Elcomsoft Phone Breaker 5.0 Adds Over-the-Air Acquisition of iOS 9 Devices

Moscow, Russia - October 29, 2015 - ElcomSoft Co. Ltd. updates Elcomsoft Phone Breaker, the company's mobile forensic tool for over-the-air acquisition and backup analysis of mobile devices. Version 5.0 adds support for over-the-air acquisition of Apple devices running iOS 9, becoming industry's first tool that can download iCloud Drive backups saved by devices running the latest version of Apple's mobile OS. In addition, the new release adds support for local (iTunes) backups created by iOS 9 devices.

"iOS 9 features a new Rootless security subsystem", says Vladimir Katalov, ElcomSoft CEO. "With greatly improved security, acquiring iOS 9 devices becomes even more difficult without knowing the user's device passcode. Our product becomes the first forensic tool offering the possibility of extracting data from these devices even if the original passcode is not known."

Over-the-air acquisition is available in Professional and Forensic editions. Support for two-factor authentication and binary authentication tokens is exclusive to the Forensic edition. Investigators must supply the correct Apple ID and Password. Access to secondary authentication factor is required if two-step authentication is enabled for a given Apple account (unless authenticating with a binary token).

Our Commitment to Privacy

Elcomsoft Phone Breaker 5.0 becomes industry's first cloud acquisition solution for iOS 9, and remains the only true stand-alone cloud acquisition tool. The tool does not require a third-party server to operate, and never transmits Apple ID and password to any server, using login credentials directly with Apple to authenticate an account. All communications occur strictly between the expert's computer and Apple servers with no third parties involved. No single piece of information is ever transmitted to ElcomSoft or any servers other than Apple's.

Over-the-Air Acquisition in iOS 9

Since initial public beta, iOS 9 was known for its much tighter security compared to the already secure iOS 8. By seriously improving security at all points including the iCloud, Apple strives to deliver a mobile platform with exemplary security.

Newly implemented in iOS 9 are changes in the location of iCloud device backups, which have now been moved completely into iCloud Drive (while still inaccessible via iCloud Control Panel). The cloud backups now have a different structure, and feature notable changes and improvements to encryption. In addition, iOS 9 introduces the new ATS (App Transport Security) protocol that prevents traffic sniffing and rules out man-in-the-middle attacks.

With no possibility for the man-in-the-middle attack, the traditional research path was effectively shut. Developing support for over-the-air acquisition of cloud backups produced by iOS 9 devices required ElcomSoft to perform tremendous amounts of intense low-level research.

iOS 9 and Physical Acquisition

Long before the release of iOS 9, the ability to perform physical acquisition was limited to jailbroken 32-bit devices. This automatically rules out recent devices (iPhone 5S and newer, iPad mini Retina and newer). At this time, the possibility of physical acquisition of 32-bit devices running iOS 9 is still under research, even if the device is jailbroken.

iOS 9 is now installed on 57% of eligible devices. With no physical acquisition tools available for the new platform and considering the fast acceptance rate of iOS 9, the future of physical acquisition does not look bright. Alternative acquisition methods such as logical and over-the-air extraction remain the only possible options for iOS 9 devices. Elcomsoft Phone Breaker 5.0 is one of the few mobile forensic solution to download iOS 9 device backups, and remains the only tool for pulling iOS backups without transmitting authentication information to a third party.

iCloud Backups

Cloud backups offer Apple users the convenience of being able to restore the look and content of the original on a new device without user interaction. Once enabled, backups are created automatically every time the device is charging while connected to a known Wi-Fi network. Thanks to exemplary implementation, iCloud backups are used by the majority of iOS users. In recent versions of iOS, the option to create iCloud backups is enabled by default.

iCloud backups contain a nearly full copy of all relevant data available in the device. Cloud backups contain call and message logs, the list of installed apps complete with application data, communication history in social networks and instant messengers, notes, pictures with geotags, device settings, cached Web forms and passwords, and lots of other data. A notable exception is downloaded mail, which is not included into cloud backups.

Retrieving and analyzing iCloud backups enables investigators collect valuable evidence that may not be available elsewhere.

About Elcomsoft Phone Breaker

Elcomsoft Phone Breaker (formerly Elcomsoft Phone Password Breaker) provides forensic access to encrypted information stored in popular Apple and BlackBerry devices, Apple iCloud/iCloud Drive and Windows Live! accounts. By recovering the original password protecting offline backups produced with compatible devices, the tool offers forensic specialists access to SMS and email messages, call history, contacts and organizer data, Web browsing history, voicemail and email accounts and settings stored in those backup files. The new iteration of the product can also retrieve information from online backups stored in Apple iCloud.

Pricing and Availability

At this time, only the Windows version of Elcomsoft Phone Breaker is updated to receive iOS 9 support. A Mac OS version is in the works. The Windows edition of Elcomsoft Phone Breaker 5.0 is available immediately. Home, Professional and Forensic editions are available. iCloud recovery is only available in Professional and Forensic editions, while password-free iCloud access as well as the ability to download arbitrary information from iCloud and iCloud Drive are only available in the Forensic edition. Elcomsoft Phone Breaker Pro is available to North American customers for $199. The Forensic edition enabling over-the-air acquisition of iCloud data and support for binary authentication tokens is available for $799. The Home edition is available for $79. Local pricing may vary.

System Requirements

Elcomsoft Phone Breaker 5.0 supports Windows Vista, Windows 7, 8, 8.1, and Windows 10 as well as Windows 2003, 2008 and 2012 Server. Elcomsoft Phone Breaker operates without Apple iTunes or BlackBerry Link being installed. Downloading iOS backups and files from iCloud requires iCloud for Windows to be installed.

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 is a Microsoft Partner (Gold Application Development), Intel Premier Elite Partner and member of NVIDIA's CUDA/GPU Computing Registered Developer Program.