Un nuevo troyano bancario para Android está apuntando a las instituciones financieras brasileñas, con el fin de cometer fraude aprovechando la plataforma de pagos PIX.

La compañía italiana de seguridad cibernética Cleafy, que descubrió el malware entre finales de 2022 y principios de 2023, lo rastrea con el nombre de PixPirate.

> *«PixPirate pertenece a la última generación de troyanos bancarios para Android, ya que puede realizar ATS (Automatic Transfer System), lo que permite a los atacantes automatizar la inserción de una transferencia de dinero maliciosa por medio de la plataforma de pago instantáneo Pix, adoptada por distintos bancos brasileños»,* dijeron los investigadores Francesco Lubatti y Alessandro Strino.

También es la última incorporación en una larga lista de malware bancario para Android que abusa de la API de servicios de accesibilidad del sistema operativo para realizar sus funciones maliciosas, incluyendo la desactivación de Google Play Protect, la interceptación de mensajes SMS, la prevención de la desinstalación y la publicación de anuncios falsos por medio de notificaciones automáticas.

Además de robar las contraseñas ingresadas por los usuarios en las aplicaciones bancarias, los atacantes detrás de la operación aprovecharon la ofuscación y el cifrado del código usando un marco conocido como Auto.js con el fin de resistir los esfuerzos de ingeniería inversa.

Las aplicaciones cuentagotas usadas para entregar PixPirate vienen bajo la apariencia de aplicaciones de autenticación. No existen indicios de que las aplicaciones se hayan publicado en la tienda oficial de Google Play.

Los hallazgos llegan más de un año después de que ThreatFabric revelara detalles de otro malware llamado BrasDex que también cuenta con capacidades ATS, además de abusar de PIX para realizar transferencias de fondos fraudulentas.

> *«La introducción de capacidades ATS junto con marcos que ayudarán al desarrollo de aplicaciones móviles, usando lenguajes flexibles y más extendidos (reduciendo la curva de aprendizaje y el tiempo de desarrollo), podría conducir a malware más sofisticado que, en el futuro, podría compararse con sus contrapartes de estaciones de trabajo»,* dijeron los investigadores.

El desarrollo también se produce cuando Cyble lanzó luz sobre un nuevo troyano de acceso remoto de Android con nombre en código Gigabud RAT, dirigido a usuarios en Tailandia, Perú y Filipinas desde al menos julio de 2022 haciéndose pasar por aplicaciones bancarias y gubernamentales.

> *«El RAT tiene características avanzadas como la grabación de pantalla y el abuso de los servicios de accesibilidad para robar credenciales bancarias»,* agregaron los investigadores señalando su uso de sitios de phishing como vector de distribución.

La firma de seguridad cibernética reveló además que los hackers detrás del mercado de la red oscura InTheBox, están anunciando un catálogo de 1984 inyecciones web que son compatibles con varios malware bancarios de Android como Alien, Cerberus, ERMAC, Hydra y Octo.

Los módulos de inyección web, que se utilizan principalmente para recopilar credenciales y datos confidenciales, están diseñados para destacar aplicaciones bancarias, de pago móvil, de intercambio de criptomonedas y de comercio electrónico móvil que abarcan Asia, Europa, Medio Oriente y las Américas.

Pero en un giro más preocupante, las aplicaciones fraudulentas encontraron una forma de eludir las defensas en Apple App Store y Google Play para realizar lo que se conoce como una estafa de matanza de cerdos llamada CryptoRom.

La técnica implica el uso de métodos de ingeniería social, como acercarse a las víctimas por

medio de aplicaciones de citas como Tinder con el fin de tentarlas a descargar aplicaciones de inversión fraudulentas con el objetivo de robar su dinero.

Las aplicaciones iOS maliciosas en cuestión son Ace Pro y MBM_BitScan, las cuales han sido eliminadas por Apple desde entonces. Google también eliminó una versión de Android de MBM_BitScan.

La compañía de seguridad cibernética Sophos, que hizo el descubrimiento, dijo que las aplicaciones de iOS presentaban una *«técnica de evasión de revisión»* que permitía a los autores de malware superar el proceso de investigación.

> *«Ambas aplicaciones que encontramos usaban contenido remoto para proporcionar su funcionalidad maliciosa, contenido que probablemente estuvo oculto hasta después de que se completó la revisión de la App Store»,* dijo el investigador de Sophos, Jagadeesh Chandraiah.

Las estafas de matanza de cerdos comenzaron en China y Taiwán, y desde entonces se han expandido mundialmente en los últimos años, con una gran parte de las operaciones realizadas desde zonas económicas especiales en Laos, Myanmar y Camboya.

En noviembre de 2022, el Departamento de Justicia de Estados Unidos (DoJ), anunció la eliminación de siete nombres de dominio en relación con una estafa de criptomonedas de matanza de cerdos que les reportó a los hackers más de 10 millones de dólares de cinco víctimas.