Elcomsoft Extracts Apple Health Data from iCloud

ElcomSoft Co. Ltd. updates Elcomsoft Phone Breaker, the company's forensic extraction tool. Version 9.0 gains the ability to remotely access Apple Health data stored in Apple iCloud, becoming the first forensic tool on the market to extract Health information from the cloud. Health data is added to the long list of extractable information, which includes call logs, photo libraries, passwords, messages and multiple other types of data. Elcomsoft Phone Viewer received an update to support the new data category.

Background

Apple makes active use of cloud sync, and is continuously expanding the amount of information synchronized with iCloud. Synchronized information is removed from iCloud backups. Starting with iOS 11, Apple began synchronizing Health data with iCloud, making Health information available on all devices registered on the same Apple ID.

Elcomsoft Phone Breaker 9.0 can automatically extract Apple Health data from the user's iCloud account just moments after they arrive. To access that data, experts must use a combination of Apple ID and password. Entering the user's lock screen password allows Elcomsoft Phone Breaker to retrieve significantly more Health information than available without a passcode.

Health data is a vital piece of evidence. Heartrate, sleeping habits, location points, workouts, steps and walking routines are just a few things that come to mind speaking of Apple Health. Introduced in September 2014 with iOS 8, the Apple Health app is pre-installed on all iPhones. The app makes use of low-energy sensors, constantly collecting information about the user's physical activities. With optional extra hardware (e.g. Apple Watch or Bluetooth fitness trackers), the Health app can aggregate significantly more information. Additional information can be manually added by the user or imported via CDA documents.

Accessing Apple Health Data

In many cases, Apple Health can be only extracted through the cloud. End-to-end encryption makes it impossible for Apple to release most of Health data when serving law enforcement or GDPR requests, while extracting Health data from the device may not be possible if the device is damaged or unavailable.

Extracting Apple Health data from iCloud is possible with Elcomsoft Phone Breaker 9.0 Forensic Edition. Apple ID and password are required as well as access to the secondary authentication factor as well as the user's screen lock password. In some configurations, Health data may not employ any additional encryption; therefore, a device passcode is not always required to access Health information. However, entering the user's screen lock password helps retrieve significantly more information than available without a passcode. More information about Health data protection and acquisition in ElcomSoft Blog: Apple Health Is the Next Big Thing: Health, Cloud and Security.

About Elcomsoft Phone Breaker

Elcomsoft Phone Breaker is an all-in-one mobile acquisition tool to extract information from a wide range of sources. Supporting offline and cloud backups created by Apple, BlackBerry and Windows mobile devices, the tool can extract and decrypt user data including cached passwords and synced authentication credentials to a wide range of resources from local backups.

Pricing and Availability

Elcomsoft Phone Breaker 9.0 is immediately available for Windows and macOS. This update is free to existing users with currently valid licenses. Home, Professional and Forensic editions are available. iCloud support 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. Two-Factor Authentication is available in all editions.

Elcomsoft Phone Breaker Pro is available to North American customers for $199. The Forensic edition enabling over-the-air acquisition of iCloud data, iCloud Keychain, Messages and protected Health data as well as 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 supports Windows 7, 8, 8.1, and Windows 10 as well as Windows 2008, 2012 and 2016 Server. The Mac version supports macOS X 10.8 and newer. Elcomsoft Phone Breaker operates without Apple iTunes or BlackBerry Link being installed. In order to access iCloud Keychain, Health and Messages, Windows users must have iCloud for Windows installed, while Mac users must run macOS 10.11 or newer.

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.