

Elcomsoft Phone Breaker извлечёт удалённую историю браузера Safari из iCloud



Москва, Россия – 9 февраля 2017 - Компания «Элкомсофт» обновляет продукт для мобильной криминалистики [Elcomsoft Phone Breaker](#) до версии 6.40, добавляя возможность извлечения удалённых записей истории браузера Safari. Удалённые записи извлекаются непосредственно из «облака» iCloud. Журнал посещений Safari синхронизируется с iCloud в режиме реального времени; в то же время, удалённые пользователям записи на самом деле остаются в «облаке» и доступны для извлечения с помощью [Elcomsoft Phone Breaker](#). Извлекаются как сами удалённые записи, так и информация о дате и времени последнего посещения ссылки, а также дате и времени её удаления. Одновременно получил обновление инструмент для просмотра извлечённых из «облака» данных [Elcomsoft Phone Viewer](#).

Данные синхронизируются регулярно и не зависят от настроек резервных копий, что позволяет вести наблюдение за тем, какие сайты посещает пользователь, с минимальной задержкой.

*«История посещений пользователя в браузере Safari синхронизируется с другими устройствами через iCloud», говорит CEO компании «Элкомсофт» **Владимир Каталов**. «Подобные «облачные» способы синхронизации получили широкое распространение среди производителей мобильных операционных систем. В то же время, Apple оказалась единственной компанией, которая продолжает хранить на своих серверах записи из истории браузера даже после того, как пользователь их удалит. Без сомнения, такая реализация «облачной» синхронизации способна оказать правоохранительным органам помощь в раскрытии преступлений.»*

Для извлечения журнала звонков из «облака» iCloud требуется указать учётные данные пользователя (логин и пароль Apple ID) либо использовать двоичный маркер аутентификации, извлечённый с его компьютера. Использование маркера аутентификации позволяет обойти защиту методом двухфакторной авторизации.

Синхронизация истории браузера и удалённые записи

При использовании смартфонов и планшетов Apple под управлением iOS 9 многие типы данных синхронизируются с «облаком» iCloud. В первую очередь в «облако» сохраняются резервные копии устройств и фотографии. Кроме того, в iOS доступна «облачная» синхронизация, с помощью которой между устройствами, зарегистрированными в одной учётной записи, передаётся актуальная информация о последних звонках пользователя, открытых в браузере вкладках, контактах, заметках и т.д.

Через «облако» синхронизируется и история посещений пользователя в браузере Safari. Информация о сайтах и страницах, которые открывал пользователь, автоматически передаётся на серверы Apple. С них она попадает на другие устройства пользователя, привязанные к той же учётной записи.

Пользователь может удалить историю посещений браузера Safari как целиком, так и в виде отдельных записей. Удалённые записи исчезают как с основного устройства, так и с других синхронизированных устройств (если они подключены к Интернет). Если попробовать сбросить устройство, а потом восстановить его из «облака» - на нём окажутся только те записи, которые не были удалены, и только за последний месяц.

Исследователям «Элкомсофт» удалось выяснить, что «удалённые» пользователем записи истории браузера Safari на самом деле не исчезают из «облака», а остаются в iCloud в течение длительного времени. Разработчикам удалось извлечь из «облака» записи, которые были удалены больше года назад.

Извлечь удалось как сами записи, так и информацию о том, когда именно запись была удалена пользователем, а также данные о времени последнего посещения ссылки.

В новой версии [Elcomsoft Phone Breaker 6.40](#) добавлена возможность извлечения из «облака» удалённых записей о посещённых веб-узлах из синхронизированной истории Safari. Теперь с помощью [Elcomsoft Phone Breaker](#) можно извлечь не только те записи истории посещений Safari, которые видны пользователю на устройствах или в «облаке» iCloud, но и записи, которые пользователь удалил.

Одновременно до версии 3.25 обновился и продукт для просмотра скачанной информации, [Elcomsoft Phone Viewer](#).

О продукте Elcomsoft Phone Breaker

[Elcomsoft Phone Breaker](#) предоставляет экспертам доступ к информации, извлечённой из мобильных устройств под управлением Apple iOS, Windows Phone, Windows 10 Mobile и BlackBerry 10. Поддерживаются режимы логического извлечения (расшифровка и анализ локальных резервных копий) и удалённое извлечение данных из облачных хранилищ Apple iCloud и iCloud Drive, а также учётных записей Microsoft Account. Дистанционное извлечение данных из iCloud доступно как при наличии логина (Apple ID) и пароля пользователя, так и без них с использованием вместо пароля маркера аутентификации, извлечённого из компьютера пользователя. Поддерживается полный и выборочный доступ к данным. Доступ к самому устройству при этом не требуется.

В [Elcomsoft Phone Breaker](#) интегрированы инструменты, необходимые для извлечения и использования маркеров аутентификации Apple iCloud. С использованием маркеров аутентификации, извлечённых с компьютера пользователя, становится возможным доступ в «облачное» хранилище iCloud даже если логин и пароль пользователя неизвестны эксперту.

Поддержка мультимедийного хранилища iCloud Photo Library позволяет извлекать фотографии, в том числе удалённые пользователем в течение последних 30 дней. Извлечение депонированных ключей от криптоконтейнера FileVault 2 позволяет расшифровывать защищённые тома FileVault 2 без проведения лобовой атаки.

Стоимость и редакции

В продаже доступны редакции [Elcomsoft Phone Breaker](#) Home (5495p), Professional (14995p) и Forensic (59995p). Расширенный доступ к «облачному» хранилищу iCloud доступен пользователям редакции Forensic. Лицензированные пользователи «домашней» редакции могут приобрести профессиональную версию продукта, заплатив разницу в стоимости лицензий. Для работы Elcomsoft Phone Breaker установка Apple iTunes не требуется.

Системные требования

[Elcomsoft Phone Breaker](#) совместим с 32- и 64-разрядными версиями Windows, Windows 7, 8, 8.1, Windows 10, Windows 2003, 2008 и 2012 Server.

О компании «ЭлкомСофт»

Компания «ЭлкомСофт» – российский разработчик программного обеспечения и поставщик услуг в области восстановления паролей и данных. Решения компании «ЭлкомСофт» используются корпорациями, входящими в список Fortune 500, а также правительственными организациями, правоохранительными органами и спецслужбами по всему миру. Компания «ЭлкомСофт» является членом Российской Криптологической Ассоциации, имеет статус сертифицированного партнера Microsoft (Microsoft Gold Certified Partner) и Intel (Intel Software Partner). Компания основана в 1990 году, головной офис «ЭлкомСофт» находится в Москве. Для получения более подробной информации посетите <http://www.elcomsoft.ru>