Las instituciones financieras están siento atacadas por una nueva versión de malware de Android llamado SpyNote, al menos desde octubre de 2022, que combina características de spyware y troyano bancario.

> *«La razón detrás de este aumento es que el desarrollador del spyware, que anteriormente lo vendía a otros atacantes, hizo público el código fuente. Esto ha ayudado a otros actores a desarrollar y distribuir el software espía, a menudo también dirigido a instituciones bancarias»,* dijo ThreatFabric.

Algunas de las instituciones notables que se hacen pasar por el malware incluyen Deutsche Bank, HSBC UK, Kotak Mahindra Bank y Nubank.

SpyNote (también conocido como SpyMax) es rico en funciones y cuenta con una gran cantidad de capacidades que le permiten instalar arbitrariamente, recopilar mensajes SMS, llamadas, videos y grabaciones de audio, rastrear ubicaciones de GPS, e incluso obstaculizar los esfuerzos para desinstalar la aplicación.

También sigue el modus operandi de otro malware bancario al solicitar permisos a los servicios de accesibilidad para extraer códigos de autenticación de dos factores (2FA) de Google Authenticator y registrar las pulsaciones de teclas para desviar las credenciales bancarias.

Además, SpyNote incluye funcionalidades para saquear las contraseñas de Facebook y Gmail, así como para capturar el contenido de la pantalla aprovechando la API MediaProjection de Android.

La compañía de seguridad holandesa dijo que la iteración más reciente de SpyNote (llamada SpyNote.C) es la primera variante que afecta a las aplicaciones bancarias, así como a otras aplicaciones conocidas como Facebook y WhatsApp.

También se sabe que se hace pasar por el servicio oficial de Google Play Store y otras

aplicaciones genéricas que abarcan fondos de pantalla, productividad y categorías de juegos. Una lista de algunos de los artefactos de SpyNote, que se entregan principalmente por medio de ataques de smishing, es la siguiente:

- Bank of America Confirmation (yps.eton.application)
- Burla Nubank (com.appser.verapp)
- Conversations_(com.appser.verapp)
- Current Activity (com.willme.topactivity)
- HSBC UK Mobile Banking (com.employ.mb)
- Kotak Bank (splash.app.main)
- Virtual SIM Card (cobi0jbpm.apvy8vjjvpser.verapchvvhbjbjq)

Se estima que SpyNote.C fue comprado por 87 clientes distintos entre agosto de 2021 y octubre de 2022 después de que su desarrollador lo anunciara con el nombre de CypherRat a través de un canal de Telegram.

Sin embargo, la disponibilidad de código abierto de CypherRat en octubre de 2022 ha llevado a un aumento dramático en la cantidad de muestras detectadas en la naturaleza, lo que sugiere que varios grupos criminales están cooptando el malware en sus propias campañas.

ThreatFabric dijo además que el autor original comenzó a trabajar en un nuevo proyecto de software espía con nombre en código CraxsRat, que se ofrecerá como una aplicación paga con características similares.

> *«Este desarrollo no es tan común dentro del ecosistema de spyware de Android, pero es extremadamente peligroso y muestra el potencial inicio de una nueva tendencia, que verá una desaparición gradual de la distinción entre spyware y malware bancario, debido al poder que tiene el abuso de servicios de accesibilidad que brinda a los ciberdelincuentes»,* dijo la compañía.

Se recomienda a los usuarios que se abstengan de descargar aplicaciones de fuentes no

confiables, analicen las revisiones antes de instalar cualquier aplicación y otorguen solo aquellos permisos que sean relevantes para el propósito de la aplicación.

> *«Google Play Protect verifica los dispositivos Android con Google Play Services en busca de aplicaciones potencialmente dañinas de otras fuentes. Los usuarios están protegidos por Google Play Protect, que puede advertir a los usuarios o bloquear aplicaciones maliciosas identificadas en dispositivos Android»*, dijo un portavoz de Google.

Los hallazgos se producen cuando un grupo de investigadores demostró un nuevo ataque contra dispositivos Android denominado EarSpy, que brinda acceso a conversaciones de audio, ubicaciones en interiores y entradas de pantalla táctil al aprovechar los sensores de movimiento integrados de los smartphones y el altavoz del oído como un canal lateral.