CryptoRom: el nuevo ‘estafador de Tinder’ ahora cobra un falso impuestos por ganancias

CIUDAD DE MÉXICO. 16 de marzo de 2022.- Sophos, líder mundial en ciberseguridad de última generación, publicó nuevos datos sobre CryptoRom, una estafa internacional que ha robado cientos de miles de dólares en criptomonedas dirigida a usuarios de iPhone y Android mediante aplicaciones de citas populares, como Bumble y Tinder.

La nueva investigación, **"CryptoRom Swindlers Continue to Target Vulnerable iPhone/Android Users",** se basa en historias y contenido compartido con Sophos por parte de algunas víctimas de esta estafa que se pusieron en contacto con la compañía.

En 2021, Sophos detalló en un informe que los atacantes de CryptoRom publican perfiles falsos, muy convincentes, en sitios de citas. Una vez que se han puesto en contacto con un objetivo, intentan persuadirlo para que invierta en una aplicación de *trading* de criptomonedas falsa. Cuando la víctima intenta acceder a los fondos, son rechazados y su dinero, de pronto, desaparece.

En la nueva investigación, Sophos informa que ahora, cuando lo anterior sucede, los estafadores le indican al usuario que para recuperar el acceso a su dinero, deben pagar cientos de miles de dólares en un falso "impuesto sobre las ganancias”.

Casi como lo vio en Netflix…

Sophos tuvo acceso a datos que indican que a una víctima se le cobraron USD $625,000 para recuperar el acceso al USD $1 millón que había invertido en un esquema falso de intercambio de criptomonedas.

El “amigo” de esa víctima le dijo, además, que había invertido de su propio dinero para sumar en conjunto USD $4 millones. Luego, le dijo que esa inversión generó una ganancia de USD $3.13 millones que estaban sujetos a un impuesto sobre las ganancias del 20%, o USD $625,000. La víctima debía pagar para acceder a los fondos, pero ni la co-inversión ni las ganancias fueron reales, y ese “amigo” realmente era el estafador.

“*La estafa de CryptoRom es un fraude financiero centrado en gran medida en la ingeniería social*”, dijo Jagadeesh Chandraiah, investigador principal de amenazas de Sophos. “*Los estafadores atraen objetivos a través de perfiles falsos en sitios de citas legítimos y luego intentan persuadirlo para que instale e invierta en una aplicación de comercio de criptomonedas falsa. Las aplicaciones generalmente se instalan como clips web y están diseñadas para parecerse mucho a las aplicaciones legítimas y confiables”*, añade.

“*Según las víctimas de esta estafa que contactaron a Sophos después de nuestros artículos anteriores, el 20% de 'impuesto a las ganancias' solo se menciona cuando intentan retirar sus fondos o cerrar la cuenta. A las víctimas que luchan por pagar el impuesto se les ofrece un*

préstamo. Incluso hay sitios web falsos que prometen ayudar a las personas a recuperar sus fondos si han sido estafados. En resumen, en cualquier camino que sigan las víctimas, cada vez más desesperadas para intentar recuperar su dinero, los estafadores estarán esperándolos. Las personas nos dicen que han perdido los ahorros de toda una vida o sus fondos de jubilación debido a la estafa", concluye el especialista.

La investigación de Sophos también encontró algunos casos en los que los operadores de CryptoRom se habían acercado a los objetivos directamente a través de WhatsApp y mensajes SMS, probablemente utilizando información robada.

Nuevas características técnicas

La investigación de Sophos también detalla nuevos aspectos técnicos del funcionamiento de CryptoRom. Por ejemplo, los estafadores están haciendo un mal uso de la función TestFlight de Apple que permite que un grupo limitado de personas instale y pruebe una nueva aplicación de iOS y pase por un proceso de revisión menos estricto.

Los investigadores de Sophos también descubrieron que todos los sitios web relacionados con CryptoRom utilizados por los estafadores tienen una estructura y un contenido de back-end muy similares y que solo las marcas, los íconos y las URL eran diferentes.

La firma de ciberseguridad cree que esto puede permitir que los estafadores cambien rápidamente los sitios web que usan para emitir el fraude cuando uno de ellos es detectado y cerrado.

Mantenerse a salvo: un problema de la industria

"Es profundamente preocupante que la gente siga cayendo en estos esquemas criminales, particularmente porque el uso de transacciones extranjeras y los mercados de criptomonedas no regulados significan que las víctimas no tienen protección legal para los fondos que invierten", dijo Chandraiah.

"Este es un problema de toda la industria que no va a desaparecer. Necesitamos una respuesta colectiva que incluya la trazabilidad de las transacciones con criptomonedas, advertir a los usuarios sobre estas estafas para detectar y eliminar rápidamente los perfiles falsos que permiten este tipo de fraude", indicó.

Sophos ha publicado investigaciones previas sobre CryptoRom y otros fraudes financieros y de intercambio de criptomonedas. Sophos también ha publicado informes sobre otras ciberamenazas a las que se enfrentan los consumidores y los usuarios domésticos, incluido el "fleeceware" en el que se cobra de más a los usuarios por los servicios de aplicaciones móviles.

###

Sobre Sophos

Sophos es un líder mundial en ciberseguridad de próxima generación y protege a más de 500.000 organizaciones y millones de consumidores en más de 150 países de las ciberamenazas más avanzadas de la actualidad. Con tecnología de inteligencia de amenazas, inteligencia artificial y aprendizaje automático de SophosLabs y SophosAI, Sophos ofrece una amplia cartera de productos y servicios avanzados para proteger a los usuarios, las redes y los puntos finales contra ransomware, malware, exploits, phishing y una amplia gama de otros ciberataques. Sophos proporciona una única consola de gestión integrada basada en la nube, Sophos Central, la pieza central de un ecosistema de ciberseguridad adaptable que cuenta con un lago de datos centralizado que aprovecha un amplio conjunto de API abiertas disponibles para clientes, socios, desarrolladores y otros proveedores de ciberseguridad. Sophos vende sus productos y servicios a través de socios revendedores y proveedores de servicios administrados (MSP) en todo el mundo. Sophos tiene su sede en Oxford, Reino Unido. Hay más información disponible en www.sophos.com

Síguenos en:
Facebook: https://www.facebook.com/SophosLatam/
Twitter: https://twitter.com/SophosLatAm
LinkedIn: https://www.linkedin.com/company/sophos/