Una de las herramientas más poderosas y avanzadas de software espía comercial de nivel gubernamental, apodada como FinSpy, también conocida como FinFisher, ha sido descubierta entre los usuarios en Myanmar.

FinSpy, creado por la compañía alemana Gamma International, es un software de espionaje que puede dirigirse a varias plataformas móviles, como iOS, Android y sistemas operativos de escritorio.

El Grupo Gamma supuestamente vende su controvertida herramienta de espionaje FinSpy exclusivamente a agencias gubernamentales de todo el mundo, pero también ganó notoriedad por atacar a activistas de derechos humanos en muchos países.

El spyware es capaz de robar una gran cantidad de información personal de dispositivos móviles específicos, como mensajes SMS/MMS, grabaciones de llamadas telefónicas, correos electrónicos, contactos, fotos, archivos y datos de ubicación.

Los investigadores de Kaspersky publicaron un informe hoy, en el que revelaron una campaña de ciberespionaje que involucra a los usuarios de Myanmar con las últimas versiones de los implantes de FinSpy para iOS y Android.

Debido a que algunas funcionalidades avanzadas requieren que FinSpy tenga privilegios de root en un dispositivo específico, el implante no funciona correctamente en iOS sin jailbreak, lo que puede lograrse con acceso físico o de forma remota en combinación con algunas vulnerabilidades de día cero.

Sin embargo, en el caso de Android, los investigadores descubrieron que el implante ha estado utilizando el exploit de DirtyCow para obtener automáticamente privilegios de root en un dispositivo Android sin que esté rooteado, lo que permite a los atacantes infectar con éxito un dispositivo de forma remota.

Según los investigadores, las nuevas versiones de FinSpy para ambos sistemas operativos

móviles, también son capaces de grabar llamadas VoIP a través de aplicaciones externas como Skype, WeChat, Viber, LINE y aplicaciones de mensajería seguras como WhatsApp, Threema, Signal y Telegram.

> *«El módulo .chext apunta a las aplicaciones de mensajería y enlaza sus funciones para filtrar casi todos los datos accesibles: contenido de mensajes, fotos, geolocalización, contactos, nombres de grupos, etc. Los datos recopilados se envían al servidor local implementado por el módulo principal»*, dijeron los investigadores.

FinSpy también incluye la funcionalidad de registro de teclear y se ha diseñado para cubrir las pistas de sus actividades en dispositivos.

> *«Desde la filtración en 2014, Gamma Group ha recreado partes significativas de sus implantes, extendió la funcionalidad compatible, como la lista de mensajeros instantáneos, y al mismo tiempo ha mejorado el cifrado y ofuscación, que permitieron mantener su posición en el mercado»*, agregaron los investigadores.

Al realizar su investigación, los investigadores de Kaspersky detectaron las versiones actualizadas de los implantes FinSpy utilizados en la naturaleza en casi 20 países, pero *«asumiendo el tamaño de la base de clientes de Gamma, es probable que el número real de víctimas sea mucho mayor».*

Gamma está trabajando continuamente en las actualizaciones para el malware FinSpy, ya que los investigadores han encontrado otra versión de la amenaza en el momento de publicar su informe y actualmente están investigando la muestra.