

Elcomsoft Phone Breaker извлекает пароли из iCloud Keychain



Москва, Россия – 22 августа 2017 - Компания «ЭлкомСофт» обновляет продукт для мобильной криминалистики [Elcomsoft Phone Breaker](#). В версии 7.0 появилась возможность удалённого извлечения паролей из связки ключей iCloud (iCloud Keychain), привязанной к учётной записи пользователей устройств Apple. Elcomsoft Phone Breaker – первый и единственный продукт на рынке, с помощью которого можно извлечь iCloud Keychain непосредственно из «облака» iCloud.

«Мы продолжаем работать над извлечением данных из iCloud», комментирует CEO компании «Элкомсофт»

Владимир Каталов. *«Наш арсенал пополнился исключительно мощным средством. Актуальные пароли пользователя теперь можно извлечь дистанционно, что может оказать неоценимую помощь в проведении расследований.»*

В связке ключей iCloud хранятся самые разнообразные пароли пользователей – как от веб-сайтов из браузера Safari, так и беспроводных сетей, программ мгновенного обмена сообщениями, социальных сетей и множества сторонних приложений. Извлечение iCloud Keychain позволит экспертам получить доступ к почте и учётным записям пользователя, закрытым постингам и сообщениям в социальных сетях, переписке через программы мгновенного обмена сообщениями и многому другому.

Для извлечения сохранённых паролей пользователя из связки ключей iCloud потребуются данные учётной записи Apple ID пользователя (логин и пароль), а также доступ к одному из авторизованных устройств. Если в учётной записи пользователя активирована двухфакторная аутентификация, потребуется ввести пароль от устройства iOS или системный пароль от учётной записи macOS. Если двухфакторная аутентификация не включена, то для доступа к iCloud Keychain потребуется ввести код iCloud Security Code.

Предыстория

В мобильной операционной системе iOS, под управлением которой работают устройства iPhone и iPad, предусмотрен механизм «облачной» синхронизации и хранения паролей. В связку ключей iCloud (iCloud Keychain) могут сохраняться как логины и пароли, которые пользователь вводит в браузере Safari, так и данные аутентификации сторонних приложений.

В зависимости от ряда условий iCloud Keychain может храниться в «облаке» iCloud. Все данные надёжно шифруются, а доступ к ним жёстко контролируется Apple. Единственный официальный способ доступа к iCloud Keychain – инициализация устройства производства Apple, такого как iPhone, iPad или компьютер Mac. Не существует инструментов или механизмов для скачивания iCloud Keychain на компьютер или экспорта паролей, а обходные способы (через привязку нового устройства iPhone или iPad и его синхронизацию с iCloud Keychain) не могут быть использованы экспертами-криминалистами, т.к. они модифицируют содержимое iCloud Keychain пользователя.

[Elcomsoft Phone Breaker 7.0](#) стал первым и на данный момент единственным инструментом, который может корректно использоваться в криминалистических целях. С помощью Elcomsoft Phone Breaker эксперт сможет авторизовать в iCloud Keychain не устройство под управлением iOS (извлечь из которого зашифрованные пароли – задача нетривиальная и далеко не всегда возможная), а приложение, запущенное на компьютере эксперта. С помощью Elcomsoft Phone Breaker весь iCloud Keychain целиком скачивается и расшифровывается за считанные секунды, в то время как синхронизация iCloud Keychain с iPhone или iPad может занять несколько часов.

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 7, 8/8.1, Windows 10, а также серверных версий Windows.

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>