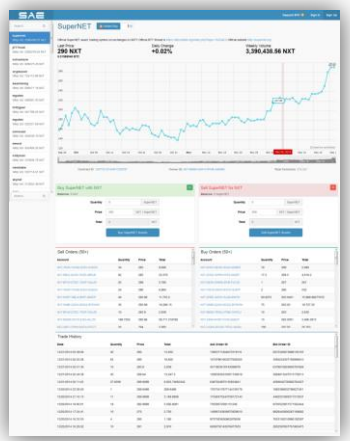
NOTA DE FUTURO 4/2018

25 de abril de 2018

*Yaiza Ibarra**

Los nuevos Ciberdelitos

Nota de futuro: Los nuevos Ciberdelitos



Bolsa de intercambios

1. Una aproximación al Bitcoin

La palabra "criptomoneda" ha saltado de un tiempo a esta parte a los medios de comunicación y se ha colado en conversaciones de quienes no son expertos en el tema. Eso conlleva, por un lado, que sean cada vez más los usuarios que deciden invertir en estas monedas virtuales y que, por ende, el mercado se amplíe con nuevos consumidores. Por otro, el usuario que se lanza a ello no suele tener los conocimientos adecuados para invertir dinero de forma segura o, al menos, siendo consciente de las consecuencias. Normalmente el perfil de quienes se deciden a entrar en estos mercados son personas con interés por escapar del control de instituciones y gobiernos, y con la idea de que las criptomonedas permiten enriquecerse mucho en muy poco tiempo.

Lo que se desconoce del trato con las criptomonedas es que su fluctuación es muy intensa a lo largo de un solo día y, aunque cada vez más bancos y entidades prestan atención a lo que suceda en ellos, tradicionalmente se enmarcan dentro de acciones cuando menos alegales. A inicios del año 2015, un Bitcoin valía poco más de 300 dólares y, al finalizar 2017, la divisa virtual superó la barrera de los 10.000 dólares.

Algunos expertos tildan el enorme crecimiento de "burbuja" que no tardará en explotar. Aunque existen más criptomonedas, además de Bitcoin, esta es una de las más populares, junto con Ethereum.

Bitcoin nació en 2009 de la mano de Satoshi Nakamoto, una persona o un grupo de ellas -algo que nunca se llegó a esclarecer- que publicó la información del Bitcoin en un somero mensaje, explicando su funcionamiento a través de códigos y la cadena de bloques -o blockchain- y también su finalidad: que la riqueza escapase al control gubernamental.

* Alumna en prácticas del Máster de RRII de la Universidad de San Pablo CEU

Desde entonces no solo se ha "democratizado" el término de criptomoneda, o la intención de invertir en ella, sino que el blockchain se erige como la puerta a una nueva revolución tecnológica que puede hacer avanzar y rediseñar nuestra interacción con Internet.

La premisa del blockchain es que los datos se almacenan por nodos, siendo un nodo cada ordenador de una misma cadena. Por tanto, la información no se puede alterar o modificar porque para ello habría que hacerlo en todos los ordenadores, o nodos, al mismo tiempo y tampoco se necesita una autoridad superior que verifique un movimiento o transacción, sino que se va registrando o "minando", en los bloques a medida que se realizan. Esta acción de minar requiere no solo a un buen número de personas grabando cada transacción en los nodos, sino también cantidades ingentes de electricidad que, a veces, se consiguen de dispositivos de usuarios mediante malware instalado en sitios web.

Estos registros se hacen de forma anónima, de manera que queda patente el movimiento, pero no su emisor ni tampoco su receptor. El anonimato que promulga blockchain y con el que trabajan Bitcoin y las demás criptomonedas hace pensar, en primera instancia, por qué los criminales de todo tipo prefieren operar con monedas virtuales.

Redes sociales como Facebook han tomado la determinación de eliminar anuncios que invitaban a la compra e inversión de Bitcoin, Ethereum y otras monedas virtuales en aras de evitar arrastrar a un público no conocedor de los riesgos de estas acciones.

El mercado de las criptomonedas está descentralizado, es decir, no hay que acudir a un espacio físico para entrar y comprar divisas virtuales. Basta con abrirse un perfil en algunos de los portales más conocidos, como Binance, Coinbase, CoinMarketCap, HitBTC o ETHDelta. Para quienes realizan transacciones en este tipo de mercados es esencial contar con un monedero virtual en el que se guardan tanto las claves y contraseñas para acceder a las diferentes sesiones como la cantidad que cada usuario posea de estas criptodivisas.

Los monederos pueden ser físicos o virtuales. No dan acceso a los Bitcoins como tal -que están dentro de la cadena de bloques- sino que es donde se almacenan las claves personales de cada usuario para acceder a las monedas virtuales. Hay variedad a la hora de hablar de monederos de Bitcoin: desde los llamados "monederos fríos", discos duros externos que almacenan las

contraseñas, hasta las casas de cambio de los propios bancos, pasando por aplicaciones de carteras y monederos en línea. Estos son los más vulnerables ante un ataque.

2. Amenazas actuales para la sociedad

Es precisamente el auge de los delitos motivados por Bitcoin y demás criptomonedas que los cuerpos de seguridad de muchos países están dando la voz de alarma. Los delincuentes y ladrones más avezados ahora también se fijan en las monedas virtuales que tenga su víctima para poder hacerse con un botín que no deja huella y que llega prácticamente al instante a su cuenta.
Mientras que los bancos pueden revertir transacciones que se hayan emitido por coacción de un robo, el funcionamiento de Bitcoin no solo no lo permite sino que tampoco deja al descubierto la identidad del ladrón, haciendo que sea prácticamente imposible que las fuerzas de seguridad rastreen el recorrido del dinero.

El protocolo es que los ladrones que entran en un domicilio no van buscando joyas o dispositivos electrónicos de gran valor, sino las contraseñas de los monederos virtuales de los que dispone cada usuario que posee algo de dinero en Bitcoins.

Los secuestros de datos para conseguir dinero virtual o secuestros físicos también se producen por el aumento de intercambios de usuarios que quedan para vender o comprar Bitcoins. Los ladrones aprovechan el encuentro para extorsionar al individuo o a sus familiares.
En 2018 ya se han producido varios casos en Reino Unido o Taiwán[1], en los que los usuarios quedaban con los ladrones en un espacio físico, alentados por la compra de Bitcoins billete en mano. En ese momento, eran extorsionados para revelar sus datos y contraseñas a los ladrones.

Otra de las amenazas para la sociedad que con más asiduidad se están produciendo es la de los malwares dedicados a páginas web y sitios populares, que se alimentan de la red eléctrica de los usuarios y sus dispositivos electrónicos para minar criptomonedas. Un estudio reciente puso de manifiesto que sistemas operativos como la red eléctrica y de agua de algunos países europeos, Reino Unido y Estados Unidos estaban infectados con este tipo de virus. En otro plano, páginas web tan visitadas como YouTube también tenían el malware que provoca que el dispositivo desde

[1] https://www.aljazeera.com/news/2018/02/bitcoin-robbery-taiwan-leads-arrests-180222085146715.html

el que el usuario entra a la plataforma se ponga automáticamente y sin que este se entere a ofrecer su batería o conexión a la red eléctrica para minar criptomonedas.

3. Amenazas actuales para la seguridad

El principal problema de seguridad que se fomenta con la compra y venta de Bitcoins es que las vulnerabilidades pueden aparecer en cualquier parte del mundo y extenderse rápidamente a otros ordenadores o dispositivos desde los que se opere en el mercado virtual. Al ser una amenaza descentralizada, muchos de los ciberdelincuentes se afanan por encontrar una brecha de seguridad, en los negocios de cambio de divisas virtuales y también en los monederos de los usuarios. Algunos monederos de este estilo han visto cómo el aumento de los ataques a sus servidores les han hecho perder clientes de forma masiva, que se han ido espantados por los robos de dinero virtual, los secuestros de datos o simplemente por el miedo al contagio.

La segunda gran amenaza podría entenderse como el desconocimiento de los usuarios que acceden y compran en estos mercados de criptomonedas, que acaban por perder todo su dinero por haber invertido sin entender cómo funciona este tipo de mercado. Este "miedo a quedarse fuera" ya ha sucedido con anterioridad en otras burbujas, que impelían al consumidor a formar parte del nuevo y boyante sistema que parecía simple y que otorgaba beneficios sin apenas margen de riesgo.

Otra amenaza para la seguridad relacionada también con la actitud del usuario frente a su información y sus datos es la poca consciencia del peligro que en general tienen los usuarios frente a Internet y lo que en la red se publica. Quizá publicar en Facebook que se está operando con Bitcoins, o decir en qué monedero se están acumulando las criptodivisas no sea el mejor mensaje en aras de protegerse de los ciberdelincuentes o hackers malintencionados.

La poca regulación de los mercados de Bitcoin lleva también a que los Estados no puedan valorar si lo que se compra o vende tiene que ver con material ilegal, desde drogas a armas pasando por pornografía o datos de usuarios que se emplean como objeto del spam. Algunos países han optado por prohibir su uso, como China, y otros lo regulan, como Suecia o Corea del Sur, que es el tercer mercado mundial de criptomonedas por detrás de Estados Unidos y Japón.

La falta de protocolos impide que los cuerpos de seguridad sepan manejar los nuevos delitos con la rapidez con la que se realizan. A día de hoy, estos primeros ataques asimétricos, que mezclan

elementos de los robos tradicionales con nuevos métodos de obtención del dinero, se están combatiendo con medios offline: cámaras de vídeo, registros de audio, imágenes…que pueden ayudar, pero que no son una herramienta útil en el medio plazo.

4. Conclusiones

Aún hay mucho camino por recorrer. La sociedad debe comenzar a preocuparse por aprender qué tipo de huella digital está dejando por Internet, y las instituciones y los gobiernos deben dedicar esfuerzos para elaborar planes de acción y prevención de estos robos virtuales, que acaban por suponer también una amenaza física para las víctimas.

La educación es la clave para poder evitar situaciones para las que, todavía, la sociedad civil no tiene un referente de respuesta contundente. Los proyectos de la Oficina de Seguridad del Internauta permiten conocer los nuevos ataques y los últimos riesgos de la hiperconexión en la que vivimos inmersos, pero pocos usuarios hacen uso de este tipo de herramientas de divulgación. Según un estudio sobre la Ciberseguridad y confianza en los hogares españoles llevado a cabo por el observatorio nacional de las telecomunicaciones y de la SI en abril de 2017, más del 41,2% de los encuestados confía bastante en Internet y un 69% afirma que sus dispositivos, tanto ordenador como móvil, están protegidos frente a amenazas, pero en el 63,9% se ha encontrado malware. Esto pone de manifiesto que los usuarios tienen, generalmente, una concepción errónea de lo que implica mantener una correcta protección de su propia información.

Del mismo modo, los cuerpos y fuerzas de seguridad deben gestionar las nuevas amenazas desde un nuevo punto de vista, sin ayudarse de herramientas que quedan obsoletas para este tipo de situaciones. Adelantarse a la actividad de los hackers y terroristas también en Internet supondrá una verdadera protección para la ciudadanía, que no puede ceder libertades en pos de la seguridad sin ver resultados.

En cuanto a la proliferación de transacciones con moneda virtual y la escasa preparación que se les exige a los compradores y vendedores, algunos países ya han establecido protocolos para tratar de vigilar y aclarar, en la medida de lo posible, de dónde viene y hacia dónde va el dinero que transita los mercados virtuales a una velocidad sin precedentes. Corea del Sur, sin ir más lejos, ha tratado en varias ocasiones de fiscalizar la actividad de las casas de compraventa de Bitcoin, bajo las que siempre recae la sospecha de estar evadiendo dinero. Su último movimiento a este respecto es el de

manifestar su intención de regular la compra anónima de Bitcoin a través de un proyecto de ley. En otros países como Bangladesh, Bolivia, Vietnam, Tailandia, Rusia, Ecuador, India o Islandia ya están prohibidos los cambios entre sus monedas nacionales y las criptomonedas. China limita actualmente su uso[2]. No parece, sin embargo, que la cuestión vaya a solventarse en un futuro próximo: los atracos y robos físicos para conseguir un botín virtual deben paliarse, de momento, con una extrema precaución y conciencia.

[2] http://www.ticbeat.com/tecnologias/8-paises-bitcoin-ilegal/