Publicado en Ciudad de México el 11/05/2017

# [Avast se une al proyecto No More Ransom](http://www.notasdeprensa.es)

## Avast se une al proyecto No More Ransom como socio adjunto para ayudar a las víctimas del ransomware a descifrar sus archivos

 Avast anunció que se sumó al proyecto No More Ransom, una iniciativa que ayuda a las víctimas del ransomware a recuperar sus archivos cifrados, sin pagar el rescate a los ciberdelincuentes. El ransomware se ha convertido en una de las mayores amenazas que enfrentan los usuarios de PC, dispositivos móviles e, incluso, usuarios de Mac. No More Ransom tiene cuatro socios principales y cuenta con el apoyo de organismos de seguridad de países de todo el mundo. El ransomware es un malware que bloquea un dispositivo o cifra los archivos, haciéndolos inaccesibles. Luego, los delincuentes exigen el pago de un rescate para desbloquear el dispositivo o los archivos. Los montos varían, pero en promedio, el año pasado rondaban en un bitcoin (aproximadamente, 500 dólares en ese momento). Habitualmente se disemina por medio del phishing en el correo electrónico o exploits, y se dirige tanto a usuarios individuales como a empresas. Hemos monitoreado el crecimiento masivo de los ataques de ransomware dirigidos a nuestros usuarios en México durante 2016. El crecimiento año con año fue 10 veces mayor comparado con el 2015, y cinco veces mayor en comparación con el total mundial año tras año. Observamos picos en Q2 y Q4 de 2016. Paramos más de dos ataques de ransomware cada minuto en México el año pasado. Hablando de ransomware, México fue el quinto país más atacado en 2016, después de Estados Unidos, Brasil, Rusia y Reino Unido, basado en nuestras estadísticas. ¿Por qué hay que tener cuidado? Avast identificó 60 millones de incidencias del ransomware Locky en 2016 Un rescate promedio es de 1 bitcoin (USD 533) Avast ahorró USD 64 mil millones en pagos de rescate Los equipos de TI se enfrentan a hasta 4 ataques por semana Las industrias más vulnerables a ataques de ransomware Sector Riesgo (%)Educación 13,0Sector público 5,9Sanidad 3,5Energía/Servicios públicos 3,4Sector minorista 3,2Finanzas 1,5 El proyecto No More Ransom comenzó a mediados de 2016 y ahora tiene 40 herramientas de descifrado gratuitas, seis de las cuales son provistas por Avast. Permanentemente, Avast está creando nuevas herramientas contra este flagelo, que se pueden encontrar en la página de herramientas gratuitas de descifrado de ransomware. "El ransomware se ha convertido en un negocio rentable para los ciberdelincuentes. Hubo un incremento de 105% de estos ataques de 2015 a 2016", afirmó Jakub Kroustek, que dirige el equipo del laboratorio de amenazas y es el cocreador de las herramientas de descifrado de ransomware de Avast. "Esperamos que el proyecto No More Ransom difunda el conocimiento de las herramientas de descifrado gratuitas que existen. Si podemos reducir la cantidad de rescates pagados, podremos hacer que el ransomware sea menos atractivo para los ciberdelincuentes". Si bien las herramientas de descifrado pueden ayudar a desbloquear archivos, deben considerarse la última opción. El ransomware se ha vuelto tan lucrativo que hasta se promociona y se vende en la red oscura, de modo que incluso los hackers con menos conocimientos técnicos pueden comprar, modificar y diseminar ransomware. Esto significa que todos los días aparecen versiones nuevas y un dispositivo se puede infectar con una variedad para la que no existe una herramienta de descifrado. Por lo tanto, recomendamos instalar un antivirus, que funcione como una red de seguridad y proteja contra el ransomware, si llegara a aparecer; y que, periódicamente, se haga una copia de resguardo de los archivos en un disco duro externo, que no esté conectado a la computadora o a internet. Desde 2013, los investigadores de Avast Threat Labs han visto un aumento enorme en la cantidad de amenazas de ransomware. Solo el año pasado, monitorearon más de 150 variedades nuevas, y Avast creó herramientas gratuitas de descifrado de ransomware para ayudar a las víctimas a desbloquear archivos cifrados. Los sistemas de Windows son los blancos habituales, pero también los usuarios de Mac sufren estos ataques. La forma más común para que el ransomware entre en un sistema es a través de enlaces maliciosos y archivos adjuntos de correo electrónico. Según una encuesta de Osterman Research, efectuada de junio de 2016, en los Estados Unidos y Alemania, casi la mitad de los ataques se debieron a que algún empleado pulsó un enlace que no debía en un correo electrónico. Para protegerse de ataques de ransomware Instale un antivirus No abra adjuntos desconocidos Sea cuidadoso con las descargas Haga una copia de resguardo de sus datos en forma habitual Si sufre un ataque, utilice el paquete de herramientas descifradoras de ransomware de Avast

**Datos de contacto:**

Flor Carreño

Marketing Q S

5552866201

Nota de prensa publicada en: [https://www.mexicopress.com.mx/avast-se-une-al-proyecto-no-more-ransom](http://www.notasdeprensa.es/educalivecom-disfruta-de-cursos-presenciales-y-clases-particulares-a-traves-de-internet)

Categorías: Telecomunicaciones Comunicación E-Commerce Software Ciberseguridad



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