Без срока давности: Elcomsoft Phone Breaker извлечёт удалённые заметки из iCloud

Москва, Россия – 19 мая 2017 - Компания «Элкомсофт» обновляет продукт для мобильной криминалистики Elcomsoft Phone Breaker. В версии 6.50 появилась возможность извлечения удалённых заметок и вложений, созданных приложением Notes. Удалённые записи извлекаются непосредственно из «облака» iCloud. Заметки пользователя синхронизируется с iCloud в режиме реального времени; в то же время, заметки, которые пользователь удаляет в приложении, на самом деле не удаляются из «облака» и остаются доступными в течение неопределённого времени. С помощью Elcomsoft Phone Breaker 6.50 такие удалённые заметки можно извлечь из «облака» вместе с информацией о дате и времени создания или последнего обновления заметки, а также дате и времени её удаления. Одновременно получил обновление инструмент для просмотра извлечённых из «облака» данных Elcomsoft Phone Viewer.

Так же, как и данные о телефонных звонках или истории браузера Safari, заметки синхронизируются регулярно и не зависят от настроек резервных копий. Удалённые заметки остаются доступны пользователю в течение 30 дней после удаления. Elcomsoft Phone Breaker 6.50 позволяет восстановить заметки, которые были удалены и по прошествии 30-дневного периода.

«Заметки, которые пользователь делает с помощью приложения Notes собственной разработки Apple, синхронизирует данные с другими устройствами через iCloud», говорит CEO компании «Элкомсофт» ***Владимир Каталов****. «Аналогичные продукты других производителей – например, Evernote, Microsoft OneNote или Google Keep, – тоже синхронизируют заметки с использованием собственных онлайновых сервисов. В то же время, Apple оказалась единственной компанией, которая продолжает хранить на своих серверах даже те заметки, которые пользователь удалил. Такая реализация «облачной» синхронизации вызывает вполне обоснованные сомнения у пользователей, озабоченных приватностью персональной информации.»*

Для извлечения заметок 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.

Предыстория

Пользователям экосистемы Apple доступна сквозная синхронизация многих видов данных. Информация о звонках, фотографии, закладки и история браузера Safari, заметки – все эти данные могут автоматически синхронизироваться между устройствами через «облако» iCloud. Посредством «облачной» синхронизации между устройствами, зарегистрированными в одной учётной записи, передаётся актуальная информация о создании, изменении и удалении записей.

В то же время, ожидания пользователя не всегда совпадают с тем, как фактически работает синхронизация. Так, пользователь ожидает, что заметки, которые он удалит с устройства, будут также удалены и из «облака» iCloud (разумеется, если пользователь вообще знает о том, что его заметки хранятся в «облаке»). Однако этого не происходит: исследователям из компании «Элкомсофт» удалось обнаружить, что удалённые заметки остаются в iCloud и могут сохраняться в «облаке» в течение неопределённого времени. Это позволило разработчикам выпустить версию Elcomsoft Phone Breaker, которая извлекает из «облака» заметки, удалённые много месяцев назад.

Данный эпизод – далеко не первый. В августе 2016 года в «Элкомсофт» обнаружили, что из iCloud не удаляются фотографии. В феврале 2017 той же командой исследователей в iCloud были обнаружены записи истории посещений пользователей браузера Safari, некоторые из которых были удалены в 2015 году. Теперь же оказалось, что из «облака» никуда не исчезают и заметки, которые пользователь полагает удалёнными.

В новой версии Elcomsoft Phone Breaker 6.50 добавлена возможность извлечения из «облака» удалённых записей о заметках, которые ведёт пользователь в предустановленном приложении Notes. С помощью Elcomsoft Phone Breaker можно извлечь как те заметки, которые видны пользователю на устройствах или в «облаке» iCloud, так и записи, которые пользователь удалил.

Одновременно вышло обновление продукта для просмотра скачанной информации, Elcomsoft Phone Viewer 3.35.

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 (5495р), Professional (14995р) и Forensic (59995р). 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 7, 8, 8.1, Windows 10, Windows 2008, 2012 и 2016 Server. Версия для macOS требует macOS 10.7 или более новой.

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» находятся в Москве. Для получения более подробной информации посетите http://www.elcomsoft.ru