Group-IB, compañía de seguridad cibernética con sede en Singapur, descubrió miles de registros personales de usuarios de Reino Unido, Australia, Sufráfrica, Estados Unidos, Singapur, España, Malasia, y otros países, expuestos en una etapa múltiple dirigida de estafa relacionada con Bitcoin.

La compañía encontró números telefónicos, nombres completos y correos electrónicos contenidos en URL personalizadas utilizadas para redirigir a las personas a sitios web que se hacían pasar por medios locales con comentarios inventados sobre personalidades locales sobre inversión en criptomonedas que *«los ayudó a construir una fortuna».*

La investigación conjunta de los equipos de Inteligencia de Amenazas y Protección de Marca de Group IB, reveló 284,926 conjuntos de información de identificación personal expuesta en lo que resultó ser un fraude muy elaborado en tres etapas de diseño.

El análisis de los códigos telefónicos de los países expuestos mostró que la mayoría de las víctimas eran de Reino Unido (147,610), seguidas de Australia (82,263), Sudáfrica (4,149), Estados Unidos (4,147), Singapur (3,499), Malasia (2,491), España (2,420) y otros países.

Según la investigación, una víctima recibe un mensaje de texto, que los estafadores envían utilizando el nombre de un medio de comunicación conocido.

> *«Cada mensaje contenía un enlace corto único. Un análisis más detallado de las URL reveló que un enlace corto lleva a la víctima a otra URL que ya muestra sus datos personales, como el número de teléfono, nombre y/o apellido, y a veces una dirección de correo electrónico, y se utiliza para redireccionar a sitios web falsos que se enmascaran como un medio de comunicación local»,* dice Group-IB.

Según los investigadores, todas las páginas falsas descubiertas son casi idénticas en términos de diseño, pero la URL y el código de la página son únicos cada vez y contienen

registros personales de los usuarios.

Si una víctima hace clic en algún enlace del sitio falso, es llevada a un sitio web de plataforma de inversión de bitcoin, donde sus datos, contenidos en la URL, ya se completarán previamente en el formulario de registro sin el consentimiento del usuario. Después, se le pide a la víctima que agregue saldo a su cuenta de Bitcoin.

Group-IB encontró 6 dominios activos con la misma plataforma de inversión de bitcoin, bajo los nombres de Crypto Cash, Bitcoin Rejoin, Bitcoin Supreme y Banking on Blockchain.

> *«Las estafas de inversión de bitcoin han existido durante bastante tiempo y detectamos regularmente nuevos casos de fraude criptográfico. Esta vez, sin embargo, el esquema se actualizó significativamente y se filtró una enorme cantidad de información personal. Los malos se volvieron más inteligentes en un intento por aumentar la tasa de éxito de sus operaciones fraudulentas. El uso de datos personales les permite llevar a cabo ataques dirigidos y hacer que el viaje de una víctima sea más fácil y fluido, lo que nivela la efectividad general del esquema. En general, muchas personas tienden a subestimar los riesgos de que sus nombres, teléfonos o correos electrónicos circulen en línea hasta que sucedan cosas malas. De hecho, una cantidad tan grande de datos confidenciales en las manos equivocadas abre un mundo completamente nuevo de oportunidades para los estafadores. Estos datos pueden venderse más o pueden impulsar una nueva ronda de fraude»*, dijo Ilya Sachkov, CEO de Group-IB.