ElcomSoft обновляет программу iOS Forensic Toolkit, добавляя поддержку iOS 5 и ускоряя извлечение данных

Москва, Россия – 1 ноября 2011 – компания ElcomSoft Co. Ltd. обновляет продукт iOS Forensic Toolkit, добавляя iOS 5 в список поддерживаемых систем. Благодаря поддержке iOS 5, Elcomsoft iOS Forensic Toolkit теперь может восстанавливать пароль и создавать полный побитовый образ файловой системы устройств Apple, работающих под управлением iOS 3.x, 4.x и 5. Кроме того, время извлечения информации сокращено в 2-2.5 раза, что позволяет создавать образ 16-гигабайтной модели iPhone 4 всего за 20 минут.

Обеспечивая практически мгновенный доступ к зашифрованной информации, хранящейся в iPhone и iPad, программа Elcomsoft iOS Forensic Toolkit эффекьтивно работает даже в тех случаях,когда неизвестен пароль устройства.

Криминалистический анализ устройств с iOS 5

В новой версии iOS 5 компания Apple сделала некоторые улучшения и изменения в шифровании данных. *“Реального прорыва в защите iOS не произошло”*, комментирует Андрей Беленко, ведущий разработчик компании ElcomSoft. *“Архитектурные изменения являются эволюционным развитием существующей модели. Однако мы приветствуем все изменения, так как они предоставляют пользователям улучшенную защиту. В частности, теперь сокращено количество записей в системном хранилище (keychain), доступных без пароля. Использование пароля к устройству является одним из ключевых элементов модели безопасности Apple, с помощью которой компания стремиться ограничить несанкционированный доступ к данным”*

В то время как большинство криптоалгоритмов претерпели незначительные улучшения, значительные изменения произошли в настройках безопасности, а именно в защите keychain: существенно изменена схема шифрования ключей. В дополнение к этому депонированные ключи (Escrow Keybag) стали совершенно бесполезными для экспертов-криминалистов, поскольку тоже стали защищаться паролем. Очевидно, что защита важной информации, хранящейся в устройствах iOS 5, стала намного сильнее зависеть от пароля к устройству, чем в предыдущих версиях iOS.

“Я люблю вызовы”, говорит Дмитрий Скляров, ведущий специалист по криптоанализу компании ElcomSoft. *“ Когда мы только начинали исследование архитектуры защиты iOS, мы даже не знали есть ли у нас шансы взломать её. Сейчас было несколько проще, однако используются новые алгоритмы шифрования, изменена защита Keychain, новые структуры данных… список велик. Большинство из этого мы делали и раньше во времена iOS 4, но новая версия системы поставила некоторые неожиданные задачи.”*

Системное хранилище паролей (keychain) содержит значительное количество информации, которая особенно ценна для компьютерных криминалистов. Эта информация включает учётные записи к сайтам, пароли доступа к беспроводным сетям, пароли к электронной почте и приложениям и многое другое. Принимая во внимание новое шифрование, использованное в iOS 5 для защиты ключей, Elcomsoft iOS Forensic Toolkit является первой коммерчески доступной программой, предоставляющей полную восстановление keychain-а.

Восстановление большинства данных keychain-а требует знания пароля к устройству. Elcomsoft iOS Forensic Toolkit может восстановить пароль с помощью атаки методом «грубой силы», который в данном случае достаточно эффективен.

Предыстория

Специалисты судебно-криминалистической экспертизы хорошо знают о том, какое количество ценной информации хранится в устройствах на базе iOS (iPhone и других). Пользователи iPhone накапливают в своих смартфонах огромное количество важных данных. Помимо (очевидно полезных) фотографий, электронной почта и SMS-сообщений, смартфоны iPhone соодержат дополнительную пользовательскую информацию, такую как хронологические данные геолокации, просмотренные в Google карты и маршруты, веб-страницы, записи о вызовах, учётные записи (имена пользователей и пароли), а также почти все, что когда-либо набиралось на виртуальной клавиатуре iPhone.

Часть этих данных (но далеко не все) хранится в резервных копиях iPhone, которые создаются в Apple ITunes. Тем не менее, объем информации, которую можно извлечь из резервных копий телефона, существенно ограничен.

Физическое извлечение данных происходит при помощи использования сохраненного содержимого устройства, что позволяет выполнить всестороннее исследование пользовательских и системных данных, хранящихся в устройстве. Физический анализ данных обеспечивает доступ к гораздо большему объёму информации (по сравнению с резервной копией), а также предлагает исследователям ряд дополнительных преимуществ, не доступных при анализе файлов резервной копии. До Elcomsoft iOS Forensic Toolkit расшифровка зашифрованных образов устройства была просто невозможна, с паролем или без него. Последняя версия Elcomsoft iOS Forensic Toolkit извлекает данные примерно за 20 минут для 16-гигабайтной модели iPhone 4 (соответственно в два раза дольше для модели с 32 ГБ).

О программе Elcomsoft iOS Forensic Toolkit

Elcomsoft iOS Forensic Toolkit предоставляет доступ к зашифрованной информации, хранящейся в популярных устройствах Apple, работающих под управлением iOS 3.x, 4.x и iOS 5. Выполняя копирование данных напрямую с устройства, программа обеспечивает быстрый доступ ко всей защищенной информации, включая сообщения, электронную почту, историю звонков, контакты, данные органайзера, историю просмотра веб-страниц, голосовую почту, учетные записи и настройки электронной почты, сохранённые учётные записи (включая пароли), историю перемещений, а также пароль к резервной копии. Программа также может проводить логическое извлечение данных (на уровне файловой системы).

Наличие и стоимость

Elcomsoft iOS Forensic Toolkit уже в продаже. Доступ к программе предоставляется преимущественно экспертам правоохранительных органов и государственным учреждениям. Стоимость предоставляется по запросу; обладателям других продуктов компании предоставляются скидки.

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 .

Elcomsoft iOS Forensic Toolkit поддерживает Windows (XP, Vista, Windows 7, Server 2003 и Server 2008), а также MacOS X (10.6 'Snow Leopard' и 10.7 'Lion'), и предоставляется экспертам правоохранительных органов. Более погдробная информация доступна на сайте http://www.elcomsoft.ru/eift.html