INFORME FORENSE – HALLAZGOS CLAVE

iPhone 15 Pro Max – Espionaje Digital Avanzado

1. ¿Qué software infectó el teléfono?

Pegasus, software espía de alta sofisticación atribuido a NSO Group Technologies.

- Hallazgo positivo
- 4 indicadores de compromiso (IOC) coincidentes con infraestructura NSO
- Nivel de certeza: ALTO

2. ¿Desde qué fecha se evidencia la infección?

Desde el 1 de agosto de 2025.

- 2025-08-01 14:32:05 – Activación de servicio camuflado
- 2025-08-01 14:32:17 – Inyección de librería maliciosa
- Persistencia y reinfección posterior documentada

3. ¿Cuánta información fue exfiltrada?

2.3 gigabytes (GB) de información.

- Datos enviados a servidores de comando y control (C2)
- Exfiltración silenciosa y continua

4. ¿Cuántos eventos o acciones remotas se realizaron?

Mínimo 8.876 eventos documentados:

- 8.742 eventos de registro de teclas (keylogging)
- 134 activaciones remotas de micrófono
- Eventos adicionales de control y persistencia del sistema

5. ¿Qué aplicaciones o componentes fueron afectados?

- Sistema operativo iOS
- Servicios del sistema (SpringBoard, Launch Daemons)
- Aplicación MobileMail
- Bases internas de contactos, WhatsApp y ubicación
- Perfiles de configuración fraudulentos
- Servicios ejecutados con privilegios root

6. ¿Hubo afectación de cámara y micrófono?

Micrófono:

- Sí hubo afectación comprobada
- 134 activaciones remotas documentadas

Cámara:

Calle 98 No. 22 – 64 Oficina 607 / Bogotá D.C., Colombia
notificacionesjudiciales@fsg.legal

Juan Carlos Angarita Cruz
Director & Auditor Forense

Mauricio Javier Vargas Sánchez
Director de Informática Forense

- En los artefactos analizados no se evidencian registros concluyentes de grabación o extracción de información; no obstante, se identifican eventos técnicos compatibles con activaciones del componente afectado, es decir, de la cámara en sí misma.

- La ausencia de registro no descarta capacidad, pero no se afirma por rigor pericial

Párrafo ejecutivo

El iPhone 15 Pro Max fue infectado por Pegasus desde agosto de 2025, permitiendo espionaje continuo, exfiltración de 2.3 GB de información y más de 8.800 acciones remotas, incluyendo escuchas ambientales, con pleno soporte técnico y forense.

Calle 98 No. 22 – 64 Oficina 607 / Bogotá D.C., Colombia
notificacionesjudiciales@fsg.legal

Juan Carlos Angarita Cruz
Director & Auditor Forense

Mauricio Javier Vargas Sánchez
Director de Informática Forense