ELCOMSOFT
PROACTIVE SOFTWARE

ElcomSoft Discovers Security Weakness in iOS 10 Backups, Develops Exploit

Moscow, Russia – September 23, 2016 - ElcomSoft Co. Ltd. discovers a major security weakness in iOS 10 backups, builds tool enabling quick recovery of complex passwords. Elcomsoft Phone Breaker 6.10, the company's mobile acquisition tool, can break iOS 10 backup passwords significantly faster compared to iOS 9 passwords using a newly discovered exploit using a CPU alone. The newly discovered security weakness in iOS 10 backups potentially allows recovery speeds thousands times faster compared to password-protected iOS 9 backups.

"All versions of iOS prior to iOS 10 used to use extremely robust protection", says ***Vladimir Katalov***, *ElcomSoft CEO. "Chances of recovering a long, complex password were slim, and even then a high-end GPU would be needed to accelerate the recovery. As a result of our discovery, we can now break iOS 10 backup passwords much faster even without GPU acceleration."*

Forcing an iPhone or iPad to produce an offline backup and analyzing resulting data is one of the very few acquisition options left to forensic specialists. At this time, it remains the only acquisition option available for iPhone 5s, 6/6Plus, 6s/6sPlus and 7/7Plus running iOS 10 that offers access to device keychain.

Starting with iOS 8, acquisition options for locked iPhones are severely restricted. If no Apple ID or authentication token is available, cloud acquisition may not be available. Logical acquisition may be the only option available for locked iPhones. It may be possible to produce an iTunes backup using a pairing record extracted from a trusted computer.

iOS 10 Backups: Significantly Weaker Protection

iOS 10 is a huge update to Apple's mobile OS. Among other things, the new OS features an unencrypted kernel and introduces changes to for both offline (iTunes) and online (iCloud) backups.

Elcomsoft Phone Breaker 6.10 adds support for both new backup formats, enabling forensic customers to break password protection and download iOS 10 backups from the cloud. iOS 10 support itself would be big enough news. However, ElcomSoft were able to discover a major change in protection for iOS 10 backups compared to prior versions of iOS.

Contrary to recent trend of ever-increasing security, these changes make it much easier to try passwords. Best-ever recovery rate achieved on iOS 9 backups was slightly more than 150,000 passwords per second using a single PC equipped with an NVIDIA GTX 1080 accelerator. For iOS 10, Elcomsoft Phone Breaker peaks at 6 million passwords per second using a CPU alone without the help of a GPU. At this time, GPU acceleration for this exploit is still in development.

In practice, that means that a truly random, 6-character alphanumerical password (single-case letters) protecting iOS 10 backup will only take a few minutes to break. Add an extra character, and it still takes several hours to brute-force, which is also very reasonable. For reference, the same 7-character password protecting an iOS 9 backup would take almost a week to break.

Benchmarks

The following benchmarks were obtained for iOS 9 and iOS 10 backups using the same hardware.

- **iOS 9 (CPU): 2,400 passwords per second (Intel i5)**
- **iOS 9 (GPU): 150,000 passwords per second (NVIDIA GTX 1080)**
- **iOS 10 (CPU): 6,000,000 passwords per second (Intel i5)**

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 6.10 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 6.10 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.