Un reciente análisis del troyano bancario para Android conocido como Hook ha descubierto que está basado en su predecesor, llamado ERMAC.

*«El código fuente de ERMAC sirvió como punto de partida para Hook», i*nformaron los investigadores de seguridad de NCC Group, Joshua Kamp y Alberto Segura, en un análisis técnico publicado la semana pasada.

> *«Todos los comandos (un total de 30) que el operador de malware puede enviar a un dispositivo infectado con ERMAC, también existen en Hook. La implementación del código para estos comandos es prácticamente idéntica».*

Hook fue documentado por ThreatFabric por primera vez en enero de 2023, describiéndolo como una *«rama de ERMAC»* que se ofrece a la venta por $7,000 al mes. Ambas variantes son obra de un autor de malware conocido como DukeEugene.

Dicho esto, Hook expande las capacidades de ERMAC con más funciones, admitiendo hasta 38 comandos adicionales en comparación con este último.

Las características centrales de ERMAC están diseñadas para enviar mensajes SMS, mostrar una ventana de phishing sobre una aplicación legítima, extraer una lista de aplicaciones instaladas, recopilar mensajes SMS y robar frases de recuperación de múltiples billeteras de criptomonedas.

Por otro lado, Hook va un paso más allá al transmitir la pantalla de la víctima y interactuar con la interfaz de usuario para obtener un control completo sobre el dispositivo infectado. También captura fotos de la víctima usando la cámara frontal, obtiene cookies relacionadas con las sesiones de inicio de sesión de Google y saquea frases de recuperación de más billeteras de criptomonedas.

Además, Hook puede enviar mensajes SMS a varios números de teléfono, propagando eficazmente el malware a otros usuarios.

A pesar de estas diferencias, tanto Hook como ERMAC pueden registrar las pulsaciones de teclas y aprovechar los servicios de accesibilidad de Android para llevar a cabo ataques de superposición con el fin de mostrar contenido encima de otras aplicaciones y robar credenciales de más de 700 aplicaciones. La lista de aplicaciones a atacar se obtiene dinámicamente a través de una solicitud a un servidor remoto.

Ambas familias de malware también están diseñadas para monitorear eventos del portapapeles y reemplazar el contenido con una billetera controlada por el atacante si la víctima copia una dirección de billetera legítima.

La mayoría de los servidores de comando y control (C2) de Hook y ERMAC se encuentran en Rusia, seguidos por los Países Bajos, el Reino Unido, Estados Unidos, Alemania, Francia, Corea y Japón.

Hasta el 19 de abril de 2023, parece que el proyecto Hook ha sido cerrado, según un mensaje compartido por DukeEugene, quien afirmó que se iba a una *«operación militar especial»* y que otro actor llamado RedDragon proporcionaría soporte para el software hasta que expiren las suscripciones de los clientes.

Posteriormente, el 11 de mayo de 2023, se dice que el código fuente de Hook fue vendido por RedDragon por $70,000 en un foro clandestino. A pesar de la corta vida útil de Hook, este desarrollo ha aumentado la posibilidad de que otros actores de amenazas puedan retomar el trabajo y lanzar nuevas variantes en el futuro.

Este hallazgo se produce en un momento en el que se ha vinculado a un actor de amenazas con conexiones en China a una campaña de spyware para Android dirigida a usuarios en Corea del Sur desde principios de julio de 2023.

> *«El malware se distribuye a través de sitios web de phishing engañosos que se hacen pasar por sitios para adultos, pero que en realidad entregan el archivo APK malicioso. Una vez que el malware ha infectado la máquina de la víctima, puede*

> *robar una amplia gama de información sensible, incluyendo contactos, mensajes SMS, registros de llamadas, imágenes, archivos de audio, grabaciones de pantalla y capturas de pantalla»*, afirmó Cyble.

Además, el malware (nombre del paquete APK «com.example.middlerankapp») aprovecha los servicios de accesibilidad para monitorear las aplicaciones utilizadas por las víctimas y evitar la desinstalación. También contiene una función que permite al malware redirigir las llamadas entrantes a un número de teléfono móvil designado por el atacante, interceptar mensajes SMS e incluir una funcionalidad de registro de teclas incompleta, lo que indica que probablemente está en desarrollo activo.

Las conexiones con China se derivan de referencias a Hong Kong en la información de registro WHOIS del servidor C2, así como de la presencia de varias cadenas de texto en chino, incluyendo «□□□□□□□», en el código fuente del malware, que se traduce como *«Larga vida al Partido Comunista de China».*

En un desarrollo relacionado, el periódico israelí Haaretz reveló que una empresa de spyware doméstica llamada Insanet ha desarrollado un producto llamado Sherlock que puede infectar dispositivos a través de anuncios en línea para espiar a objetivos y recopilar datos sensibles de sistemas Android, iOS y Windows.

Se dice que el sistema fue vendido a un país que no es una democracia, y varias empresas de ciberseguridad israelíes han intentado desarrollar tecnología ofensiva que explota anuncios para perfilar víctimas (un término llamado AdInt o inteligencia de anuncios) y distribuir spyware.