Publicado en Ciudad de México el 27/02/2018

# [Los cibercriminales podrían construir ejércitos que minen criptomonedas usando dispositivos IoT vulnerables](http://www.notasdeprensa.es)

## Un experimento de Avast demuestra que consumidores de dispositivos IoT y smartphones fueron ilegalmente utilizados para minar criptomonedas

 En el Mobile World Congress 2018, Avast, líder global en productos de seguridad digital, estará realizando un experimento para incrementar el nivel de alerta acerca de las vulnerabilidades del Internet de las cosas (IoT) y de dispositivos móviles al minar la criptomoneda Monero usando un Smart TV. El año pasado se ha visto un incremento en cómo los cibercriminales han abusado de smartphones y dispositivos IoT para minar criptomonedas en segundo plano sin que los usuarios se den cuenta. Para experimentar cómo sus propios dispositivos pueden ser infectados, los asistentes serán invitados a ser parte del experimento usando sus teléfonos inteligentes para minar Monero, una popular criptomoneda entre ciberdelincuentes debido a su anonimato. Investigaciones recientes de Avast muestran que sería necesario un ejército de más de 15,800 dispositivos para minar $1,000 dólares en monedas Monero durante los cuatro días del congreso. Los smartphones y dispositivos IoT, como un Smart TV, cámaras web o termostatos, normalmente tienen muy bajo poder computacional, lo que es malo para la minería. Por esta razón, los ciberdelincuentes están buscando atacar dispositivos a gran escala para maximizar beneficios. Minar sobre dispositivos IoT sigue siendo, en su mayoría, invisible para los consumidores; ya que a diferencia de las PC’s, no es notable cuando un dispositivo IoT se calienta o baja su desempeño. "Hasta hace poco, los ciberdelincuentes estaban enfocados en expandir malware para convertir las PC’s en máquinas mineras de criptomonedas, sin embargo ahora estamos presenciando un incremento en ataques enfocados a los dispositivos IoT y teléfonos inteligentes," dijo Gagan Singh, Vicepresidente Senior y Gerente General, Mobile de Avast. "De acuerdo con datos recientes de Shodan.io, un motor de búsqueda para el Internet de las Cosas, 58.031 dispositivos inteligentes en Barcelona son vulnerables. Si cada uno de estos dispositivos fuera reclutado a una botnet para minar Monero en el Mobile World Congress, los ciberdelincuentes podrían ganar aproximadamente el equivalente de $3.600 dólares o €3.000 euros. Los costos involucrados en minería son tan altos que los beneficios de minar criptomonedas son muy bajos, motivando a los cibercriminales a no solo atacar a miles sino a millones de dispositivos." El complejo ecosistema de dispositivos IoT en hogares y lugares públicos crea nuevas oportunidades para los ciberdelincuentes para comprometer la seguridad y la privacidad de las personas. En 2017, aparecieron las primeras botnets de IoT, una nueva versión del infame Mirai botnet, para minar criptomonedas. Desde entonces, el riesgo de que los ciberdelincuentes tomen el control de los dispositivos IoT para sacar beneficios de la minería de criptomonedas se ha incrementado. Para los usuarios, esto puede significar altas cuentas de energía, pobres desempeños de sus dispositivos y una reducción en la vida útil de sus dispositivos. Sin embargo, la minería de criptomonedas por malware es sólo uno de los muchos riesgos que los hogares conectados enfrentan. Otro riesgo mayor es la amenaza a la privacidad, que se eleva con el número de cámaras de seguridad vulnerables que graban nuestras vidas día a día, así como los altavoces inteligentes que escuchan y graban nuestras conversaciones y que podrían ser hackeados. Avast anunció hoy Avast Smart Life, una solución que aborda las amenazas de seguridad de los dispositivos IoT para mantener seguros los hogares de la personas y sus vidas privadas. En el stand de Avast, los visitantes tendrán la oportunidad de ver cómo muchos de los Smart TV y teléfonos inteligentes han sido minados en tiempo real. Los asistentes que participen en el experimento de minado con sus propios teléfonos recibirán un banco de energía y el participante que mine más monedas ganará un Samsung Galaxy S8 con la aplicación Avast Mobile Security instalada, protegiendo a los usuarios de las amenazas incluyendo malware de criptominería. Avast mantendrá el Monero minado y donará el monto final en el Mobile World Congress 2019 a la organización española Pantallas Amigas, una iniciativa que promueve el uso seguro y saludable de las nuevas tecnologías, así como también la responsabilidad digital durante la infancia y adolescencia. Acerca de Avast:Avast 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/los-cibercriminales-podrian-construir](http://www.notasdeprensa.es/educalivecom-disfruta-de-cursos-presenciales-y-clases-particulares-a-traves-de-internet)

Categorías: Internacional Ciberseguridad Dispositivos móviles



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