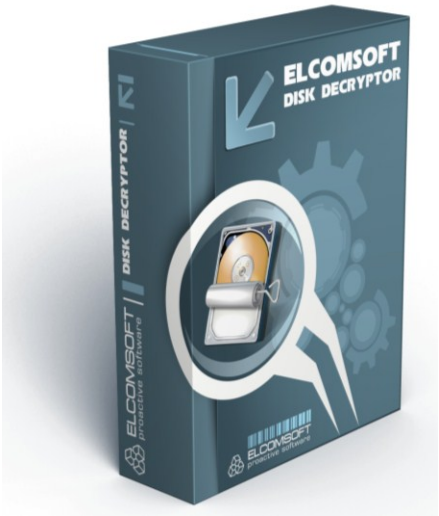
ElcomSoft вскрывает защиту криптоконтейнеров BitLocker, PGP и TrueCrypt



Москва, Россия, 20 декабря 2012 - Компания ElcomSoft Co.Ltd. разработала продукт для расшифровки информации, хранящейся в динамических криптоконтейнерах BitLocker, PGP и TrueCrypt. Новый продукт компании Elcomsoft Forensic Disk Decryptor предназначен для расшифровки содержимого трёх самых популярных криптоконтейнеров. Продукт позволяет снимать защиту мгновенно, извлекая необходимые для расшифровки ключи из слепка оперативной памяти компьютера или файла гибернации и расшифровывая данные «на лету».

Elcomsoft Forensic Disk Decryptor представляет интерес для следователей, криминалистов и экспертов, позволяя проводить криминалистический анализ хранящихся в защищённых томах данных. ElcomSoft гарантирует целостность и неизменность извлечённых с помощью Elcomsoft Forensic Disk Decryptor данных.

«*Все три криптоконтейнера обеспечивают действительно стойкую защиту*», говорит Андрей Малышев, криптоаналитик компании ElcomSoft. «*Но даже самым устойчивым ко взлому продукту никто не будет пользоваться, если пользоваться им неудобно. Неизбежные компромиссы, на которые пришлось пойти разработчикам BitLocker, PGP и TrueCrypt, являются тем самым слабым звеном, которое мы смогли использовать для снятия защиты.*»

"*До появления Elcomsoft Forensic Disk Decryptor с зашифрованными дисками работал только Elcomsoft Distributed Password Recovery*", говорит Юрий Коненков, ведущий крипто-аналитик компании ElcomSoft. "*Программа использовала метод прямого перебора пароля. Сегодня мы представляем специальный инструмент, который использует совершенно иной подход к расшифровке дисков, защищенных с помощью PGP, True Crypt, BitLocker и BitLocker To Go. Кроме того, мы добавили возможность перебора паролей к контейнерам TrueCrypt и BitLocker To Go в программу Elcomsoft Distributed Password Recovery.*"

ElcomSoft также добавляет поддержку True Crypt и BitLocker To Go в программу Elcomsoft Distributed Password Recovery для восстановления текстовых паролей, защищающих зашифрованные контейнеры с помощью ряда современных атак, включая атаку по словарю с мутациями, атаку по маске и прямой перебор паролей.

Принцип работы Elcomsoft Forensic Disk Decryptor

С помощью Elcomsoft Forensic Disk Decryptor можно как полностью расшифровать всё содержимое защищённого тома целиком, так и получать выборочный доступ к данным в режиме реального времени. В этом режиме зашифрованные тома подключаются в виде отдельных дисков, а необходимые данные расшифровываются «на лету». Режим выборочного доступа позволяет следователям получить доступ к важным материалам максимально оперативно.

Ключи, необходимые для расшифровки данных, хранятся в оперативной памяти компьютера – это необходимо для возможности получения доступа к файлам самими программами-криптоконтейнерами. Эти ключи сохраняются в файл гибернации в момент выключения компьютера (а точнее – перевода в спящий режим). Существует масса продуктов, способных снять слепок памяти работающего компьютера. Elcomsoft Forensic Disk Decryptor способен извлечь необходимые для расшифровки данных ключи из файлов гибернации и слепков оперативной памяти, созданных любой криминалистической программой, а также полученных методом атаки через порт FireWire.

Для корректной работы программы в момент снятия образа оперативной памяти (или в момент «засыпания» компьютера) криптоконтейнер должен быть подключен. В противном случае ключи расшифровки данных моментально уничтожаются, и зашифрованные диски не могут быть расшифрованы без знания оригинального текстового пароля, вводимого пользователем в момент подключения защищённого диска.

О продукте Elcomsoft Forensic Disk Decryptor

Elcomsoft Forensic Disk Decryptor позволяет криминалистам получить доступ к содержимому зашифрованных томов, созданных криптоконтейнерами BitLocker, PGP и TrueCrypt, позволяя полностью расшифровать данные или подключать защищённые тома для оперативного доступа с расшифровкой файлов «на лету». Ключи, необходимые для расшифровки защищённой информации, извлекаются из слепков оперативной памяти компьютера, полученных с использованием одной из множества специализированных программ либо методом атаки через порт FireWire. Для выключенных компьютеров поддерживается извлечение ключей из файлов гибернации.

Системные требования

Elcomsoft Forensic Disk Decryptor поддерживает 32- и 64-разрядные версии Windows XP, Vista, Windows 7, 2003 и 2008 Server. Программой поддерживаются как фиксированные, так и портативные носители, включая PGP в режиме шифрования всего диска и также флеш-карты, защищённые с помощью BitLocker To Go.

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

Более подробная информация доступна по адресу http://www.elcomsoft.ru/efdd.html