Los investigadores de seguridad cibernética descubrieron una nueva pieza de malware de vigilancia móvil que se cree, fue desarrollada por un contratista de defensa ruso y que ha sido sancionada por interferir en las elecciones presidenciales de 2016 en Estados Unidos.

Apodado Monokle, el troyano móvil de acceso remoto ha estado apuntando activamente a los teléfonos Android desde al menos marzo de 2016, y se está utilizando principalmente en ataques altamente dirigidos contra un número limitado de personas.

Según los investigadores de seguridad de Lookout, Monokle posee una amplia gama de funciones de espionaje y utiliza técnicas avanzadas de exfiltración de datos, incluso sin requerir acceso de raíz a un dispositivo específico.

Particularmente, el malware abusa de los servicios de accesibilidad de Android para filtrar datos de una gran cantidad de aplicaciones populares de terceros, como Google Docs, Facebook Messenger, WhatsApp, WeChat y Snapchat, al leer el texto que se muestra en la pantalla de un dispositivo en cualquier momento.

El malware también extrae diccionarios de texto predictivo definidos por el usuario para *«obtener una idea de los temas de interés para un objetivo»*, y también intenta grabar la pantalla del teléfono durante un evento de desbloqueo de pantalla para comprometer el PIN, el patrón o contraseña del dispositivo.

Además, si el acceso root está disponible, el spyware instala certificados de CA especificados por el atacante en la lista de certificados de confianza en un dispositivo comprometido, lo que potencialmente permite a los atacantes interceptar fácilmente el tráfico de red cifrado protegido por SSL mediante ataques Man in the Middle (MiTM).

Otras funcionalidades de Monokle son:

- Rastrear la ubicación del dispositivo
- Grabar audio y llamadas
- Hacer grabaciones de pantalla

- Keylogger y dispositivo de huellas dactilares
- Recuperar la navegación y las historias de llamadas
- Tomar fotos, videos y capturas de pantalla
- Recuperar correos electrónicos, SMS y mensajes
- Robar contactos e información de calendario
- Hacer llamadas y enviar mensajes de texto en nombre de las víctimas
- Ejecutar comandos de shell arbitrarios, como root, si el acceso root está disponible

En total, Monokle contiene 78 comandos predefinidos diferentes, que los atacantes pueden enviar a través de SMS, llamadas telefónicas, intercambio de mensajes de correo electrónico a través de POP3 y SMTP y conexiones TCP entrantes y salientes, indicando al malware que filtre los datos solicitados y los envíe al comando remoto de los atacantes.

El spyware se disfraza de apps como PornHub y Google Apps para Android

Según los investigadores, los atacantes están distribuyendo Monokle por medio de apps falsas que se asemejan a Evernote, Google Play, PornHub, Signal, UC Browser, Skype y otras apps populares de Android.

La mayoría de estas aplicaciones incluso siguen una funcionalidad legítima, lo que evita que los usuarios específicos sospechen que las apps son maliciosas.

Además, algunas muestras recientes de Monokle incluso vienen con módulos Xposed, que permiten que el malware personalice algunas características del sistema, lo que eventualmente amplía su capacidad para enganchar y ocultar la presencia en la lista de procesos.

El paquete de malware utiliza un archivo DEX en su carpeta de activos que *«incluye todas las funciones criptográficas implementadas en la biblioteca de código abierto spongycastle, varios protocolos de correo electrónico, extracción y exfiltración de los datos, serialización y deserialización de datos mediante el protocolo Thrift y rooting y funcionalidad de enganche,*

entre otros».

El nuevo malware de Android y sus capacidades se parecen al potente malware de vigilancia Pegasus, desarrollado por NSO Group con sede en Israel para dispositivos Apple, iOS y Android.

Sin embargo, a diferencia del spyware ruso Monokle, Pegasus viene con poderosas vulnerabilidades de día cero que instalan el spyware en un dispositivo específico con poca o ninguna interacción del usuario.

Pegasus ha sido utilizado anteriormente para atacar a activistas de derechos humanos y periodistas, especialmente por el gobierno de México, y el año pasado nuevamente, contra un miembro del personal de Amnistía Internacional en Arabia Saudita.

Monokle fue desarrollado por una compañía con sede en Rusia, llamada Special Technology Center Ltd. (STC), un contratista de defensa privado conocido por producir UAV y equipos de radiofrecuencia (RF) para el ejército ruso y otros clientes gubernamentales.

Según los investigadores de Lookout, la suite de seguridad de Android Monokle y STC llamada Defender, está firmada digitalmente con los mismos certificados criptográficos y también comparte la misma infraestructura de control y comando.

> *«La infraestructura de comando y control que se comunica con la aplicación Defender también se comunica con muestras de Monokle. Los certificados de firma utilizados para firmar paquetes de aplicaciones de Android también se superponen entre Defender y Monokle. Investigadores de Lookout observaron una superposición adicional entre Monokle y el software de seguridad defensivo producido por STC en las opciones de desarrollo e implementación de los autores»,* dice el informe.

Monokle para iOS está en desarrollo

Además de Android, los investigadores descubrieron muestras de Monokle, cuyo análisis reveló la existencia de versiones de iOS de Monokle dirigidas a dispositivos Apple, aunque los investigadores no encontraron evidencia de ninguna infección activa de iOS a partir de ahora.

Algunos comandos en las muestras de malware parecen no servir a ningún propósito como parte del cliente de Android y probablemente se agregaron involuntariamente, lo que sugiere que las versiones de iOS de Monokle pueden estar en desarrollo.

Esos comandos incluyen funciones de iOS para las conexiones de iCloud, los datos del acelerómetro iWatch de Apple, los permisos de iOS y otras funciones o servicios de dicho sistema operativo.

Según los investigadores de Lookout, Monokle se utiliza en ataques altamente dirigidos contra un número limitado de personas en las regiones del Cáucaso de Europa del Este, así como en personas interesadas en el Islam y el grupo militante Ahrar al-Sham en Siria, y en individuos en la nación de Asia Central y la ex república soviética de Uzbekistán.

Puedes obtener más información en el informe detallado publicado por Lookout.