BitMEX, una popular plataforma de intercambio de criptomonedas, filtró accidentalmente los datos confidenciales relacionados con sus usuarios, siendo esto el resultado de que la compañía no tuviera un protocolo de copia oculta en sus servidores de correo masivo.

La compañía reconoció el problema unas horas después. El subdirector de operaciones de BitMEX, Vivien Khoo, emitió un comunicado diciendo que BitMEX envió de forma accidental un mensaje a la mayoría de sus usuarios que contenía las direcciones de correo electrónico de otros usuarios en el campo *«para».*

> *«Lamentamos profundamente la preocupación que esto ha causado a nuestros usuarios. El problema fue causado por un error en el software utilizado para enviar correos electrónicos. Tan pronto como nos enteramos del problema, de inmediato evitamos que se enviaran más correos electrónicos y desde entonces hemos abordado el problema para garantizar que esto no vuelva a pasar».*

Para colmo, piratas informáticos desconocidos pudieron tomar el control de la cuenta oficial de Twitter de BitMEX por un corto tiempo luego de la filtración. Mientras tenían el control, los delincuentes pudieron publicar varios mensajes, como *«Toma tu BTC y corre. Último día para retiros».*

Como respuesta, el equipo de relaciones públicas de BitMEX procedió rápidamente a eliminar los mensajes y emitió una declaración alegando que el hackeo no puso en peligro la seguridad de los fondos de los clientes.

Una cuenta de Twitter llamada *«Bitmexdatabaseleak»*, que había sido suspendida, surgió luego del hackeo, supuestamente filtrando una gran cantidad de datos de clientes, como ID de usuario individuales y correos electrónicos.

Larry Cermak, director de investigación de The Block, el reciente incidente de datos de BitMEX coincidió con un volcado de correo electrónico de alrededor de 30 mil direcciones en la deep web. Esto ha llevado a las personas a creer que algunos o todos los datos filtrados de

los clientes podrían haberse vendido en línea a terceros.

BitMEX deshabilitó temporalmente los retiros para los clientes que cambiaron las contraseñas de su cuenta o los detalles de seguridad luego de la filtración de la dirección de correo electrónico.

Después de un tiempo de seguridad, un día después de la fuga de datos, el pasado 1 de noviembre, el volumen total de retiro de BTC de la plataforma no se vió afectado en gran medida.

Jeffrey Liu Xun, CEO de la puerta de enlace fiduciaria de igual a igual, XanPool, compartió sus comentarios con Cointelegraph, sobre cómo una empresa de la talla de BitMEX podría permitir errores como ese.

> *«Debido a que he recibido los correos electrónicos anteriores de BitMEX, sin este problema, esto probablemente se deba a que un novato de marketing interno está cometiendo un error ENORME, o su proveedor de servicios de correo masivo está en mal estado. Creo que es lo primero porque servicios como MailChimp no cometen estos errores. Este problema definitivamente no puede dejarse de lado».*

Luego, dijo que como resultado de los riesgos de privacidad planteados por la filtración, los competidores de BitMEX pueden enviar ahora correos electrónicos masivos a sus clientes en un intento de caza.

Xun también cree que existe un segundo riesgo más peligroso, que radica en el hecho de que la gran mayoría de las personas que utilizan las plataformas de negociación no emplean contraseñas complejas, por lo que los hackers serios ahora pueden tener la opción de revisar sus repositorios de contraseñas para tratar de obtener acceso a las billeteras de usuarios desprevenidos.

> *«Doxear los correos electrónicos de los usuarios es por lo general tan perjudicial como doxear sus contraseñas, ya que los hackers tienen grandes depósitos de contraseñas que las personas tienden a usar. Finalmente, la liberación de los correos electrónicos de sus usuarios también los abre a ataques de spam y phishing»*, agregó Xun.

Craig Russo, inversor de criptomonedas y propietario de Peer, una startup con sede en Boston, detrás del popular medio de comunicación SludgeFeed, opinó que toda esta situación ha sido un terrible lapso de seguridad por parte de BitMEX y se enfrentará a la plataforma siempre que esté involucrado en cualquier tipo de controversia en el futuro.

> *«La confianza es primordial en esta industria y las consecuencias de un evento como este probablemente persistirán por un tiempo. Creo que en el corto plazo algunos inversores abandonarán la plataforma, pero en general, BtiMEX puede recuperarse del incidente dada su participación de mercado y los recursos a su disposición»,* dijo Russo.

¿Qué pasará ahora?

BitMEX lanzó una publicación el lunes admitiendo que, aunque sus procesos internos realmente habían fallado la semana pasada, la situación se solucionó gracias al sistema interno de detección de errores recientemente diseñado por la compañía, que es capaz de manejar la representación necesaria, traducción, puesta en escena y envío parcial de correos electrónicos importantes.

Según el proveedor de datos Skew, la información personal de 22,000 usuarios de BitMEX probablemente ha sido expuesta en línea. Según Dovey Wan, de Primitive Crypto, esto podría hacer que el gobierno de Estados Unidos haga uso de las direcciones de correo electrónico filtradas para investigar las declaraciones de impuestos de muchas personas involucradas con BitMEX. La plataforma no está registrada en la Comisión de Comercio de Futuros de

Productos Básicos y, por lo tanto, los ciudadanos estadounidenses no pueden participar en la plataforma.

Además, el IRS lanzó recientemente un nuevo conjunto de reglas que requieren que los titulares de criptomonedas informen todas sus existencias de criptomonedas con detalles meticulosos. Los propietarios de criptomonedas ahora están sujetos a impuestos sobre las ganancias de capital que puedan haber adquirido por medio del intercambio o la tenencia de dichos activos digitales.

BitMEX enfrenta la posibilidad de incurrir en acciones legales como resultado de este problema. Aaron Wagener, cofundador y director de operaciones de la red descentralizada de datos globales MXC Foundation, dijo que debido a los términos y condiciones presentados por BitMEX en el momento de la incorporación del cliente, cualquier acción legal potencial contra la empresa podría resultar extremadamente difícil.

Wagener agregó que debido a la situación, que se produjo claramente debido a la falta de juicio humano, el problema más importante girará en torno a BitMEX para garantizar la seguridad de sus usuarios, especialmente porque esta información ya entró a dominio público.

> *«Es extremadamente difícil decir simplemente que el problema se ha reducido. Los usuarios se encuentran bajo una amenaza potencial de correos electrónicos de phishing, estafas y spam de una amplia gama de fuentes. Este es un problema que seguirá siendo una espina en el lado de los usuarios por bastante tiempo»,* dijo Wagener.

Por otro lado, Ray Walsh, experto en privacidad digital de la plataforma educativa ProPrivacy, cree que según el Reglamento General de Protección de Datos, la compañía podría enfrentar grandes multas. Además, la Comisión Federal de Comercio podría iniciar una investigación, o los usuarios de BitMEX podrían decidir entablar una demanda colectiva contra la empresa por el mal manejo de sus datos personales.

> *«Después de la filtración, los usuarios de BitMEX recibieron correos electrónicos inusuales y no parece haber dudas de que esos correos electrónicos fueron el resultado de la filtración. También parece que las direcciones de correo electrónico filtradas ya se han vendido en la web oscura, lo que significa que los piratas informáticos muy serios, intentarán robar las contraseñas de las personas para robar criptomonedas»*, aregó.