Varios grupos de amenazas vinculados a Rusia han sido detectados atacando a personas de interés mediante la aplicación de mensajería Signal, conocida por su enfoque en la privacidad, con el fin de obtener acceso no autorizado a sus cuentas.

> *«La táctica más innovadora y utilizada por estos actores para comprometer cuentas de Signal es el uso indebido de la función legítima de 'dispositivos vinculados', que permite emplear Signal en múltiples dispositivos al mismo tiempo»,* explicó el Grupo de Inteligencia de Amenazas de Google (GTIG) en un informe.

Según las investigaciones de los equipos de ciberseguridad de Google, los atacantes, entre ellos un grupo identificado como UNC5792, han utilizado códigos QR maliciosos que, al ser escaneados, conectan la cuenta de la víctima con una instancia de Signal bajo el control de los atacantes.

Como consecuencia, los mensajes futuros se envían de manera simultánea tanto a la víctima como a los ciberdelincuentes, permitiéndoles escuchar en tiempo real las conversaciones del usuario comprometido. Google también señaló que UAC-0195 guarda ciertas similitudes con un colectivo de hackers previamente identificado con el mismo código.

Estos códigos QR fraudulentos han sido disfrazados como invitaciones a grupos, notificaciones de seguridad o instrucciones falsas de emparejamiento de dispositivos supuestamente provenientes del sitio oficial de Signal. Además, se han encontrado estos códigos en sitios web de phishing que pretenden ser aplicaciones utilizadas por el ejército ucraniano.

> *«UNC5792 ha alojado versiones manipuladas de invitaciones a grupos de Signal en servidores bajo su control, diseñadas para parecerse exactamente a las invitaciones legítimas de la plataforma»,* detalló Google.

Otro grupo de ciberdelincuentes asociado con ataques a cuentas de Signal es UNC4221 (también denominado UAC-0185), que ha dirigido sus esfuerzos contra cuentas pertenecientes a miembros del ejército de Ucrania mediante un kit de phishing personalizado, el cual imita características de la aplicación Kropyva, utilizada por las Fuerzas Armadas de Ucrania para la guía de artillería.

Además, se ha empleado una herramienta basada en JavaScript denominada PINPOINT, cuya función es recopilar datos básicos del usuario y su ubicación mediante páginas de phishing.

Junto con UNC5792 y UNC4221, otros grupos de amenazas que han enfocado sus ataques en Signal incluyen a Sandworm (conocido también como APT44), que ha empleado un script por lotes de Windows llamado WAVESIGN; Turla, que ha desarrollado un script ligero en PowerShell; y UNC1151, que ha utilizado la herramienta Robocopy para extraer mensajes de Signal desde computadoras infectadas.

Google reveló esta información poco después de que el equipo de inteligencia de amenazas de Microsoft atribuyera al grupo Star Blizzard una campaña de phishing dirigida a secuestrar cuentas de WhatsApp mediante una técnica similar de vinculación de dispositivos.

La semana pasada, Microsoft y Volexity también informaron que diversos actores de amenazas rusos han empleado un método denominado *«phishing de código de dispositivo»* para acceder a las cuentas de sus víctimas a través de aplicaciones de mensajería como WhatsApp, Signal y Microsoft Teams.

> *«La reciente actividad de múltiples grupos de amenazas en Signal es una señal de alerta sobre el incremento de los ataques contra plataformas de mensajería segura, una tendencia que probablemente se intensificará en el futuro cercano»,* advirtió Google.
>
> *«Los intentos de comprometer cuentas de Signal no se limitan únicamente a ataques remotos como el phishing o la distribución de malware, sino que también*

> *incluyen tácticas en las que los atacantes logran acceso directo y temporal a dispositivos desbloqueados de sus objetivos».*

Este informe también coincide con el hallazgo de una nueva campaña de manipulación de motores de búsqueda (SEO) que utiliza páginas de descarga falsas para distribuir programas maliciosos disfrazados de aplicaciones populares como Signal, LINE, Gmail y Google Translate, con el objetivo de infectar dispositivos de usuarios que hablan chino.

> *«Los archivos ejecutables obtenidos a través de estas páginas falsas siguen un proceso estándar de ejecución que involucra la extracción de archivos temporales, inyección de procesos, alteración de configuraciones de seguridad y establecimiento de comunicación con servidores maliciosos»*, informó Hunt.io, agregando que el malware detectado, identificado como MicroClip, presenta características propias de un ladrón de información.