Publicado en Madrid el 06/03/2024

Cleafy alerta a los grandes bancos de una ciberamenaza con malware Copybara

Los ciberdelincuentes ya han suplantado aplicaciones de entidades con aplicaciones de apariencia verdadera como "Caixa Sign Nueva", "BBVA Código" o "Sabadell Código" para propagar este software malicioso infectando los terminales de los usuarios

La startup de detección de fraudes bancarios, Cleafy, ha presentado las conclusiones de su análisis en el informe 'Aumento de los fraudes on-device: exposición de la nueva campaña de fraude con Copybara', en el que informa de una nueva campaña de fraude bancario de alta sofisticación que amenaza sobre todo a grandes bancos.

En 2023, el modelo conocido como 'apropiación de cuentas' (ATO, por sus siglas en inglés) fue uno de los fraudes más perjudiciales para los usuarios de banca online y actualmente representa el 90% de los intentos de fraude según Cleafy. Asimismo, la compañía ha detectado a principios de 2024 una campaña de fraude en curso que afecta a las principales entidades bancarias de España, Italia y Reino Unido. Este fraude consiste en la creación y difusión de aplicaciones falsas que simulan ser de entidades reales -entre ellas Caixa Sign Nueva, BBVA Código o Sabadell Código- que los usuarios descargan infectando sus dispositivos con el malware Copybara y permitiendo a los atacantes realizar transferencias no autorizadas desde el propio dispositivo de la víctima.

Copybara es una familia de amenazas móviles diseñadas específicamente para infectar dispositivos Android que utiliza ingeniería social y que se inicia con el envío de un SMS malicioso. Al hacer clic en el enlace del mensaje, los usuarios descargan una aplicación fraudulenta. Dado que este ataque se realiza directamente en el dispositivo (on-device), no muestra señales de alerta durante la navegación web, lo cual limita la efectividad de los mecanismos antifraude tradicionales. Este tipo de ataque se ha vuelto viable gracias a que más del 80% de los troyanos bancarios modernos para Android, tales como Vultur, TeaBot y SpyNote, pueden ser controlados de forma remota por los actores maliciosos en estos escenarios on-device.

El informe incluye un espectro completo de las tácticas, técnicas y procedimientos utilizados por los agentes maliciosos, que van desde componentes iniciales de Ingeniería Social (como phishing y vishing) utilizados para iniciar el ataque a la distribución de Copybara por infección de dispositivos y la gestión meticulosa de estas fases de ataque para asegurar el éxito de sus campañas.

Cleafy ha estado detrás de la detección, denominación y clasificación de otras amenazas recientes como Teabot, SharkBot y Revive. La compañía ha establecido unos altos estándares en la lucha contra el fraude cibernético, y trabaja protegiendo las instituciones financieras más grandes del mundo.

Datos de contacto:
Cleafy
Cleafy

917188509

Nota de prensa publicada en: Madrid

Categorías: Finanzas Software Ciberseguridad Dispositivos móviles Innovación Tecnológica