Publicado en Ciudad de México el 09/05/2018

# [Ciberataque WannaCry un año después](http://www.notasdeprensa.es)

## Ondrej Vlcek, CTO de Avast repasa el año transcurrido desde el ataque cibernético de WannaCry y pregunta si la industria de la tecnología ha hecho lo suficiente para evitar que vuelva a suceder

 El 12 de mayo de 2017 estalló el mayor ataque de ransomware de la historia. `WannaCry´, el infame ransomware que se extendió afectando indiscriminadamente a las PCs de todo el mundo, incluyendo los equipos de consumidores, empresas, servicios de atención e incluso departamentos gubernamentales. Casi un año después, el malware WannaCry, que explota la vulnerabilidad de EternalBlue continúa en circulación, como en el reciente caso en el que afectó al fabricante de aviones Boeing. Avast, líder global en productos de seguridad digital, ha detectado y bloqueado más de 176 millones de ataques de WannaCry en 217 países desde el ataque inicial del año pasado y, en marzo de 2018, Avast impidió 54 millones de ataques que intentaban abusar de EternalBlue. Datos de Avast, sin embargo, muestran que casi un tercio (29%) de las computadoras basadas en Windows en todo el mundo todavía son vulnerables. La intención detrás del ataque inicial de WannaCry parece haber sido la destrucción, llevada a cabo por un estado-nación y no por ciberdelincuentes con fines de lucro, lo que tradicionalmente ha sido la principal motivación que impulsa los ataques de ransomware. Se estima que los actores detrás de WannaCry cobraron aproximadamente $ 140,000 a fines de agosto. El éxito de WannaCry se reduce a tres factores clave: explotó una vulnerabilidad que prevalecía en muchas PCs con sistemas operativos antiguos; los sistemas operativos antiguos no estaban soportados y, por lo tanto, eran vulnerables al exploit; y no se requirió la acción del usuario para ayudar a la propagación, ya que tomó la forma de un gusano. Avast, a lo largo del año transcurrido desde que causó su daño, ha investigado y recopilado ideas que pueden ayudar a comprender qué se debe hacer para evitar que este tipo de ataque cibernético vuelva a suceder. La mala adopción de parches hizo posible WannaCryWannaCry se propaga agresivamente usando la vulnerabilidad de Windows EternalBlue, o MS17-010, infectando computadoras sin interacción del usuario. EternalBlue es un error crítico en el código de Windows de Microsoft que es al menos tan viejo como Windows XP. La vulnerabilidad permite a los atacantes ejecutar código de forma remota creando una solicitud para el servicio de Compartir archivos e impresoras de Windows. El malware WannaCry ya activo en una PC escanea tanto la red local como la subred y elige aleatoriamente las direcciones IP. Una vez que encontró una PC vulnerable, el ransomware se extendió a esa PC también, lo que fue posible debido a la funcionalidad de un gusano. Microsoft lanzó un parche para EternalBlue en marzo, dos meses antes del éxito de WannaCry. Sin embargo, WannaCry atacó con éxito a cientos de millones de usuarios porque las personas no aplicaron el parche para la vulnerabilidad de EternalBlue. Si solo hubiera un parche para una mala adopción de parchesA pesar de la atención generalizada de WannaCry y los efectos devastadores que tuvo en empresas y consumidores, la gente aun no aplicó el parche en sus sistemas. Esto plantea la pregunta: ¿por qué las personas no están utilizando el parche? A continuación algunas conjeturas sobre las razones más probables. En primer lugar, podría deberse a una falta de comprensión sobre los parches o actualizaciones de software. El consumidor promedio puede no ser plenamente consciente de que los sistemas contienen vulnerabilidades y que los ciberdelincuentes pueden aprovechar para propagar malware. La segunda posibilidad sobre la pobre adopción de parches es que a los consumidores no les gustan las interrupciones y aplicar un parche requiere que los usuarios detengan lo que están haciendo y esperen a que se descargue. Otra razón por la que las personas no pueden actualizar es resistirse al cambio. Las actualizaciones pueden cambiar los entornos y las interfaces del programa familiar, lo que no siempre es bienvenido por todos los usuarios. En tercer lugar, para algunas empresas y organizaciones la interrupción causada por el parche, puede requerir la reducción de servicios mientras se lleva a cabo la actualización. Por último, pero no menos importante, algunos sistemas no fueron reparados cuando WannaCry llegó porque los sistemas más antiguos, como Windows XP, ya no eran compatibles y, por lo tanto, quedaron indefensos. Parche perfecto: lo que la industria de la tecnología debe hacer mejorPara mejorar la adopción de parches, la industria de la tecnología necesita trabajar en conjunto para aumentar la consciencia sobre los parches, su propósito, los problemas que solucionan y los posibles ataques que evitan. Esto se puede hacer explicando el propósito de los parches emitidos a los usuarios cuando se les pide que actualicen, usando términos simples para describir la actualización y su relevancia. Si bien es importante no alarmar, las personas pueden estar más inclinadas a utilizar el parche si se dan cuenta de que existe un problema que podría afectarlos negativamente. Finalmente, los desarrolladores de software deben considerar que sus sistemas pueden vivir más allá de los años previstos gracias a un hardware robusto y que necesitan soporte continuo. Windows XP, por ejemplo, sigue siendo utilizado por el 4.3% de los usuarios de Avast y Windows Vista todavía se usa en un 1.5%, aunque Microsoft ya no brinda soporte para estos populares sistemas operativos. Asegurar actualizacionesEn última instancia, está claro que la industria de la tecnología no puede esperar que los usuarios comprendan por completo y lleven a cabo las mejores prácticas de seguridad por sí mismos. Los usuarios necesitan ayuda y educación sobre seguridad y orientación a través de los pasos necesarios para que sus experiencias sean lo más fáciles, simples y cómodas posible. Al mismo tiempo, los distribuidores de software deben asegurarse de que las actualizaciones que envían a sus clientes estén limpias. Si esto se puede hacer, la colaboración y la contribución de los usuarios con la industria de la tecnología y con los investigadores y las empresas de seguridad es verdaderamente poderosa en la lucha contra el malware. Si bien aún no se sabe qué impacto podría tener el próximo WannaCry, con base a estas ideas críticas del año pasado, está claro que la industria de la tecnología, en colaboración con los usuarios, debe hacer más para evitar que un ataque tan importante vuelva a ocurrir.

**Datos de contacto:**

Flor Carreno

56152196

Nota de prensa publicada en: [https://www.mexicopress.com.mx/ciberataque-wannacry-un-ano-despues\_1](http://www.notasdeprensa.es/educalivecom-disfruta-de-cursos-presenciales-y-clases-particulares-a-traves-de-internet)

Categorías: Internacional Telecomunicaciones Software Ciberseguridad Ciudad de México



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