

Изучаем теневое копирование

Роман Васильев

Теневое копирование файлов, записываемых на внешние носители, стало практически обязательным инструментом в арсенале корпоративных хранителей секретов. Разберемся в особенностях реализации и работы этой технологии.

Ит-отделы и службы безопасности современных предприятий уже хорошо знают, какую опасность для конфиденциальных данных представляют портативные USB-устройства с возможностью

хранения данных, например, флешки, MP3-плееры, цифровые камеры и т. д. Если в организации отсутствует какой-либо контроль использования этих устройств, с их помощью нечестный или просто невнимательный пользо-

ватель может стать причиной утечки существенных объемов конфиденциальной информации. Именно поэтому программные продукты, реализующие контроль использования таких устройств в масштабах предприятия,

стали обязательным средством в арсенале борьбы за сохранение конфиденциальности информации.

На сегодняшний день известно множество программных продуктов, которые реализуют не только базовый функционал по разграничению доступа, но и дополнительные возможности, такие как журналирование и мониторинг действий пользователей, централизованное администрирование, управление через групповые политики Active Directory и т. д. В число этих возможностей у большинства продуктов включено так называемое «теневое копирование». Данная функция при условии разрешенного доступа к внешнему носителю на запись обеспечивает копирование всей информации, которую пользователь записывает на внешний носитель, сначала на локальный жесткий диск, а потом перенос ее на сервер для последующего анализа. Это может быть очень удобно в случае, если по каким-либо причинам сотруднику необходимо иметь возможность записывать информацию на внешний носитель, поскольку позволяет провести расследование возможного инцидента и сохранить контроль над ситуацией.

Данная функция реализована во многих современных продуктах, например, Safend от одноименной компании, Sanctuary Device Control компании Lumension, Smartline DeviceLock и Zlock компании SecurlIT.

Принцип работы теневого копирования довольно прост: при записи файлов на внешний носитель копия записываемых данных вместе с дополнительной информацией (имя пользователя, приложение, дата, время) сохраняется на жестком диске компьютера и в дальнейшем переносится на сервер. Затем сотрудник службы безопасности может обратиться к базе данных теневых копий и просмотреть подозрительные файлы.

Очевидно, что использование данной функции имеет ряд ограничений, поскольку массовое внедрение этой функции в крупной организации с большим числом пользователей может создать существенные проблемы.

Во-первых, если все пользователи будут копировать на внешние носители большое количество инфор-

Таблица 1. Измерение времени копирования файлов

	Без теневого копирования	DeviceLock	Zlock
Один большой файл	125 с.	150 с. (+20 %)	175 с. (+40%)
Множество маленьких файлов	760 с.	880 с. (+15 %)	935 с. (+23 %)

мации, это создаст повышенную нагрузку на сеть.

Во-вторых, для того чтобы анализировать всю эту информацию, нужно большое количество людей или какие-либо интеллектуальные автоматизированные средства, при том что задача их поиска, закупки, настройки и интеграции с системой разграничения доступа далеко не тривиальна.

В связи с этим более оправданным может быть выборочное использование теневого копирования на компьютерах отдельных сотрудников. Принцип выбора таких сотрудников может быть различным, например, для новых сотрудников во время испытательного срока, для сотрудников, в отношении которых имеются какие-либо подозрения, для каждого сотрудника одну неделю в году и т. д.

Итак, попробуем разобраться, что представляет собой теневое копирование с технической точки зрения и как оно на самом деле работает на примере двух продуктов: DeviceLock 6.3 (Build 14161) от компании SmartLine Inc. и Zlock 2.0.1.597 от компании SecurlIT.

Выбор для сравнения этих продуктов был обусловлен тем, что именно они в наибольшей степени представлены на российском рынке, тогда как другие упомянутые системы при всех их достоинствах не имеют какого-либо одного, а чаще всего нескольких из перечисленных ниже атрибутов:

- представительство на территории РФ;
- наличие технической поддержки на территории РФ;

- русскоязычный интерфейс;
- документация на русском языке.

Очевидно, что для средних и крупных компаний, для которых наиболее актуальна защита от утечек информации через внешние устройства, невыполнение перечисленных условий делает внедрение системы довольно рискованным.

Приведенные ниже тесты проводились на ноутбуке IBM ThinkPad T43p с процессором Pentium M 1.8 МГц и 1 Гб RAM, операционная система Windows XP SP2. В качестве внешнего носителя использовалась флешка Transcend JF V60 с файловой системой FAT32.

Копируем файлы

Наиболее распространенная операция с внешними носителями – копирование файлов с жесткого диска ПК или из сети. Проведем два теста: копирование большого файла (418 Мб) и множества маленьких файлов (1 072 файла общим размером 393 Мб) на флеш-накопитель. Без теневого копирования время записи составило соответственно 125 и 760 секунд. Теневое копирование Zlock увеличило время записи большого файла до 175 секунд (на 40%) и множества маленьких файлов до 935 секунд (на 23%). DeviceLock показал немного лучшие результаты – 150 (+20%) секунд для крупного файла и 880 (+15%) секунд для набора мелких файлов (см. таблицу 1).

Но нам необходимо оценить не только скорость записи данных, но и корректность работы теневого копирования. При копировании неболь-

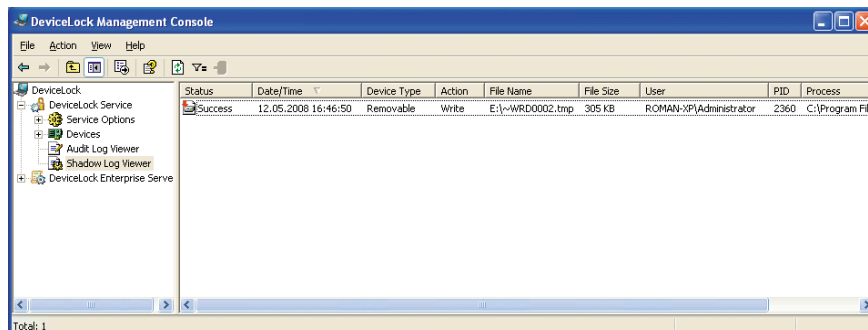


Рисунок 1. В консоли DeviceLock сохраненный файл «Секретный документ.doc» отображается как «~\WRD0002.tmp»

Закон суров, но он закон

Следует обратить внимание на один важный момент, про который часто забывают. В настоящее время Законом РФ «Об оперативно-розыскной деятельности» всем, кроме специально уполномоченных организаций, запрещается негласное получение информации с использованием специальных технических средств (ст. 6). При этом в качестве негласного получения информации может иметься в виду не только контроль телефонных переговоров сотрудников и их электронной почты, но и рассматриваемый в данной статье контроль файлов, копируемых на внешние носители. Это означает, что руководитель предприятия и/или другие должностные лица, пытаясь обеспечить свои законные права по обеспечению конфиденциальности информации, могут сами стать нарушителями закона и близко познакомиться со статьей 138 Уголовного кодекса, которая запрещает нарушение тайны переписки, телефонных разговоров и иных сообщений граждан. Для того чтобы этого не произошло, необходимо, чтобы процесс получения и конт-

роля информации по крайней мере не был негласным. Для этого, во-первых, надо приказом руководителя предприятия принять регламент использования корпоративных средств обработки и передачи информации (телефон, компьютер, сети передачи данных и т. д.), который должен запрещать их использование для обработки личной информации. Во-вторых, надо включить в этот регламент положение о том, что компания имеет право прослушивать, просматривать, архивировать и анализировать всю информацию, которая хранится, передается и обрабатывается с использованием корпоративных средств. Наконец, необходимо у каждого сотрудника получить письменное подтверждение о том, что он знаком с этим регламентом и согласен с ним. Как известно, незнание закона не освобождает от ответственности, поэтому, чтобы не иметь лишних неприятностей и не оказаться крайним, надо все эти вопросы задать руководителю компании или своему начальнику, желательно также в письменном виде, и настоять на их разрешении.

ших файлов в теневой копии все фиксируется корректно, а с файлом в 418 Мб поджидал сюрприз. Итак, в локальном каталоге Zlock теневая копия этого файла появилась сразу же при начале копирования, и ее размер увеличивался одновременно с процессом записи на накопитель. В случае с DeviceLock такого не произошло. Даже после окончания записи на флешку система продолжала активно работать с жестким диском, и копия полностью сформировалась только через 135 секунд после окончания записи.

Теперь представим, что потенциальный злоумышленник сохранит данные на внешний носитель и сразу после этого выключит компьютер, используя процедуру завершения

Windows. В случае с большим файлом при теневом копировании DeviceLock в локальном хранилище обнаружилась теневая копия размером всего лишь 30 Мб, а это 7% от общего объема файла. А что, если не пользоваться процедурой завершения Windows, а нажать RESET сразу после окончания записи на носитель? Рассмотрим это в конце статьи, а пока продолжим изучать работу теневого копирования в штатных ситуациях.

Работа приложений

В качестве набора тестовых приложений был взят широко распространенный пакет MS Office 2003. Для каждого приложения из списка было проведено два теста: сохранение документа на флешку с помощью команды «Сохранить как» и модификация существующего файла на носителе.

Word

Как при создании нового файла, так и при модификации имеющегося документа с именем «Секретный документ.doc», при просмотре теневых ко-

пий в консоли DeviceLock отображались файлы с именем вида «-WRD0002.tmp» (см. рис. 1), в то время как в консоли Zlock имена документов отображались корректно (см. рис. 2).

Excel

У DeviceLock ситуация с Excel не сильно отличается от Word: теневые копии с именем вроде «FBAD1000» могут существенно затруднить анализ журнала теневого копирования. При этом в некоторых случаях вместо приложения Excel в журнале теневого копирования был зафиксирован процесс explorer (проводник Windows). С Zlock подобных проблем не наблюдалось.

PowerPoint

Правка находящегося на USB-флешке файла с презентацией PowerPoint отобразилась в DeviceLock как изменение файла ppt1d.tmp, что не соответствует действительности. У Zlock все в порядке.

Access

Создание базы данных на носителе отображается в обоих продуктах, но при изменении БД у DeviceLock возникли серьезные проблемы. Дело в том, что правка каких-либо таблиц и последующее сохранение документа не фиксируется вовсе! В теневых копиях фигурирует только файл с расширением .ldb – это служебный файл Access. Измененный mdb-файл, пусть даже с каким-нибудь другим названием, в DeviceLock отсутствует. Zlock корректно обрабатывает данную ситуацию и корректно фиксирует изменения в обоих файлах.

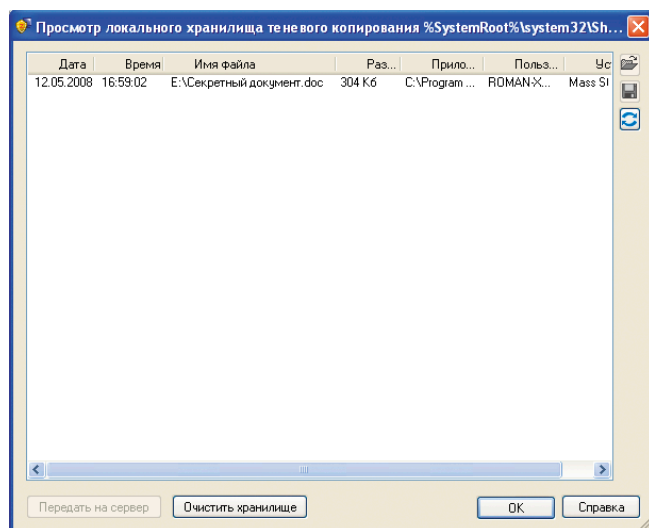


Рисунок 2. Консоль Zlock корректно отображает имя сохраненного файла

Outlook

Похоже, что Outlook работает аналогично Access: при добавлении писем в pst-хранилища происходит модификация только части файла. В такой ситуации DeviceLock, в отличие от Zlock, теневые копии .pst-файлов не сохраняет.

Следует отметить, что сохранение файлов из Блокнота Windows (Notepad) фиксируется обеими системами корректно, отображается правильное имя файла и сохраняется все его содержимое. Очевидно, что проблема с именами файлов возникает у DeviceLock в связи с некорректной обработкой функции переименования, поскольку известно, что приложения MS Office при редактировании создают временные файлы с такими «неудобоваримыми» именами, а потом их переименовывают.

Проблема же с Access и Outlook более серьезна. Дело в том, что эти приложения работают с файлами с помощью функций их отображения в память (memory-mapped files), и, судя по результатам теста, данные функции DeviceLock также не обрабатывает или обрабатывает некорректно. Таким образом, любое приложение, которое сохраняет данные с использованием этой технологии, позволяет «обмануть» теневое копирование DeviceLock, что может быть использовано потенциальным нарушителем.

Надежность теневого копирования

Изучение механизма теневого копирования навело на мысль прервать работу Windows нажатием на кнопку RESET как во время копирования, так и сразу после окончания записи на носитель и посмотреть, что записалось на флешку и что при этом сохранилось в теневой копии.

В рамках данного теста были проведены следующие испытания:

1. Копирование файла размером 18 Мб на флешку. Во время копирования, когда по индикатору прогресса было скопировано порядка 60-70% файла, нажатие RESET.
2. Копирование файла размером 1 Мб на флешку. Сразу после копирования, когда светодиодный индикатор флешки переставал мигать,

Таблица 2. Объем данных, записываемых в теневую копию

Вид испытания	Расположение файла	DeviceLock	Zlock
RESET в процессе записи файла размером 18 Мб	файл на флешке	10 207 232 байт	12 828 672 байт
	теневая копия	отсутствует	12 845 056 байт (100,1% от объема записанного файла)
RESET сразу после записи маленького файла (1 Мб)	файл на флешке	записан полностью	записан полностью
	теневая копия	отсутствует	записана полностью
RESET сразу после записи большого файла (60 Мб)	файл на флешке	записан полностью	записан полностью
	теневая копия	3 276 800 байт (5,2% от объема файла)	записана полностью

нажатием RESET. После перезагрузки скопированный файл побитно сравнивался с оригиналом – утилитой fc.exe, для того чтобы убедиться, что файл скопировался полностью.

3. Аналогично п. 2, но копировался файл размером 60 Мб.

Копирование выполнялось проводником Windows. Результаты тестов приведены в **таблице 2**.

Как видно из результатов, особенности реализации теневого копирования в системе DeviceLock могут стать причиной утечки данных. Путем несложных манипуляций с кнопкой RESET злоумышленник может «вынести» приличные объемы конфиденциальной информации в обход теневого копирования, и служба безопасности об этом может только догадываться. Эта особенность может быть связана с не очень удачным проектированием системы – формирование теневой копии осуществляет системная служба, выступая в качестве дополнительного звена, что приводит к созданию копии после записи данных на внешний носитель.

В Zlock теневое копирование осуществляет драйвер, благодаря чему можно реализовать превентивное теневое копирование – запись теневой копии производится до записи данных на внешний носитель. Если обратить внимание на результаты первого теста, то видно, что в теневую копию Zlock записалось больше информации, чем успело скопироваться на флешку. Правда, разработчикам Zlock удалось добиться более высокой надежности ценой снижения скорости копирования данных на отслеживаемые устройства, что может быть критично для организаций, в которых сотрудники интенсивно работают с внешними носителями данных.

Выводы

Реализация теневого копирования в DeviceLock обладает рядом существенных недостатков, которые не только затрудняют анализ деятельности пользователей службой безопасности, но и могут привести к записи данных на носитель в обход функции теневого копирования.

В первую очередь, имеются в виду некорректная обработка операций с файлами, отображаемыми в память (memory-mapped files), и запись теневой копии в локальное хранилище после копирования данных.

С другой стороны, DeviceLock позволяет вести теневое копирование записываемых данных на другие устройства – порты ввода/вывода, КПК и CD/DVD-приводы. Кроме того, система позволяет фиксировать прямую запись на диск.

Что касается Zlock, то, несмотря на более позднее появление теневого копирования, разработчики смогли реализовать эту функциональность гораздо надежнее, но с рядом ограничений, кроме уже упомянутого падения производительности. В частности, в теневых копиях Zlock не фиксируется прямая запись на диск. Конечно, она может быть выполнена только какими-либо специальными утилитами для работы с диском и только пользователем с администраторскими привилегиями, а, как известно, защищаться от такого пользователя не имеет смысла, поскольку он и так может отключить любую систему, но всегда хочется стремиться к идеалу.

В заключение хотелось бы выразить надежду, что данная статья станет источником дополнительной информации для потенциальных пользователей теневого копирования и поможет сэкономить время и усилия на этапе выбора решения.

Удачи! 