Las Últimas Noticias

Fecha: 24/03/2024 Audiencia: 271.020 Sección: NACIONAL
Vpe: $6.809 Tirada: 91.144 Frecuencia: DIARIO
Vpe pág: $7.430 Difusión: 91.144
Vpe portada: $7.430 Ocupación: 91,65%

Es un sistema de extracción forense, desarrollado por la compañía Cellebrite

Ufed: detalles del software israelí con el que rescataron los polémicos mensajes del celular de Luis Hermosilla

ARIEL LARA

"La tecnología está cambiando la naturaleza de la delincuencia y está poniendo en riesgo el futuro de la seguridad pública. Obtenga más información sobre la creciente brecha de seguridad pública y la oportunidad de adelantarse a ella". Así versa el lema con el que la compañía de tecnología en ciberseguridad israelí Cellebrite promociona en su sitio web cellebrite.com un avanzado sistema de extracción forense de datos desde dispositivos móviles o Ufed, por su sigla en inglés (Universal Forensic Extraction Device).

Este es el formato tipo tablet que ofrece la empresa.

De qué se trata

La empresa ofrece la venta del software Ufed para computadores, además de un aparato similar a una tablet con el sistema ya instalado, y una tercera opción tipo laptop. En la audiencia de formalización del exdirector de la PDI, Sergio Muñoz, la fiscal Lorena Parra mencionó que la Fiscalía Oriente utilizó dicho software para extraer 777.256 páginas de chats de WhatsApp desde el iPhone 14 Max que el OS-7 de Carabineros incautó en noviembre pasado al abogado Luis Hermosilla, diálogos que entre otras cosas revelaron la entrega de información de causas reservadas que le hacía el ahora detenido exalto oficial de la policía civil, causa derivada de la investigación del caso Audios. Puede revisar los datos de los productos de Cellebrite Ufed en el siguiente link (https://goo.su/kjrc34y).

La tecnología es utilizada por cuerpos policiales y servicios de inteligencia de varios países, incluido el asesoramiento al FBI de los Estados Unidos. En simple, un equipo con la tecnología Ufed instalada puede acceder conectándose a través de puertos USB, bluetooth o wifi, a la memoria de celulares, tablets, computadores, notebooks y otros dispositivos que almacenen datos que se encuentren bloqueados con clave, obteniendo registros de llamadas, de contactos, mensajes de audio, registros de videos, fotos, información de geolocalización, etcétera.

Sirve para acceder a equipos bloqueados. Del peritaje al teléfono del abogado se extrajeron más de 700 mil páginas de conversaciones, entre esas, el diálogo con el imputado exdirector de la PDI.

"Las versiones recientes de Ufed indican que pueden obtener información de múltiples modelos de Android y iPhone sin dañar el contenido del dispositivo", introduce Edson Vittoriano, de la Facultad de Ingeniería Informática Universidad del Desarrollo. El sistema tiene una interfaz amigable que entrega la opción de bajar la información en una memoria externa o donde se desee. En Youtube es posible ver videos que muestran cómo funciona, ingresando la búsqueda "Cellebrite Ufed".

El experto en tecnología de protección de datos y perito judicial informático para el Poder Judicial, Alejandro Barros, explica: "Estas tecnologías no se venden a público general, quienes las adquieren son las policías, agencias de inteligencia, etcétera. El sistema utiliza las vulnerabilidades de seguridad de los dispositivos para extraer la información y una vez que acceden al dispositivo toman la data almacenada y la transfieren a otro equipo para su análisis". El costo de uno de estos dispositivos en Europa puede llegar a los 15 mil dólares.

Gabriel Bergel, experto en ciberseguridad CEO de 8.8 Computer Security Conference (o whitehat, conocido como un "hacker ético"), manifiesta: "Quien lo compre debe justificar muy bien para qué se necesita una herramienta como esta. Los Ufed se hicieron muy famosos cuando el FBI necesitaba entrar al celular de un terrorista en San Bernardino, Estados Unidos, y hubo una polémica porque no se podía acceder a un iPhone bloqueado y vulnerar su seguridad (lo que generó una disputa legal entre Apple y el FBI)".

"Exploits"

Pablo Schwarzenberg, director de la carrera de Ciberseguridad de la Universidad Andrés Bello, dice sobre el funcionamiento del sistema forense al conectarse a un equipo bloqueado: "Nuestros celulares se comportan como pequeños computadores, tienen el equivalente a un disco duro y un sistema operativo que controla su funcionamiento, tal como lo hace Windows o MacOS con nuestros computadores. El sistema operativo es el que provee la protección a la información, pero como todo software puede tener vulnerabilidades que permiten saltar estos controles y acceder a la información, esto es lo que se llama un exploit. Una de las barreras para encontrar estos exploits es que el código de los sistemas operativos no es público, luego, para lograr analizarlos mejor se requieren procesos de ingeniería inversa, que tratan de producir el código de ciertas partes relevantes del sistema para encontrar un punto débil".

Pedro Huichalaf, académico del Centro de Investigación en Ciberseguridad de la Universidad Mayor, expone la importancia de contar con autorizaciones para acceder a los equipos: "Si no se cuenta con la autorización del dueño del dispositivo podría ser considerado un delito, ahora, cuando es utilizado por las policías o cuerpos investigativos, debe ser previamente autorizado por la justicia de otra manera se podría caer en la obtención licita de una prueba para presentar en un juicio".