McAfee
Together is power.

Informe sobre amenazas contra blockchain

Blockchain, una revolucionaria plataforma para la descentralización de las transacciones online, presenta riesgos para la seguridad

Índice

Los usuarios particulares de blockchain son con frecuencia el objetivo más fácil, debido a una mentalidad de start-up, en la que la seguridad queda relegada en segundo plano

En la investigación y redacción de este informe han participado:

- Charles McFarland
- Tim Hux
- Eric Wuehler
- Sean Campbell

Introducción

A finales de 2017, la criptomoneda bitcoin acaparó los titulares de todo el mundo. Su valor se disparó hasta los casi 20 000 dólares por moneda, despertando el interés de los medios de comunicación, así como de inversores potenciales. Bitcoin, la criptomoneda más extendida, se basa en blockchain, una nueva tecnología revolucionaria: Blockchain (literalmente, cadena de bloques), registra las transacciones de una forma descentralizada, ha comenzado a cambiar nuestra forma de ver el dinero y ofrece innovadoras soluciones a viejos problemas de las empresas.

Sin embargo, las nuevas tecnologías traen de la mano nuevos problemas para la seguridad. Los ciberdelincuentes ya han dirigido sus ataques a muchas implementaciones de blockchain a través de la ingeniería social, el malware y los exploits. El aumento de la adopción de blockchain y la creación de herramientas relacionadas debe ir acompañado de un conocimiento en profundidad de los riesgos para la seguridad. En este informe examinaremos los problemas de seguridad actuales y algunos incidentes específicos relacionados con las implementaciones de blockchain. Abordaremos las técnicas empleadas por los ciberdelincuentes, los objetivos y el malware utilizado en los ataques.

En 2009, la primera implementación de un blockchain (o una cadena de bloques), Bitcoin, despertó un enorme entusiasmo entre especialistas en tecnología e investigadores. Parecía ser una solución viable para un problema ya conocido: cómo asegurar el acuerdo entre pares. Blockchain lo consiguió a través de una rigurosa investigación que dio como resultado un sistema de pagos descentralizado mediante el que los pares podían acordar y confiar en un libro de contabilidad, que representa el estado actual de la red. Este acuerdo habilitaba ahora sistemas de pago descentralizados que no habían sido fiables anteriormente, y prometía mucho más.

¿Qué es exactamente blockchain? Un blockchain (o cadena de bloques) es una serie de registros o transacciones, recogidas en un bloque que define una porción de un libro de contabilidad. El libro de contabilidad se distribuye entre pares, que lo emplean como una autoridad de confianza en la que los registros son válidos. Cada bloque del libro de contabilidad está vinculado al siguiente bloque, lo que crea una cadena, de ahí el nombre. Cualquiera puede ver los últimos bloques y sus bloques "principales" para determinar el estado de una dirección. En el caso de las criptomonedas, podemos determinar el valor de una dirección y rastrear cada transacción, lo que nos lleva a la creación de cada moneda participante. La validación de las transacciones es fundamental. Cada nodo verifica de manera individual la exactitud de cada cadena.

Pero, ¿cómo sabe cada nodo que una cadena no ha sido modificada incluso si las transacciones se agregan? Un elemento clave de la tecnología blockchain es la forma en la que se encadenan los bloques. Gracias al uso de funciones hash, un nuevo bloque incrusta información de integridad de los bloques de los que procede (principales). Si la información de un bloque principal cambia, el hash también lo hace, lo que rompe el proceso de validación. Además, en la creación de cada bloque, es necesario proporcionar una prueba. Esta prueba demuestra que se utilizó la misma fuente para crear el bloque.

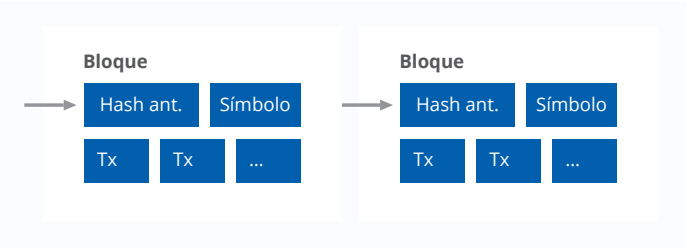
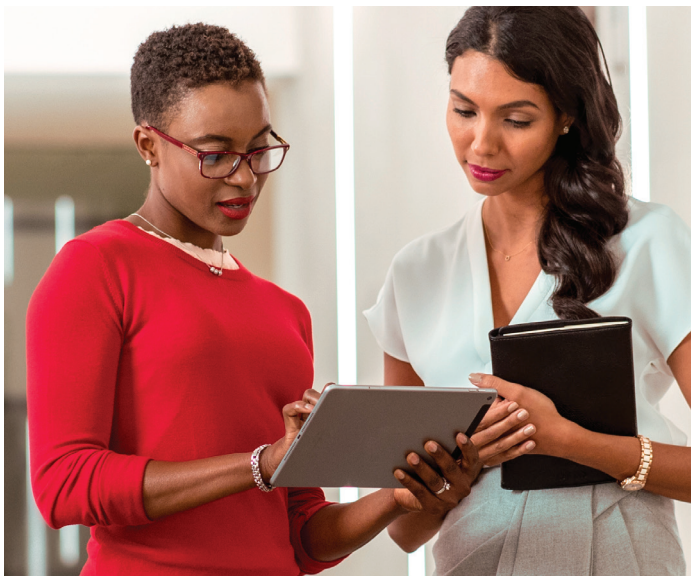


Figura 1. Blockchain de prueba de trabajo.

Fuente: https://bitcoin.org/bitcoin.pdf

La creación de cada bloque se conoce como minería, y la prueba necesaria para la minería es distinta con cada implementación de blockchain. La más común es la prueba de trabajo, un algoritmo de uso intensivo de la CPU que requiere una solución para todas las etapas de un problema. No hay atajos matemáticos conocidos. Descubrir la solución correcta a un problema demuestra que se han completado todas las etapas, en este caso empleando recursos de la CPU. Encontrar la respuesta requiere mucho trabajo, pero validar si una respuesta es correcta es relativamente sencillo. Puesto que cada bloque requiere un intenso trabajo de prueba y los bloques posteriores se encadenan, se puede validar que la cadena más larga necesitaba la mayor parte del trabajo y que es la más fiable. Haría falta una enorme cantidad de recursos para que un ciberdelincuente creara una cadena más larga y superara cualquiera de los libros de contabilidad más populares. La combinación de comprobaciones de integridad con las funciones hash dentro de los bloques, además de la prueba de trabajo, permite que redes enteras de personas confíen en los registros de un libro de contabilidad distribuido.

Las criptomonedas son implementaciones de blockchain centradas principalmente en el valor y las transacciones monetarias. Representan el uso más común de blockchain. Sin embargo, en un libro de contabilidad de blockchain no solo se puede registrar dinero. Bitcoin permite almacenar en sus transacciones una pequeña cantidad de información adicional. Los investigadores han encontrado documentos filtrados, datos arbitrarios e incluso pornografía almacenada y recuperable en el libro de contabilidad de Bitcoin. Algunos libros de contabilidad están diseñados para almacenar programas enteros que pueden ejecutar los participantes del blockchain. Ether, la segunda criptomoneda en popularidad, hace esto con un "*smart contract*" (contrato inteligente). En esa implementación, el código, o contrato, se carga en el libro de contabilidad.



Cualquier puede ejecutar ese código. Los efectos de ejecutar el contrato dependen de las reglas programadas por su creador. En un ejemplo sencillo, el contrato podría crear una cuenta de fondos de garantía para retener los fondos hasta que ambas partes cumplan sus obligaciones. Si alguien desea ejecutar el contrato, el poder de computación se paga mediante "gas", una forma de pago para los mineros. El gas asigna un coste, en monedas Ethereum (Ether), a todos los contratos inteligentes para impedir un número excesivo de ejecuciones, lo que podría ralentizar la red.

Algunos sectores intentan resolver sus problemas empresariales con blockchains personalizados. Por ejemplo, un importante comercio minorista ha registrado patentes para utilizar blockchain para el seguimiento y la protección de los envíos. Se han desarrollado plataformas de blockchain empresariales para hacer frente a la creciente demanda de nuevas implementaciones.

Ataques a blockchain

En la mayoría de los casos, los usuarios particulares de tecnología blockchain son los objetivos más fáciles. Con una mentalidad de start-up generalizada, en la que la seguridad suele quedar relegada a un segundo plano, las empresas de criptomonedas entran en esta categoría. Esta categoría incluye las empresas de implementaciones de blockchain de gran envergadura y de amplia adopción, como Bitcoin y Ethereum. Los ciberdelincuentes han adoptado varios métodos para atacar a particulares y empresas a través de técnicas muy consolidadas.

Los principales vectores de ataque incluyen:

- Phishing
- Malware (por ejemplo: ransomware, mineros y criptojacking)
- Vulnerabilidades de implementación
- Tecnología

Phishing

Los timos de phishing son los ataques más habituales a blockchain debido a sus tasas de prevalencia y éxito. Por ejemplo, pensemos en la criptomoneda IOTA. Las víctimas perdieron 4 millones de dólares en un timo de phishing que se prolongó durante varios meses. El agresor registró iotaseed[.]io, que proporcionaba un generador de semillas funcional para un monedero de IOTA. El servicio funcionaba tal y como se anunciaba, y permitía a las víctimas crear y utilizar correctamente sus monederos sin problemas, dando un falso sentimiento de seguridad y confianza. Mientras tanto, el ciberdelincuente esperaba pacientemente para aprovechar la confianza generada. Durante seis meses, el ciberdelincuente recogió registros, que incluían las semillas secretas y, entonces, inició el ataque. En enero, con la información robada previamente, el agresor transfirió todos los fondos de los monederos de las víctimas.

En general, a los ciberdelincuentes no les importa quiénes son sus víctimas. Siempre que la criptomoneda acabe en sus manos, no hay víctimas mejores que otras. Un buen ejemplo es el caso del ataque de intermediario Tor. La red Tor se utiliza habitualmente para ocultar la ubicación de un navegador con el fin de evitar la vigilancia del tráfico por parte de terceros. Muchos emplean Tor para crear servicios ocultos desde los que los particulares pueden comprar y vender bienes. Las criptomonedas son la forma de pago preferida, o la única. Estos servicios son también los que a menudo aprovechan las familias de ransomware para ocultar sus sistemas de pago. Hay quien no conoce bien Tor, así es que, por comodidad, se ponen a disposición de las víctimas servidores proxies de Tor de fácil acceso a fin de ayudarles a llegar a estos sitios y recuperar sus archivos. Por lo general, estos incluyen dominios de servidores proxy de Tor que se han encontrado a través de un motor de búsqueda o siguiendo las instrucciones del ransomware. Desafortunadamente para la víctima, es posible que el agresor no reciba el rescate. En algunos casos, los fondos se derivaron a un monedero ajeno mediante un servidor proxy malicioso. Eso fue lo que ocurrió a principios de 2018 cuando se detectó un servicio de servidores proxy de Tor sustituyendo direcciones de Bitcoin asociadas a ransomware por otras que estaban bajo su control. Los investigadores de seguridad descubrieron a operadores explorando sitios en la Web profunda en busca de monederos de Bitcoin detrás del servicio de servidores proxy Tor2web onion[.]top. Una vez localizado el monedero, los ciberladrones sustituían la dirección por una propia.

Malware

En 2016, el número de nuevas familias de ransomware aumentó de manera espectacular. Fue la herramienta principal utilizada por los ciberdelincuentes para conseguir criptomoneda. Aunque el ransomware no era nuevo, se convirtió en el método favorito debido a las ventajas de transferir y ocultar los fondos a través de criptomonedas.

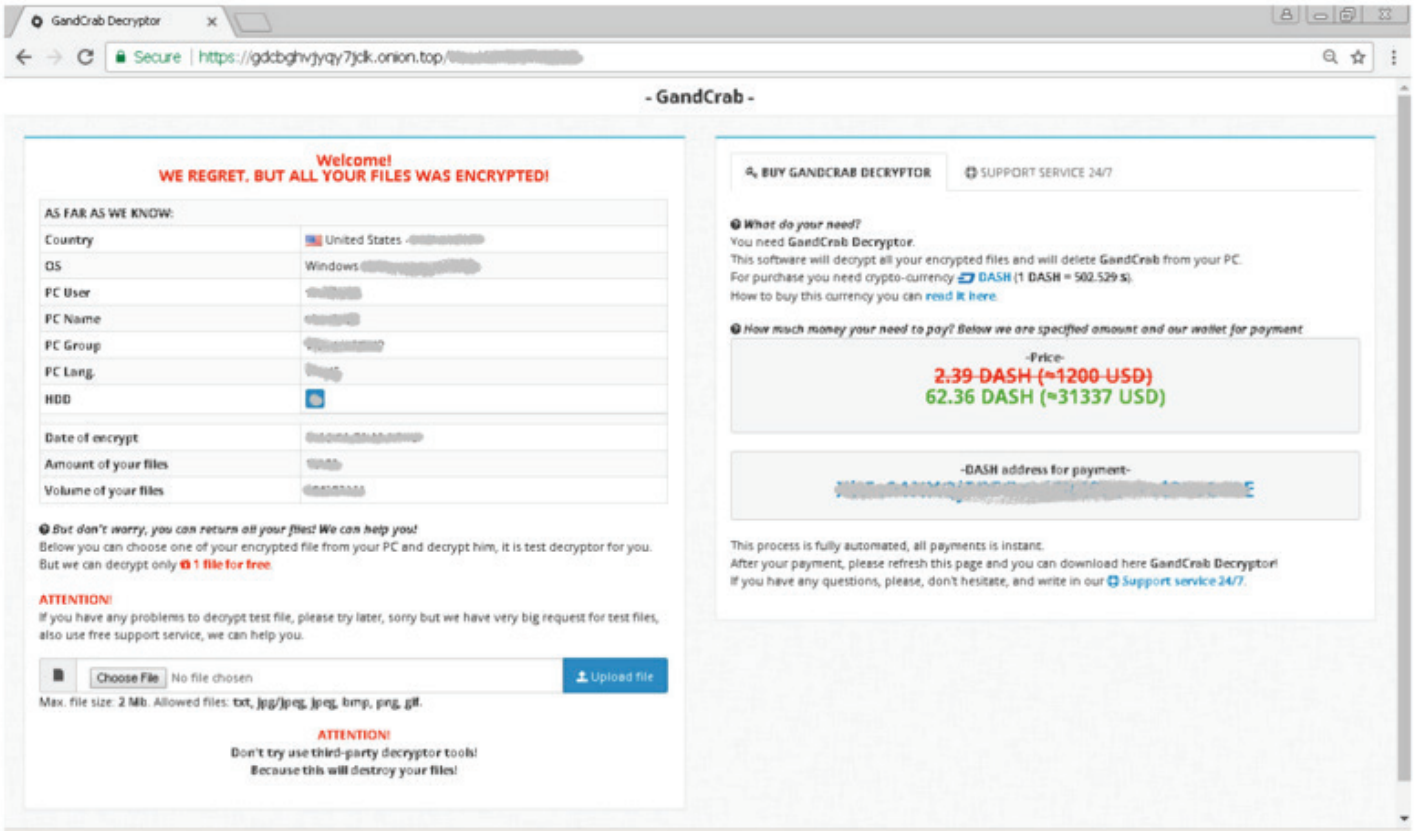


Figura 2. Una página de descifrado de GandCrab a la que se ha accedido a través de un servidor proxy onion[.]top Tor.

Los ciberdelincuentes también disponían de herramientas de fácil acceso, concretamente HiddenTear, que supuestamente eran "educativas" sobre ransomware, pero que fueron rápidamente utilizadas por los agresores para crear cientos de variantes. Por lo general, estas variantes exigían pagos en bitcoin como rescate, con algunas excepciones como Monero con el ransomware Kirk.

En 2017, aumentó el interés de los desarrolladores de ransomware en las monedas. Los ciberdelincuentes empezaron a experimentar con una serie de cibermonedas alternativas, también conocidas como altcoins. Monero fue la favorita, aunque también se utilizaron otras menos conocidas, como Dash. El ransomware GandCrab descartó Bitcoin en favor de Dash. GandCrab se incluyó en el conocido kit de exploits RIG, junto con una variedad de tipos de malware.

GandCrab y otros tipos de malware lanzaron ataques frecuentes contra Microsoft Internet Explorer y Adobe Flash Player a través de publicidad engañosa.

Los desarrolladores de ransomware también adoptaron la moneda de uso generalizado Ethereum a principios de 2018. Planetary, una variante de HC7, es el primer ransomware conocido en atacar Ethereum, aunque no de manera exclusiva. Para ofrecer a las víctimas opciones y mayores incentivos, Planetary les permite pagar el equivalente a 700 dólares por sistema infectado o 5000 dólares por todos los nodos infectados de sus redes. El ransomware también acepta Bitcoin y Monero.

Criptojacking

El criptojacking es el método utilizado para secuestrar un navegador para minar criptomonedas, y sorprendentemente lo hemos visto resurgir. Al igual que el ransomware, las campañas de criptojacking experimentaron con altcoins. A finales de 2017, se detectó que el complemento Archive Poster para el navegador Chrome extraía monedas Monero sin consentimiento.

Figura 3. API de Coinhive.

Fuente: https://gist.github.com/coinhive-com/dc37d300b2f4f909006a07139c9d2c71

Seguir

Compartir

Las víctimas conocieron por primera vez el problema cuando algunas empezaron a quejarse de un uso elevado de la CPU. Para entonces, más de 100 000 personas habían descargado el minero. Al menos cuatro versiones de la aplicación incluían código JavaScript de criptojacking de Coinhive, que incrusta fácilmente funciones de minería en los sitios web o herramientas, en principio con una API de código abierto fácil de utilizar. El criptojacking se encuentra en una especie de tierra de nadie. Muchas empresas implementan Coinhive y otros mineros para ganar dinero con los recursos de los dispositivos de sus visitantes. Si están de acuerdo, la minería no se considera un comportamiento malicioso, sino potencialmente no deseado. Sin embargo, muchos sitios web no informan de la minería y los visitantes no saben qué pensar sobre el bajo rendimiento.

Podría ocurrir que el propietario del sitio web no fuera el que añadió el código de criptojacking —así ocurrió con YouTube. Un fallo en el popular sitio de intercambio de vídeos permitió que anunciantes maliciosos inyectaran código de criptojacking en anuncios para minar Bitcoin o Ethereum. (YouTube reaccionó rápidamente y eliminó los anunciantes maliciosos de su red y bloqueó los anuncios causantes de la minería). Los ciberdelincuentes tienen años de experiencia en publicidad engañosa y han personalizado ese conocimiento para adecuar sus campañas de criptomonedas.

Se sabe que hay casi 30 000 sitios web que alojan código de Coinhive para actividades de minería, con o sin consentimiento. Este número corresponde solamente a sitios web no camuflados. El número real es probablemente mucho mayor. A medida que aumente el control de este comportamiento, podemos esperar que se descubran más mineros de criptojacking.

Los mineros de endpoints

Antes de 2016, la minería maliciosa de monedas fue uno de los métodos principales para obtener criptomonedas. Aunque menos común que el ransomware, la minería experimentó un explosivo resurgimiento a finales de 2017 y principios de 2018. Rápidamente aparecieron nuevos mineros y el malware antiguo se rediseñó con funciones de minería. Las familias de ransomware empezaron incluso a desdoblarse mediante la incorporación de funciones de minería. Por ejemplo, a principios de 2018 se descubrió Black Ruby, y exige un rescate de 650 dólares en bitcoins. El malware utiliza el popular software de minería y código abierto XMRig Monero en los dispositivos infectados.

Seguir
Compartir

Otra operación de minería a gran escala descubierta en enero de 2018 también utiliza XMRig. Herramientas de código abierto como estas contribuyeron en parte al importante aumento del malware de minería.

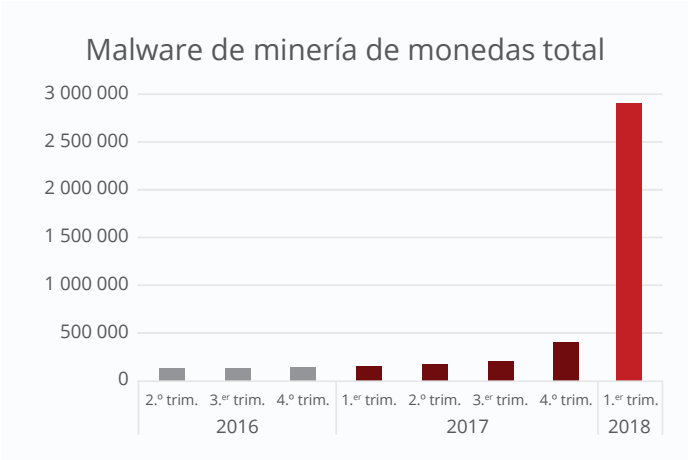


Figura 4. El malware de minería de monedas ha crecido de manera explosiva.

Fuente: McAfee Labs

En los últimos seis meses, parece que muchos desarrolladores de malware han pasado del ransomware a la minería de criptomonedas, según datos de McAfee® Global Threat Intelligence, que demuestran que los ataques de ransomware han descendido un 32 % en el primer trimestre de 2018 respecto al 4.º trimestre de 2017, mientras que la minería de monedas ha aumentado un 1189 %. El objetivo de los mineros es principalmente el PC, pero otros dispositivos también han sufrido ataques. Por ejemplo, en China, se llevaron a cabo ataques a teléfonos Android para recopilar monedas Monero con ADB.Miner, que actúa como gusano y se ejecuta en el puerto 5555, que es el que se utiliza con más frecuencia para la interfaz de depuración ADB. También se infectaron dispositivos con el recopilador XMRig. Una consulta en shodan.io muestra más de un millón de dispositivos conectados a Internet que se ejecutan en el puerto 5555. Un subconjunto es el minero XMRig. Se detectó ADB.Miner reutilizando código desde la red de bots Mirai, que surgió a mediados de 2016 y se ha observado en una serie de ataques de ataques a nivel mundial. Para febrero de 2018, los ciberdelincuentes responsables del malware habían infectado aproximadamente 7000 dispositivos, la mayoría ubicados en China y Corea.

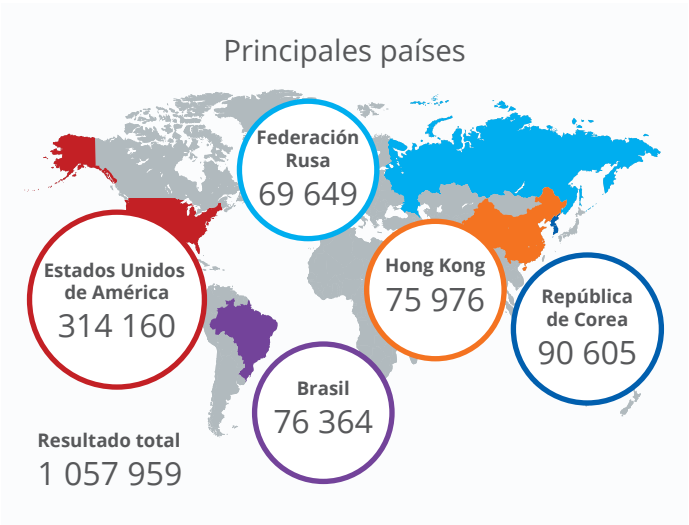


Figura 5. Búsqueda en Shodan.io de dispositivos con el puerto 5555.

Seguir

Compartir

En algunos casos, se trataba de ataques selectivos a grupos específicos y no de ataques masivos. Un minero malicioso atacó a jugadores desprevenidos de un foro ruso con el malware camuflado como un "mod" para mejorar juegos populares. Consiguió engañar a los jugadores para que descargaran el software malicioso, que utilizó sus recursos informáticos para conseguir un beneficio económico. Para mantener la persistencia y no levantar sospechas, el minero vigilaba para localizar títulos de ventanas abiertas, como el Administrador de tareas de Windows, Process Hacker u otros administradores de procesos. Si los detectaba, detenía las operaciones de minería, ocultando así su actividad. El ciberdelincuente sospechoso de esta operación es presuntamente el principal responsable de otro software "trampa" de juegos y es conocido por publicar su malware en varios foros rusos sin preocuparse demasiado por mantener el anonimato.

La creación de malware puede ser una tarea costosa y laboriosa para los ciberdelincuentes. En lugar de investigar y escribir sus propios exploits, muchos creadores del malware eligen exploits públicos y vulnerabilidades conocidas, dando por hecho que siempre hay un número importante de máquinas a las que no se les ha aplicado el parche correspondiente y que, por tanto, pueden ser atacadas. A menudo no se equivocan. Se calcula que en la segunda mitad de 2017 el minero ilegal Smominru creó más de 3 millones de dólares en monedas Monero. La campaña aprovecha el exploit EternalBlue, que fue filtrado públicamente por el grupo de hackers The Shadow Brokers. El exploit tuvo una gran repercusión mediática por el enorme éxito del malware WannaCry, que afectó a equipos de todo el mundo. Este exploit, que aprovecha un fallo en el protocolo Bloque de mensajes del servidor (SMB, Server Message Block) versión 1 de Microsoft Windows, se publicó en el boletín MS17-010.

Smominru no fue la única familia de malware que aprovechaba EternalBlue. WannaMine, un recopilador de Monero, también utiliza el EternalBlue para propagarse por la red. Para la infección inicial, WannaMine emplea mensajes de correo electrónico de phishing habituales para ejecutar un archivo batch y descargar un script PowerShell malicioso desde su servidor de control. A continuación utiliza XMRpool para conectar el dispositivo a grupos (pool) de minería públicos, lo que convierte al sistema de la víctima en colaborador involuntario. Las tres cadenas de conexiones siguientes se utilizaron para conectar a la víctima con los grupos de minería.

```
stratum+tcp://pool.supportxmr.com:80
stratum+tcp://mine.xmrpool.net:80
stratum+tcp://pool.minemonero.pro:80
```

En otro ejemplo, aprovechando la vulnerabilidad CVE-2017-10271, los ciberdelincuentes convirtieron servidores Oracle WebLogic en una red de bots de minería de Monero. (Oracle ya ha corregido la vulnerabilidad). A pesar de la presencia de los ciberdelincuentes en los servidores, aparentemente no tenían interés en robar datos o solicitar un rescate. Su pasividad a la hora de robar datos prueba el valor que dan a la minería.

Vulnerabilidades de las implementaciones

Otro tipo de amenaza es la que representa un ataque a la propia implementación de blockchain, así como a sus herramientas de soporte. Sin embargo, cuanto más cerca se está del núcleo de la tecnología blockchain, más difícil es conseguir que el ataque tenga éxito. Generalmente, estos ataques se parecen más a exploits de software tradicional y aplicaciones web.

La wiki de Bitcoin tiene una lista de vulnerabilidades y riesgos comunes (CVE) relacionados con sus herramientas oficiales. Estas vulnerabilidades han dado lugar, entre otros, a ataques de denegación de servicio, robo de monedas y exposición de información. Aunque las vulnerabilidades pueden ser muy impactantes, habitualmente se descubren y corrigen tras la comunicación. Resulta complicado generar y mantener código seguro; la popularidad y el explosivo crecimiento de blockchain han exacerbado este problema. Se ha ralentizado el descubrimiento de vulnerabilidades de gravedad alta relacionadas con herramientas de Bitcoin esenciales, lo que ofrece a los usuarios una sensación de confianza. No se puede atribuir la misma confianza a la comunidad y a las herramientas de terceros.

En febrero de 2018, un exploit de tipo zero-day atacó PyBitmessage, una herramienta de transferencia de mensajes P2P que imita el sistema de transacciones y transferencia de bloques de Bitcoin. PyBitmessage utiliza el concepto de prueba de trabajo de blockchain para "pagar" las transferencias de mensajes y reducir el spam. Los ciberdelincuentes utilizaron este exploit para ejecutar código en los dispositivos mediante el envío de mensajes especialmente diseñados.

A partir de ahí, ejecutaron scripts automatizados para buscar monederos de Ethereum mientras creaban un shell inverso para acceder en el futuro.

Las herramientas de terceros son por lo general un objetivo más fácil porque cuentan con comunidades más pequeñas y menos recursos para proteger su código y responder a los problemas. En raras ocasiones observamos un riesgo para la propia implementación. Ese fue el caso, hecho público a mediados de julio de 2017, de un ataque contra IOTA. Las vulnerabilidades permitían a los agresores crear colisiones de hash y firmas falsificadas, lo que les permitía robar monedas de otros monederos. Aunque se han corregido, los fallos requieren, en parte, una bifurcación fuerte (*hard fork*) en la red para eliminar el uso de Curl, una función hash criptográfica personalizada. El problema se produce por incumplir la regla de oro de la criptografía: "No cree su propia criptografía". La criptografía es una tecnología increíblemente difícil de dominar. Cualquier código personalizado o cambios en las funciones relacionadas con la criptografía deben investigarse en profundidad antes de la fase de producción. Incluso las tecnologías consolidadas pueden enfrentarse a problemas, como demuestra la migración que hizo el sector desde funciones hash MD5 a SHA-1 y a SHA-256, debido a fallos de seguridad fundamentales.

Podemos mencionar más ejemplos de implementaciones blockchain inseguras. El equipo de desarrollo de Verge no estaba lo suficientemente preparado para hacer frente a numerosas vulnerabilidades en su implementación cuando recibió un ataque a principios de abril.

Los agresores aprovecharon los fallos para minar nuevas monedas sin gastar poder de minería alguno. El parche tenía el desafortunado efecto secundario de "bifurcar" la moneda; básicamente creaba una nueva moneda distinta de la original. El efecto en el valor de las monedas todavía está por ver, pero se espera que perjudique de manera importante la capacidad de Verge de seguir siendo un actor importante.

En implementaciones de blockchain como Ethereum, el código de usuario es parte del libro de contabilidad a través de los contratos inteligentes. Un usuario escribe el contrato inteligente y este se envía como parte del libro de contabilidad. El contrato puede ejecutar lógica basada en las reglas del mismo. Si se les permite, pueden participar otros, creando una aplicación descentralizada autosuficiente disponible para todos. Como cualquier código, puede presentar errores y vulnerabilidades. En noviembre de 2017, se detectó una vulnerabilidad crítica en la biblioteca de monederos Parity, que se utiliza junto con los contratos inteligentes de Ethereum. El problema, detectado de forma accidental, permite a un agresor inutilizar algunos monederos multifirma y bloquear a los titulares de las cuentas. Esto provocó la congelación de monedas Ethereum (Ether) por valor de 150 millones de dólares. La magnitud del ataque superó el que hasta la fecha era el mayor incidente contra contratos inteligentes, y causó la pérdida de más de 50 millones de dólares en valor. En este ataque contra "The DAO", una organización anónima basada en Ethereum, un pirata utilizó un error recurrente para extraer fondos.

Robo de monederos

En enero se detectaron ciberdelincuentes que eludían hosts de minería conectados a Internet y cambiaban las direcciones de los monederos en los hosts por una dirección bajo su control. Los ciberdelincuentes hacían el cambio de monederos sorteando el puerto de administración del conocido software de recopilación Claymore Miner que, de forma predeterminada, escucha en el puerto 3333. El malware, Satori.Coin.Robber, es sucesor de la conocida red de bots Satori, que causó estragos a finales de 2017 en dispositivos del Internet de las cosas (IoT). Esta variante utiliza una dirección IP codificada para el tráfico del servidor de control, y la mayoría de las direcciones IP que buscan posibles objetivos se encuentran en Corea del Sur. Además, el creador del malware deja una nota en la que afirma que la red no es maliciosa y que se puede contactar con él a través del correo electrónico.

Los ciberdelincuentes han reconvertido otras técnicas conocidas y las han adaptado para llevar a cabo ataques a criptomonedas. Un ataque descubierto a finales de 2017 sustituía monederos digitales en el Portapapeles de una víctima. Aunque la eliminación de datos y la sustitución de contenido no es algo nuevo, estos ciberdelincuentes perseguían específicamente las criptomonedas. El troyano CryptoShuffler, que ataca portapapeles, lleva activo desde 2016, y tiene como objetivo una amplia variedad de monedas digitales, como Bitcoin, Dogecoin, Litecoin, Dash, Ethereum, Monero y Zcash. El mismo autor también fue el responsable del troyano Evrial, que atacaba los portapapeles. Cada troyano se instala en el ordenador de una víctima a la espera de cadenas que parezcan

direcciones de criptomonedas y sustituye la dirección en cuestión por una bajo el control del agresor. Esta técnica puede ser muy rentable; la sustitución del monedero ha reportado más de 140 000 dólares para CryptoShuffler.

Que el nuevo malware pueda utilizar viejos trucos no significa que el malware antiguo no pueda cambiar su comportamiento. Las criptomonedas también son objetivo de los troyanos bancarios. En 2016 aparecieron dos que cabe destacar. El tristemente famoso troyano bancario Trojan Dridex incorporó funciones de robo de monederos a las habituales de robo de credenciales bancarias. El troyano Trickbot tenía entre sus objetivos tanto instituciones financieras como criptomonedas. Trickbot añadió coinbase.com, un conocido sitio de intercambio de criptomonedas, como uno de sus vectores de ataque. Una vez infectado el sistema, el malware inyectaba una página de inicio de sesión falsa cuando la víctima visitaba el sitio de cambio de moneda digital, lo que permitía a los ciberdelincuentes robar los datos de inicio de sesión de la víctima, así como una amplia variedad de activos digitales, incluidos Bitcoin, Ethereum y Litecoin.

Ataques a la tecnología

Antes del lanzamiento de la primera implementación de blockchain, no existía una alternativa de confianza a la banca descentralizada. Sin embargo, los problemas de seguridad asociados a la creación de un sistema de esas características ya se habían estudiado en profundidad. Años de investigación, incluida la cadena de bloques de Habert y Stornetta, infundieron confianza en el concepto de blockchain. Sin embargo, la seguridad de un blockchain se basa en algunos supuestos. Si no se cumplen, hay riesgo para la seguridad.

Una de las principales suposiciones respecto a un blockchain es que la contribución a la red, la "tasa de hash" de Bitcoin, es distribuida. Concretamente, ninguna entidad o grupo colaborador procesa más del 50 % de la red en ningún momento. Un ataque 51 % se produce cuando un atacante acumula más del 50 % de la red. Si superan el 50 %, básicamente pueden procesar bloques más rápidamente que el resto, lo que les permite crear sus propias cadenas a voluntad. Esta capacidad da pie o simplifica otros ataques, como el de "doble gasto", que permite gastar muchas veces la misma moneda y dejar a un receptor con las manos vacías. Un ataque 51 % nunca ha llegado a producirse con éxito contra Bitcoin debido a su gran base de participantes, pero sí contra Verge y otras monedas. Las monedas mucho más pequeñas corren un enorme riesgo. Poco después de que se demostrara que Krypton era susceptible a este tipo de ataques, el grupo 51 Crew atacó otras monedas pequeñas y las retuvo para pedir un rescate. Este riesgo también se aplica a blockchains desarrollados internamente. Muchas empresas están analizando las tecnologías de blockchain para administrar el inventario, los datos y otros activos. Si la base de participantes, o la tasa de hash, de estas redes personalizadas no es lo suficientemente grande, un atacante podría utilizar tecnología de nube, redes de bots o grupos para atacar el sistema.

Una suposición relacionada es que la mayoría de los nodos son "honestos", lo que significa que existe una alta probabilidad de que al menos una conexión se haga a un nodo legítimo. La imposibilidad de conectar con un nodo honesto permite un ataque Sybil, por el que

el agresor fuerza a la víctima a comunicarse solamente con nodos maliciosos. El agresor puede controlar la información a la que puede acceder la víctima, incluido el libro de contabilidad. Solo hace falta un nodo honesto para frustrar este tipo de ataque, ya que es imposible para el agresor comprobar una cadena más larga que la red. Recuerde que una cadena larga puede poner de manifiesto la cantidad de trabajo necesario para crear una cadena. El agresor debe superar la potencia de proceso de toda la red si la víctima detecta la cadena válida. Por lo tanto, el éxito de este tipo de ataque depende de impedir que los nodos honestos revelen información de la verdadera red. Un nodo honesto no impide que los ciberdelincuentes intenten un ataque Sybill. En 2016, se detectaron grandes grupos de nodos creados conjuntamente. En cuanto a los ataques 51 %, una red más pequeña es un objetivo más fácil, sobre todo si no se han implementado en el sistema contramedidas adicionales.

La tercera suposición es que las colisiones de hash son infrecuentes. Bitcoin utiliza una longitud de 256 bits para identificar la propiedad de un monedero. Cada clave se asigna a una dirección pública a la que otros pueden enviar fondos. Siempre que un propietario disponga de acceso exclusivo a una clave, nadie puede enviar transacciones a partir de ese monedero. Pero, ¿qué pasaría si las colisiones no fueran tan poco frecuentes? Un agresor, o cualquiera, podría retirar fondos accidentalmente del monedero de alguien. Sería difícil demostrar quién es el propietario de los monederos y los fondos porque, desde el punto de vista de la red, ambas partes tendrían los mismos derechos.

Afortunadamente parece que las colisiones que utilizan algoritmos estándar son efectivamente improbables. Nadie ha sido capaz de generar, de manera intencionada o no, la clave de otro, al menos con Bitcoin, siempre que las claves se crearan adecuadamente. Esto no impide que los propietarios creen claves de forma inapropiada. Sobre todo con Bitcoin, y en menor medida con altcoins, muchos intentan facilitar la gestión de sus claves privadas con "monederos mentales" (*brain wallets*), que han generado claves con una palabra o semilla fácil de recordar. Ese comportamiento convierte al monedero en posible objetivo de ataques de diccionario especialmente diseñados. Otras claves pueden ser víctimas de la propia implementación. La dependencia de IOTA de claves mal generadas provoca colisiones que generan graves riesgos de seguridad para quien las utiliza. Un análisis más profundo de los algoritmos, incluido el estándar actual, podría aumentar la probabilidad de que se produjeran colisiones, como hemos observado con algoritmos como MD5 y SHA-1.

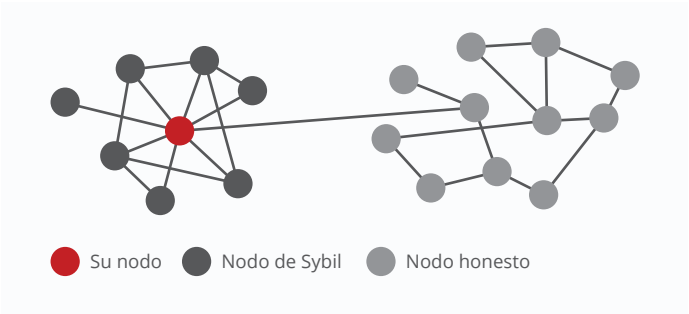


Figura 6. Un nodo honesto impide un ataque Sybil.

Fuente: https://www.coindesk.com/bitcoins-security-model-deep-dive/

Seguir

Compartir

Ataques antiguos modernizados

La mayoría de los esfuerzos de seguridad en relación con blockchain se centran en la integridad del libro de contabilidad y las tecnologías subyacentes. Sin embargo, para disponer de una visión completa de los riesgos de seguridad, también hay que tener en cuenta el comportamiento de los usuarios. Un ataque bien conocido, posible gracias a un comportamiento inseguro, se ha rediseñado específicamente contra las implementaciones de blockchain actuales.

Ataques de diccionario

Los ataques de diccionario son viejos conocidos desde hace décadas. Normalmente intentan descifrar la contraseña de la víctima u otro mecanismo de autenticación. Vamos a analizar un ataque de diccionario típico, concretamente los denominados ataques de tabla arcoiris (o *rainbow*).

Cuando creamos una contraseña para una cuenta online, el proveedor de servicios no debe almacenarla como texto simple. Debe utilizar un hash criptográfico de la contraseña y guardar su valor. Por ejemplo, si usamos la contraseña "password", que es muy poco segura, el servidor puede guardarla como *5baa61e4c9b93f3f0682250b6cf8331b7ee68fd8* que es el hash SHA-1 de la cadena "password". Podemos utilizar varios algoritmos de hash y otros procedimientos, como el empleo de sal, para que la contraseña sea más segura. Sin embargo, ¿qué pasaría si los agresores ven la cadena precedente? Es posible que pudieran reconocer esa cadena como el hash de "password".

Aunque en la mayoría de los casos es difícil encontrar una cadena basada en un hash, no ocurre igual a la inversa. Encontrar el hash correspondiente a una cadena es extremadamente sencillo mediante un interpretador de línea de comandos como Bash.

- $echo -n 'password' | shasum

Las funciones de hash son un algoritmo de "sentido único": si los agresores solo conocen el valor hash, en teoría no pueden hallar la contraseña original. En este caso, resulta que conocemos la contraseña y el valor hash, por lo que su traducción es fácil. ¿Cuál es el valor SHA-1 de "password1"? Esto también es fácil de obtener y el resultado es *e38ad214943daad1d64c102faec29de4afe9da3d*. Si los agresores ven el valor hash de "password" o "password1", pueden traducirlo para obtener el texto original.

Esta traducción puede ejecutarse millones de veces con todas las contraseñas imaginables. El único límite es el tiempo, pero los agresores pueden centrarse en las contraseñas más habituales. La asociación entre el valor hash y su correspondiente contraseña en texto simple se denomina una tabla de arcoiris. La traducción del hash criptográfico en texto plano se conoce como ataque de tabla de arcoiris.

Se pueden llevar a cabo ataques de tabla de arcoiris modificados contra blockchain, concretamente, contra bitcoins y otras monedas relacionadas. En lo que queda de este informe, todos los ejemplos serán sobre bitcoin, pero muchas de esas técnicas son aplicables a otras criptomonedas parecidas, y posiblemente a otras implementaciones nuevas de blockchain, distintas de las criptomonedas.

Hashes SHA-1	Texto plano
5baa61e4c9b93f3f0682250b6cf8331b7ee68fd8	password
e38ad214943daad1d64c102faec29de4afe9da3d	password1
2aa60a8ff7fcd473d321e0146afd9e26df395147	password2
...	...
e13fc576c44eacd178e21b8b253f59fa59aa4cc8	passwordN

En bitcoin, una dirección representa la interfaz pública en la que reside la moneda. Los usuarios transfieren las divisas utilizando esa dirección, cuando pagan en esa moneda, la transacción procede de esa dirección. Sin embargo, para verificar que están autorizados a iniciar una transacción y gastar monedas desde una dirección, deben utilizar su clave privada. Esta clave solo la conocerá el propietario y debe utilizar el algoritmo de firmas digitales de curva elíptica de bitcoin. En la práctica, esto significa que casi todos los números de 256 bits que se puedan generar con el algoritmo de hash SHA-256 son válidos, lo que puede facilitar que haya quien haga un uso incorrecto de un monedero mental. En lugar de recordar o guardar los 64 caracteres supuestamente aleatorios, bastaría con recordar las contraseñas y utilizar el algoritmo de hash SHA-256 cada vez que se necesiten sus claves privadas. Hace tiempo había quien seguía esta práctica, que era increíblemente peligrosa. Los ciberdelincuentes buscan constantemente monederos mentales.

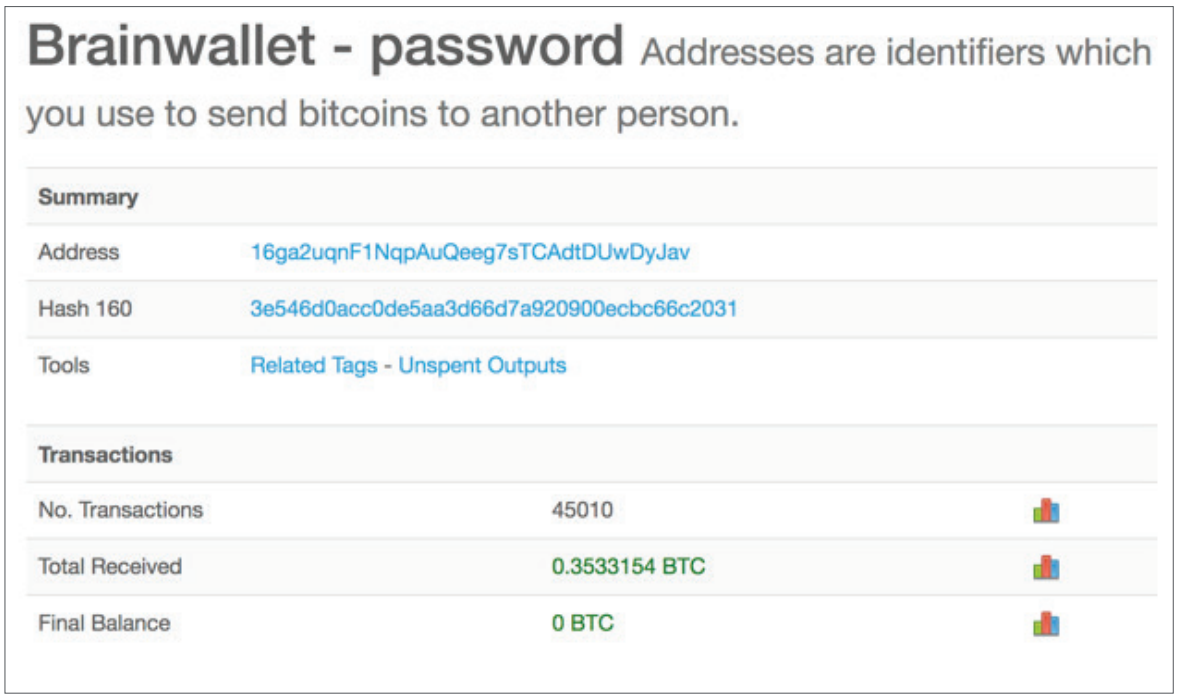


Figura 7. Una cuenta con la clave privada generada por “password", de marzo de 2018. Fuente: https://blockchain.info/

Seguir

Compartir

En la imagen anterior, observamos que entre julio de 2012 y marzo de 2018 se realizaron 45 010 transacciones, con un saldo final de cero. Si examinamos las transacciones, observamos un patrón de entradas de pequeñas cantidades seguidas por una transacción saliente. Entre las cuentas que utilizan "password", "password1" y "password2", hemos contado 117 212 transacciones en las que no pudimos determinar el propietario, ni qué importes se robaron. Pero bitcoin no es el único problema, aunque es cierto que la mayoría de las criptomonedas se han desarrollado después de que fuera conocida la vulnerabilidad de los monederos mentales.

Los investigadores llevan tiempo estudiando dichas vulnerabilidades y han descubierto 18 000 monederos vulnerables en 2016, así como la optimización de la velocidad de los ataques. Los resultados no se limitaban a contraseñas cortas y sencillas. Muchas de las incluidas en la lista eran frases que contenían espacios, puntuación y números también.

En nuestra investigación, nos hemos encontrado con un monedero mental muy habitual. Nos tememos que habrá otras personas que hayan utilizado este monedero de manera accidental y que, por lo tanto, habrán perdido su dinero. Posiblemente por error, varias personas han generado la misma clave privada y han compartido este monedero, permitiendo así lo que han considerado un robo. Veamos los dos comandos Bash siguientes para extraer un código hash SHA-1 de una cadena:

- $echo -n “$password” | shasum
- $echo -n “$Cryt0p4sswordV3rySecure” | shasum

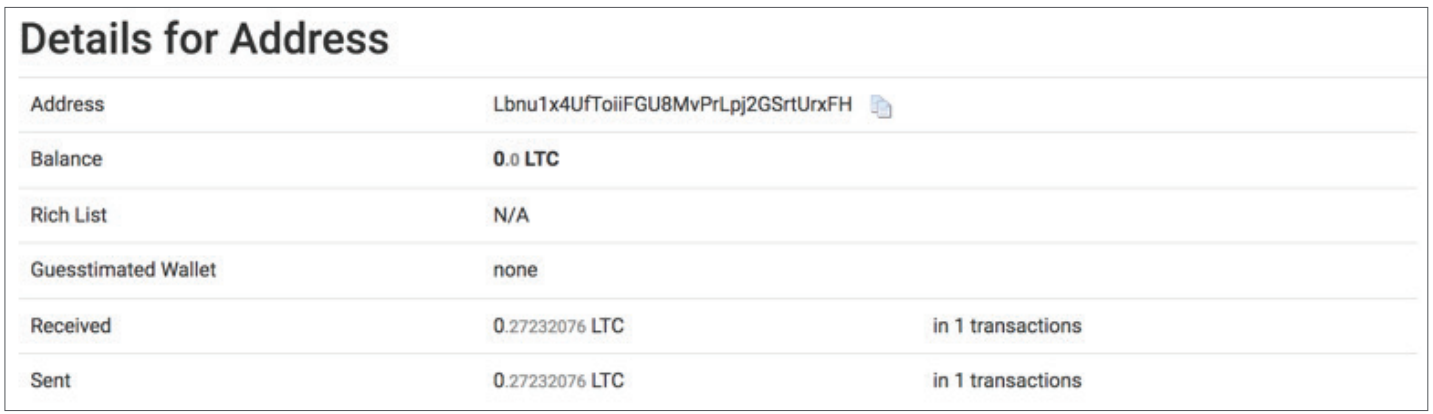


Figura 8. Un monedero mental de Litecoin.

Fuente: https://chainz.cryptoid.info/ltc/

Seguir

Compartir

Obtendremos dos hashes SHA-1 diferentes, pero los dos devolverán el mismo valor: *da39a3ee5e6b4b0d3255bfef 95601890afd80709*. Es un error común relacionado con el usuario y los detalles de la sintaxis de Bash. El símbolo $ de la cadena de contraseña es un carácter especial de Bash, que denota una variable o parámetro especial. El empleo de $ al principio de la cadena hace que Bash trate la cadena completa como una variable y la sustituya por el valor de la variable. En este caso, no existe ninguna de las variables, por lo que Bash devuelve la misma cadena vacía. Este error provoca que se comparta de manera no intencionada una clave privada. También es posible que haya causado la pérdida de casi 59 BTC (530 120 $ hasta marzo). (Véase la captura siguiente).

Aunque hay excepciones, la mayoría de los monederos mentales conocidos se basan en las mismas contraseñas comunes que se utilizan para otras cuentas. Para poder apreciarlo con claridad, hemos generado nuestra propia tabla de arcoiris para comprobarla con la contabilidad de bitcoin. Nuestra tabla consta de un grupo relativamente reducido de 200 000 de las contraseñas más comunes, más de 160 000 contraseñas generadas para bitcoin, una lista de citas famosas y varios libros disponibles, como *Guerra y paz y Alicia en el país de las maravillas*. Aunque nuestra muestra era comparativamente pequeña (muchos diccionarios contienen millones de entradas), encontramos 852 monederos vulnerables. Se han retirado más de 102 bitcoins (casi 1 000 000 de dólares cuando se redactó este documento) de esos monederos. Estos números pueden aumentar a medida que crezca nuestra muestra.

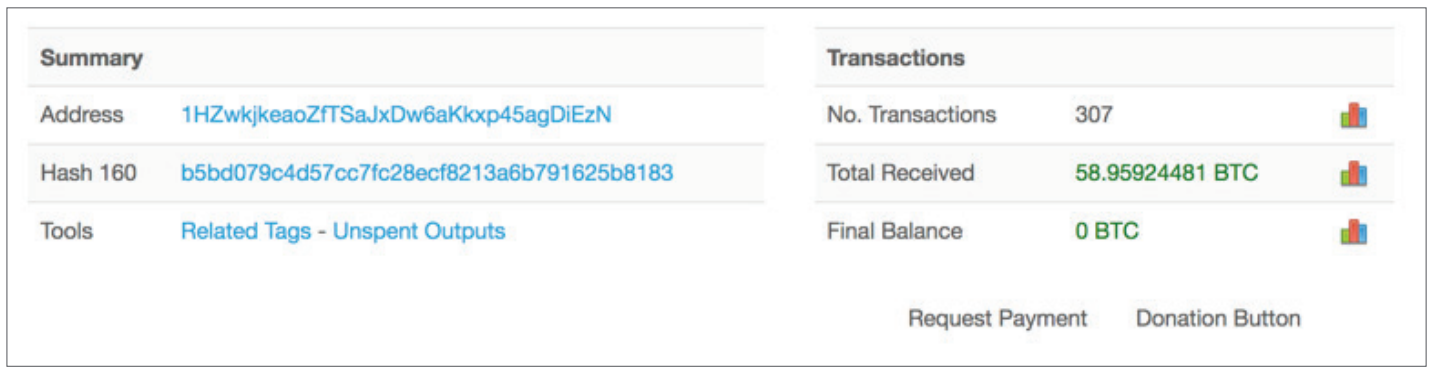


Figura 9. Este monedero registró dos transacciones el 5 de marzo de 2018. Se produjo una transacción entrante y una saliente en solo prácticamente 15 minutos.

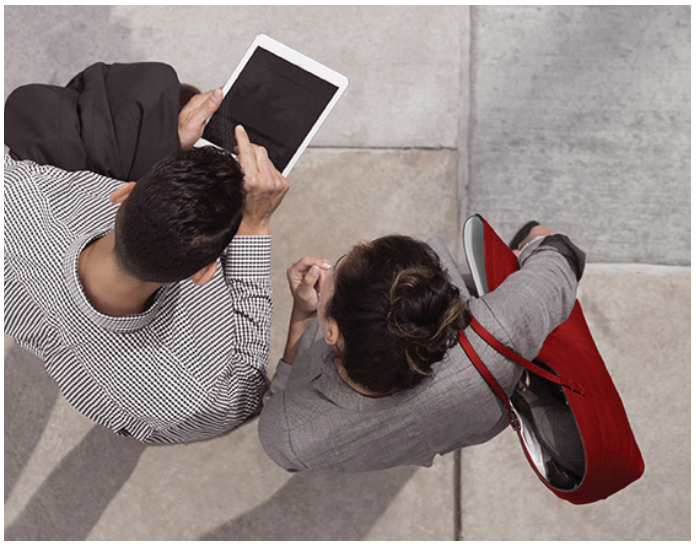
Fuente: https://blockchain.info

Como podemos ver en muchas cuentas online, incluidos los monederos mentales, "password" sigue siendo una contraseña muy utilizada. Hemos encontrado muchas contraseñas, incluidas algunas de las nuestras para criptomoneda, en bases de datos filtradas. Utilizando la base de datos de hashes de Troy Hunt "Have I Been Pwned", hemos cruzado nuestros resultados con hashes de contraseñas que sabíamos se habían filtrado a través de varias fugas de datos. Con nuestro diccionario para bitcoin hemos encontrado 5098 contraseñas distintas, a partir de 501 millones de registros filtrados. Entre ellas, algunas eran también monederos mentales, y se sospecha que más de 30 bitcoins habían sido robadas.

Los operadores de cambio en el punto de mira

Los operadores de cambio de criptomonedas, que se han convertido en el objetivo número uno, juegan un papel fundamental en este campo. Un operador de cambio de criptomonedas ayuda a los usuarios particulares a gestionar su moneda virtual y a efectuar transacciones con otras monedas virtuales o monedas físicas, como dólares. Estos operadores actúan como los bancos tradicionales, que ofrecen un servicio de gran utilidad para muchas personas. Los titulares de una cuenta pueden crear cuentas, añadir o distribuir fondos, y gestionar su criptomoneda sin necesidad de tener conocimientos sobre el software de monedero local. Los operadores de cambio importantes operan con varias monedas y gestionan las transacciones entre ellas. En muchos casos, un cambio de divisa es la única forma de utilizar las criptomonedas y uno de los métodos principales que pueden emplear los clientes para adquirir moneda.

Los ciberdelincuentes son conscientes de la popularidad de los operadores de cambio y dirigen sus ataques contra ellos. Como ocurre en el sector bancario, los operadores de cambio pueden ser una mina de oro si no se protegen convenientemente. Los bancos cuentan con la ventaja de la experiencia que han acumulado en décadas tratando con problemas de seguridad y respuestas a incidentes. Sin embargo, a pesar de ello, los problemas de seguridad siguen siendo una realidad, como hemos visto con numerosos ataques contra la red bancaria SWIFT en los últimos años. Los operadores de cambio no tienen el lujo de poseer esa experiencia y están aprendiendo por las malas. Las lecciones pueden salirles caras tanto a ellos como a su base de clientes.



Incidentes destacables

En enero de 2018, Coincheck, uno de los primeros operadores de cambio de Japón y uno de los más populares, perdió 532 millones de dólares en monedas NEM, lo que afectó a 260 000 inversores. Las operaciones se detuvieron generando el desconcierto de las víctimas. Un ciberdelincuente había conseguido acceso al ordenador de un empleado y había instalado malware diseñado para robar claves privadas de monederos digitales. El agresor logró apoderarse de la clave privada de un monedero "caliente" ("hot wallet"), que se utilizaba online para las transacciones inmediatas. Tras vaciar las cuentas, el resultado fue una de las mayores operaciones de hacking de criptomoneda conocidas hasta la fecha.

Pero el ataque de Coincheck no fue el único. Los operadores de cambio han sido objetivo de los ataques de ciberdelincuentes durante todo 2016 y 2017. Durante ese período, hemos observado muchos ataques. A principios de 2017, descubrimos que casi 120 000 bitcoins habían sido robadas de Bitfinex en agosto de 2016. Las monedas se cambiaron a otros operadores, como LocalBitcoins, Xzzx, BTC-e, Bitcoin.de, Coinbase, Kraken, CoinsBank y QuadrigaCX. A pesar de la recompensa ofrecida del 5 % sobre su valor, las monedas robadas no se han recuperado. "Básicamente sabemos lo que ocurrió", escribió Drew Samsen, Jefe del equipo de aplicaciones de Bitfinex. "Fue obra de uno o varios profesionales (o de un equipo) que durante varios meses cubrieron hábilmente su rastro".

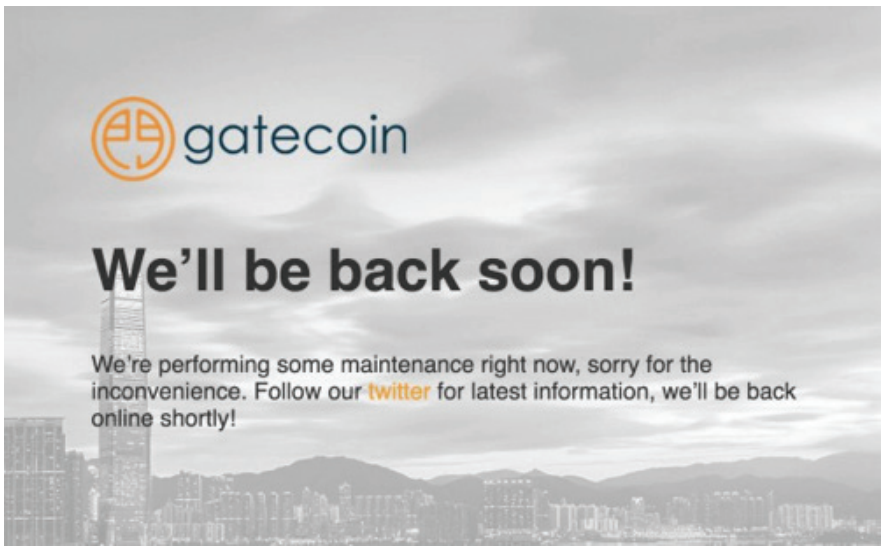


Figura 10. Una captura de pantalla del operador de cambio Gatecoin en mayo de 2016. Fuente: CoinDesk.com

Gatecoin, un operador de cambio de Hong Kong, es conocido por su rápida adopción de Ethereum. En mayo de 2016, Gatecoin comunicó no solo la pérdida de 250 bitcoins, sino también la gigantesca pérdida de 185 000 Ether (aproximadamente, 2 millones de dólares). Resultaron afectados tanto sus monederos calientes como sus monederos offline "almacenados en frío". El agresor consiguió sortear las protecciones multifirma colocadas en el almacenamiento en frío, alterando los sistemas del operador de cambio de manera que se utilizaran monederos calientes.

El objetivo no es siempre la propia infraestructura de cambio de divisas. Los clientes de un operador de cambio también pueden ser víctimas de un ataque directo. En su momento álgido, Bithumb procesaba el 10 % de todas las operaciones con bitcoin en el mundo y era el operador surcoreano más grande de Ether, con aproximadamente el 44 % de las transacciones.

En junio de 2017, Bithumb informó de la pérdida de información de identificación personal de 31 800 usuarios web (aproximadamente el 3 % de su base de usuarios), debido a un ataque contra el ordenador de un empleado. En lugar de atacar la infraestructura, el agresor fue directamente contra los clientes, en algunos casos haciéndose pasar por ejecutivos de Bithumb y mediante el empleo de técnicas de phishing y de ingeniería social.

Los clientes de Enigma, que opera como una plataforma de inversión, recibieron ataques similares. Mediante el uso de técnicas de ingeniería social habituales y bien conocidas, los agresores convencieron a los clientes de Enigma para que utilizaran una dirección de Ethereum maliciosa. Al atacar el sitio web oficial de Enigma, sus boletines de noticias y las cuentas de Slack, el agresor distribuyó direcciones de pago de Ethereum incorrectas que eran de su propiedad. Se robaron más de 1500 Ether, y algunas transacciones se realizaron después de que el ataque se divulgara y se solucionara.

TxHash	Block	Age	From		To	Value	[TxFee]
0xcf6b4ccc0f91b32...	5059624	14 days 8 hrs ago	0x21e229f2d307d7f...	IN	Fake_EnigmaPhish	0.002 Ether	0.000105
0xbf45b27df99f5f74...	4825731	55 days 3 hrs ago	0xdc4ee4e2580b4c...	IN	Fake_EnigmaPhish	0.00124579 Ether	0.00042
0x12580af9ab49fee...	4313854	150 days 6 hrs ago	Fake_EnigmaPhish	OUT	0x99e331fa7c45671...	20.2 Ether	0.000441
0xbd96745cea0723...	4262418	165 days 10 hrs ago	0xf4a2f01cd178b88...	IN	Fake_EnigmaPhish	3 Ether	0.000441

Figura 11. Registro de transacción.

Fuente: https://etherscan.io/

Tras algunos años de importantes ataques relacionados con cambio de divisas, las noticias del ataque de Coincheck tuvieron un impacto palpable en la confianza. Ahora, ante el menor síntoma de un problema los clientes alzaban su voz para hacer llegar sus preocupaciones a otros operadores de cambio. Binance, obligado a someterse a operaciones de mantenimiento imprevistas, optó por adelantarse y avisar a sus clientes para que estuvieran alerta para detectar timos e impostores que amenazaran sus cuentas.

Aunque Binance no sufrió una fuga de datos, fue víctima de un ataque de denegación de servicio poco después del mantenimiento del servidor. Las noticias del ataque no apaciguaron los ánimos de los usuarios, que ya tenían sus dudas sobre las tareas de mantenimiento del servidor no programadas. Para mantener la confianza del cliente, Binance ofreció un descuento del 70 % en las comisiones durante la mayor parte de febrero.

Los usuarios de criptomoneda buscan cada vez más estabilidad en un mercado muy volátil. Muchos clientes aconsejan dividir las monedas en varios operadores de cambio para protegerse frente a los inevitables ataques. Para los usuarios avanzados, los monederos locales o basados en hardware son una alternativa razonable. Estas opciones, sin embargo, presentan sus propios riesgos de seguridad que cada individuo debe gestionar. Está disminuyendo el nivel de confianza del usuario en la seguridad de las operaciones de cambio, debido a la dificultad que tiene el sector para encontrar un equilibrio entre crecimiento y seguridad.

Figura 12. Un mensaje del operador de cambio Binance. La cuenta ha sido suspendida por Twitter.

Seguir

Compartir

Recuperación

La recuperación tras sufrir un robo de criptomoneda es más difícil y complicada que con la mayoría de las demás divisas, debido a su naturaleza descentralizada. Solo el propietario de un monedero puede realizar cambios en su saldo, aunque hubiera adquirido dicho saldo de manera ilegal. Aunque un operador de cambio puede ser capaz de rastrear a dónde han ido las monedas, necesita la ayuda del propio dueño para devolver los fondos. Básicamente, el operador debe localizar al delincuente y encontrar las claves del monedero para poder devolver las monedas robadas. En el caso de movimientos entre operadores, siempre que la legislación local lo permita, es posible llegar a un acuerdo para la devolución de los fondos. Los operadores generalmente gestionan sus claves de blockchain internamente, y guardan las cuentas de forma centralizada, lo que les ofrece mucho más control de los monederos. Sin embargo, si los fondos se transfieren a un monedero privado, la víctima no tiene opciones. La única esperanza es que las fuerzas de seguridad puedan seguir el rastro del ladrón y adquirir la clave privada asociada al monedero. Sea cual sea el caso, es básicamente una causa perdida debido a la limitación de recursos y a la falta de legislación o problemas de jurisdicción.

En incidentes ocurridos recientemente, los operadores de cambio han intentado compensar a sus clientes por las pérdidas, por lo menos los que han sobrevivido al ataque. Coincheck, Bitfinex, y Gatecoin son un ejemplo de los afortunados que lo han conseguido. En marzo de 2018, Coincheck comenzó a compensar a las víctimas por sus pérdidas en monedas NEM. En abril de 2017, Bitfinex devolvió a las víctimas el importe perdido en el ataque de agosto de 2016. Sin embargo, en lugar de utilizar fondos directamente de la empresa, utilizaron la versión en criptomoneda de un pagaré. Tras hacer público el ataque, crearon tokens BTX y prometieron que recomprarían cada uno por 1 dólar en el futuro. Distribuyeron estos tokens a los titulares de sus cuentas y efectuaron la recompra en abril. En febrero de 2017, el operador de cambio Gatecoin de Hong Kong completó el reembolso de las bitcoins robadas en una operación de hacking en mayo de 2016. Las bitcoins valían entre 450 y 750 dólares en el momento del robo, pero alrededor de 1190 dólares una vez que se realizó el reembolso. Además, diseñaron un plan de reembolso para las Ether robadas restantes. En este caso, el operador de cambio obtuvo los fondos de otras partes del negocio, como los servicios de consultoría y las tasas de cambio, y reasignó los ingresos a la recompra.

No todos los operadores de cambio pudieron recuperarse. El ejemplo más conocido es el de la caída de Mt. Gox, un operador japonés que recibió un ataque entre 2011 y 2014. Se robaron más de 450 millones de bitcoins. En ese año esto condujo a la liquidación y el cierre de Mt. Gox. Otros dos operadores destacados recientes tampoco pudieron recuperarse de las repercusiones sufridas por los ciberataques. Bitcurex, el mayor y uno de los más antiguos de Polonia, cerró el negocio un mes después del ataque. Al principio se informó de algunos problemas de servicio de manera bastante imprecisa, pero más tarde se descubrió que habían desaparecido 2300 bitcoins.

Tras dos semanas de confusión pública Bitcurex cerró repentinamente y los usuarios se vieron obligados a asumir las pérdidas. En marzo de 2017, la policía polaca anunció investigaciones de las circunstancias del cierre y solicitó la comparecencia de las partes.

Youbit, un operador de cambio surcoreano, no pudo seguir operando tras recibir un ataque. Solo un mes después de que comenzara la investigación de Bitcurex, Youbit, llamada entonces Yapizon, perdió 4000 bitcoins a manos de los hackers, lo que equivalía aproximadamente al 36 % de sus fondos. Según los detalles que aparecieron más tarde los hackers robaron la moneda después de conseguir acceder a los sistemas internos y a cuatro monederos calientes. Youbit intentó utilizar métodos parecidos a los de Bitfinex para compensar a sus clientes. Repartieron las pérdidas entre todos los titulares de cuentas y emitieron tokens en forma de pagarés, que prometieron recomprar más tarde. Sin embargo, en diciembre de 2017, Youbit sufrió otro ataque, que supuso la pérdida del 17 % de sus fondos y obligó a la empresa a declararse en bancarrota. Los clientes que aún tenían fondos pudieron retirar el 75 % de su saldo; el resto se destinó al procedimiento de quiebra.

Conclusión

La tecnología blockchain sigue afectando, tanto positiva como negativamente, a las industrias de todo el mundo, por lo que debemos ser diligentes y adelantarnos a las implicaciones que esto tiene en la seguridad. Como hemos visto, los ciberdelincuentes aguzarán el ingenio y hallarán

"El 13/10/2016, como resultado de sistemas de terceros, www.bitcurex.com sufrió interferencias externas en la recopilación de datos automática y el procesamiento de información. La consecuencia de estas acciones es la pérdida de parte de los activos gestionados por bitcurex.com/dashcurex.com".

—Traducción de la declaración publicada en bitcurex.com

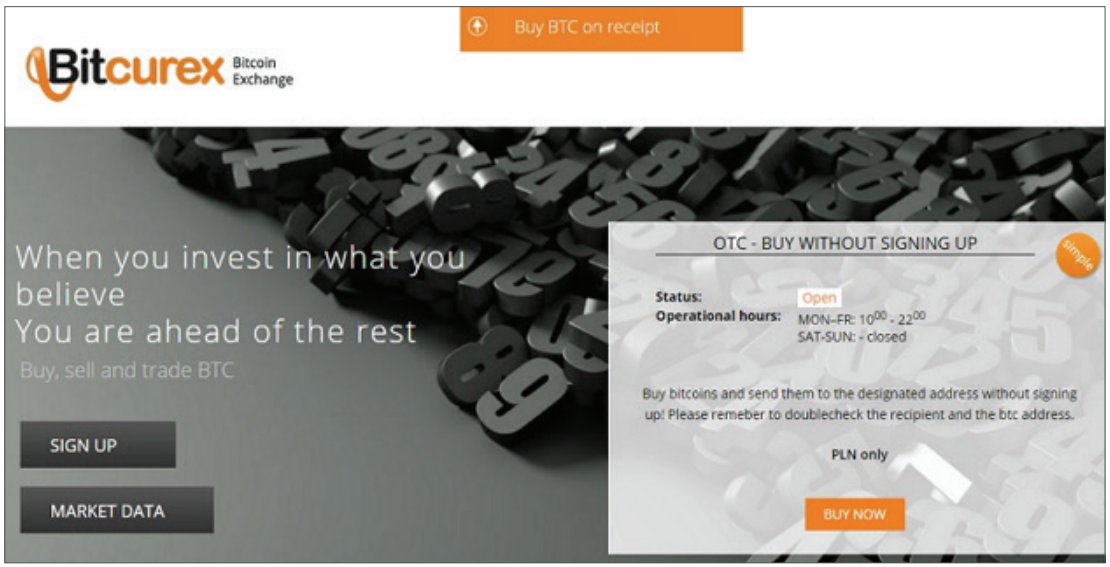


Figura 13. Aviso publicado en el operador de cambio polaco cerrado Bitcurex.

Seguir

Compartir

siempre la forma de conseguir sus objetivos. Aunque hay numerosas investigaciones sobre la tecnología blockchain y ya hay respuestas en relación a la confianza en la descentralización, no se garantiza todavía la seguridad de los usuarios o las aplicaciones que se conectan a su red. Hemos podido ver cómo un comportamiento no seguro que hace uso de monederos mentales lleva al robo de criptomonedas. Los agresores han conseguido utilizar técnicas antiguas de formas nuevas, como los ataques de diccionario, contra las claves privadas de bitcoin. Incluso los ataques de phishing tradicionales funcionan para conseguir acceso a monederos o recursos informáticos. Y hemos observado cómo el único objetivo no son solo los usuarios de blockchain. Los que han adoptado blockchain a nivel comercial de manera más generalizada son los operadores de cambio, que han sufrido un interminable aluvión de ataques que lograban su objetivo. Los organismos reguladores tienen dificultades para mantenerse al día y entender las implicaciones legales de las pérdidas derivadas de ciberataques.

Las empresas, por su parte, también deben ser diligentes. La tecnología blockchain atrae mucho interés para satisfacer distintas necesidades empresariales, no solamente los pagos descentralizados. Se están construyendo empresas completamente automatizadas mediante contratos inteligentes. Los minoristas y otras empresas recurren a blockchain para la gestión de inventarios. El sector sanitario examina métodos para gestionar los documentos médicos. El número de ataques que han logrado su objetivo y han causado daños a operadores de cambio va mucho más allá de los límites de este informe, y debe servir de advertencia.

No basta con implementar y utilizar nuevas tecnologías sin efectuar una evaluación de riesgos pormenorizada. A medida que los distintos sectores vayan investigando e implementando sus propios blockchains, es previsible que los ciberdelincuentes desplieguen una combinación de técnicas conocidas y otras aún desconocidas para atacarlos. Si no conoce perfectamente dónde están los riesgos, puede depositar su confianza en sus implementaciones de blockchain, y equivocarse. Como hemos visto, es muy fácil cometer un error. Es aún más difícil controlar a los usuarios, y ellos pueden contribuir negativamente a aumentar el riesgo. Necesitamos aprender de los últimos acontecimientos para tomar mejores decisiones en cuanto a la protección de nuestras tecnologías para el futuro.

Acerca de McAfee

McAfee es la empresa de ciberseguridad que ofrece protección total, desde los dispositivos a la nube. Inspirándose en el poder de la colaboración, McAfee crea soluciones para empresas y particulares que hacen del mundo un lugar más seguro. Al diseñar soluciones compatibles con los productos de otras firmas, McAfee ayuda a las empresas a implementar entornos cibernéticos verdaderamente integrados en los que la protección, la detección y la corrección de amenazas tienen lugar de forma simultánea y en colaboración. Al proteger a los consumidores en todos sus dispositivos, McAfee protege su estilo de vida digital en casa y fuera de ella. Al trabajar con otras empresas de seguridad, McAfee lidera una iniciativa de unión frente a los ciberdelincuentes en beneficio de todos.

www.mcafee.com/es

McAfee
Together is power.

Avenida de Bruselas nº 22
Edificio Sauce
28108 Alcobendas, Madrid, España
www.mcafee.com/es