Elcomsoft Phone Breaker Extracts and Decrypts iCloud Keychain

Moscow, Russia – August 22, 2017 - ElcomSoft Co. Ltd. updates Elcomsoft Phone Breaker, the company's forensic extraction tool. Version 7.0 becomes a major release that gets the ability to extract, decrypt and access passwords stored in Apple's cloud password storage, the iCloud Keychain. Elcomsoft Phone Breaker 7.0 is the first forensic solution that can gain access to passwords and other sensitive information from iCloud Keychain.

"*iCloud Keychain was long considered to be unbreakable", says **Vladimir Katalov**, ElcomSoft CEO. "Gaining access to passwords from iCloud Keychain was a major challenge. iCloud Keychain is a complex and extremely secure online password storage and storage synchronization system. Building a tool that can enroll into iCloud Keychain was a major achievement."*

By extracting user's saved passwords from iCloud Keychain, experts can log in to the user's online accounts, access social network accounts, and extract chats, messages and postings. In addition, saved passwords are perfect for building custom dictionaries for targeted brute-force attacks on user's encrypted containers, archives and documents.

Information is obtained directly from the user's iCloud account. In order to access iCloud Keychain, the original Apple ID login and password are required. Access to a trusted device is mandatory if two-factor authentication is enabled on the user's account, along with device passcode (iOS) or system passwords (macOS) of a device already enrolled to iCloud Keychain. Without two-factor authentication, the expert will need to confirm a notification prompt on one of the trusted devices and supply the user's iCloud Security Code.

Background

iOS and macOS implement a system-wide protected storage for sensitive information such as Web site logins and passwords, Wi-Fi passwords, credit card data and so on. These items are stored in the system keychain. For iOS devices, the keychain can be saved and restored via local or cloud backups.

Forensic access to iOS keychain is difficult due to several layers of encryption. The keychain saved into an iCloud backup is securely encrypted with a hardware-based encryption key, and can only be restored onto exactly the same device it was saved from. Forensic access to hardware-encrypted keychains is impossible with very few exceptions (legacy devices, jailbreak). A password-protected local backup can be used for keychain extraction; however, if the backup is protected with a long, unknown password, brute-forcing that password may take significant time of may not be possible.

In addition to local keychains, Apple offers a cloud password storage and synchronization system, the iCloud Keychain. iCloud Keychain is a service designed to keep user's passwords synchronized across multiple devices. The service provides a secure storage, authentication and synchronization mechanism, allowing newly registered devices to obtain keychain items from the user's other enrolled devices. Access to iCloud Keychain is securely protected with multiple layers of protection including industry-standard encryption and access restrictions imposed by the chain of trust.

The system is so secure that, until now, third-party access to iCloud Keychain was through to be impossible.

Elcomsoft Phone Breaker 7.0 becomes the first tool to access passwords and payment information secured by iCloud Keychain. In order to gain access, the user's original Apple ID and passwords (as well as a 2FA code) are required. In addition, the expert must approve the request on an already enrolled device (if there is no two-factor authentication on that account). If two-factor authentication is enabled on the user's account, the expert will have to provide device passcode for any iOS device already enrolled for iCloud Keychain, or system password if the enrolled device is a Mac.

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 System Requirements

Elcomsoft Phone Breaker 7.0 is available for both Windows and macOS. 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. 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.

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.