ElcomSoft Tool Decrypts WhatsApp iCloud Backups

Moscow, Russia – July 20, 2017 - ElcomSoft Co. Ltd. updates Elcomsoft eXplorer for WhatsApp, the company's all-in-one tool for extracting, decrypting and analyzing WhatsApp communication histories. The tool gains the ability to decrypt WhatsApp stand-alone backups produced by the iPhone app and stored in Apple's iCloud Drive. The decryption is possible with access to a verified phone number or SIM card, and requires authenticating into the user's Apple ID account. A WhatsApp encryption key must be only obtained once, and can be used to access all previously created and all future backups for a given combination of Apple ID and phone number. The tool provides automatic download and decryption for WhatsApp backups and comes with a built-in viewer.

*"WhatsApp remains the most popular instant messaging tool in North America and Europe, and is the one communication tool most frequently picked by the criminals", says **Vladimir Katalov**, ElcomSoft CEO. "With our tool, investigators can now access iPhone users' encrypted WhatsApp communication histories stored in Apple iCloud Drive – provided that they have access to the user's Apple ID account and can receive a confirmation code sent to their verified phone number."*

Decrypting iPhone Users' WhatsApp Backups

Since December 2016, both manual and daily stand-alone backups produced by WhatsApp iPhone app and stored in the user's iCloud Drive are automatically encrypted with industry-standard AES256 encryption. The encryption key, generated by WhatsApp at the time of the first backup, is unique per each combination of Apple ID and phone number. Different encryption keys are generated for different phone numbers registered on the same Apple ID. These encryption keys are generated and stored server-side by WhatsApp itself; they are never stored in iCloud, and they cannot be extracted from the iOS device.

Elcomsoft Explorer for WhatsApp 2.10 gains the ability to retrieve cryptographic keys used to encrypt and decrypt WhatsApp's iCloud backups, successfully bypassing encryption and gaining access to WhatsApp conversation history and underlying messages. In order to generate the encryption key, experts must be able to receive a WhatsApp verification code sent to the phone number for which a given backup was created. In addition, the user's Apple ID and password (or binary authentication token) are required to gain access to the backup itself. The cryptographic key can be used to access all previously created and all future backups for a given combination of Apple ID and phone number.

Experts with access to the user's verified phone number of SIM card as well as Apple ID authentication credentials can now use Elcomsoft Explorer for WhatsApp to circumvent encryption and gain access to iCloud-stored encrypted messages.

More information as well as the detailed how-to guide available at
https://blog.elcomsoft.com/2017/07/extract-and-decrypt-whatsapp-backups-from-icloud/

Current State of WhatsApp Security

Despite recent discoveries regarding WhatsApp encryption of the tool's iCloud backups, the app's end-to-end message delivery still remains secure, and the messaging service remains one of the most secure on the market. WhatsApp securely encrypts messages sent and received, and makes use of encryption when producing cloud backups. Decrypting WhatsApp-produced backups requires access to the trusted phone number or SIM card, as well as access to the user's Apple ID account.

WhatsApp does not keep communication histories on their servers, making them unavailable to hacker attacks. For the same reason, government requests result in very limited data. As a result, acquisition is only possible from physical devices, iOS system backups or proprietary WhatsApp backups.

About Elcomsoft Explorer for WhatsApp

Elcomsoft Explorer for WhatsApp is an all-in-one tool for extracting, decrypting and viewing WhatsApp communication histories from iOS and Android devices and cloud services. Supporting a wide range of acquisition options, Elcomsoft Explorer for WhatsApp can extract WhatsApp data from local iTunes backups, retrieve WhatsApp databases from iCloud backups and download stand-alone WhatsApp backups from Apple iCloud Drive. The tool can extract WhatsApp communication histories from most rooted and non-rooted Android devices. Cloud acquisition requires entering the correct authentication credentials (Apple ID and password), while stand-alone WhatsApp backup decryption requires access to a verified phone number or SIM card. Encrypted backups can be decrypted automatically once the correct password is supplied.

The built-in viewer offers convenient access to contacts, messages and pictures sent and received during conversations. Multiple WhatsApp databases can be analyzed at the same time. Searching and filtering make it easy locating individual messages or finding communication sessions that occurred over a certain date range.

Pricing, availability and system requirements

Elcomsoft eXplorer for WhatsApp is immediately available to North American customers for $79. Its test version is available free of charge. Local pricing may vary. Elcomsoft eXplorer for WhatsApp supports Windows 7, 8, 8.1, and Windows 10 as well as Windows 2008, 2012 and 2016 Server.

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.