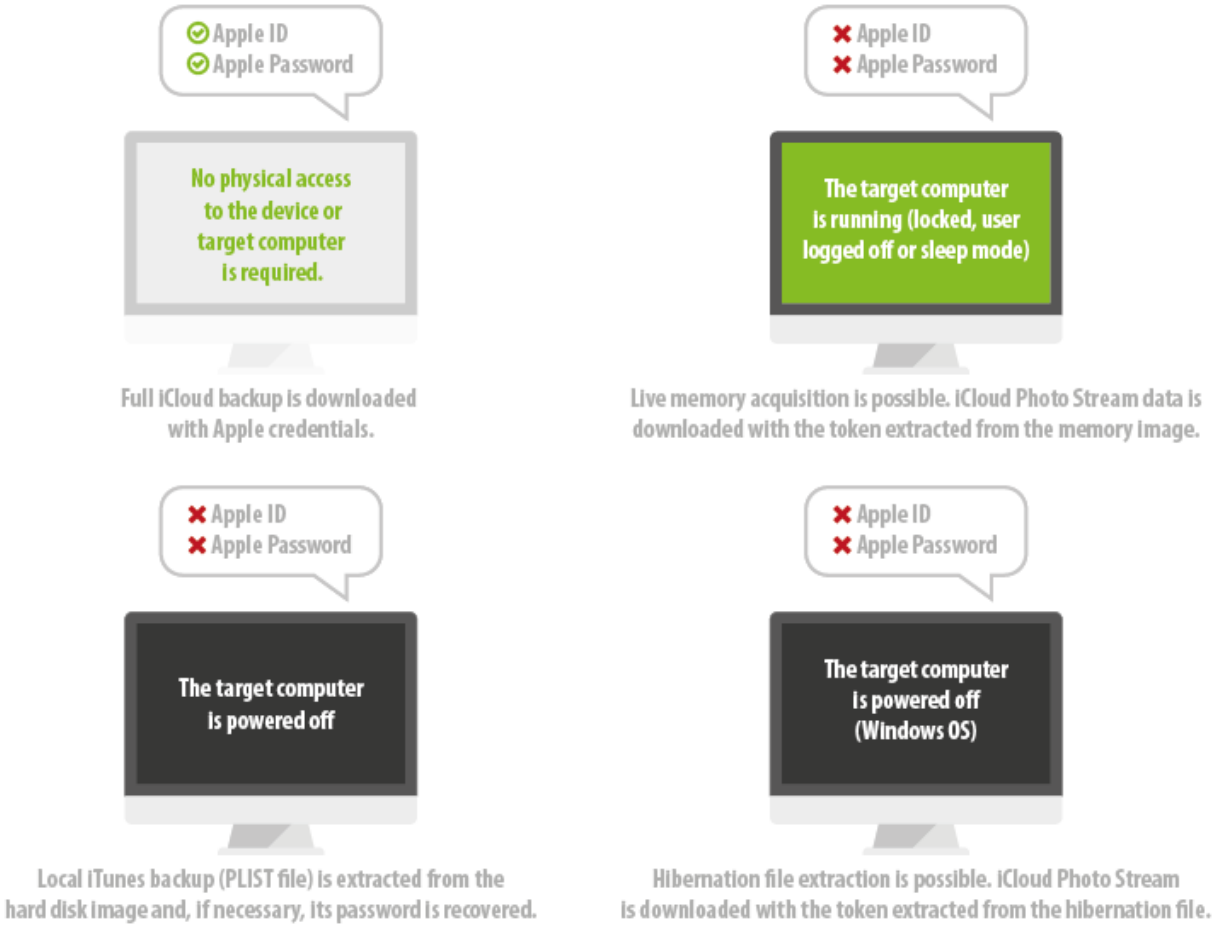
Contact:
Nataly Koukoushkina
Passware Inc.
+1 (650) 472-3716 ext. 101
media@lostpassword.com

Passware Exposes Suspects' Photo Stream to Computer Forensics

Investigators now have a unique tool that leverages Passware's research in live-memory analysis for over-the-air acquisition of Apple Photo Stream contents without Apple ID or password



Mountain View, Calif. (March 24, 2015) – Passware, Inc., a provider of password recovery, decryption, and electronic evidence discovery software for computer forensics, law enforcement organizations, government agencies, and private investigators, announces version 2 of its flagship encrypted electronic evidence discovery product – Passware Kit Forensic 2015. This new release now acquires suspects' iPhone and iPad photos without Apple ID or password, provided the physical access to the computer with iCloud application installed.

According to apple.com, “Your new photos appear automatically on the iOS devices, computers, and Apple TV you set up with My Photo Stream, no matter which iOS device or computer you use to take or import new photos.” (Source: https://support.apple.com/kb/PH13693?viewlocale=en_US&locale=en_US). This also concerns shared photo stream where photos and videos of trusted contacts are automatically synchronized with the Apple device.

An authentication token, which replaces Apple credentials and thus allows iPhone/iPad photo stream download, resides in the computer memory and hibernation file (for Windows OS). This token allows downloading of photos and videos from the owner’s photo stream and, additionally, from the shared albums of his trusted contacts.

Until now, the only solution for acquiring iCloud data without Apple ID and password was extracting the iCloud token from the target hard disk, which further required a user password for the operating system to decrypt the token. Passware has found a way to acquire the token from a live memory image and, which is more applicable, from a Windows hibernation file. This makes it unnecessary to have a user password for the OS. Moreover, if the target computer is shut down and live memory data no longer available for acquiring, the hibernation file with the token resides there until the next hibernation even after the power-off.

Each photo and video contains invaluable evidence, such as GPS coordinates, time taken, and device name. Thorough analysis of this data occurs in Oxygen Forensic Passware Analyst, which also provides detailed reports and graphs for computer forensic investigations. Supported are all versions of iOS, including the latest 8.2.

Cases Enabling Acquisition of iPhone and iPad Full Backups
Computer forensics can now acquire full backups of a suspect’s iPhone or iPad using Passware in unique cases, including:

- Apple ID and password are known: No physical access to the device or target computer is required. Full iCloud backup is downloaded with Apple credentials.
- Apple ID and password are unknown and the target computer is powered off. Local iTunes backup (PLIST file) is extracted from the hard disk image and, if necessary, its password is recovered.
- Apple ID and password are unknown and the target computer is running (locked, user logged off or sleep mode). Live memory acquisition is possible. iCloud Photo Stream data is downloaded with the token extracted from the memory image.
- Apple ID and password are unknown and the target computer (Windows OS) is powered off. Hibernation file extraction is possible. iCloud Photo Stream is downloaded with the token extracted from the hibernation file.

A graph of these unique cases where Passware acquires data of a suspect’s iPhone or iPad are available here: http://www.lostpassword.com/f/downloads/press/2015-2-icloud.pdf.

”With the introduction of bullet-proof encryption in the latest version of iOS, over-the-air acquisition becomes the only applicable way to gain access to data from Apple devices,” said Dmitry Sumin, CEO of Passware. “With the proliferation of Apple devices, this is yet another powerful tool available to forensic experts conducting investigations.”

Additional features of Passware Kit Forensic 2015 v.2 include:

- Hardware-accelerated password recovery for hidden TrueCrypt containers
- Automatic software updates
- Improved performance of Passware Kit Agent for Linux
- Decryption of FileVault 2 from Mac OS X Yosemite
- Extraction of passwords and credentials from KeePass databases
- Exporting results to CSV format for further analysis and forensic reports

Passware Kit Forensic Demonstration
The new features of Passware Kit Forensic will appear for the first time at Computer & Cell Phone Forensics Users Conference (PATCtech) 2015, May 5-7, Davie, Fla. (http://www.patc.com/training/detail.php?ID=13108). Visit Passware's booth there, as well as its presentation "Digital Encrypted Evidence Discovery and Decryption: Computers and Mobile Devices."

Pricing and Availability
Passware Kit Forensic is available directly from Passware and a network of resellers worldwide. The price is $995 with one year of free updates. Additional product information and screen shots are available at http://www.lostpassword.com/passware-kit-forensic/index.html.

About Passware, Inc.
Founded in 1998, Passware, Inc. is the worldwide leading maker of password recovery, decryption, and electronic evidence discovery software. Law enforcement and government agencies, institutions, corporations and private investigators, help desk personnel, and thousands of private consumers rely on Passware software products to ensure data availability in the event of lost passwords. Passware customers include many Fortune 100 companies and various US federal and state agencies, such as the IRS, US Army, US Department of Defense (DOD), US Department of Justice, US Department of Homeland Security, US Department of Transportation, US Postal Service, US Secret Service, US Senate, and US Supreme Court.

Passware is a privately held corporation with its headquarters in Mountain View, Calif. More information about Passware, Inc. is available at http://www.lostpassword.com/.

###