Actores de amenaza vinculados a los servicios de inteligencia de Rusia están llevando a cabo campañas de *phishing* con el objetivo de comprometer aplicaciones comerciales de mensajería (CMA) como WhatsApp y Signal, buscando tomar el control de cuentas pertenecientes a personas con alto valor en materia de inteligencia, informaron el viernes la Agencia de Seguridad de Infraestructura y Ciberseguridad de Estados Unidos (CISA) y el Buró Federal de Investigaciones (FBI).

«La campaña se dirige a individuos de alto valor estratégico, incluidos funcionarios actuales y anteriores del gobierno de EE. UU., personal militar, figuras políticas y periodistas,» señaló el director del FBI, Kash Patel, en una publicación en X. *«A nivel global, esta operación ha derivado en accesos no autorizados a miles de cuentas personales. Una vez dentro, los atacantes pueden leer mensajes y listas de contactos, enviar mensajes haciéndose pasar por la víctima y lanzar nuevas campañas de phishing aprovechando una identidad confiable.»*

CISA y el FBI indicaron que esta actividad ha provocado la vulneración de miles de cuentas individuales en aplicaciones de mensajería. Cabe destacar que estos ataques están diseñados para infiltrarse directamente en las cuentas objetivo, sin explotar fallos de seguridad ni debilidades en los mecanismos de cifrado de las plataformas.

Aunque las agencias no atribuyeron la actividad a un actor específico, informes previos de Microsoft y el Google Threat Intelligence Group han relacionado este tipo de campañas con varios grupos alineados con Rusia, identificados como Star Blizzard, UNC5792 (también conocido como UAC-0195) y UNC4221 (también llamado UAC-0185).

En una alerta similar, el Centro de Coordinación de Crisis Cibernéticas (C4), que forma parte de la Agencia Nacional de Ciberseguridad de Francia (ANSSI), advirtió sobre un aumento en campañas de ataque dirigidas a cuentas de mensajería instantánea asociadas con funcionarios gubernamentales, periodistas y líderes empresariales.

«Estos ataques, cuando tienen éxito, permiten a los actores maliciosos acceder a historiales de conversaciones o incluso tomar el control de las cuentas de mensajería de las víctimas y enviar mensajes suplantando su identidad,» indicó el C4.

El objetivo final de estas campañas es obtener acceso no autorizado a las cuentas de las víctimas, lo que permite a los atacantes consultar mensajes y contactos, enviar mensajes en su nombre e incluso realizar ataques de phishing secundarios aprovechando relaciones de confianza.

Según alertas recientes de agencias de ciberseguridad de Alemania y los Países Bajos, el ataque consiste en que el adversario se hace pasar por «Signal Support» para contactar a las víctimas y persuadirlas de hacer clic en un enlace (o alternativamente escanear un código QR) o proporcionar su PIN o código de verificación. En ambos casos, la técnica de ingeniería social facilita el acceso de los atacantes a la cuenta de mensajería.

No obstante, la campaña puede tener dos resultados distintos para la víctima dependiendo del método utilizado:

- Si la víctima decide proporcionar el PIN o el código de verificación al atacante, pierde el acceso a su cuenta, ya que este lo utiliza para recuperarla desde su propio dispositivo. Aunque no podrá ver mensajes anteriores, el atacante podrá monitorear nuevos mensajes y enviar comunicaciones haciéndose pasar por la víctima.
- Si la víctima hace clic en el enlace o escanea el código QR, un dispositivo controlado por el atacante se vincula a la cuenta, permitiéndole acceder a todos los mensajes, incluidos los antiguos. En este caso, la víctima mantiene el acceso a la cuenta, a menos que sea eliminada manualmente desde la configuración de la aplicación.

Para reducir el riesgo, se recomienda no compartir nunca códigos SMS ni PIN de verificación, ser cauteloso ante mensajes inesperados de contactos desconocidos, verificar los enlaces antes de abrirlos y revisar periódicamente los dispositivos vinculados, eliminando aquellos que resulten sospechosos.

«Estos ataques, como cualquier campaña de phishing, se basan en la ingeniería social. Los atacantes se hacen pasar por contactos o servicios de confianza (como el inexistente 'Signal Support Bot') para engañar a las víctimas y hacer que revelen sus credenciales u otra información sensible,» señaló Signal en una publicación en X a inicios de este mes.

«Para evitar este tipo de incidentes, recuerda que el código SMS de verificación de Signal solo es necesario al registrarte por primera vez en la aplicación. Además, queremos enfatizar que el soporte de Signal nunca iniciará contacto mediante mensajes dentro de la app, SMS o redes sociales para solicitar tu código de verificación o PIN. Si alguien te pide un código relacionado con Signal, se trata de una estafa.»