Elcomsoft Password Digger: расшифровка паролей из защищённого хранилища Mac OS Keychain

Москва, Россия – 16 сентября 2015 - Компания «Элкомсофт» представляет новый инструмент для мобильной криминалистики Elcomsoft Password Digger. Новый продукт расшифрует содержимое системных и пользовательских защищённых хранилищ паролей, используемых в компьютерах под управлением Mac OS X, извлечёт пароли и сохранит их в виде файла XML. Программа может сохранять пароли пользователя в текстовый файл, который можно использовать в качестве словаря для ускорения перебора паролей соответствующими инструментами.

Keychain: защищённое хранилище в Mac OS

Mac OS X – одна из немногих операционных систем, предлагающих удобный и безопасный инструмент для хранения и управления паролями пользователя. Защищённое хранилище Keychain появилось в версии Mac OS 8.6, и используется по сей день в современных версиях операционной системы.

В Mac OS есть два типа защищённых хранилищ: системное, в котором сохраняются пароли, общие для всего компьютера (к примеру, пароль к точке доступа Wi-Fi), и пользовательское, в котором хранятся все остальные пароли.

В пользовательском keychain хранятся пароли от веб-сайтов, социальных сетей, учётной записи Apple ID, сессий VPN, RDP, FTP и SSH, почтовых клиентов (включая популярные Gmail и Microsoft Exchange), сетевых ресурсов и документов iWork. Сторонние приложения (к примеру, программы мгновенного обмена сообщениями) также хранят учётные данные пользователя в защищённом хранилище keychain.

Извлечение паролей из защищённого хранилища открывает доступ к огромному массиву информации, представляющей высокую ценность для криминалистов. К примеру, использование пароля от учётной записи Apple ID открывает доступ к данным из «облачных» резервных копий устройств под управлением iOS (телефонов iPhone, планшетов iPad). Для извлечения данных из «облачного» сервиса iCloud требуется продукт Elcomsoft Phone Breaker.

Для доступа к паролям из защищённого хранилища Apple предлагает встроенный инструмент – программу Keychain Access. Пользоваться инструментом во время расследования неудобно, т.к. Keychain Access требует ручного ввода пароля для просмотра каждой из множества записей. Elcomsoft Phone Breaker позволяет автоматизировать процесс, извлекая всё содержимое защищённого хранилища и сохраняя его в файл XML.

Извлечение данных из защищённого хранилища

С помощью Elcomsoft Password Digger данные извлекаются из защищённого хранилища Mac OS, расшифровываются и сохраняются в файл XML для последующего анализа. В файл сохраняются все пароли и сопутствующие данные включая URL, дату создания и последнего доступа к записи.

Elcomsoft Password Digger работает на компьютерах под управлением Windows. Для расшифровки защищённого хранилища Mac OS требуется наличие самого файла keychain, а также дополнительной информации. Для расшифровки системного хранилища потребуется файл-ключ, который нужно будет скопировать с компьютера пользователя (потребуется администраторский доступ). Для расшифровки пользовательского хранилища потребуется указать пароль для компьютера либо пароль keychain, если он отличается от основного пароля пользователя.

Словарь для перебора паролей
Перебор паролей – чрезвычайно медленный процесс. Такие продукты, как Microsoft Office 2010-2013 шифруют документы с помощью стойких алгоритмов, затрудняющих и замедляющих перебор. Даже с использованием аппаратного ускорения с применением видеокарт последних поколений, скорость перебора паролей к документам в форматах последних версий офиса не превышает 20,000 паролей в секунду. Существенно увеличить вероятность успешной атаки позволяет атака по словарю.

С помощью Elcomsoft Password Digger можно создать чрезвычайно релевантный словарь, содержащий все пароли, сохранённые пользователем на компьютере. С помощью такого словаря программы класса Elcomsoft Distributed Password Recovery могут существенно увеличить вероятность успешной атаки. Словарь создаётся путём экспортирования извлечённых данных в текстовый файл, который содержит только пароли без метаданных.

О продукте Elcomsoft Password Digger
Elcomsoft Password Digger предоставляет криминалистам доступ к паролям пользователя, сохраняемым в зашифрованном виде в безопасном хранилище keychain на компьютерах под управлением операционной системы Mac OS X. Информация извлекается из защищенных системных и пользовательских хранилищ. Для расшифровки системного хранилища требуется извлечь с компьютера пользователя файл-ключ, путь к которому указывается программой. Расшифровка пользовательского хранилища требует ввода пароля от учётной записи пользователя (либо отдельного пароля keychain, если таковой установлен).

С помощью Elcomsoft Password Digger извлекаются все виды паролей, включая пароли веб-сайтов, пароль от учётной записи Apple ID, пароли к серверам VPN, RDP, FTP и SSH, пароли к таким почтовым приложениям как Gmail и Microsoft Exchange, пароли к сетевым соединениям и документам iWork. Данные могут экспортироваться либо полностью в файл XML, либо сохраняться в текстовом файле в отфильтрованном виде. Текстовый файл может быть использован в качестве пользовательского словаря для ускорения перебора паролей соответствующими программами (к примеру, Elcomsoft Distributed Password Recovery).

Пароль от учётной записи Apple ID позволит пользователям продукта Elcomsoft Phone Breaker извлекать резервные копии данных, создаваемые устройствами Apple iPhone/iPod/iPad при синхронизации с «облаком» iCloud. Доступ к самим устройствам при этом не требуется.

Программа Elcomsoft Password Digger устанавливается и работает на компьютерах под управлением операционной системы Windows.

Стоимость и редакции
В продаже доступна базовая редакция продукта (11995руб.). Для работы Elcomsoft Password Digger установка Apple iTunes не требуется.

Системные требования
Elcomsoft Password Digger совместим с 32- и 64-разрядными версиями Windows XP, Vista, Windows 7, 8 и 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