Investigadores de seguridad cibernética expusieron las operaciones de un proveedor de malware de Android que se asoció con un segundo actor de amenazas para comercializar y vender un troyano de acceso remoto (RAT), capaz de tomar el control de dispositivos y exfiltrar fotos, ubicaciones, contactos y mensajes de aplicaciones populares como Messenger de Facebook, Instagram, WhatsApp, Skype, Telegram, Kik, Line y Google.

El proveedor, conocido como Triangulum en distintos foros de la darknet, supuestamente es un sujeto de 25 años de edad de origen indio, y abrió una tienda para vender el malware hace tres años, el 10 de junio de 2017, según un análisis publicado hoy por Check Point Research.

> *«El producto era un RAT móvil, dirigido a dispositivos Android y capaz de exfiltrar datos confidenciales de un servidor C&C, destruyendo datos locales e incluso borrando todo el sistema operativo, en ocasiones»,* dijeron los investigadores.

Al reconstruir el rastro de actividades de Triangulum, la compañía de seguridad dijo que el desarrollador de malware, además de generar publicidad para la RAT, también buscó inversores y socios potenciales en septiembre de 2017 para mostrar las características de la herramienta antes de ofrecerla a la venta.

Posteriormente, se cree que Triangulum se salió de la red durante aproximadamente año y medio, sin signos de actividad en la darknet, solo para resurgir el 6 de abril de 2019, con otro producto llamado Rogue, en ese tiempo en colaboración con otro adversario denominado HeXaGon Dev, que se especializó en el desarrollo de RAT basadas en Android.

Al señalar que Triangulum había comprado anteriormente varios productos de malware ofrecidos por HeXaGon Dev, Check Point dijo que Triangulum anunciaba sus productos en distintos foros de la red oscura, con infografías bien diseñadas que enumeraban las características completas de la RAT. Además, HeXaGon Dev se hizo pasar por un comprador potencial en un intento por atraer más clientes.

Aunque el producto de 2017 se vendió por una tarifa de 60 dólares como suscripción de por vida, los proveedores pasaron a un modelo más fiable financieramente en 2020, al cobrar a los clientes entre 30 dólares al mes y 190 dólares por acceso permanente al malware Rogue.

Los intentos de Triangulum de expandirse al mercado de la red oscura rusa fracasaron tras la negativa del pirata informático a compartir videos de demostración en la publicación del foro que anunciaba el producto.

Rogue v6.2, que parece ser la última versión de un malware llamado Dark Shades v6.0 que inicialmente vendió HeXaGon Dev antes de ser comprado por Triangulum en agosto de 2019, también cuenta con características tomadas de una segunda familia de malware, llamada Hawkshaw, cuyo código fuente se hizo público en 2017.

> *«Triangulum no desarrolló esta creación desde cero, tomó lo que estaba disponible en ambos mundos, el código abierto y la red oscura, y unió estos componentes»*, dijeron los investigadores.

Dark Shades es un *«sucesor superior»* de Cosmos, una RAT separada vendida por el actor de HeXaGon Dev, lo que hace que la venta de Cosmos sea redundante.

Rogue se comercializa como un RAT *«hecho par ejecutar comandos con funciones increíbles sin necesidad de una computadora»*, con capacidades adicionales para controlar a los clientes infectados de forma remota mediante un panel de control o un teléfono inteligente.

La RAT cuenta con una amplia gama de funciones para obtener el control sobre el dispositivo host y exfiltrar cualquier tipo de datos (como fotos, ubicación, contactos y mensajes), modificar los archivos en el dispositivo e incluso descargar cargas útiles maliciosas adicionales, asegurando al mismo tiempo que el usuario concede permisos intrusivos para llevar a cabo sus actividades maliciosas.

Además, está diseñado para frustrar la detección al ocultar el icono del dispositivo del

usuario, eludir las restricciones de seguridad de Android al explotar las funciones de accesibilidad para registrar las acciones del usuario y registra su propio servicio de notificación para espiar cada notificación que aparece en el teléfono infectado.

Rogue utiliza la infraestructura Firebase de Google como un servidor de comando y control (C2) para disfrazar sus intenciones maliciosas, abusando de la función de mensajería en la nube de la plataforma para recibir comandos del servidor, y Realtime Database y Cloud Firestore para cargar datos y documentos acumulados del dispositivo víctima.

Triangulum puede estar activo y expandiendo su clientela en la actualidad, pero en abril de 2020, el malware se filtró.

El investigador de ESET, Lukas Stefanko, dijo en Twitter el 20 de abril de 2020, que el código fuente del backend de la botnet de Android, Rogue, se publicó en un foro clandestino, y dijo que *«tiene muchos problemas de seguridad y es un nuevo nombre para Dark Shades v6.0″.*

Pero a pesar de esa filtración, los investigadores de Check Point afirman que el equipo de Triangulum todavía recibe mensajes de clientes interesados en el foro de la Darknet del actor.

> *«Los proveedores de malware para dispositivos móviles se están volviendo mucho más ingeniosos en la red oscura. Nuestra investigación nos permite vislumbrar la locura de la red oscura: cómo evoluciona el malware y lo difícil que es rastrearlo, clasificarlo y protegerse contra él de una forma eficaz»*, dijo el jefe de investigación cibernética de Check Point, Yaniv Balmas.
>
> *«El mercado clandestino sigue siendo como el salvaje oeste en cierto sentido, lo que hace que sea muy difícil entender qué es una amenaza real y qué no».*