ElcomSoft Actualizaciones iOS Forensic Toolkit con soporte y rapidez adquirida para el iOS 5

Moscú, Rusia - 1 de noviembre de 2011 – ElcomSoft Co. Ltd. actualiza iOS Forensic Toolkit, agregando el iOS 5 a la lista de sistemas soportados. Con la compatibilidad para iOS 5, Elcomsoft iOS Forensic Toolkit puede recuperar contraseñas de dispositivos y / o realizar análisis de la adquisición física de los dispositivos Apple con iOS 3.x, 4.x y 5. Además, la velocidad de adquisición física fue mejorada en 2 a 2,5 veces. Con más del doble de la velocidad de adquisición de las versiones anteriores, la actualización de Elcomsoft iOS Forensic Toolkit puede realizar una adquisición física a un iPhone 4 de 16 Gb en 20 minutos, o una versión de 32 Gb en 40 minutos.

Proporcionando un acceso casi inmediato a la información forense encriptada almacenada en el último iPhone y dispositivos iPad, Elcomsoft iOS Forensic Toolkit permite el acceso a los puntos de protección del sistema de archivos extraídos de los dispositivos compatibles de Apple, incluso si la contraseña del dispositivo original es desconocida.

El análisis forense de dispositivos iOS 5

Con el lanzamiento de iOS 5, Apple hizo algunos pequeños retoques y algunos cambios importantes para la encriptación de datos. *"No hubo ningún avance en el modelo de seguridad de iOS"*, dice Andrey Belenko, desarrollador líder de ElcomSoft. *"Los cambios en la arquitectura son más bien una evolución del modelo existente. Sin embargo, estos cambios son bienvenidos, ya que presentan una mayor seguridad para el usuario final. En particular, el número de elementos keychain que pueda ser descifrado sin la clave es ahora menos de lo que solía ser. La contraseña del dispositivo es una de las características del modelo de seguridad de Apple, y se están expandiendo el uso del mismo para cubrir más datos que nunca antes."*

Mientras que los algoritmos de cifrado la mayoría parecen ser simplemente un reajuste, Apple hizo un cambio significativo en la configuración de seguridad en materia de protección "keychain", en sustitución del algoritmo de cifrado "keychain" por completo. Además, Apple hizo un "Keybag" dependencia inútil para los especialistas forenses de la protección de las claves de depósito como garantía de acceso al dispositivo por medio de un código. Al parecer, la protección de información confidencial almacenada en dispositivos iOS 5 se basa más en contraseña del dispositivo comparada con versiones anteriores.

"Me encantan los retos", dice Dmitry Sklyarov, líder de ElcomSoft especialista en criptoanálisis. *"El lanzamiento del nuevo sistema presenta un caso perfecto. Poco después de haber iniciado, ni siquiera sabíamos si teníamos la oportunidad de romperlo. Hay cualquier cantidad de nuevos algoritmos de cifrado, cambio "keychain" de protección, nuevas estructuras de datos ... y la lista continua y continua. Hicimos la mayor parte antes del lanzamiento del iOS 4, pero el nuevo sistema presentó algunas dificultades inesperadas."*

Los "keychain" contienen cantidades significativas de información que es muy valiosa para los investigadores forenses. Esta información incluye los inicios de sesión y contraseñas almacenados en sitios web, contraseñas de acceso Wi-Fi, contraseñas de correo electrónico y aplicaciones, y mucho más. A la luzde la nueva encriptación utilizada para proteger los puntos "keychain", Elcomsoft iOSForensic Toolkit es el primer producto disponible en el mercado para ofrecer soporte completo para la recuperación de la información en el "keychain" de dispositivos con iOS 5.

La recuperación total de elementos del "keychain" quiere el conocimiento de la contraseña del dispositivo original. Elcomsoft iOS Forensic Toolkit puede recuperar la contraseña original desempeñando un ataque de fuerza bruta. Conociendo la contraseña de texto plano, Elcomsoft iOSForensic Toolkit puede descifrar todos los elementos almacenados en el "keychain".

Antecedentes

Los especialistas forenses son muy conscientes de la cantidad de información valiosa almacenada en dispositivos Apple iOS como el iPhone. Los usuarios de iPhone acumulan enormes cantidades de información altamente confidencial en sus teléfonos inteligentes. Además de las cosas obvias tales como imágenes, correo electrónico y mensajes SMS, los dispositivos iPhone almacenan la información de uso avanzado como los datos de historial de geolocalización, mapas y rutas de Google vistos, el historial de la navegación por Internet y registros de llamadas, información de inicio de sesión (nombre de usuario y contraseñas), y casi todo lo escrito en el iPhone.

Alguna, pero no toda esta información termina siendo almacenada en copias de seguridad de iPhone cuando son producidas por iTunes de Apple. Sin embargo, la cantidad de información que se puede extraer a partir de copias de seguridad del teléfono es naturalmente limitada.

El análisis de la adquisición física utiliza el contenido objeto del depósito del dispositivo real para llevar a cabo una investigación exhaustiva de los datos almacenados del usuario y del sistema en el dispositivo. El análisis de adquisición física permite acceder a mucha más información de un dispositivo iOS del que un archivo de copia de seguridad puede almacenar, y ofrece a los investigadores una serie de beneficios adicionales no disponibles con el análisis de los archivos de copia de seguridad. Antes de Elcomsoft iOS Forensic Toolkit todo esto era simplemente imposible, ya sea con el código original disponible o sin él. La última versión de Elcomsoft iOS Forensic Toolkit hace posible dicha adquisición en unos 20 minutos de un iPhone de 16 GB o 40 minutos para un iPhone de 32 GB.

Acerca de Elcomsoft iOS Forensic Toolkit

Elcomsoft iOS Forensic Toolkit proporciona acceso forense a la información cifrada almacenada en los dispositivos populares de Apple con iOS 3.x, 4.x, y el iOS 5.
Realizando un análisis de adquisición física del dispositivo en sí, el kit de herramientas ofrece acceso instantáneo a toda la información protegida, incluyendo SMS y mensajes de correo electrónico, historial de llamadas, contactos y datos del organizador, historial de navegación por Internet, correo de voz, correo electrónico y configuraciones, accesos y contraseñas almacenados, historial de geolocalización y el código original en texto plano del usuario. La herramienta también puede llevar a cabo la adquisición lógica de los dispositivos IOS, o facilitar el acceso forense a la información cifrada en los depósitos del sistema de archivos iOS.

Disponibilidad y distribución

Elcomsoft iOS Forensic Toolkit está disponible de inmediato. El acceso a la nueva herramienta se limita a los forenses, la policía, y agencias gubernamentales selectas. El precio está disponible bajo petición y descuentos para los clientes actuales se encuentran disponibles.

Acerca de ElcomSoft Co. Ltd.

Fundada en 1990, ElcomSoft Co. Ltd. desarrolla el estado de la técnica de las herramientas de la informática forense, ofrece capacitación en informática forense y servicios de consultoría de evidencia informática. Desde 1997, ElcomSoft ha estado brindando apoyo a las empresas, la policía, el ejército y las agencias de inteligencia. Las herramientas de ElcomSoft son utilizadas por la mayoría de las corporaciones de Fortune 500, múltiples ramas de las fuerzas armadas en todo el mundo, gobiernos extranjeros y todas las empresas de contabilidad. ElcomSoft y sus funcionarios son miembros de la Asociación Rusa de Criptología. ElcomSoft es un partner certificado de Microsoft y partner de Intel Software.

Elcomsoft iOS Forensic Toolkit es compatible con Windows (XP, Vista / 7,2003 y Server 2008) y MacOS X 10.6/10.7, y está disponible para clientes gubernamentales selectos y entidades de la ley. Más información en http://ios.elcomsoft.com/