Un troyano de acceso remoto basado en Windows, que posiblemente fue diseñado por hackers paquistaníes para infiltrarse en computadoras y robar datos de los usuarios, ha resurgido luego de un período de dos años, con nuevas capacidades para atacar dispositivos Android y macOS.

Según la compañía de seguridad cibernética Kaspersky, el troyano denominado GravityRAT, ahora se hace pasar por aplicaciones legítimas de Android y MacOS para capturar datos del dispositivo, listas de contactos, direcciones de correo electrónico y registros de llamadas y mensajes de texto, para transmitirlos a un servidor controlado por el atacante.

Documentado por primera vez por el Equipo de Respuesta a Emergencias Informáticas de la India (CERT-In) en agosto de 2017, y posteriormente por Cisco Talos en abril de 2018, se sabe que GravityRAT apunta a entidades y organizaciones indias a través de documentos de Microsoft Office Word con malware, al menos desde 2015.

Cisco asegura que los piratas informáticos desarrollaron al menos cuatro versiones distintas de la herramienta de espionaje, y agregó que *«el desarrollador fue lo suficientemente inteligente para mantener segura la infraestructura y no tenerla en la lista negra de un proveedor de seguridad».*

El año pasado también se supo que los espías paquistaníes utilizaron cuentas falsas de Facebook para comunicarse con más de 98 funcionarios de distintas fuerzas y organizaciones de defensa, como el Ejército, la Fuerza Aérea y la Armada de la India, y engañarlos para que instalen en malware disfrazado de aplicación de mensajería segura llamada Whisper.

La forma de operar del malware, a pesar de contar con nuevas capacidades, sigue siendo el mismo: enviar enlaces de objetivos a Android con una trampa, por ejemplo, mediante la aplicación Travel Mate Pro, y aplicaciones para macOS como Enigma o Titanium.

Kaspersky asegura que encontró más de diez versiones de GravityRAT que se estaban distribuyendo bajo la apariencia de aplicaciones legítimas mediante referencias cruzadas de las direcciones de comando y control (C2) utilizadas por el troyano.

Las aplicaciones troyanizadas abarcaron categorías de viajes, intercambio de archivos, reproductores multimedia y cómics para adultos, dirigidas a usuarios de Android, macOS y Windows, lo que permitió a los atacantes obtener información del sistema, documentos con extensiones específicas y una lista de procesamiento de pulsaciones de teclas y toma de capturas de pantalla, e incluso ejecuta comandos Shell arbitrarios.

> *«Nuestra investigación indica que el actor detrás de GravityRAT sigue invirtiendo en sus capacidades de espionaje. Un disfraz astuto y una cartera de sistemas operativos ampliada no solo nos permiten decir que podemos esperar más incidentes con este malware en la región APAC, sino que también respalda la tendencia más amplia de que los usuarios malintencionados no están necesariamente enfocados en desarrollar nuevo malware, sino en un intento de tener el mayor éxito posible»,* dijo Tatyana Shishkova, de Kaspersky.