

Apple хранит журнал звонков iPhone в «облаке», доступен инструмент для извлечения



Москва, Россия – 17 ноября 2016 - Специалисты компании «Элкомсофт» обнаружили, что информация о входящих и исходящих вызовах, совершаемых пользователями смартфонов Apple iPhone, автоматически сохраняется в «облако» iCloud. Данные синхронизируются регулярно и независимо от настроек резервных копий, что позволяет вести наблюдение за телефонным общением пользователя с минимальной задержкой. «Элкомсофт» обновляет продукт для мобильной криминалистики [Elcomsoft Phone Breaker](#) до версии 6.20, добавляя возможность извлечения журнала звонков из «облачного» сервиса iCloud. Одновременно получил обновление инструмент для просмотра скачанной информации Elcomsoft Phone Viewer.

«Большая часть сервисов Apple направлен на улучшение пользовательского опыта», говорит CEO компании «Элкомсофт» Владимир Каталов. «Мы не смогли понять, какой именно пользовательский опыт призвана улучшить синхронизация журнала звонков с облаком. Тем не менее, мы не сомневаемся, что наш продукт способен оказать заметную помощь в оперативно-следственной работе правоохранительных органов.»

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 журнала звонков

При использовании смартфонов Apple iPhone под управлением iOS 9 и более новая информация о входящих и исходящих вызовах, включая пропущенные и отклонённые звонки, автоматически отправляется в «облачный» сервис iCloud. Для подавляющего большинства пользователей наличие данной функции стало неприятным сюрпризом: в официальных материалах Apple нет упоминаний ни о самом сервисе, ни о возможности его отключения.

В мобильной операционной системе от Apple не предусмотрен механизм деактивации данной функции. Отключить хранение журнала звонков в «облаке» можно лишь полным отключением службы iCloud Drive в настройках устройства. С учётом того, что на службу iCloud Drive завязано заметное количество системных сервисов, её полное отключение приводит к невозможности доступа к файлам в «облачном» хранилище iCloud Drive, невозможности создания резервных копий (например, для приложения WhatsApp и многих других) и недоступности ряда других нововведений, появившихся в iOS 9.

С технической точки зрения, звонки не отправляются на вечное хранение, а синхронизируются с учётной записью пользователя. При наличии второго iPhone, привязанного к той же учётной записи, список звонков одного устройства будет доступен и на другом. Данные о звонках синхронизируются периодически с небольшой задержкой, и могут храниться в «облаке» до нескольких месяцев. Удаление информации о звонке на одном синхронизированном устройстве приведёт к исчезновению этой записи и с других синхронизированных устройств.

В новой версии [Elcomsoft Phone Breaker 6.20](#) добавлена возможность извлечения из «облака» как синхронизированных журналов звонков, так и контактов пользователей iPhone. Одновременно 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, удалённые более 30 дней назад. 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>