Se ha detectado un nuevo troyano bancario para Android llamado MMRat que hasta ahora no había sido documentado previamente. Este malware está dirigido a usuarios de dispositivos móviles en el sudeste asiático desde finales de junio de 2023 con el objetivo de llevar a cabo fraudes financieros mediante el control remoto de los dispositivos.

> *«El troyano, que recibe su nombre del paquete com.mm.user, es capaz de capturar la entrada del usuario y el contenido de la pantalla, además de controlar remotamente los dispositivos víctima utilizando diversas técnicas, lo que permite a los operadores llevar a cabo fraudes bancarios en el dispositivo de la víctima»,* según ha informado Trend Micro.

Lo que distingue a MMRat de otros troyanos similares es su protocolo personalizado de comando y control (C2) basado en protocol buffers (también conocido como protobuf). Este protocolo permite transferir grandes volúmenes de datos desde los teléfonos comprometidos de manera eficiente, lo cual demuestra la creciente sofisticación del malware para Android.

Los posibles objetivos del malware, según el lenguaje utilizado en las páginas de phishing, incluyen Indonesia, Vietnam, Singapur y Filipinas.

El punto de entrada de los ataques se encuentra en una red de sitios de phishing que imitan tiendas de aplicaciones oficiales, aunque no se sabe cómo se dirige a las víctimas hacia estos enlaces. MMRat suele hacerse pasar por una aplicación gubernamental legítima o una aplicación de citas.

Una vez instalado, el malware utiliza intensivamente el servicio de accesibilidad de Android y la API de MediaProjection, que también son aprovechados por otro troyano financiero para Android llamado SpyNote, para llevar a cabo sus actividades. Además, el malware puede abusar de sus permisos de accesibilidad para otorgarse otros permisos y modificar configuraciones.

Además, establece la persistencia para sobrevivir entre reinicios e inicia comunicaciones con

un servidor remoto para esperar instrucciones y enviar los resultados de la ejecución de esos comandos. El troyano utiliza diferentes combinaciones de puertos y protocolos para funciones como la exfiltración de datos, transmisión de video y control C2.

MMRat tiene la capacidad de recopilar una amplia gama de datos del dispositivo e información personal, como la intensidad de la señal, el estado de la pantalla, estadísticas de batería, aplicaciones instaladas y listas de contactos. Se sospecha que el actor malicioso utiliza esta información para llevar a cabo algún tipo de perfilado de las víctimas antes de pasar a la siguiente etapa.

Entre otras características, MMRat puede grabar contenido en tiempo real de la pantalla y capturar el patrón de bloqueo para permitir al actor malicioso acceder remotamente al dispositivo víctima cuando está bloqueado y no se está utilizando activamente.

Según Trend Micro, el malware MMRat utiliza el servicio de Accesibilidad para controlar el dispositivo de la víctima de forma remota, realizando diversas acciones como gestos, desbloquear pantallas e ingresar texto.

Los ciberdelincuentes pueden utilizar esta técnica junto con credenciales robadas para cometer fraudes bancarios.

El ataque termina cuando MMRat se elimina a sí mismo al recibir la orden C2 UNINSTALL_APP, que normalmente ocurre después de realizar una transacción fraudulenta con éxito, eliminando cualquier rastro de infección en el dispositivo.

Para reducir las amenazas causadas por este malware tan potente, se aconseja que los usuarios solo descarguen aplicaciones desde fuentes oficiales, revisen las reseñas de las apps y comprueben los permisos que solicita una aplicación antes de usarla.