Elcomsoft Phone Breaker 6.0: расшифровка FileVault 2, извлечение удалённых фотографий, пароля Apple ID

Москва, Россия – 25 августа 2016 - Компания «ЭлкомСофт» обновляет инструмент для мобильной криминалистики Elcomsoft Phone Breaker. В шестой версии программы добавлен ряд возможностей по расшифровке криптоконтейнеров FileVault 2, извлечению удалённых фотографий из iCloud Photo Library и просмотру паролей, извлечённых из резервных копий iPhone и iPad. Кроме того, в новой версии продукта данные аутентификации (логин и пароль или маркер аутентификации) сохраняются для использования в последующих сессиях.

«Мы продолжаем работать с облачными хранилищами», говорит CEO компании «ЭлкомСофт» ***Владимир Каталов****. «Из iCloud извлекается всё больше информации. Доступ к депонированным ключам позволяет быстро расшифровать криптоконтейнеры FileVault 2, а работа с iCloud Photo Library – восстановить фотографии, которые пользователь удалил более 30 дней назад. Мы извлекаем заметно больше удалённых изображений, чем доступно в альбоме удалённых фото.»*

Для доступа к iCloud и iCloud Photos требуется указать логин и пароль от Apple ID либо использовать действительный маркер аутентификации. Если в учётной записи активирована двухфакторная аутентификация, потребуется доступ к дополнительному фактору при использовании логина и пароля. Работа с облачными сервисами доступна только пользователям редакций Professional и Forensic. Поддержка двухфакторной аутентификации и маркеров аутентификации доступна только пользователям редакции Forensic.

Расшифровка томов FileVault 2

В операционной системе Mac OS X используется встроенный механизм шифрования дисков FileVault 2. Криптоконтейнер FileVault 2 шифрует разделы с помощью 256-битных ключей алгоритмом XTS-AES. Зашифрованные тома могут быть разблокированы пользователями, которым присвоена привилегия “unlock”.

Если пользователь забудет пароль, в системе предусмотрена возможность восстановления доступа к зашифрованным данным. Для этого используются ключи Recovery Key, которые депонируются в облачное хранилище iCloud, привязанное к учётной записи Apple ID пользователя. Ключи доступны исключительно через внутренние API, и недоступны для просмотра самим пользователем.

Новая версия Elcomsoft Phone Breaker извлекает депонированные ключи FileVault 2 и позволяет расшифровать зашифрованные криптоконтейнером тома. Для доступа к депонированным ключам требуются логин и пароль от Apple ID (или маркер аутентификации), а также информация, идентифицирующая зашифрованный том (извлекается из образа диска FileVault 2).

Извлечение удалённых фотографий из iCloud Photo Library

В iOS 8.1 и Mac OS X Yosemite (10.10) пользователям устройств Apple стал доступен новый механизм для хранения и синхронизации фото и видео. iCloud Photo Library позволяет сохранять фотографии и видеоролики и синхронизировать их между различными устройствами. Необходимо отметить, что если этот сервис активирован, то фотографии более не попадают в резервные копии устройств в iCloud.

Интересной особенностью iCloud Photo Library является то, что удалённые пользователем фотографии хранятся в «облаке» в течение длительного времени. В альбоме «недавно удалённых» файлов, который доступен пользователю как с устройств Apple, так и на сайте iCloud.com, фотографии доступны в течение 30 дней после удаления.

В Elcomsoft Phone Breaker добавлен механизм, позволяющий извлекать фотографии из iCloud Photo Library. Более того, используемый механизм позволяет скачивать и те фотографии, которые были удалены более 30 дней назад и, соответственно, недоступные обычному пользователю.

Для просмотра файлов рекомендуем использовать приложение Elcomsoft Phone Viewer 2.30, в котором добавлен режим просмотра изображений из iCloud Photo Library. Elcomsoft Phone Viewer – компактный и лёгкий в использовании инструмент для быстрого просмотра информации, извлечённой из локальных и «облачных» резервных копий.

Поиск и просмотр паролей

В Elcomsoft Phone Breaker 6.0 представлен обновлённый инструмент для просмотра паролей из защищённого хранилища Keychain, извлекаемого из локальных резервных копий iPhone и iPad. В новом инструменте добавлены удобные режимы просмотра паролей из браузера и маркеров аутентификации, используемые для входа в учётные записи пользователя в социальных сетях, чатах и форумах. Также доступен просмотр данных сохранённых платёжных средств (кредитных и дебетовых карт), паролей к сетям Wi-Fi и паролей и маркеров аутентификации к почтовым учётным записям.

Уникальная возможность обновлённого инструмента – автоматическое сканирование всех доступных источников с целью поиска пароля или маркера аутентификации к учётной записи Apple ID. Сканируются такие источники, как пароли из браузера, приложения iTunes и App Store.

Данные из Keychain извлекаются из локальных резервных копий iTunes, защищённых паролем, который известен либо был восстановлен с помощью Elcomsoft Phone Breaker.

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