Publicado en Ciudad de México el 18/07/2018

# [Avast: 87% de los mexicanos teme que malware de criptominería infecte sus dispositivos](http://www.notasdeprensa.es)

## La investigación fue realizada con el fin de entender mejor la percepción y el conocimiento de los mexicanos sobre fenómeno de la criptominería

 De acuerdo con un nuevo estudio de Avast, el líder global en productos de seguridad digital, el 87% de los consumidores de México está preocupado por la posibilidad de que malware de criptominería infecte sus dispositivos inteligentes personales y del hogar. Dentro del grupo de encuestados, alrededor de la mitad 46%, erróneamente, se cree inmune a los malware de criptominería pues dice no poseer criptomonedas ni hacer minería digital. La investigación fue realizada con el fin de entender mejor las percepciones públicas y el conocimiento existente del fenómeno de la criptominería -el proceso malicioso que mina criptomonedas de forma encubierta usando un malware insertado en el dispositivo de un individuo. Más de la mitad (52,9%) de los consumidores mexicanos dijeron que han escuchado sobre malware o de sitios web infectados en el proceso de minado de criptomonedas. Los hallazgos sugieren que los consumidores de México están adoptando una actitud apática hacia el criptominado malicioso y que el conocimiento de esta amenaza es escaso. Esto a pesar de que 76 por ciento de quienes contestaron este sondeo admiten estar familiarizados con las monedas digitales. Durante los últimos 12 meses, el malware detrás del minado de monedas se ha vuelto más sofisticado y se ha amplificado. Lo que en algún momento se trató de una amenaza cibernética dirigida a los computadores personales se ha convertido rápidamente en un riesgo mayor para los teléfonos inteligentes y para el complejo ecosistema de los dispositivos del Internet de las Cosas. Para ser efectivo y rentable, el criptominado tiene que alimentarse del poder de los computadores a gran escala. Y en virtud de que los costos derivados del minado son elevados y de que el poder de las unidades centrales de procesamiento (CPU) y de los teléfonos inteligentes es bajo, los cibercriminales intentan secuestrar dispositivos conectados a redes, conocidas como botnets, para maximizar sus ganancias. Para las víctimas, esto puede implicar un incremento en las facturas del servicio eléctrico, baja productividad o un desempeño mediocre de sus dispositivos y el acortamiento de la vida útil de esos dispositivos. Un equipo secuestrado por los cibercriminales puede afrontar un riesgo mayor de que los datos personales de ese usuario sean robados. "Estamos observando un incremento significativo de cibercriminales que captan dispositivos de Internet de las Cosas y teléfonos inteligentes hacia los botnets con la intención de minar criptomonedas. El malware puede correr imperceptiblemente en el segundo plano de cualquier dispositivo inteligente, no importa si la víctima tiene criptomonedas o no. La meta de Avast es disipar los mitos asociados con el criptominado malicioso y educar a la gente sobre los riesgos que implica esta práctica para los datos personales y el rendimiento de los dispositivos", dijo Luis Corrons, Evangelista de Seguridad de Avast. "Típicamente, los usuarios de computadores personales pueden decir si sus computadores son parte de una botnet pues tienden a responder de una forma más lenta que lo usual, se calientan o distribuye un tráfico sospechoso. Con los dispositivos del Internet de las Cosas, como un refrigerador inteligente o un asistente personal, los síntomas no son tan obvios. Los usuarios necesitan soluciones de seguridad que monitoreen el tráfico y comportamiento de estos dispositivos y que los alerten en caso de que algo irregular se presente". Se han registrado algunos casos en los cuales los sitios web han ofrecido a los visitantes elegir entre ver publicidad o minar criptomonedas en un segundo plano. El 44% de los usuarios en México dijo que elegiría el criptominado a cambio de una navegación libre de avisos publicitarios. Los usuarios de computadoras personales y de teléfonos inteligentes pueden implementar la solución Avast Free Antivirus para PC o Avast Mobile Security para dispositivos Android. Avast lanzará Smart Home Security dentro de unos meses, una solución basada en Smart Life, la plataforma de seguridad de Avast para Internet de las Cosas, que brinda a los usuarios protección basada en Inteligencia Artificial y monitoreo de las actividades en la red doméstica. Avast realizó este estudio en abril de 2018 para el cual más de 1.200 usuarios de computadores personales fueron consultados.El 11 por ciento de las personas sondeadas son dueños o invierten en criptomonedas y 45 por ciento está planeando invertir en criptomonedas. Acerca de AvastAvast (LSE: AVST) es el líder global en productos de seguridad digital. Con más de 400 millones de usuarios en línea, Avast ofrece productos bajo las marcas Avast y AVG que protegen a las personas de las amenazas en internet y el escenario en evolución de amenazas de Internet de las Cosas. La red de detección de amenazas de la compañía 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 de Avast para dispositivos móviles, PC o Mac están clasificados como los mejores y certificados por VB100, AV-Comparatives, AV-Test, OPSWAT, ICSA Labs, West CoastLabs, entre otros. Avast cuenta con el respaldo de las firmas globales líderes de capital privado CVC Capital Partners y Summit Partners. Visitar: www.avast.com.

**Datos de contacto:**

Flor Carreno

Agencia de Relaciones Públicas

56152196

Nota de prensa publicada en: [https://www.mexicopress.com.mx/avast-87-de-los-mexicanos-teme-que-malware-de](http://www.notasdeprensa.es/educalivecom-disfruta-de-cursos-presenciales-y-clases-particulares-a-traves-de-internet)

Categorías: Ciberseguridad Dispositivos móviles Ciudad de México



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