Nuevo método de minería de criptomonedas

Toda esta fiebre del BitCoin han puesto a los cibercriminales a **crear nuevas formas y técnicas para encontrar y explotar vulnerabilidades** del propio sistema para obtenerlas sin tener que pagar un peso por ellas.

Un caso reciente es la empresa **Coincheck**, denominada por sí misma como **la empresa líder en el intercambio de Bitcoins y criptomonedas de Asia**, que ha sido víctima de un multimillonaro ciberataque. Este hecho represento para la empresa una pérdida de 523 millones de unidades de la criptomoneda NEM, lo que vendrían siendo 58.000 millones de yenes (más de US$500 millones) demostrando que no es buena idea invertir nuestros ahorros en criptomonedas, no solo por **la volatilidad del mercado sino también por las fallas que aún presenta el sistema**.

Otro caso bastante nombrado por los medios digitales, fue el de la casa de cambio de Tokio, MtGox, la cual quebró en 2014 después de admitir que le habían robado US$400 millones de su red.

Minado: Otra forma de obtener monedas.

Pero el robo no es la única técnica usada por estos delincuentes para apoderarse del **“oro del nuevo orden mundial”**, otros más hábiles se inventaron una nueva técnica para obtenerlas por medio de la minería usando estaciones de

trabajo caseras como zombis. Los **usuarios sin darse cuenta realizan labores de minado** consumiendo energía eléctrica y gran parte de los recursos de sus computadoras.

A finales del 2017 se conoció el caso de la **extensión para Google Chrome llamada Archive Poster**, la cual se describía en la Google Store como una ayuda para que los usuarios republicaran entradas de blogs en Tumblr. La misma Google público que esta extensión contenía un **código oculto de Coinhive**, este código oculto realizaba su trabajo de minado en segundo plano tan pronto como el usuario abría el navegador Chrome.

Youtube Nuevo caballo de Troya.

El uso de código malicioso en Chrome, no es el único caso de minado donde toman como Caballo de Troya a un producto de Google; en el caso más **reciente el protagonista es Youtube**. Siendo más exactos el código malicioso se encuentra insertados en los anuncios que arrancan al inicio del video y que realiza minería de la moneda digital Monero.

Varios usuarios afectados manifestaron **experimentar consumos excesivos de recursos** en sus máquinas al reproducir un vídeo desde Youtube. Otros por su parte comentaron sobre las alertas que saltaban desde sus programas antivirus alertándolos del bloqueo al intento de acceso a una dirección web dedicada a la minería de monedas digitales.

El gran Google se pronunció al respecto:

> *“La minería de criptomonedas a través de anuncios es una forma relativamente nueva de abuso que infringe nuestras políticas y que hemos estado monitoreando activamente. Hacemos cumplir nuestras políticas a través de un sistema de detección de varias capas en todas nuestras plataformas que*

actualizamos a medida que surgen nuevas amenazas. En este caso, los anuncios fueron bloqueados en menos de dos horas y los actores maliciosos fueron eliminados rápidamente de nuestras plataformas”

Pasadas las dos horas luego de emitido el comunicado, aún se podía observar anuncios con este tipo de códigos de minado, por lo que no sabemos a qué se refería el representante de Google al afirmar que fueron bloqueados.

En todo caso y como método de defensa aconsejan mantener **nuestros programas antivirus actualizados**, ya que ante esta nueva amenaza las grandes empresas de antivirus han optado por incluir detecciones de códigos que se dediquen a la minería.

Y si llegaste hasta el final: Cómo funciona el bitcoin, transacciones, registro, seguridad, Todo lo que debes conocer de Ethereum