ElcomSoft Decrypts iMessages in iCloud

Moscow, Russia – June 14, 2018 - ElcomSoft Co. Ltd. updates Elcomsoft Phone Breaker, the company's forensic extraction tool. Version 8.30 gains the ability to remotely access iMessage conversations stored in Apple iCloud, and becomes the first forensic tool on the market to extract encrypted iMessage conversation histories from the cloud. Over-the-air iMessage extraction is available for users running iOS 11.4 and newer.

"The communication protocol used for exchanging iMessages is extremely secure", says ***Vladimir Katalov****, ElcomSoft CEO. "Before iOS 11.4, sent and received text messages and iMessages could be only accessed by analyzing a physical iPhone device or iPhone's full system backup. The new release of Elcomsoft Phone Breaker enables remote access to iMessage conversation histories stored in Apple iCloud, which is a breakthrough achievement considering how well-protected the iMessages and the iPhone itself are."*

In addition, Elcomsoft Phone Viewer is updated to display iMessages extracted by Elcomsoft Phone Breaker 8.30.

Background

In iOS 11.4, Apple added a major feature advertised almost a year ago during iOS 11 announce. iMessages are now automatically synchronized across all enrolled devices on the user's Apple ID using iCloud. iCloud sync works similar to existing synchronizations such as iCloud Keychain, iCloud Photo Library or iCloud contacts.

The iCloud synchronization mechanism is separate from Continuity, and works in addition to iCloud system backups. Unlike daily iCloud backups, synchronization happens near instantly. If the device has an Internet connection, information is updated with little or no delay. This enables near real-time remote access to iMessages sent and received by the user.

iMessages Unavailable With GDPR Requests

Since May 25, Apple began allowing users to request information available in their Apple account thanks to the company's GDPR compliance. However, even for European customers, iMessages are not included with GDPR data requests. According to Apple (https://support.apple.com/en-us/HT208502), "your messages are encrypted on your device and can't be accessed by anyone without your device passcode".

While it is true that iMessages cannot be accessed by anyone without device passcode, it does not appear that iMessages stored in iCloud are encrypted with a key derived from the passcode as discussed in the following article: ***iCloud and iMessage Security Concerns*** (https://blog.elcomsoft.com/2018/06/icloud-and-imessage-security-concerns/)

iMessage Extraction

Elcomsoft Phone Breaker 8.30 offers the ability to extract iMessages from the user's iCloud account. The user's iCloud/Apple ID authentication credentials are required to access iCloud data, as well as the secondary authentication factor for passing the Two-Factor Authentication prompt. In addition, one must provide a passcode (iPhone/iPad) or system password (Mac) from one of the enrolled devices.

In addition to iMessages, Elcomsoft Phone Breaker can extract iCloud Keychain as well as many types of synchronized data including call logs, Safari data (browsing history, open tabs and bookmarks), calendars, notes and contacts, Apple Maps, Wallet and iBooks data.

iMessage sync is exclusively available on Apple accounts with Two-Factor Authentication. As a result, access to the secondary authentication factor is mandatory when pulling iMessages from iCloud. In addition, a valid passcode or system password is required from one of the user's devices enrolled in iMessage sync.

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. Cloud extraction with or without a password makes it possible to decrypt FileVault 2 containers without lengthy attacks and pull communication histories and retrieve photos that've been deleted by the user a long time ago.

Pricing and Availability

Elcomsoft Phone Breaker 8.30 is available for both Windows and macOS. Home, Professional and Forensic editions are available. iCloud recovery 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 and support for binary authentication tokens is available for $799. The Home edition is available for $79. Local pricing may vary.

The update is free of charge to all customers who purchased or renewed their Elcomsoft Phone Breaker or Elcomsoft Mobile Forensic Bundle license within one year. Discounted renewal is available to customers whose maintenance plan has already expired.

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 Mac OS X 10.7 and newer. Elcomsoft Phone Breaker operates without Apple iTunes or BlackBerry Link being installed. In order to access iCloud Keychain, 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. ElcomSoft is a Microsoft Partner (Gold Application Development), Intel Premier Elite Partner and member of NVIDIA's CUDA/GPU Computing Registered Developer Program.