Investigadores en seguridad cibernética descubrieron una versión para iOS de la potente aplicación de vigilancia de teléfonos inteligentes Exodus, que inicialmente estaba dirigida a dispositivos con Android, por medio de apps en la tienda oficial de Google Play Store.

El malware fue nombrado como Exodus, los investigadores de seguridad de LookOut descubrieron la versión iOS del spyware durante el análisis de las muestras de Android que encontraron el año pasado.

A diferencia de su variante para Android, la versión para iOS de Exodus se ha distribuido fuera de la App Store oficial, principalmente por medio de sitios web de phishing que imitan a los operadores móviles italianos y turcomanos.

Debido a que Apple restringe la instalación directa de aplicación fuera de su tienda oficial, la versión para iOS de Exodus está abusando del programa Apple Developer Enterprise, que permite a las compañías distribuir sus propias aplicaciones internas directamente a sus empleados sin la necesidad de utilizar App Store de iOS.

> *«Cada uno de los sitios de phishing contenía enlaces a un manifiesto de distribución, que contenía metadatos como el nombre de la aplicación, la versión, el icono y una URL para el archivo IPA. Todos estos paquetes utilizaron perfiles de aprovisionamiento con certificados de distribución asociados con la empresa Connexxa S.R.L.»*, dicen los investigadores en una publicación.

Aunque la variante de iOS es menos sofisticada que su contraparte de Android, el spyware aún puede ser capaz de filtrar información de dispositivos iPhone específicos, como contactos, grabaciones de audio, fotos, videos, ubicación GPS e información del dispositivo.

Los datos robados se transmiten luego por medio de solicitudes HTTP PUT a un punto final en el servidor de comando y control controlado por los atacantes, que es la misma infraestructura CnC que la versión de Android y utiliza protocolos de comunicación similares.

Algunos detalles técnicos indicaron que Exodus era *«probablemente el producto de un esfuerzo de desarrollo bien financiado»* y apuntaba a los sectores gubernamentales o de aplicación de la ley.

> *«Estos incluyen el uso de la fijación de certificados y el cifrado de clave pública para las comunicaciones C2, las restricciones geográficas impuestas por el C2 al entregar la segunda etapa y el conjunto completo y bien implementado de funciones de vigilancia»,* dicen los investigadores.

Exodus, desarrollado por la compañía con sede en Italia llamada Connexxa S.R.L., salió a la luz el mes pasado cuando hackers de sombrero blanco de Security Without Borders descubrieron casi 25 aplicaciones diferentes disfrazadas de aplicaciones de servicio en Google Play Store, que el gigante tecnológico eliminó luego de ser notificado.

En su desarrollo por al menos cinco años, Exodus para Android generalmente consta de tres etapas distintas. Primero, existe un pequeño cuentagotas que recopila información de identificación básica, como el IMEI y el número de teléfono, sobre el dispositivo seleccionado.

La segunda etapa consiste en varios paquetes binarios que implementan un conjunto bien implementado de funcionalidades de vigilancia.

Finalmente, la tercera etapa utiliza el exploit de DirtyCOW (CVE-2016-5195) para obtener el control de la raíz de los teléfonos infectados. Una vez instalado con éxito, Exodus puede llevar a cabo una gran cantidad de vigilancia.

La variante para Android también está diseñada para seguir ejecutándose en el dispositivo infectado aún cuando la pantalla está apagada.

Si bien la versión para Android de Exodus potencialmente infectó *«varios cientos, si no mil o más»* dispositivos, no está claro cuántos iPhones fueron infectados por la variantes de Exodus para iOS.

Después de que los investigadores de Lookout notificaron el spyware, Apple revocó el certificado de la empresa, evitando que las aplicaciones maliciosas se instalen en nuevos iPhones y se ejecuten en dispositivos infectados.

Esta es la segunda instancia del año pasado cuando una compañía de software italiana ha sido sorprendida distribuyendo software espía. A principios del año pasado, otra compañía italiana no revelada fue encontrada distribuyendo *«Skygofree»,* una peligrosa herramienta de espionaje de Android que les da a los piratas informáticos el control total de los dispositivos infectados de forma remota.