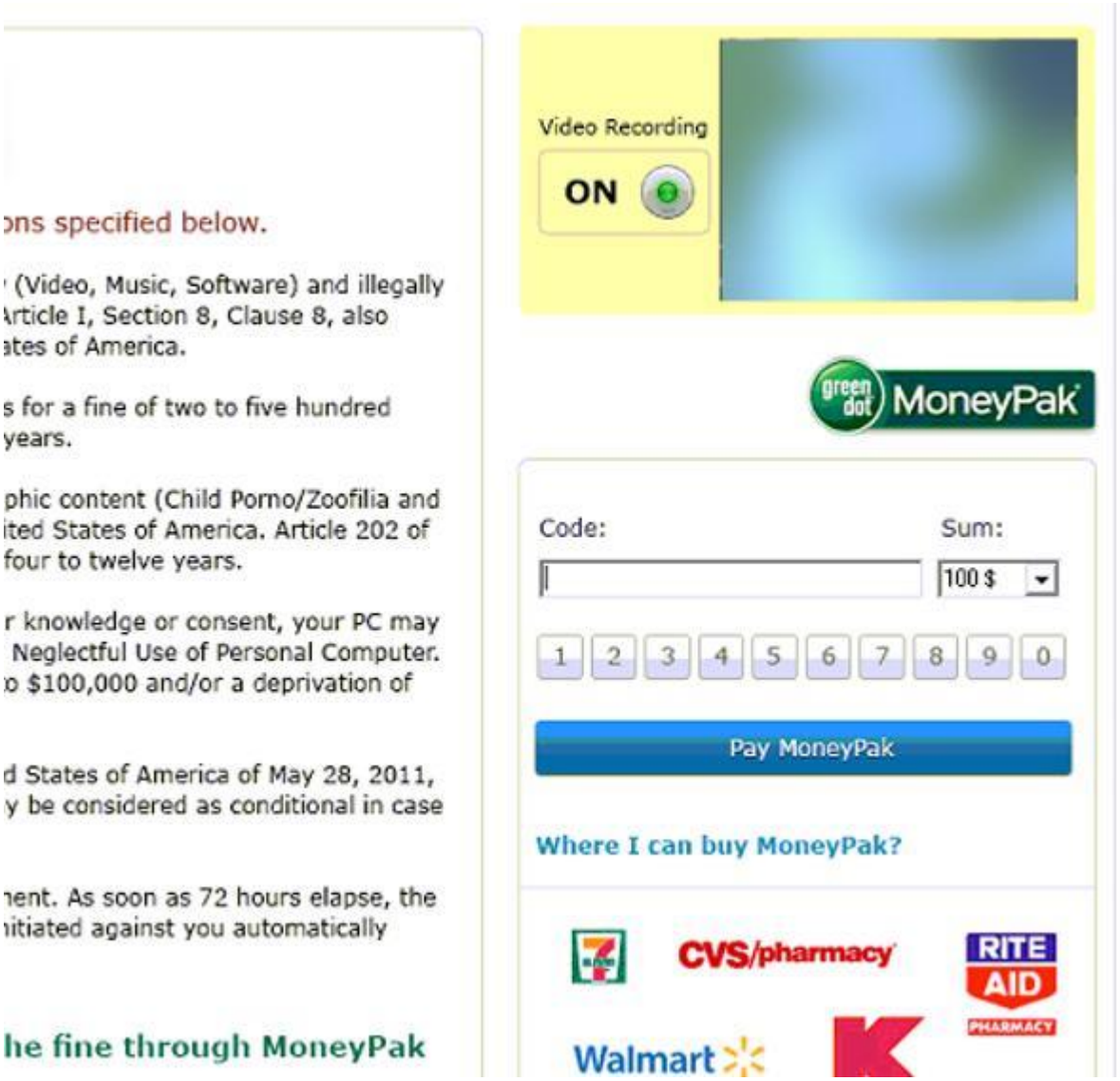
Este tipo de malware suele dañar el equipo y los datos que este contiene. Puede haber cifrado los documentos y exigir el pago de un rescate para desbloquear el acceso a ellos. Los códigos que actúan de este modo se conocen como ***filecoder*** (codificador de archivos). El más popular es **Cryptolocker**, y las soluciones de seguridad de ESET detectan muchas de sus versiones como Win32/Filecoder.

¿De qué forma puede infectarse un equipo con un ransomware como Cryptolocker? 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 Microsoft 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, como se ve a continuación:

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, como muestra la siguiente captura:



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

Otras amenazas: el *scareware*

El *scareware* (programas intimidatorios) es un *software* que intenta **asustar y engañar a las víctimas para que tomen un curso de acción** determinado. El más frecuente simula ser un producto antivirus que muestra una advertencia sobre problemas de seguridad presentes en el equipo o *smartphone,* con la intención de engañar al usuario para que le pague a los estafadores o para que siga descargando más códigos maliciosos desde la red.

En algunos casos, el falso antivirus se presenta bajo el nombre de una empresa de seguridad genuina con el objetivo de que se incremente la cantidad de damnificados. Observemos la siguiente imagen:

Al igual que el *ransomware*, el *scareware* puede estar escrito para cualquier sistema operativo. En algunas instancias del tipo falso antivirus tienen una interfaz de usuario que busca ser mucho más impactante que la del producto legítimo que están tratando de imitar con el objetivo de asustar al usuario desprevenido.

En el caso de algunos tipos de *scareware* con desarrollo más siniestro, cuando no logran asustar para que se haga la compra insensata, recurren a tácticas de *ransomware* y exigen el pago de una suma bajo una amenaza más evidente.

Consecuencias del *ransomware*

En la mayoría de los ataques, hay una fecha límite para realizar el pago: si el mismo no se realiza a tiempo, se podría perder el acceso a los archivos de manera permanente.

¿El de cifrado de archivos es el único tipo de *ransomware*?

Además del cifrado de archivos, también existe el *ransomware* del tipo *LockScreen*, que bloquea el equipo e impide que se lo utilice hasta que se realice el pago del rescate. Este *malware* a veces utiliza trucos psicológicos para engañar a la víctima y apresurar el pago.

Por ejemplo, en algunas ocasiones, el mensaje de la pantalla de bloqueo se hace pasar por un aviso de la fuerza de policía nacional donde se indica que las autoridades demandan el pago de una multa porque se encontraron en el equipo imágenes de abuso a menores o de zoofilia, evidencia de haber visitado sitios *web* ilegales, o *software* pirata.

Reveton es una de las familias encontradas con mayor frecuencia del tipo de *ransomware* que bloquea los equipos de los usuarios y muestra un mensaje supuestamente proveniente de las autoridades.

¿Qué sucede si se termina pagando el rescate?

Son muchas las personas que deciden pagar estos rescates ya que muchas veces no cuentan con una copia de seguridad (*backup*) verificada desde la cual restaurar sus archivos confidenciales o corporativos.

A los usuarios corporativos quizás no les preocupe demasiado el *malware* de pantalla de bloqueo; después de todo, con suerte tienen copias de seguridad y acceso a otros equipos de *hardware*. Pero es fácil imaginar a los usuarios domésticos, intimidados por las falsas amenazas de la policía o la mención de imágenes de abuso a menores, finalmente pagando el rescate en vez de llevar el equipo a la tienda local de reparación de computadoras.

¿El pago del rescate garantiza la recuperación de los datos?

El pago del rescate no significa que la víctima recuperará sus archivos ni que esté fuera de peligro. Los criminales **pueden dejar *malware* en el equipo** e identificar al usuario como uno dispuesto a pagar dinero en efectivo para recuperar el acceso al equipo o a los datos. En resumen, el pago del rescate podría favorecer otro ataque en el futuro.

Es por esta razón que desde ESET no recomendamos el pago. No hay forma de evitar que los atacantes exijan más dinero ni que se vayan a recuperar los archivos. Y mediante el pago del rescate se está ayudando a crear un nuevo mercado para los cibercriminales, lo que puede conducir a más ataques cibernéticos de *ransomware* y de otros tipos en el futuro.

Lo recomendable es adquirir una conducta más segura: tener solución de protección y llevar a cabo un régimen apropiado de creación de copias de seguridad para la recuperación de los archivos esenciales en caso que la empresa sufriera algún tipo de incidente.

¿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.

Entonces, ¿los filecoders que cifran los archivos confidenciales son peores que el malware de pantalla de bloqueo?

En general, la recuperación es más difícil en ataques de *ransomware* de cifrado de archivos que en otros tipos. Sin embargo, si existe una copia de seguridad que no fue alcanzada por el ataque, no será muy difícil volver a dejar todo listo y funcionando rápidamente. En definitiva, el peor tipo de *malware* siempre es el que infectó el equipo.

¿Qué sistemas operativos son el objetivo?

En teoría, no hay nada que detenga a los cibercriminales para escribir *ransomware* dirigido a cualquier sistema operativo, aunque la mayoría de los ataques son dirigidos a usuarios de Windows. De todas maneras los investigadores de ESET han encontrado familias de ransomware orientadas a smartphones con el sistema operativo Android y también existe ransomware para iOS.