La campaña de amenazas móviles rastreada como Roaming Mantis se ha relacionado con una nueva ola de compromisos dirigidos contra los usuarios de teléfonos móviles franceses, meses después de que amplió su objetivo para incluir países europeos.

Se cree que no menos de 70 mil dispositivos Android fueron infectados como parte de la operación activa de malware, dijo Sekoia en un informe.

Se sabe que las cadenas de ataque que involucran a Roaming Mantis, un atacante chino motivado financieramente, implementan un troyano bancario llamado MoqHao (también conocido como XLoader) o redirigen a los usuarios de iPhone a páginas de inicio de recolección de credenciales que imitan la página de inicio de sesión de iCloud.

> *«MoqHao (también conocido como Wroba, XLoader para Android) es un troyano de acceso remoto (RAT) de Android con capacidades de puerta trasera y robo de información que probablemente se propaga por medio de SMS»*, dijeron los investigadores de Sekoia.

Todo comienza con un SMS de phishing, una técnica conocida como smishing, que atrae a los usuarios con mensajes temáticos de entrega de paquetes que contienen enlaces falsos, que al hacer clic, proceden a descargar el archivo APK malicioso, pero solo después de determinar si la ubicación de la víctima está fronteras francesas.

Si un destinatario se encuentra fuera de Francia y el sistema operativo del dispositivo no es Android ni iOS (un factor que se determina comprobando la dirección IP y la cadena User-Agent), el servidor está diseñado para responder con un código de estado *«404 no encontrado».*

> *«Por lo tanto, la campaña de smishing está geovallada y tiene como objetivo instalar malware de Android o recopilar credenciales de Apple iCloud»,* dijeron los investigadores.

MoqHao generalmente usa dominios generados por medio del servicio de DNS dinámico Duck DNS para su infraestructura de entrega de primera etapa. Además, la aplicación maliciosa se hace pasar por la aplicación del navegador web Chrome para engañar a los usuarios para que le concedan permisos invasivos.

El troyano spyware, utilizando estos permisos, proporciona una vía para la interacción remota con los dispositivos infectados, lo que permite al adversario recopilar de forma sigilosa datos confidenciales como datos de iCloud, listas de contactos, historial de llamadas, mensajes SMS, entre otros.

Sekoia también evaluó que los datos acumulados podrían usarse para facilitar esquemas de extorsión o incluso venderse a otros atacantes con fines de lucro *«más de 90,000 direcciones IP únicas que solicitaron el servidor C2 que distribuye MoqHao»,* dijeron los investigadores.