ELCOMSOFT
PROACTIVE SOFTWARE

ElcomSoft Investigates iPhone Hardware Encryption, Provides Enhanced Forensic Access to Protected User Data

Moscow, Russia – May 24, 2011 – ElcomSoft Co. Ltd. enables enhanced and near-instant forensic access to encrypted information stored in iPhone devices, and updates Elcomsoft Phone Password Breaker with tools that can access protected file system dumps extracted from iPhone devices, even if the data is hardware-encrypted by iOS 4.

While iPhone backups store a lot of information about the usage of an iPhone device, they don't have everything. Forensic wise, dumping the contents of the physical device is the only proper way to handle an investigation. A decrypted dump of the file system can be analyzed by certified, highly advanced forensic tools such as Guidance EnCase.

It's Not About iPhone Backups

"This time around it's not about iPhone backups", says Vladimir Katalov, ElcomSoft CEO. "Backups created with iTunes software already contain a lot of data, but not quite everything that's being stored or cached in iPhone devices. In contrast, we were able to break into the heart of iPhone data encryption, providing our customers with full access to all information stored in iPhone devices running iOS 4".

"Mobile forensic specialists are well-aware of the amount of valuable information stored in these devices. Before our discovery, there was no way to get full access to all of that data", he continues. "We are responsible citizens, and we don't want this technology to fall into the wrong hands. Therefore, we made a firm decision to limit access to this functionality to law enforcement, forensic and intelligence organizations and select government agencies".

Background

Users of Apple iPhone devices accumulate huge amounts of highly sensitive information stored in their smartphones. Historical geolocation data, viewed Google maps and routes, Web browsing history and call logs, pictures, email and SMS messages, including deleted ones, usernames, passwords, and nearly everything typed on the iPhone is being cached by the device. Some of that information is available in iPhone backups made with Apple iTunes software. However, the amount of information that can be extracted from phone backups is naturally limited.

The amount and sensitive nature of information being stored in iPhone devices called for adequate protection. Apple responded by introducing a feature called Data Protection with the release of iOS 4. The new system release implemented hardware-based encryption in all devices starting with iPhone 3GS and select subsequent models, including iPhone 4, iPhone 3GS, both models of iPad and last generations of iPod Touch. The feature effectively enabled encryption of all user data stored on the device. Using an industry-standard AES-256 protection, the content of iPhone devices was considered to have adequate protection against even the best equipped intruders, including forensic analysts and law enforcement agencies.

Technically, each iPhone device uses a set of hardware-dependent encryption keys as well as data wipe keys buried securely in iPhone's protected storage area. If a data wipe key is lost or destroyed, all data stored in the iPhone is rendered inaccessible and, essentially, useless. If, however, those keys are extracted from the device, it becomes possible to make forensic analysis of the iPhone device. ElcomSoft shares some of the technical details on its blog at http://blog.elcomsoft.com.

ElcomSoft researchers were able to develop a toolkit to not only extract all relevant encryption keys from iPhone devices running iOS 4, but to make use of those keys to decrypt iPhone file system dumps. This in turn can provide enhanced forensic access to all information stored in iPhone devices, even if the device is passcode-protected.

This enhanced functionality offers access to much more information than is stored in iPhone backups. In fact, ElcomSoft believes that its new discovery opens access to too much information of a highly sensitive nature. Due to the nature of data being available to analysts using the new toolkit, ElcomSoft restrict the use of its software to established law enforcement, intelligence and forensic organizations as well as select government agencies.

About Elcomsoft Phone Password Breaker

Elcomsoft Phone Password Breaker provides forensic access to encrypted information stored in popular Apple and BlackBerry devices, decrypting all types of information including SMS and email messages, call history, contacts and organizer data, Web browsing history, voicemail and email accounts and settings. The tool can decrypt password-protected iPhone and BlackBerry backups or provide forensic access to encrypted iPhone file system dumps. Access to enhanced iPhone memory dump decryption functionality is limited to forensic, law enforcement, and select government agencies.

About ElcomSoft Co. Ltd.

Founded in 1990, ElcomSoft Co. Ltd. develops state-of-the-art computer forensics tools, provides computer forensics training and computer evidence consulting services. Since 1997, ElcomSoft has been providing support to businesses, law enforcement, military, and intelligence agencies. ElcomSoft tools are used by most of the Fortune 500 corporations, multiple branches of the military all over the world, foreign governments, and all major accounting firms. ElcomSoft and its officers are members of the Russian Cryptology Association. ElcomSoft is a Microsoft Gold Certified Partner and an Intel Software Partner.

www.elcomsoft.com

intel Software Partner

Microsoft GOLD CERTIFIED Partner