Una semana después de que surgiera que el gobierno de Kazakstán utilizó un sofisticado software espía móvil llamado Hermit dentro de sus fronteras, Google dijo que notificó a los usuarios de Android sobre los dispositivos infectados.

Además, se implementaron los cambios necesarios en Google Play Protect, el servicio de defensa de malware integrado de Android, para proteger a todos los usuarios, dijeron Benoit Sevens y Clement Lecigne de Google Threat Analysis Group (TAG).

Hermit, el trabajo de un proveedor italiano llamado RCS Lab, fue documentado por Lookout la semana pasada, destacando su conjunto de funciones modulares y sus capacidades para recopilar información confidencial, como registros de llamadas, contactos, fotos, ubicación precisa y mensajes SMS.

Una vez que la amenaza se insinúa por completo en un dispositivo, también se equipa para grabar audio y realizar y redirigir llamadas telefónicas, además de abusar de sus permisos a los servicios de accesibilidad para controlar las aplicaciones de primer plano utilizadas por las víctimas.

Su modularidad también permite ser totalmente personalizable, equipando la funcionalidad del software espía para que se amplíe o modifique a voluntad. No está claro quiénes fueron los objetivos de la campaña o cuáles de los clientes de RCS Lab estuvieron involucrados.

La compañía con sede en Milán, que opera desde 1993, asegura *«proporcionar a las fuerzas del orden de todo el mundo soluciones tecnológicas de vanguardia y soporte técnico en el campo de la interceptación legal durante más de veinte años».* Al parecer, más de 10,000 objetivos interceptados se manejan diariamente solo en Europa.

> *«Hermit es otro ejemplo más de un arma digital que se utiliza para atacar a civiles y sus dispositivos móviles, y los datos recopilados por las partes maliciosas involucradas seguramente serán invaluables»*, dijo Richard Melick, director de informes de amenazas de Zimperium.

Los objetivos tienen sus teléfonos infectados con la herramienta de espionaje por medio de descargas ocultas como vectores iniciales de infección, lo que a su vez, implica el envío de un enlace único en un mensaje SMS que, al hacer clic, activa la cadena de ataque.

Se cree que los atacantes trabajaron en colaboración con los proveedores de servicios de Internet (ISP) de los objetivos para deshabilitar su conectividad de datos móviles, y después enviaron un SMS que instaba a los destinatarios a instalar una aplicación para restaurar el acceso a datos móviles.

> *«Creemos que esta es la razón por la que la mayoría de las aplicaciones se hicieron pasar por aplicaciones de operadores móviles. Cuando la participación del ISP no es posible, las aplicaciones se disfrazan como aplicaciones de mensajería»,* dijeron los investigadores.

Para comprometer a los usuarios de iOS, se cree que el adversario se basó en perfiles de aprovisionamiento que permiten cargar aplicaciones falsas con la marca del operador en los dispositivos sin necesidad de que estén disponibles en la App Store.

Un análisis de la versión iOS de la aplicación muestra que aprovecha hasta seis vulnerabilidades: CVE-2018-4344, CVE-2019-8605, CVE-2020-3837, CVE-2020-9907, CVE-2021-30883 y CVE-2021-30983, con el fin de extraer archivos de interés, como las bases de datos de WhatsApp.

> *«A medida que la curva cambia lentamente hacia la explotación de la corrupción de la memoria y se vuelve más costosa, es probable que los atacantes también cambien»*, dijo Ian Beer, de Google Project Zero.

En Android, los ataques drive-by requieren que las víctimas habiliten una configuración para instalar aplicaciones de terceros de fuentes desconocidas, lo que hace que la aplicación no

autorizada, que se hace pasar por marcas de teléfonos inteligentes como Samsung, solicite amplios permisos para lograr sus objetivos maliciosos.

La variante de Android, además de intentar rootear el dispositivo para acceso seguro, también está conectada de forma distinta en el sentido de que, en lugar de agrupar exploits en el archivo APK, contiene una funcionalidad que le permite obtener y ejecutar componentes remotos arbitrarios que pueden comunicarse con la aplicación principal.

> *«Esta campaña es un buen recordatorio de que los atacantes no siempre utilizan exploits para obtener los permisos que necesitan. Los vectores de infección básicos y las descargas automáticas aún funcionan y pueden ser muy eficientes con la ayuda de los ISP locales»,* dijeron los investigadores.

Al asegurar que siete de los nueve exploits de día cero que descubrió en 2021 fueron desarrollados por proveedores comerciales y vendidos y utilizados por atacantes respaldados por el gobierno, Google dijo que está rastreando a más de 30 proveedores con diferentes niveles de sofisticación que se sabe que comercian exploits y capacidades de vigilancia.

Además, Google TAG expresó su preocupación de que proveedores como RCS Lab estén *«acumulando vulnerabilidades de día cero en secreto»*, y advirtió que esto presenta riesgos graves considerando que varios proveedores de software espía se han visto comprometidos en los últimos diez años, *«aumentando el espectro de que sus reservas puedan liberarse públicamente sin previo aviso».*

> *«Nuestros hallazgos subrayan hasta qué punto los proveedores de vigilancia comercial han proliferado las capacidades que históricamente solo han sido utilizadas por los gobiernos con la experiencia técnica para desarrollar y poner en funcionamiento las vulnerabilidades»,* dijo TAG.

> *«Si bien el uso de tecnologías de vigilancia puede ser legal según las leyes nacionales o internacionales, por lo general los gobiernos las utilizan con fines contrarios a los valores democráticos: atacar a disidentes, periodistas, trabajadores de derechos humanos y políticos de partidos de la oposición».*