Apple Silently Uploads iPhone Call Logs to iCloud, ElcomSoft Releases Acquisition Tool

Moscow, Russia – November 17, 2016 - ElcomSoft Co. Ltd. discovers another privacy issue with Apple cloud services, releases tool to extract iPhone call logs from iCloud. According to ElcomSoft, Apple automatically uploads iPhone call logs to Apple's remote servers. Call logs can be stored on Apple servers for months, and there is no option for the end user to disable this sync without disabling iCloud entirely on their device. ElcomSoft updates Elcomsoft Phone Breaker 6.20 to give it the ability to download call logs made with iPhones running iOS 9 and newer directly from the cloud regardless of whether or not the device is locked and whether or not the passcode is known.

"Automatic cloud sync of call logs is great if you know about it and have an option to shut it off", says Vladimir Katalov, ElcomSoft CEO. *"While Apple works hard to improve security of their physical devices, they move more and more data into the cloud where law enforcement can easily obtain it. On our side, we're working on extracting more data from the cloud, which allows compensating for ever increasing security of iOS devices."*

The user's Apple ID and password or iCloud authentication token are required to extract data from the cloud. By using authentication tokens, forensic specialists can bypass two-factor authentication checks.

Call Logs Stored in iCloud

The ability to store call logs (information about incoming and outgoing calls, including missed or rejected calls) on Apple servers is available on devices running iOS 9.x and 10.x. There is no official way to disable this feature for the end user other than switching off the iCloud Drive functionality completely. Call logs will be uploaded to Apple servers if iCloud Drive is enabled on a given iPhone. Since iOS delivers a number of services via iCloud Drive, disabling it would greatly affect its usability.

While online syncing makes perfect sense for calendar events or contacts, exact reasons behind Apple's decision to store call logs online are not clear. Any calls made, received or missed with any iPhone signed in to a certain Apple ID will automatically sync with the user's iCloud account and appear on their other iOS devices that are signed in with the same Apple ID. To some extent, this even includes non-voice enabled devices such as iPads and iPod Touch models.

Elcomsoft Phone Breaker 6.20 brings synced call logs before the eyes of the law enforcement, enabling forensic access to synced call logs from within the tool. In addition to call logs, the updated cloud extraction tool will also download contacts. Downloading call logs and contacts requires signing in to the user's Apple account using their Apple ID and password or iCloud authentication token extracted from the user's Mac or PC.

Elcomsoft Phone Viewer is also updated to support viewing additional information extracted from Apple cloud servers. Synced call logs and contacts can be viewed right next to call logs and contacts extracted from system backups.

What Else Is Synced?

At this time, things like calendars, Wallet (boarding passes, payment and discount cards etc.), books, notes and many other things are synced with iCloud. ElcomSoft is working hard on adding the ability to extract these and other things from the cloud.

In recent months, ElcomSoft has discovered that Apple may keep photos deleted from the user's iCloud Photos for much longer than the advertised period of 30 days. While Apple has seemingly fixed the issue, it is not yet known whether the photos are actually removed from Apple servers or are kept elsewhere.

Considering the above, ElcomSoft is no longer sure whether iMessages are indeed point-to-point or if they are being synced with (and kept in) iCloud or elsewhere on Apple's servers.

Other Platforms

ElcomSoft provides tools for extracting synced call logs can that are saved or synced by both major mobile operating systems.

Elcomsoft Cloud Explorer extracts call logs synced by Android 6.0 and newer devices by accessing the user's Google Account. Elcomsoft Phone Breaker 6.20 added the ability to extract call logs synced by Apple iPhones running iOS 9 and newer from Apple iCloud.

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.

System Requirements

Elcomsoft Phone Breaker 6.20 supports Windows Vista, Windows 7, 8, 8.1, and Windows 10 as well as Windows 2003, 2008 and 2012 Server. The Mac version supports Mac OS X 10.7.x and newer. Elcomsoft Phone Breaker operates without Apple iTunes or BlackBerry Link being 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 and Gold Intelligent Systems), Intel Premier Elite Partner and member of NVIDIA's CUDA/GPU Computing Registered Developer Program.