

Elcomsoft Phone Breaker 5.0: извлечение «облачных» резервных копий iOS 9



Москва, Россия – 29 октября 2015 - Компания «Элкомсофт» обновляет инструмент для мобильной криминалистики [Elcomsoft Phone Breaker](#). В версии 5.0 добавлена поддержка «облачных» резервных копий устройств под управлением последней версии Apple iOS 9. Усиленные меры безопасности в iOS 9 приводят к тому, что «облачное» извлечение данных становится последней и единственной возможностью получить вещественные доказательства, скрытые в защищённых паролем телефонах и планшетах Apple. Компания «Элкомсофт» первой выпустила продукт с полноценной поддержкой «облачных» резервных копий устройств под управлением iOS 9. Кроме того, в новой версии добавлена поддержка локальных резервных копий iOS 9, создаваемых с помощью программы iTunes на компьютере пользователя.

«iOS 9 использует новую модель безопасности, серьёзно затрудняющую исследование», говорит CEO компании «Элкомсофт» Владимир Каталов. «Закрыта возможность перехвата трафика между устройством и сервером Apple, введена сквозная проверка сертификатов. Чтобы понять, как устроена работа «облачного» копирования в iOS 9, пришлось проделать серьёзную исследовательскую работу.»

В новой версии iOS даже наличие jailbreak не гарантирует возможности физического извлечения. В условиях полной невозможности физического извлечения данных из 64-разрядных устройств производства Apple (начиная с iPhone 5S и iPad mini 2), анализ «облачных» резервных копий становится последней возможностью получить доступ к данным. Elcomsoft Phone Breaker в редакциях Professional и Forensic – один из немногих продуктов на рынке с поддержкой «облачного» извлечения резервных копий, сохраняемых устройствами под управлением iOS 9.

[Elcomsoft Phone Breaker](#) остаётся единственным автономным продуктом, способным извлечь данные из «облака» iCloud/iCloud Drive без использования промежуточного сервера. Данные аутентификации передаются напрямую в Apple без каких-либо посредников.

iOS 9: качественные изменения модели безопасности

Не секрет, что каждая новая версия iOS приносит многочисленные изменения и улучшения в модель безопасности. В предыдущей версии iOS большое количество пользовательских данных было перенесено в безопасное хранилище keychain, что заметно снизило эффективность атак на закрытые паролем устройства.

В последней версии iOS 9 разработчики применили ряд технологий под кодовым обозначением Rootless, существенно затрудняющих исследование системы. Изменились базовые сетевые протоколы, внедрена сквозная проверка сертификатов. В новой ОС внесены изменения в механизм и место хранения «облачных» резервных копий, которые теперь сохраняются непосредственно в iCloud Drive (но остаются недоступными из соответствующей панели). Изменился и механизм шифрования данных.

Усиленные меры безопасности привели к тому, что в новой версии iOS даже использование jailbreak не гарантирует возможности физического извлечения данных. Новый протокол безопасного обмена данными между устройством и сервером ATS (App Transport Security) исключает возможность перехвата трафика, существенно затрудняя исследование.

Возможности извлечения данных из современных устройств под управлением iOS 9 ограничены, при этом скорость перехода пользователей на новую версию мобильной ОС беспрецедентно высока. На сегодняшний день согласно официальной статистике Apple на iOS 9 перешло 73% активных пользователей.

Физическое извлечение недоступно для телефонов iPhone 5S и планшетов iPad Mini 2 и более поздних, при этом сама возможность физического извлечения данных даже из устройств с 32-разрядной аппаратной платформой до сих пор остаётся под вопросом. В результате на данный момент «облачное» извлечение остаётся последним и единственным вектором атаки защищённых PIN-кодом устройств Apple, а Elcomsoft Phone Breaker 5.0 – одним из немногих инструментов, способных осуществить такую атаку.

[Elcomsoft Phone Breaker](#) – единственный продукт на рынке, обеспечивающий конфиденциальность пользователя. Установленная на компьютер пользователя программа обменивается данными исключительно с сервисом Apple iCloud/iCloud Drive без использования каких-либо посредников или промежуточных серверов, что выгодно отличает продукт «Элкомсофт» от конкурентов.

О продукте Elcomsoft Phone Breaker

Elcomsoft Phone Breaker for Mac предоставляет криминалистам доступ к пользовательским данным, извлечённым из мобильных устройств производства Apple и Blackberry, а также к данным из Apple iCloud и учётных записей Windows Live (для устройств под управлением Windows Phone 8). Информация извлекается из защищенных паролем резервных файлов, создаваемых устройствами Apple iPhone/iPod/iPad и смартфонами BlackBerry при синхронизации с компьютером пользователя.

Продукт способен дистанционно извлекать информацию из «облачного» хранилища Apple iCloud и iCloud Drive при наличии логина (Apple ID) и пароля пользователя либо 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.

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 или BlackBerry Desktop Software не требуется.

Системные требования

Elcomsoft Phone Breaker совместим с 32- и 64-разрядными версиями Windows XP, Vista, Windows 7, Windows 8, 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>