Se encontró una versión actualizada de un troyano de acceso remoto de Android denominado GravityRAT disfrazado de aplicaciones de mensajería BeingChat y Chatico, como parte de una campaña específica desde junio de 2022.

> *«Notable en la campaña recién descubierta, GravityRAT puede filtrar las copias de seguridad de WhatsApp y recibir comandos para eliminar archivos»,* dijo el investigador de ESET, Lukas Stefanko.

> *«Las aplicaciones maliciosas también brindan una funcionalidad de chat legítima basada en la aplicación OMEMO Instant Messenger de código abierto».*

GravityRAT es el nombre que se le da a un malware multiplataforma que es capaz de atacar dispositivos Windows, Android y macOS. La compañía de seguridad cibernética eslovaca está rastreando la actividad bajo el nombre de SpaceCobra.

Se cree que el atacante tiene su base en Pakistán, con ataques recientes que involucran a GravityRAT contra personal militar en India y entre la Fuerza Aérea de Pakistán al camuflarlo como aplicaciones de entretenimiento y almacenamiento en la nube, como lo reveló Meta el mes pasado.

El uso de aplicaciones de chat como señuelo para distribuir el malware fue destacado previamente en noviembre de 2021 por Cyble, que analizó una muestra llamada *«SoSafe Chat»*, que se cargó en la base de datos VirusTotal desde India.

Las aplicaciones de chat, aunque no están disponibles en Google Play, se distribuyen por medio de sitios web falsos que promocionan servicios de mensajería gratuitos.

> *«Este grupo usó personajes ficticios, haciéndose pasar por reclutadores para*

> *empresas de defensa legítimas y falsas y gobiernos, personal militar, periodistas y mujeres que buscaban establecer una conexión romántica, en un intento de generar confianza con las personas a las que apuntaban»,* dijo Meta en su informe trimestral de amenazas adversarias.

El modus operandi sugiere que se contacta a los objetivos potenciales en Facebook e Instagram con el objetivo de engañarlos para que hagan clic en los enlaces y descarguen las aplicaciones maliciosas.

GravityRAT, como la mayoría de las backdoors de Android, solicita permisos intrusivos bajo la apariencia de una aplicación aparentemente legítima para recolectar información confidencial como contactos, SMS, registros de llamadas, archivos, datos de ubicación y grabaciones de audio sin el conocimiento de la víctima.

Los datos capturados finalmente se filtrar a un servidor remoto bajo el control del actor de amenazas. Cabe mencionar que el uso de la aplicación está condicionado a tener una cuenta.

Lo que destaca a la nueva versión de GravityRAT es su capacidad para robar archivos de respaldo de WhatsApp y recibir instrucciones del servidor de comando y control (C2) para eliminar registros de llamadas, listas de contactos y archivos con extensiones particulares.

> *«Estos son comandos muy específicos que normalmente no se ven en el malware de Android»,* dijo Stefanko.

El desarrollo se produce cuando los usuarios de Android en Vietnam han sido víctimas de una nueva variedad de malware bancario con un ladrón conocido como HelloTeacher, que usa aplicaciones de mensajería legítimas como Viber o Kik como tapadera para desviar datos confidenciales y realizar transferencias de fondos no autorizados abusando de los servicios de accesibilidad API.

Cyble también descubrió una estafa de minería en la nube que *«incita a los usuarios a descargar una aplicación maliciosa para comenzar a minar»,* solo para aprovechar sus permisos a los servicios de accesibilidad para recopilar información confidencial de las billeteras de criptomonedas y las aplicaciones bancarias.

El troyano financiero, cuyo nombre en código es Roamer, ejemplifica la tendencia de usar sitios web de phishing y canales de Telegram como vectores de distribución, lo que amplía efectivamente el grupo de víctimas potenciales.

> *«Los usuarios deben tener cuidado y abstenerse de seguir canales de minería de criptomonedas sospechosos en plataformas como Telegram, ya que estos canales pueden generar pérdidas financieras sustanciales y comprometer datos personales confidenciales»,* dijo Cyble.