Elcomsoft Phone Breaker 6.0 Decrypts FileVault 2, Downloads iCloud Photos, Retrieves Apple ID Password

Moscow, Russia – August 25, 2016 - ElcomSoft Co. Ltd. releases a major update to Elcomsoft Phone Breaker, the company's mobile forensic tool for logical and over-the-air acquisition of mobile devices. Version 6.0 adds support for decrypting FileVault 2 volumes by downloading the Recovery Key from iCloud. In addition, the new release adds the ability to download existing and recently deleted photos and media files from iCloud Photos. Other changes include the updated Keychain Explorer and the ability to cache online authentication credentials for streamlined subsequent logins into iCloud, Windows Phone and BlackBerry 10.

*"In this release, we're targeting two additional bits extracted from iCloud", says **Vladimir Katalov**, ElcomSoft CEO. "By extracting the FileVault 2 Recovery Key, we can decrypt data stored in Mac OS X FileVault 2 containers. Access to iCloud Photos allows us downloading existing media and recovering files that've been deleted more than 30 days ago and no longer appear in the 'Recently deleted' album on devices or iCloud.com."*

Must use the correct Apple ID and password or non-expired iCloud authentication token to access iCloud and iCloud Photos. Access to secondary authentication factor is required if two-step verification or two-factor authentication is enabled for a given Apple account unless authenticating with a binary token. Access to iCloud and iCloud Photos is available in Professional and Forensic editions. Support for two-factor authentication and binary authentication tokens is exclusive to the Forensic edition.

Decrypting FileVault 2 Volumes

FileVault 2 is a whole-disk encryption scheme used in Apple's Mac OS X. FileVault 2 protects the entire startup partition with secure 256-bit XTS-AES encryption. FileVault 2 volumes can be unlocked with a password to any account with "unlock" privileges.

If the user forgets their account password, or if the encrypted volume is moved to a different computer, a FileVault 2 can be unlocked with a Recovery Key. The Recovery Key is created at the time the user initially configures FileVault 2 protection on their disk. The key is displayed and can be saved or printed. If the user logs in with their Apple ID credentials, the Recovery Key can be saved into the user's iCloud account. Should the user forget their password, the system can automatically use the Recovery Key to unlock the encrypted volume.

© 2016 ElcomSoft Co. Ltd.
Microsoft Partner Gold Independent Software Vendor (ISV)
intel Software Partner

Apple provides no way for the user to view or extract FileVault 2 recovery keys from iCloud. In this release, Elcomsoft Phone Breaker gains the ability to extract FileVault 2 recovery keys from the user's iCloud account, and use these keys to decrypt encrypted disk images. Valid authentication credentials (Apple ID/password or iCloud authentication token) as well as volume identification information extracted from the FileVault-encrypted disk image are required in order to extract the key. Once the recovery key is successfully obtained, the user can perform full decryption for offline analysis.

Extracting iCloud Photo Library

The introduction of Apple iCloud back in 2011 allowed iPhone and iPad users back up and restore the content of their devices into the cloud. At that time, photos and videos shot with the iOS device would be included as part of the main backup. At the time, photos and videos could not be easily downloaded. The only way to gain access to those media files would be restoring the full backup onto a new Apple device.

In iOS 8.1 and OS X Yosemite (10.10), Apple introduces a new service for saving and sharing photos and videos. iCloud Photo Library stores and synchronizes media files between multiple devices by using Apple's cloud service. If iCloud Photo Library is used, media files are no longer saved to iOS iCloud backups.

iCloud Photo Library shares available storage space with Apple iCloud. However, accessing iCloud Photo Library uses a separate set of APIs. Acquiring iCloud backups or downloading files stored in iCloud Drive does not automatically provide access to media files stored in the iCloud Photo Library.

In this release, Elcomsoft Phone Breaker gains the ability to download photos and videos stored in iCloud Photo Library. Elcomsoft Phone Breaker can also extract media files that have been deleted more than 30 days ago, which can result in significantly more evidence compared to simply pulling the "Recently Deleted" album.

Experts can use recently updated Elcomsoft Phone Viewer 2.30 for viewing images extracted from iCloud Photo Library. Elcomsoft Phone Viewer is a lightweight forensic tool with support for local and cloud backups. The latest release can view photos and metadata for iCloud Photo Library.

New Keychain Viewer

Elcomsoft Phone Breaker 6.0 introduces a new look for the old keychain viewer. The new release makes it easy to access browser passwords, authentication tokens (including those to access iCloud backups and files), saved credit card data and Wi-Fi passwords synced from the iCloud keychain. The new viewer will attempt to automatically discover the user's Apple ID password and/or authentication token by analyzing browser passwords, iTunes and App Store settings. Passwords to email accounts as well as passwords and tokens to social network accounts, gaming portals and instant messaging applications are also displayed.

© 2016 ElcomSoft Co. Ltd.
Microsoft Partner Gold Independent Software Vendor (ISV)
intel Software Partner

Keychain data can be extracted from password-protected iTunes backups. The password must be known or recovered with Elcomsoft Phone Breaker.

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 6.0 is available immediately for both Windows and Mac OS X. 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 6.0 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. 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 and Gold Intelligent Systems), Intel Premier Elite Partner and member of NVIDIA's CUDA/GPU Computing Registered Developer Program.

© 2016 ElcomSoft Co. Ltd.