ELCOMSOFT
PROACTIVE SOFTWARE

Резервные копии в iCloud больше не нужны: извлечение контактов, календарей, звонков, заметок и журнала истории Safari

Москва, Россия – 21 декабря 2016 - Специалисты компании «Элкомсофт» обнаружили возможность следить за действиями пользователей iPhone и iPad в браузере Safari, извлекая информацию об открытых вкладках и истории посещений в режиме реального времени без физического доступа к устройству. Оказалось, что Safari синхронизирует информацию о действиях пользователя с «облачным» сервисом iCloud. Данные о действиях пользователя поступают в «облако» с незначительной задержкой, которая гораздо меньше периодичности создания ежедневных резервных копий в iCloud.

«Мы продолжаем развивать линейку продуктов «Элкомсофт» для мобильной криминалистики», комментирует CEO компании «Элкомсофт» ***Владимир Каталов****. «Несколько лет назад извлечение данных из iPhone было невозможно без физического доступа к телефону. С появлением iCloud и «облачных» резервных копий доступ к самому устройству уже не нужен, но резервные копии создавались не чаще одного раза в день. Извлечение синхронизированных данных из «облака» открывает возможность получать актуальную информацию о действиях пользователя, его звонках, открытых страниц в браузере, контактах, заметках и событиях в календаре.»*

В предыдущей версии Elcomsoft Phone Breaker появилась возможность извлечения информации о контактах пользователей iPhone и их входящих и исходящих вызовах. В текущем релизе функционал приложения значительно расширен. Теперь из «облака» извлекаются синхронизированные звонки (в том числе звонки через FaceTime), заметки, календари, контакты и действия пользователя в браузере Safari (открытые вкладки и история браузера). Важно отметить, что эти данные синхронизируются регулярно и независимо от настроек «облачных» резервных копий, что позволяет вести наблюдение за телефонным общением пользователя с минимальной задержкой.

Для извлечения синхронизированных данных 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.

Microsoft Partner
Gold Application Development
Gold Intelligent Systems

intel Software Partner

Данные из «облака»

Традиционные способы извлечения информации из смартфонов подразумевают как минимум наличие самого устройства. С появлением «облачных» сервисов акцент стал постепенно смещаться в сторону дистанционных методов извлечения. Начиная с iOS 8 в iPhone и iPad появился механизм для создания и восстановления резервных копий устройств в «облаке» iCloud. В iOS 9 этот механизм был существенно переработан; данные резервных копий теперь хранятся в iCloud Drive.

Слабое место «облачных» резервных копий с точки зрения правоохранительных органов – их эпизодичность: резервные копии создаются и обновляются не чаще одного раза в сутки при совпадении ряда условий (телефон находится на зарядке, экран заблокирован, устройство подключено к известной сети Wi-Fi).

В то же время в iOS существует механизм синхронизации актуальных данных между различными устройствами. Синхронизируются звонки, заметки, календари, контакты, а также открытые вкладки в браузере Safari и история открытых пользователем веб-страниц. В отличие от резервных копий, которые обновляются с максимальной частотой раз в сутки, синхронизированные данные обновляются с минимальной задержкой. Часто не проходит и нескольких минут после звонка или открытия новой вкладки в Safari, как эти данные уже поступают на сервер Apple. Наличие этой возможности не афишируется Apple, а способ её отключения не очевиден: для выключения синхронизации требуется полностью выключить службы iCloud Drive, что ведёт к заметному ухудшению опыта использования устройства в целом.

В новой версии Elcomsoft Phone Breaker 6.30 добавлена возможность извлечения из «облака» многих типов синхронизированных данных. Извлекаются как синхронизированные журналы звонков, так и другая информация: контакты, календари, заметки и история действий пользователя в браузере Safari.

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 (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 https://www.elcomsoft.ru/