Противодействие взлому

Шифрование не панацея!

Владимир Безмалый

Сегодня сотрудники многих компаний в своей работе широко используют ноутбуки. Вместе с тем стоит признать, что эти устройства так же регулярно воруют и теряют. Так, по данным исследования Ponemon Institute, только в Европе потери компаний составляют более 1 млрд евро из-за украденных ноутбуков. В исследовании принимали участие 275 крупных организаций из Европы. В результате было установлено, что ими было утрачено 72 789 ноутбуков на протяжении 12 месяцев, в среднем — 265 ноутбуков на каждую компанию. Большая часть из них была потеряна во время поездок (32%) или во время работы за пределами офиса (32%). В 13% случаев потеря ноутбука имела место в рабочей обстановке. Еще в 13% случаев респонденты не смогли уточнить, где именно они потеряли свои ноутбуки... Отмечается, что лишь 4,5% утраченных ноутбуков возвращались к владельцам.

Большинство потерянных устройств содержали конфиденциальную информацию и личные данные. Таким образом, убытки из-за каждой потери ноутбука значительно превышают стоимость нового устройства. В результате выяснилось, что 275 опрошенных организаций в Европе ежегодно теряют около 1,29 млрд евро из-за утраченных ноутбуков, что составляет около 4,7 млн евро на каждую из них.

В прошлом году проводилось аналогичное исследование и в США. Тогда было опрошено 329 организаций, которыми было утеряно более 86 тыс. ноутбуков, а совокупная величина финансовых потерь составила 2,1 млрд долл.

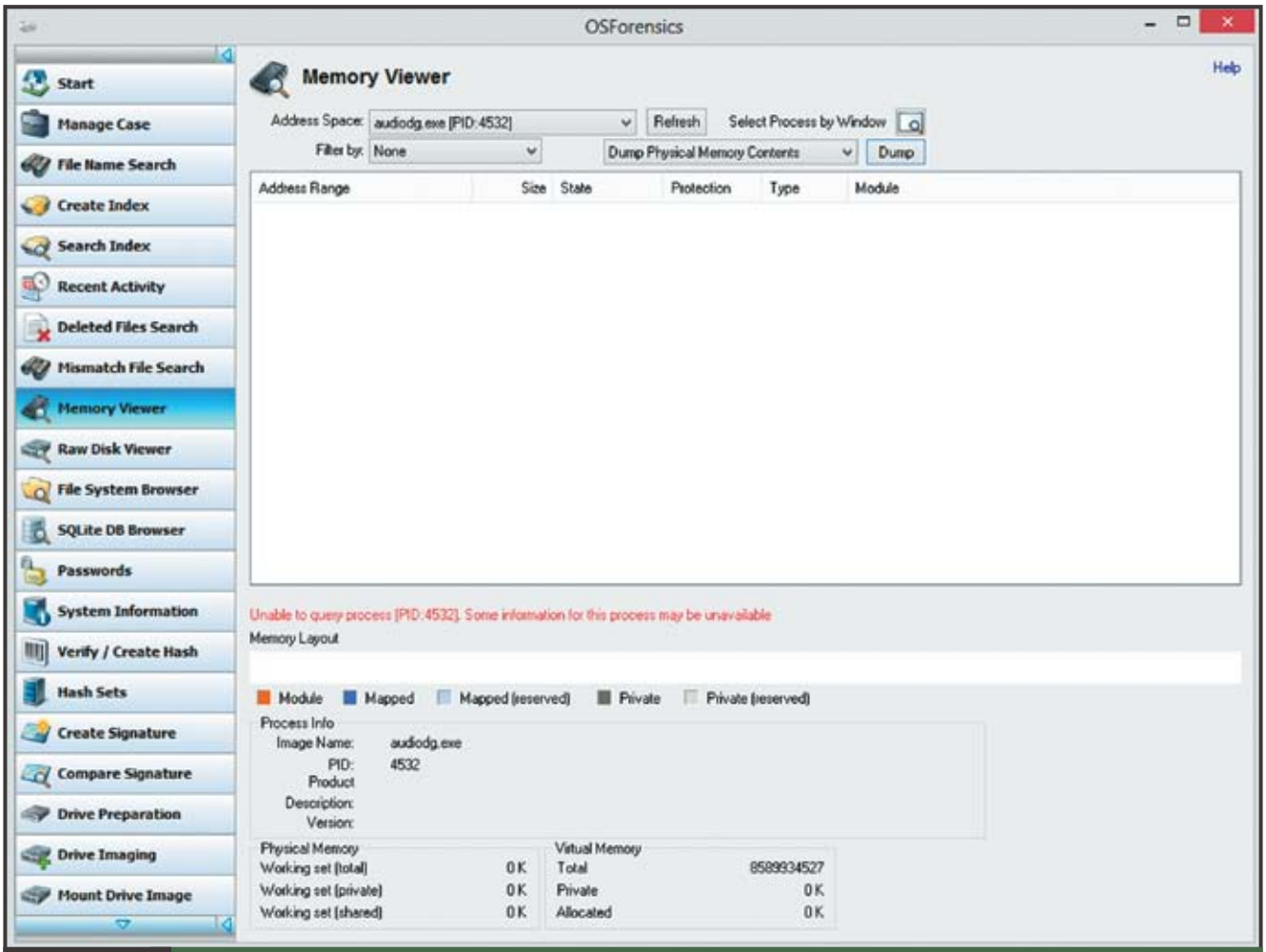
Таким образом, можно сделать вывод о том, что проблема безопасности информации, хранящейся на мобильных устройствах, приобретает угрожающий характер. Что можно представить в качестве последней линии физической защиты? Шифрование. А является ли шифрование панацеей?

Рассмотрим новый продукт компании Elcomsoft — Elcomsoft Forensic Disk Decryptor, который предназначен для расшифровки криптоконтейнеров алгоритмов шифрования BitLocker, PGP и TrueCrypt и проведения анализа хранящихся в зашифрованных томах данных. Поддерживаются как фиксированные, так и портативные носители, включая PGP в режиме шифрования всего диска, а также съемные диски, защищенные с помощью BitLocker To Go. При этом с помощью данного продукта можно как полностью расшифровать содержимое защищенного тома, так и работать в реальном времени с подключением зашифрованных томов (носителей) и расшифровкой данных «на лету».

Перечислим возможности продукта.

- Расшифровка информации, защищенной тремя самыми распространенными криптоконтейнерами.
- Поддержка защищенных томов BitLocker, PGP и TrueCrypt.
- Поддержка портативных носителей и флэш-карт, защищенных BitLocker To Go.
- Поддержка всех режимов работы PGP, включая режим шифрования всего диска.
- Доступ в режимах реального времени и полной расшифровки.
  - Извлечение ключей расшифровки данных из файлов гибернации, файла-образа оперативной памяти компьютера.
  - Извлекает все ключи из дампа оперативной памяти единовременно, даже если в системе имеется более одного криптоконтейнера.

ИЛЛЮСТРАЦИЯ APOPS© – FOTOLIA.COM



Экран 1 Получение слепка памяти

- Гарантия целостности и неизменности исследуемых данных.
- Восстановление и сохранение ключей расшифровки данных.
- Поддержка 32- и 64-разрядных версий Windows.

Следует отметить, что Elcomsoft Forensic Disk Decryptor извлекает ключи, с помощью которых были зашифрованы данные. С помощью этих ключей расшифровка осуществляется в реальном времени — практически мгновенно. Продукт поддерживает три метода извлечения ключей расшифровки:

- анализ файла гибернации (исследуемый компьютер выключен);
- анализ слепка оперативной памяти компьютера, при этом слепок памяти может быть создан с помощью соответствующих криминалистических продуктов;
- атака через порт FireWire (компьютер должен быть включен, а зашифрованные тома — подключены); для проведения атаки через порт FireWire требуется дополнительный компьютер с установленным бесплатным продуктом (например, Inception).

Извлечение ключей для расшифровки данных

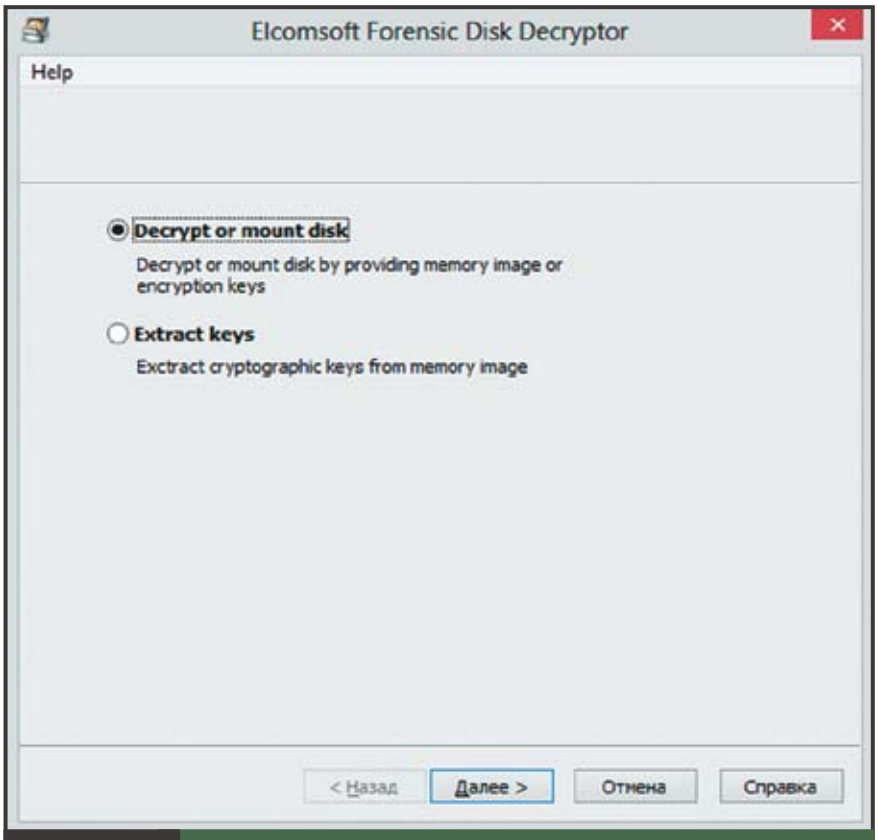
Для получения слепка памяти я использовал программное обеспечение OSForensics (http://www.osforensics.com; см. экран 1).

Далее из полученного слепка памяти можно получить ключ расшифровки. Здесь мы используем атаку на оперативную память, описанную в материалах Microsoft еще несколько лет тому назад.

Ключ расшифровки необходим для получения доступа к зашифрованным данным и расшифровки содержимого криптоконтейнера. Elcomsoft Forensic Disk Decryptor поддерживает три метода извлечения ключей, выбор зависит от того, включен или выключен исследуемый компьютер, а также от того, существует ли возможность запустить на исследуемом компьютере программу для снятия образа («слепка») оперативной памяти. Рассмотрим все варианты.

Компьютер выключен. В этом случае ключи извлекаются из файла гибернации. Защищенные тома должны быть подключены перед выключением компьютера. Если криптоконтейнер был размонтирован перед созданием файла гибернации, извлечь из него ключи будет невозможно.

Компьютер включен. При возможности на исследуемом компьютере запускается программа для снятия слепка оперативной памяти. Содержимое оперативной памяти сохраняется в файл, из которого Elcomsoft Forensic Disk Decryptor извлекает ключи расшифровки.



Экран 2 Стартовое окно программы Elcomsoft Forensic Disk Decryptor

Зашифрованные тома в момент снятия слепка должны быть подключены; в противном случае ключ расшифровки извлечь не удастся. Подробное описание этой технологии и полный список как коммерческих, так и бесплатных программ доступны по адресу http://www.forensicswiki.org/wiki/Tools: Memory_Imaging.

Компьютер включен в режиме ограниченного доступа. Если запуск программ на исследуемом компьютере невозможен (не хватает прав, нет пароля от учетной записи пользователя и т. д.), извлечение ключей возможно посредством проведения атаки через порт FireWire. Атака производится с отдельного компьютера или ноутбука, подключенного к исследуемому компьютеру по интерфейсу FireWire. Для проведения атаки используется бесплатная утилита, устанавливаемая отдельно (например, Inception, по ссылке http://www.breaknenter.org/projects/inception/). Данный вид атаки дает результат, близкий к стопроцентному. Зашифрованные тома на момент атаки должны быть подключены. После извлечения ключи расшифровки сохраняются в базе данных, затем Elcomsoft Forensic Disk Decryptor предложит провести полную расшифровку содержимого криптоконтейнера или подключить защищенные тома в виде новых дисков для расшифровки «на лету» (см. экран 2).

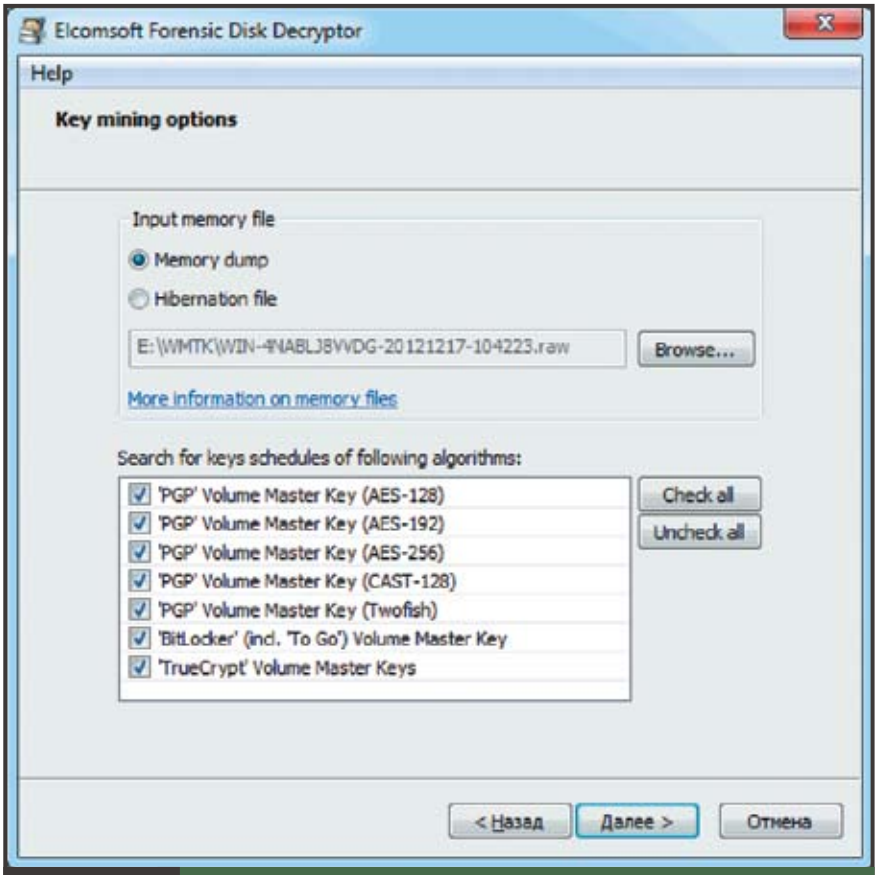
После указания режима Extract keys мы должны уточнить, какой именно ключ будем искать (экран 3).

Всегда ли поиск ключей будет эффективным? На самом деле нет.

Методы противодействия

Если вы применяете BitLocker и внимательно читали рекомендации Microsoft по использованию режима шифрования BitLocker, то должны были запомнить, что:

- не рекомендуется шифровать диски данных до того как вы зашифруете системный диск;
- по окончании работы компьютер рекомендуется выключать,



Экран 3 Поиск ключей в файле дампа памяти

а не использовать режим сна или гибернации.

Вы никогда не задавались вопросом, а почему так? Причины на самом деле просты.

1. Если вы шифруете только диск данных, да еще при этом используете гибернацию, ваш ключ шифрования можно извлечь из файла гибернации, который будет находиться на незашифрованном системном разделе.
2. Если даже оба раздела зашифрованы, но вы используете гибернацию, ваш компьютер, пробудившись, не будет спрашивать пароль BitLocker, а сразу запросит ваш пароль пользователя. Большинство предпочитает беспарольную учетную запись, да еще с правами локального администратора. А кто мешает снять дамп памяти? Никто! А следовательно, злоумышленник просто может получить ваши ключи шифрования.

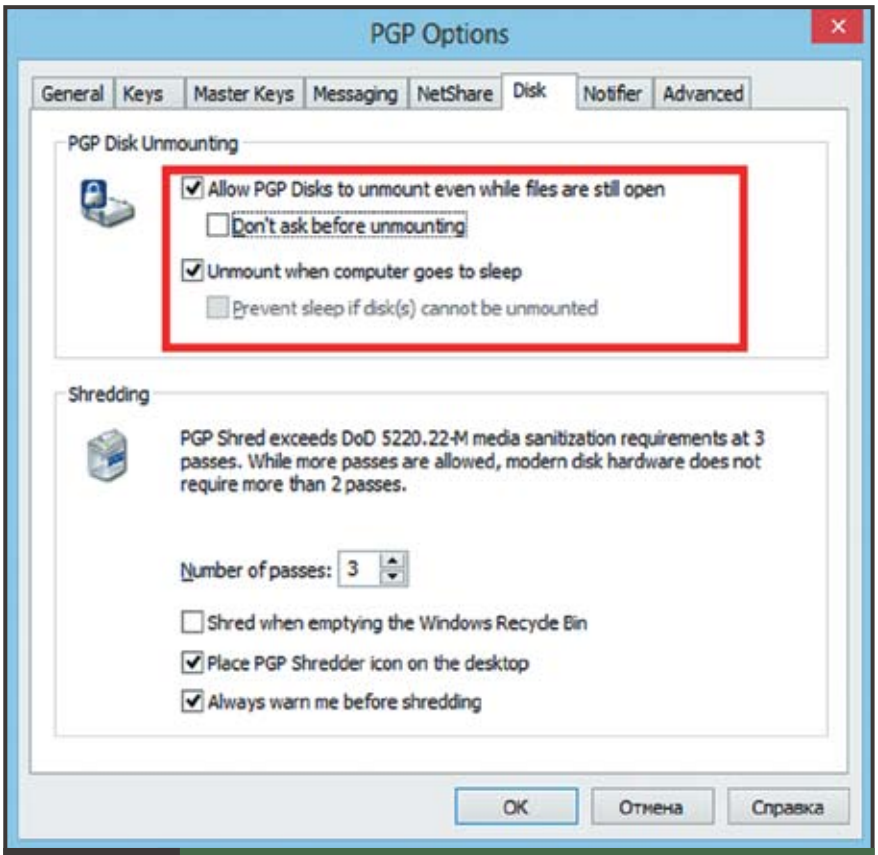
При использовании алгоритма PGP для противодействия взлому пользователь может предусмотреть принудительное отключение зашифрованных дисков и криптоконтейнеров (экран 4). Но все ли это делают?

Не забудьте об этой настройке, и ваш компьютер будет куда сложнее взломать.

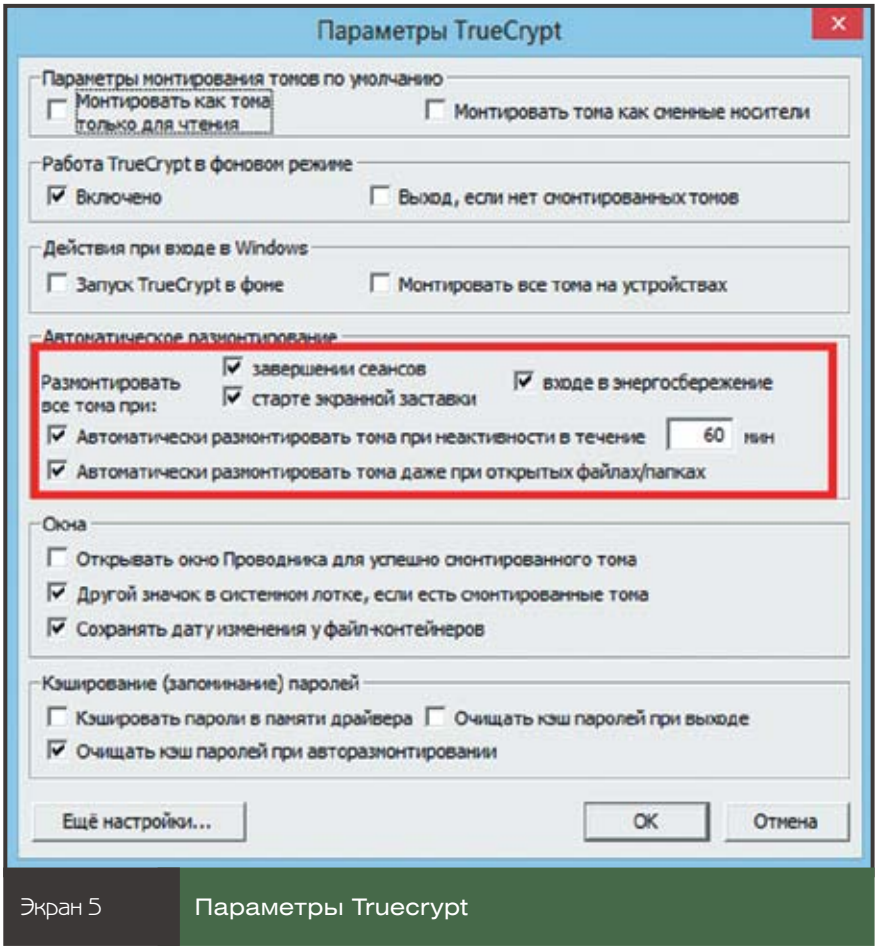
Truecrypt пользуется заслуженным уважением, но и с ним, перед тем как включить шифрование, не забудьте зайти в настройки и установить флажки у отмеченных на экране 5 параметров.

Вместе с тем необходимо учесть, что если заряд батареи ноутбука чрезвычайно мал и происходит автоматический переход в режим энергосбережения, то тома могут быть не размонтированы автоматически! Поэтому внимательно следите за уровнем заряда батарей.

Надеюсь, эти несложные рекомендации помогут вам обеспечить безопасность вашей информации.



Экран 4 Экран настроек PGP



Экран 5 Параметры Truecrypt

Владимир Безмалый (vladb@windowslive.com) — специалист по обеспечению безопасности, имеет звания MVP Consumer Security, Microsoft Security Trusted Advisor