Publicado en Ciudad de México el 18/01/2018

# [4 maneras de protegerse contra la creciente ola de ataques ransomware](http://www.notasdeprensa.es)

## El ransonmware se ha convertido en una táctica popular en el mundo del delito cibernético, es por ello que Avast comparte estos consejos para protegerse

 Avast, líder global en productos de seguridad digital, desglosa toda la información, herramientas y consejos necesarios para defenderse contra el malware cada vez más común, el llamado ransomware. El ransomware ha existido en formas primitivas desde finales de los 80, pero el primer acercamiento de su versión moderna llegó en 2013, cuando un insidioso virus llamado CryptoLocker infectó miles de computadoras y recaudó aproximadamente 3 millones de dólares en estos pagos de extorsión. Ese éxito, combinado con la forma tan simple en que es ejecutado por delincuentes, lo ha impulsado a convertirse en una táctica popular en el mundo del delito cibernético. Cómo el ransomware hace su trabajo sucioEl ransomware generalmente infecta el sistema a través de un correo electrónico de phishing que lo engaña para hacer clic en un enlace malicioso, pero también puede entrar si el sistema operativo no cuenta con las actualizaciones que corrigen ciertas vulnerabilidades. Sin embargo, los ciberdelincuentes siempre están desarrollando nuevos métodos de infección, como el ransomware WannaCry que atacó redes de computadoras enteras el año pasado, golpeando más de 400,000 equipos sin que el usuario haya tenido la necesidad de hacer clic en nada. Esta es la terrible realidad de los gusanos: se duplican para poder `esconderse´ en cada computadora conectada a una red en la que se infiltran. El ransomware típicamente escanea los archivos de una computadora, identificando los que parecen valiosos y encriptándolos. Si una organización grande es víctima de un ataque de ransomware, los archivos secuestrados pueden ser bases de datos importantes sin las cuales la empresa detendría esencialmente sus actividades. Si son usuarios domésticos, esos archivos pueden ser personales o confidenciales -como documentos financieros o fotografías. Al hacer clic en los archivos secuestrados, se activa una pantalla que exige el pago de un rescate para recuperar el acceso. La cantidad varía según el delincuente, pero el monto promedio es de trescientos dólares. El ransomware también suele dar una fecha límite, después de la cual, si no se hace el pago, los archivos se perderán para siempre. Si bien está es la forma más común de ransomware, existen variaciones. ScreenLocker es una cepa que congela el sistema, lo que impide realizar cualquier tarea excepto pagar el rescate. Doxware, otra variedad, captura información personal para chantajear, ya que amenaza con hacer pública la información si no se realiza el pago. Con un 99% de intención de infundir miedo, ScareWare exige un rescate, diciendo que el sistema está siendo atacado, cuando en realidad los perpetradores no están dañando los datos, solo intimidando. ¿Cómo defenderse contra el ransomware?El ransomware no es a prueba de balas, puede evitarse con estas 4 prácticas anti-ransomware: El primer consejo, el más básico, es también el más fuerte: hacer copias de seguridad. Si se tiene copia de seguridad de lo que los ciberdelincuentes han ´secuestrado´, ellos no tienen poder sobre nosotros. Mantener siempre actualizados el sistema operativos y software, para contar con las últimas protecciones. De igual manera, instalar un software antivirus sólido que incluya protección contra ransomware, como Avast Free Antivirus o AVG AntiVirus Free. Si los archivos se infectan, hay que mantener la calma y buscar en internet las herramientas de descifrado disponibles para ver si alguien ha desarrollado una forma de liberar los archivos encriptados. Los `chicos buenos´ lanzan herramientas de descifrado tan a menudo como los `tipos malos´ lanzan ataques de cifrado. No pagar el rescate. Pagar no garantiza el retorno seguro de los archivos. Una vez que tengan el dinero, los ciberdelincuentes pueden decidir simplemente dejar los archivos encriptados. Pagar también los motiva a atacar una y otra vez. Avast tiene nuevas soluciones ransomwareLa tecnología antivirus de Avast bloquea más de mil millones de ataques de malware cada mes, incluyendo al ransomware basado en Petya. Y si un ransomware de alguna manera pasa a través de los análisis de seguridad de varios niveles, hay una protección de nivel profundo llamada Behavior Shield que se activa, escaneando todo el software en ejecución en busca de actividades sospechosas. Si un archivo muestra signos de actuar de manera anormal, Behavior Shield lo detecta de inmediato, lo pone en cuarentena y lo destruye. También ofrecen una protección llamada Ransomware Shield, misma que evita que sus archivos más valiosos sean encriptados al envolverlos en capas adicionales de defensa. La amenaza es real, pero también la solución. Adquirir el conocimiento para defenderse de la ola actual de ataques. Cuando se sabe que se está protegido, no se vive con miedo. Obtener más información sobre la nueva protección de Avast contra el ransomware. Acerca de AvastAvast Software (www.avast.com), líder global en productos de seguridad digital para consumidores y empresas, protege a más de 400 millones de personas en línea. Avast ofrece productos con las marcas Avast y AVG que protegen a los usuarios de amenazas en internet y el escenario de amenazas de Internet de las Cosas que está en constante evolución. La red de detección de amenazas de la empresa está entre las más avanzadas del mundo, y utiliza tecnologías de aprendizaje automático e inteligencia artificial para detectar y detener amenazas en tiempo real. Los productos de seguridad digital Avast para dispositivos móviles, PC o Mac están clasificados como los mejores y certificados por VB100, AV-Comparatives, AV-Test, OPSWAT, ICSA Labs, West Coast Labs, entre otros. Avast cuenta con el respaldo de CVC Capital Partners y Summit Partners, que son sociedades de inversión de capital privado líderes en el mundo.

**Datos de contacto:**

Flor Carreno

56152196

Nota de prensa publicada en: [https://www.mexicopress.com.mx/4-maneras-de-protegerse-contra-la-creciente](http://www.notasdeprensa.es/educalivecom-disfruta-de-cursos-presenciales-y-clases-particulares-a-traves-de-internet)

Categorías: Software Ciberseguridad



[**http://www.mexicopress.com.mx**](http://www.notasdeprensa.es)