CryptoRom: la amenaza que ‘se ligó’ a los usuarios de iOS para robar casi USD $1.4 millones en Bitcoin

- *Los atacantes cuentan con una amplia gama de víctimas estadounidenses y europeos a las que contactan desde aplicaciones como Bumble y Tinder, para luego adquirir la capacidad de administrar de forma remota sus iPhones.*

CIUDAD DE MÉXICO. 18 de octubre de 2021.- Sophos, líder mundial en ciberseguridad de última generación, publicó un nuevo informe sobre una estafa internacional en el mercado de criptomonedas dirigida a usuarios de iPhone, que ataca a través de aplicaciones de citas populares, como Bumble y Tinder.

La investigación titulada **‘**CryptoRom Fake iOS Cryptocurrency Apps Hit US and European victims for $1.4 millions**’**, detalla que la operación se ha intensificado y que los atacantes se han expandido para apuntar a personas en Asia, Estados Unidos y Europa.

Sophos descubrió que los atacantes tienen una billetera de Bitcoin que contiene casi **USD $1.4 millones de dólares en la criptomoneda**, supuestamente recolectados de las víctimas. Los investigadores de Sophos han bautizado la amenaza con el nombre en código **"CryptoRom"**.

"*La estafa de CryptoRom se basa en gran medida en la ingeniería social en casi todas las etapas"*, dijo Jagadeesh Chandraiah, Investigador Senior de Amenazas en Sophos. *“Primero, los atacantes publican perfiles falsos, muy convincentes, en sitios de citas. Una vez que se han puesto en contacto con un objetivo, los atacantes sugieren continuar la conversación en una plataforma de mensajería. Luego intentan persuadir al objetivo para que instale e invierta en una aplicación de comercio de criptomonedas falsa”,* explica.

“*Al principio, las operaciones se ven muy bien, pero si la víctima solicita la devolución de su dinero o intenta acceder a los fondos, son rechazados y su dinero, de pronto, desaparece. Nuestra investigación muestra que es ahí en dónde los ciber atacantes realizaron la estafa, ganando millones de dólares de esas inversiones falsas“* añade el especialista.

- **Doble problema**

Además de robar dinero, los atacantes también obtienen acceso a los iPhones de las víctimas, según la investigación de Sophos. En esta versión del ataque, los ciberdelincuentes aprovechan "Enterprise Signature", un sistema para desarrolladores de software que ayuda a las organizaciones a probar nuevas aplicaciones iOS con usuarios seleccionados de iPhone antes de enviarlas a la App Store oficial de Apple para su revisión y aprobación.

Con la funcionalidad del sistema Enterprise Signature, los atacantes pueden apuntar a grupos más grandes de usuarios de iPhone con sus aplicaciones de comercio de cifrado falsas y obtener control remoto sobre sus dispositivos. Esto significa que los atacantes podrían hacer más que simplemente robar inversiones falsas en criptomonedas de las víctimas, sino que

también podrían, por ejemplo, recopilar datos personales, agregar y eliminar cuentas e instalar y administrar aplicaciones para otros fines maliciosos.

"*Hasta hace poco, los operadores criminales distribuían principalmente las aplicaciones criptográficas falsas a través de sitios web falsos que se asemejan a un banco confiable o la App Store de Apple*", dijo Chandraiah. "*La adición del sistema de desarrollo empresarial de iOS presenta un riesgo adicional para las víctimas porque podrían estar entregando a los atacantes los derechos de su dispositivo y la capacidad de robar sus datos personales".*

"Para evitar ser víctimas de este tipo de estafas, los usuarios de iPhone solo deben instalar aplicaciones originales de la App Store de Apple. La regla de oro es que si algo parece arriesgado o demasiado bueno para ser verdad, como el hecho de que alguien a quien apenas conoces te invite a un plan de inversión en línea 'excelente' que generará una gran ganancia, entonces, lamentablemente, probablemente sea un fraude", concluye.

Sophos recomienda que los usuarios instalen una solución de seguridad en sus dispositivos móviles, como Intercept X for Mobile, para proteger los dispositivos iOS y Android de las ciberamenazas. También vale la pena proteger todas las computadoras personales y domésticas con soluciones como Sophos Home.

###

Sobre Sophos

Sophos es la empresa líder mundial en ciberseguridad de última generación, que 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 para la detección 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, redes y endpoints contra ransomware, malware, exploits, phishing y una amplia gama de ciberataques. Sophos proporciona una plataforma única de gestión integral basada en la nube llamada Sophos Central, el eje 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 distribuidores y proveedores de servicios administrados (MSP) en todo el mundo. Sophos tiene su sede en Oxford, Reino Unido. Para más información, ingresa a www.sophos.com.

Síguenos en:

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