9. Жданов А. А., Устюжанин А. Е. Возможности использования технологии детерминированного хаоса в системах автономного адаптивного управления // Сб. трудов ИСП РАН. – 2001. – С. 141–180.
10. Андреев Ю. В., Бельский Ю. Л., Дмитриев А. С. Запись и восстановление информации с использованием устойчивых циклов двумерных и многомерных отображений // Радиотехника и электроника. – 1994. – Т. 39. – С. 114–123.
11. Andreyev Yu. V. Dmitriev A. S., Kuminov D. A. Pavlov V. V. Information processing in 1-d and 2-d map: recurrent and cellular neural networks implementation, CNNA'96, Seville, Spain, 1996.
12. Guttman A., 'R-trees: A Dynamic Index Structure for Spatial Searching', Proc. ACM SIGMOD Int. Conf. on Data Management, Boston, MA, 1984. – P. 47–57.
13. Lars Arge, Mark de Berg, Herman Haverkort, Ke Yi. The Priority R-Tree: A Practically Efficient and Worst-Case Optimal R-Tree. In Proc. of the 2004 ACM SIGMOD International Conference on Management of Data (SIGMOD '04), Paris, France, June 2004. – P. 347–358.

Статья поступила в редакцию 26.09.2006

УДК 004.056.53

А. А. Кузнецов

СПОСОБЫ КАМУФЛИРОВАНИЯ ВИРТУАЛЬНЫХ ДИСКОВ

Рассмотрены методы обнаружения шифрованных виртуальных дисков и способы их камуфлирования.

Виртуальный диск представляет собой файл-контейнер, сформированный на жестком диске компьютера, который используется для хранения конфиденциальной информации в зашифрованном виде. Специальная программа при введении установленного пароля может подключать файл-контейнер к операционной системе таким образом, чтобы он был виден для приложений как обычный диск, и обеспечивать шифрование "на лету" всей переносимой на него информации [1].

Таким образом, виртуальный диск, с одной стороны, обеспечивает произвольный доступ к данным, с другой стороны, хранит их в едином защищенном контейнере, что упрощает задачу камуфлирования данных. Сокрытие самого факта наличия секретной информации является одной из основных задач при использовании виртуальных дисков. Кроме того, многие приложения создают на жестком диске временные файлы, которые могут содержать конфиденциальную информацию. Создание же временных файлов на виртуальном диске позволит предотвратить хранение секретных данных в открытом виде.

Использование виртуальных дисков удобно при хранении секретной информации на локальном компьютере и целесообразно при переносе больших объемов информации между удаленными компьютерами, не имеющими выхода в сеть по соображениям безопасности.

О возможности присутствия в компьютере секретной информации может свидетельствовать ряд признаков, привлекающих внимание заинтересованных лиц и побуждающих их к тщательному поиску размещенного на жестком диске файла-контейнера. Рассмотрим эти признаки и варианты их устранения поподробнее.

Наличие программы для работы с виртуальными дисками. Естественным способом демонстрации отсутствия программы для управления виртуальными дисками на компьютере является удаление как ее самой, так и ее инсталляционных файлов, либо их сокрытие путем камуфлирования. Это легко осуществить, например, простым переименованием инсталляционного файла и сменой его расширения, либо путем размещения его среди исполняемых файлов установленных в компьютере программ или операционной системы.

Второй вариант предусматривает хранение инсталляционного файла программы в сети или на одном из CD дисков (естественно, среди множества других программ).

Спрятав инсталляционный файл, можно в любой момент либо деинсталлировать программу для работы с виртуальными дисками обычным образом, либо выполнить ту же операцию с помощью нескольких горячих клавиш, предусмотренных в некоторых программах.

Наличие на жестком диске крупных файлов, не открывающихся имеющимися в компьютере программами, позволяет идентифицировать такие файлы, как предполагаемые файлы-контейнеры.

В этом случае существует несколько способов сокрытия существования виртуальных дисков в компьютере.

1. Самым очевидным решением при появлении опасности является удаление файла-контейнера. Такое поведение является вполне разумным при наличии резервных копий скрываемой информации, хранящихся в надежном месте. Однако при традиционном удалении файла сама информация, находившаяся в нем, на жестком диске остается. Ее можно легко восстановить, определить, что восстановленный файл — виртуальный диск и потребовать у пользователя пароль для работы с обнаруженным диском [2].

Это означает, что необходимо также физически удалить эту информацию с жесткого диска. Существуют специальные программы — шредеры, которые позволяют затереть информацию в файлах перед их

удалением. Однако они не способны справиться с задачей затирания файла размером в несколько гигабайт за считанные секунды [3].

Поэтому при уничтожении виртуальных дисков рекомендуется применять следующий прием: для выработки ключа шифрования используется не только пароль, вводимый пользователем, но и модификатор ключа шифрования [4]. Он должен быть таким, чтобы даже при знании правильного пароля невозможно было его подобрать. Для этого следует использовать модификаторы размером порядка 128. . . 192 бит. При необходимости срочного предотвращения доступа к виртуальному диску нажатие "горячих клавиш" приводит к затиранию встроенным шредером этого модификатора, после чего файл-контейнер удаляется уже обычным образом. Без модификатора ключа, который был надежно уничтожен, даже при наличии правильного пароля восстановить зашифрованную информацию оказывается невозможно.

2. Другим решением является сокрытие наличия на диске файлов-контейнеров методами стеганографии. Иными словами, размещение файла-контейнера, скажем, в серии изображений, сборнике музыкальных записей или в аудиокниге. Изображение в формате BMP может практически без потери качества содержать до трети своего объема дополнительной информации, необходимое для хранения файла-контейнера дисковое пространство превышает его размеры в этом случае примерно в 3 раза [5, 6].

Такой способ может быть совсем неплох для использования в домашних условиях, когда количество скрываемой информации сравнительно невелико, однако наличие большого количества репродукций галерей Эрмитажа на рабочем компьютере может вызвать вполне законное подозрение.

3. Третьим вариантом является камуфлирование файла-контейнера путем его модификации и размещения среди большого количества других подобных файлов. Существует множество различных форматов данных. Можно дать файлу-контейнеру имя с расширением, скажем, DOC или XLS, а затем разместить его среди подобных файлов (удобным местом является, например, системный каталог Windows, где находится порядка тысячи файлов с расширением DLL). При попытке открыть такой файл он будет казаться просто поврежденным. Однако этой меры зачастую бывает недостаточно. При просмотре файлов стандартных форматов с помощью простых текстовых редакторов (таких как блокнот, или редактор файлового менеджера Far) можно легко обнаружить, что большинство из них имеют стандартные заголовки, находящиеся в начале файла. Отсутствие такого заголовка и может привлечь внимание к скрываемому файлу-контейнеру.

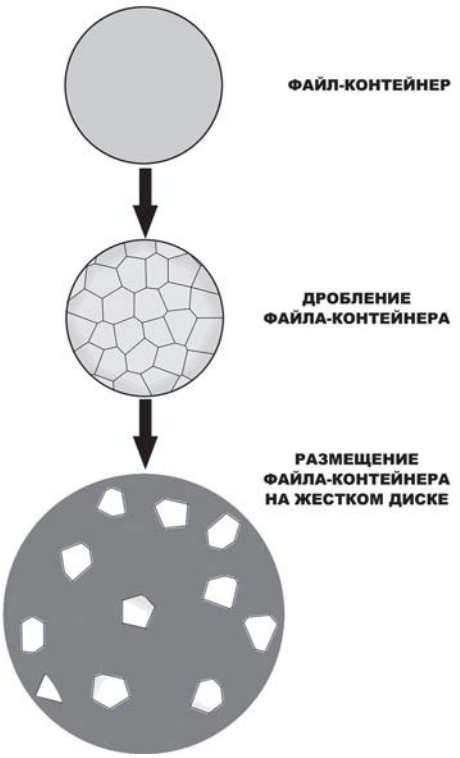

Рис. 1. Фрагментация виртуального диска

Чтобы файл-контейнер не привлекал внимания своими размерами, его разбивают на множество небольших файлов-фрагментов (рис. 1). Один или несколько файлов в этом случае представляют собой каталог размещения секторов виртуального диска по файлам.

Параметры такого виртуального диска оцениваются следующим образом:

$$S_{\text{д}} = S_{\text{ф}} \frac{S_{\text{к}}}{S_{\text{з}}},$$

где $S_{\text{д}}$ — размер виртуального диска; $S_{\text{к}}$ — размер файла-каталога; $S_{\text{ф}}$ — средний размер одного файла, принадлежащего виртуальному диску; $S_{\text{з}}$ — средний размер записи, хранящей ссылку на файл виртуального диска.

Соответственно, необходимое количество файлов для камуфлирования виртуального диска определяется как

$$C_{\text{ф}} = \frac{S_{\text{к}}}{S_{\text{з}}},$$

где $C_{\text{ф}}$ — необходимое количество файлов, содержащих элементы виртуального диска.

Таким образом, при условии $S_{\text{ф}} = S_{\text{к}} = 128$ кб возможно создание дисков размером до 512 Мб, а для его размещения требуется порядка 4000 файлов.

На рис. 2 представлена структура файла-каталога такого диска, а на рис. 3 — структура самого виртуального диска.

Чтобы файлы виртуального диска не вызывали подозрения, их можно дописывать в конец существующих документов. Тогда эти файлы будут нормально открываться, но иметь несколько больший размер.

Адрес	Ссылка
Список каталогов, в которых размещены файлы виртуального диска	
Список файлов виртуального диска	

Рис. 2. Структура файла-каталога фрагментированного виртуального диска

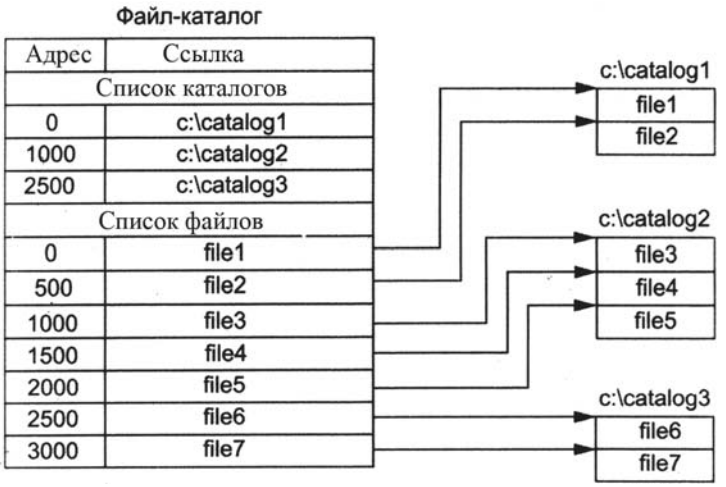

Рис. 3. Пример структуры фрагментированного виртуального диска

При этом, правда, нельзя будет такие файлы перезаписывать. Следовательно, такой способ подходит лишь при условии использования в качестве базовых файлов для виртуального диска несекретных архивных документов.

Однако на практике применение такого способа для больших контейнеров (размером несколько гигабайт) зачастую весьма затруднительно из-за необходимости хранения значительного числа архивных документов лишь в целях камуфлирования.

Необходимо учитывать, что дата создания и модификации формируемых файлов также не должна вызывать подозрений. Просмотр содержимого компьютера позволяет легко выделить файлы, время модификации которых не характерно для их окружения, и идентифицировать их как потенциально интересные для изучения. Например, системные файлы имеют определенную производителем операционной системы дату создания (часто файлы бывают созданы несколько лет назад). Если размещать файлы виртуального диска среди них, то "системный" файл, созданный на прошлой неделе, может вызвать подозрение. Следовательно, при создании и модификации таких файлов необходимо устанавливать для них даты, характерные для каталога, в котором они размещаются.

Анализ перечисленных признаков хранения секретной информации в файлах-контейнерах и средств их камуфляжа позволил сформулировать основные требования к программам, формирующим виртуальные диски, повышающие безопасность хранения информации в созданных ими файлах-контейнерах.

1. Созданный виртуальный диск должен представлять собой набор файлов-контейнеров случайного размера.

2. Файл-контейнер не должен иметь собственного заголовка, позволяющего его идентифицировать.

3. Должна быть обеспечена возможность снабжения файлов-контейнеров стандартными заголовками файлов других форматов.

4. Должна быть обеспечена возможность установки искусственных дат создания, модификации и времени последнего доступа к файлу-контейнеру.

5. Вся дополнительная информация, необходимая для работы с виртуальным диском, должна быть зашифрована паролем пользователя.

Кроме перечисленных условий, может быть также весьма полезным введение в программы для работы с виртуальными дисками режима отсроченного подтверждения пароля (при отсутствии правильно введенного пароля в течение определенного времени после загрузки системы производится автоматическое удаление заданных виртуальных дисков и самой программы). Пароль при этом должен вводиться пользователем по собственной инициативе, а не по запросу программы. Эта функция крайне необходима при существовании угрозы потери физического доступа к компьютеру с конфиденциальной информацией [7].

Тем не менее, опытный злоумышленник может проанализировать статистическое распределение содержимого файлов и выделить среди них зашифрованные участки. Рассмотрим еще один способ сокрытия виртуальных дисков, позволяющий предотвратить такую возможность. Он предназначен, главным образом, для работы с дисками большого размера (свыше гигабайта).

Контейнер может находиться в двух состояниях: рабочем и скрытом. В рабочем состоянии контейнер приписан в конец некоторого архивного файла. В кластере, следующим непосредственно за исходным файлом, сохраняется информация о физическом расположении контейнера на диске. Эта информация хранится в зашифрованном виде и используется для восстановления контейнера после скрытия. Далее размещается уже сам контейнер (его физическое расположение на диске может быть произвольным). Таким образом, исходный файл, информация о положении контейнера и сам контейнер образуют единый файл (рис. 4).

Кроме того, когда контейнер находится в рабочем состоянии, периодически с помощью шредера производится заполнение свободного пространства на жестком диске случайными данными.

Для обеспечения возможности сокрытия контейнера в любой момент времени размер исходного файла сохраняется в открытом виде

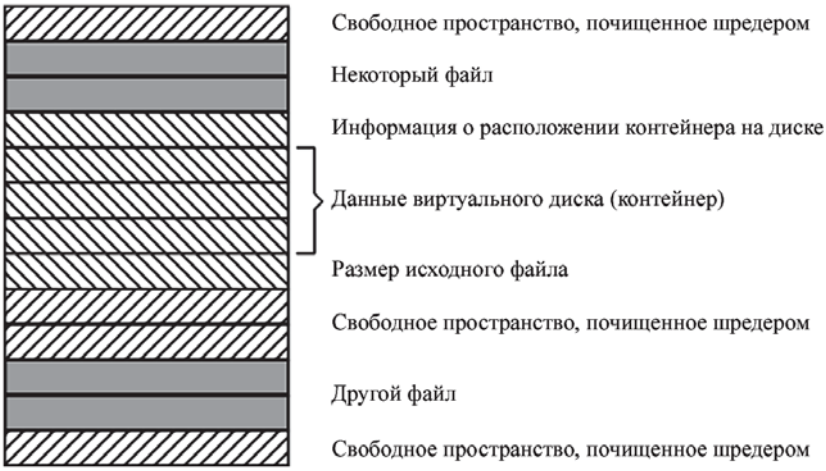

Рис. 4. Пример расположения контейнера на диске

в конце контейнера. При выполнении скрытия файл обрезается до исходного объема, а хранимый в контейнере размер затирается случайными данными. После скрытия всех контейнеров производится полная деинсталляция программы для работы с виртуальными дисками.

Таким образом, для стороннего наблюдателя контейнер на жестком диске выглядит точно так же, как и свободное пространство, заполненное случайными данными.

Для восстановления контейнера необходимо знать:

1. Файл, к которому был приписан контейнер;

2. Пароль для восстановления, с помощью которого зашифрована информация о расположении контейнера на диске (в общем случае он может отличаться от пароля, которым защищается сам контейнер).

Контейнеры желательно физически размещать не на системном диске, поскольку это снижает вероятность их случайного затирания операционной системой.

Осуществлять сокрытие контейнера можно в случае возникновения опасности, а также в конце рабочего дня перед выключением компьютера (и соответственно, восстанавливать сразу после включения). Это позволяет защищать данные как при возникновении опасности во время работы на компьютере, так и в нерабочем состоянии.

В настоящее время наиболее распространенным методом скрытия диска является физическое уничтожение ключей к нему. Этот прием имеет ряд недостатков:

- контейнер невозможно восстановить (остается только делать резервные копии);
- по содержимому диска можно определить наличие контейнера и оценить его размеры;

- если в момент возникновения опасности компьютер выключен, скрытие диска невозможно.

В отличие от традиционного, рассмотренный способ позволяет:

- скрывать и восстанавливать контейнер неограниченное число раз;
- смешивать содержимое контейнера со случайными данными на диске, что не дает возможности злоумышленнику идентифицировать его как целостный объект, содержащий зашифрованную информацию;
- скрывая контейнер перед выключением компьютера, обеспечить защиту данных даже при доступе злоумышленника в отсутствие пользователя.

Рассмотренные пути модификации программ для создания виртуальных дисков и работы с ними могут значительно повысить скрытность их использования и устойчивость защиты при появлении неблагоприятных внешних факторов.

СПИСОК ЛИТЕРАТУРЫ

1. http://www.megalib.com/books/1070/kg43106.html
2. http://infobez.net.ru/index.php?art=3
3. http://www.bnti.ru/scripts/showart.asp?lvl=&tbl=&aid=508
4. Масленников М. Е. Практическая криптография. – СПб.: БХВ-Петербург, 2003. – 464 с.
5. Кузнецов А. А. Определение предельной емкости изображений при размещении в них информации // Материалы 6-й Междунар. конф. НТИ-2002, М., ВИНИТИ, 2002 г. – С. 205–207.
6. http://anx-int.narod.ru/lek/lek7/vop3.htm
7. Кузнецов А. А. Секрет фирмы. – М.: Ось-89, 2006. – 208 с.

Статья поступила в редакцию 3.10.2006

Александр Александрович Кузнецов родился в 1983 г., окончил МГТУ им. Н.Э. Баумана в 2004 г. Аспирант кафедры “Информационная безопасность” МГТУ им. Н.Э. Баумана. Автор 30 научных работ в области защиты информации.

A.A. Kuznetsov (b. 1983) graduated from the Bauman Moscow State Technical University in 2004. Post-graduate of “Information Security” department of the Bauman Moscow State Technical University. Author of 30 publications in the field of information protection.