Un equipo de investigadores reveló las capacidades de un implante de software espía para Android, desarrollado por un actor de amenazas iraní sancionado, que podría permitir a los atacantes espiar chats privados de aplicaciones populares de mensajería instantánea, forzar conexiones WiFi y responder automáticamente llamadas de números con el propósito de espiar conversaciones.

En septiembre, el Departamento del Tesoro de Estados Unidos impuso sanciones a APT39 (conocido también como Chafer, ITG07 o Remix Kitten), un actor de amenazas iraní respaldado por el Mininsterio de Inteligencia y Seguridad (MOIS) del país, por llevar a cabo campañas de malware contra disidentes iraníes, periodistas y empresas internacionales de los sectores de las telecomunicaciones y los viajes.

Coincidiendo con las sanciones, la Oficina Federal de Investigaciones (FBI), publicó un informe de análisis de amenazas públicas que describe varias herramientas utilizadas por Rana Intelligence Computing Company, que operaba como fachada para las actividades cibernéticas maliciosas llevadas a cabo por el grupo APT39.

Al vincular formalmente las operaciones de APT39 con Rana, el FBI detalló ocho conjuntos separados y distintos de malware previamente no revelado, que utilizó el grupo para realizar sus actividades de intrusión y reconocimiento informático, incluida una aplicación de software espía para Android llamada *«optimizer.apk»* que roba información y tiene capacidades de acceso remoto.

> *«El implante de APK tenía una funcionalidad de acceso remoto y robo de información que obtenía acceso de root en un dispositivo Android sin el conocimiento del usuario»,* dijo la agencia.
>
> *«Las capacidades principales incluyen recuperar solicitudes HTTP GET del servidor C2, obtener datos del dispositivo, comprimir y cifrar con AES los datos recopilados y enviarlos a través de solicitudes HTTP POST al servidor C2 malicioso»,* agregó.

ReversingLabs, en un informe publicado recientemente, profundizó el implante («com.android.providers.optimizer») utilizando una versión anterior no confusa del malware descrito en el informe Flash del FBI.

Según el investigador Karlo Zanki, el implante no solo tenía permisos para grabar audio y tomar fotos con fines de vigilancia del gobierno, sino que también contaba con la función para agregar un punto de acceso WiFi personalizado y obligar a un dispositivo comprometido a conectarse a él.

> *«Esta función probablemente se introdujo para evitar una posible detección debido al uso inusual del tráfico de datos en la cuenta móvil del objetivo»*, dijo Zanki en un análisis.

También se debe destacar la capacidad de responder de forma automática las llamadas de números de teléfono específicos, lo que permite al actor de amenazas acceder a las conversaciones a pedido.

Además de ofrecer soporte para recibir comandos enviados a través de mensajes SMS, la última variante del malware «optimizador» al que hace referencia el FBI, abusó de los servicios de accesibilidad para acceder al contenido de aplicaciones de mensajería instantánea como WhatsApp, Instagram, Telegram, Viber, Skype y un cliente iraní no oficial basado en Telegram llamado Talaeii.

Cabe señalar que Telegram había emitido advertencias «inseguras» a los usuarios de Talaeii y Hotgram en diciembre de 2018, después de la divulgación del Centro de Derechos Humanos en Irán citando preocupaciones de seguridad.

> *«Cuando se dirigien a individuos, los actores de amenazas por lo general quieren monitorear su comunicación y movimiento. Los teléfonos móviles son más adecuados para estos objetivos debido a la potencia informática que tiene en el*

> *bolsillo y al hecho de que la mayoría de la gente los lleva todo el tiempo»*, concluyó Zanki.
>
> *«Debido a que la plataforma Android mantiene la mayor parte de la cuota de mercado mundial de teléfonos inteligentes, se deduce que también es el objetivo principal del malware móvil».*