DLP-система как объект... атаки

Александр Кузнецов, *руководитель отдела НТЦ "Вулкан"*
Александр Товстолип, *ведущий специалист НТЦ "Вулкан"*

В этой статье нам хотелось бы предложить тематику, поднятую в предыдущем спецпроекте DLP ("Защита от утечки данных: комплексная терапия", Information Security, № 3/2012), в разрезе ограничений применения систем DLP, а также взглянуть на них с точки зрения злоумышленника.

Хотели как лучше

Сначала осветим моменты, которые оказывают существенное влияние на качество внедрения DLP-решений:

- ошибки при внедрении, которые были, есть и будут, в том числе использование настроек "по умолчанию";
- обеспечение жизненного цикла работы DLP-решения (пополнение базы знаний системы, "покрытие" новых узлов сети и т.п.);
- действия по результатам расследования инцидентов ИБ, зафиксированных DLP-системой, и работа с конечными пользователями.

На практике о данных моментах "упорно" забывают. В своей работе мы часто сталкиваемся с данными ситуациями при проведении аудитов ИБ.

Кроме того, как и в любом ПО, в DLP-системах существуют уязвимости (часть из них известна, например CVE-2008-4564 и CVE-2011-1423). Но даже без эксплуатации уязвимостей злоумышленникам есть где разгуляться, и об этом мы расскажем ниже.

Если нельзя, но очень хочется

Часто в компаниях могут возникнуть ситуации, когда DLP-система должна "подвинуться в сторону" и не мешать работать. Для таких случаев вендоры предусматривают соответствующие функциональные возможности:

- выдачу уведомлений;
- запросы подтверждений;
- запросы временных разрешений на операции (по времени или количеству операций).

Сделав "шаг в сторону", конфиденциальный документ может быть выведен за границы контролируемой сети. По ошибке, намеренно или по той и другой причине одновременно – это уже не важно.

"Ты работаешь в Office"

Так называемое офисное ПО доступно для 99% всех пользователей. А что если взглянуть на эти современные многофункциональные решения как на инструмент для организации утечки?

Именно в "офисном" разрезе мы уже демонстрировали ограничения DLP в предыдущей статье. Что же, продолжим тему.

"Потайные карманы", в виде областей "Свойства документов", макросов, Word-объектов и т.п. элементов, позволяют спрятать значительные объемы данных (см. рис. 1). Суммарно этот текст по объему в 55 раз больше, чем данная статья, плюс к этому еще 27 полей во вкладке "Прочее" с таким же потенциалом.

Ну а объем текста в теле макросов практически не ограничен. В наших экспериментах мы размещали в одном макросе до тысячи страниц текста.

Примитивная стеганография путем замены символов русского алфавита англоязычными или иными символами (например, а-a-@, б-b-6) также может создать массу сложностей для DLP-решений. Ведь предусмотреть абсолютно все комбинации и варианты написания ключевых слов просто физически невозможно. А в случае использования процентного совпадения количество "фальстартов" (False Negative) существенно возрастет, что серьезно усложнит выявление действительно важных или подозрительных операций.

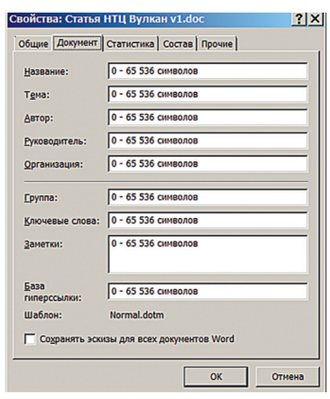

Рис. 1. Свойства doc-файла

Очень часто специалисты по ИБ забывают о контроле функции "Печать в файл", не воспринимая это как потенциальный канал утечек. При этом, как показала наша практика, утечки через PRN-файлы[1] практически не контролируются DLP-системами (если мы не говорим, о запрете сугубо по формату файла без контекстного анализа).

Позволь себе больше

Что, если нам нужно увести не документ MS Office, а, например, чертеж (DWG, VSD, DXF)?

Сделать снимок экрана, а потом работать с картинкой – это первое, что приходит в голову. Здесь некоторые производители DLP-решений предлагают блокировать результат нажатия клавиши *PrtSc*. Однако, начиная с Word, PowerPoint и Excel 2010, можно создавать снимки экрана для остальных открытых окон непосредственно из приложений (функция "Снимок"), плюс к этому в выпусках Windows 7 есть инструмент "Ножницы" для создания выборочного скриншота. Все эти процессы и приложения нужно отдельно ставить на контроль.

Также дополнительные интересные возможности предоставляет побитное копирование конфиденциальных данных с использованием команды *Copy*

[1] *PRN – Printable File, обрабатываются с использованием ПО Microsoft Office Document Imaging, Microsoft Windows Command Line, AllWeb FastPrint, Free Raw Print и др.*

в конец легальных документов. Ну и не забываем про возможности архиваторов (см. предыдущую статью).

Результаты нашего тестирования лидеров списка Gartner начала 2013 г. с использованием описанных методов, доступных в общем-то рядовому пользователю (см. рис. 2), приведены в табл. 1.

Ну а для искушенных пользователей дополнительно предлагается:

- использование шифрованных контейнеров, смонтированных как локальные диски;
- работа на виртуальных машинах;
- специализированные стенографические утилиты;
- синтезаторы речи Text to Speech и наоборот Speech to Text;
- маскировка под легальный трафик (например, DNS Tunneling);
- загрузка с внешних носителей под управлением альтернативных ОС;
- хорошо тренированная память, острый карандаш или фотоаппарат.

Убить "Агента DLP"

Насколько DLP-решения хорошо защищают сами себя? Мы попробовали ответить на этот вопрос, проведя небольшое исследование в нашей лаборатории. Вот что дали результаты тестов:

- отсутствует прямая возможность остановить службы DLP, но можно скомпрометировать исполняемый файл – вследствие чего после перезагрузки DLP-агенты не стартуют;
- можно удалить лог-файлы с зарегистрированными данными об утечках с хоста до их отправки на сервер управления[2];
- можно "реанимировать" файлы, на которые был наложен запрет копирования, например, на съемные носители, используя общедоступные программы для восстановления данных.

Реальные примеры "заказных убийств" мы демонстрировали в конце мая на форуме практической безопасности PHD III.

Рис. 2. Инструменты злоумышленника

"Шеф, все пропало!"

Было бы неправильно с нашей стороны обозначить проблемы и не указать способы их решения.

В рамках реализации DLP-проектов мы всегда придерживались комплексного подхода и выработали следующие рекомендации, которые, надеемся, помогут избежать неожиданных утечек из сетей, защищенных с использованием современных DLP-систем:

- минимизация прав и полномочий пользователей на своих рабочих местах;
- отключение возможности выбора режимов загрузки ОС;
- разграничение прав доступа к каталогам с установленными компонентами DLP, используя возможности NTFS;
- скрытие/переименование служб, отвечающих за работу сервисов DLP;
- мониторинг работы сервисов и агентов DLP, желательно скоррелированный с работой самой операционной системы;
- контроль использования приложений и форматов документов, не являющихся принятыми в организации;
- использование черных и белых списков для получателей документов вне зависимости от их содержания;
- использование учтенных корпоративных съемных носителей информации и периодический контроль наличия на них следов конфиденциальных документов;
- использование электронной подписи в документах с целью обеспечения аутентичности и неотказуемости.

С организационной стороны в первую очередь необходимо обеспечить непрерывное или хотя бы периодическое обслуживание и мониторинг состояния работы DLP-системы и ее компонентов.

Предупрежден – значит вооружен

В заключение хотим подчеркнуть, что мы ни в коем случае не пытались создать "Руководство для чайников по сливу информации" или критиковать производителей современных DLP-решений. Мы всего лишь стараемся наглядно продемонстрировать имеющиеся в DLP-системах особенности и ограничения, о которых очень часто забывают при выборе, внедрении и дальнейшей эксплуатации системы.

Надеемся, что читатели смогут выявлять данные ограничения раньше злоумышленников, и оперативно реализовывать дополнительные меры по защите чувствительной информации или принимать выявленные риски. Или как минимум знать об их существовании.

На фоне тенденции к тому, что сами средства защиты информации все чаще и чаще становятся объектами атаки, пренебрежение другими организационно-техническими мероприятиями по защите информации может обойтись слишком дорого.

Наконец, важно понимать, что DLP-система защищает не от утечки информации, а от утечки документов, а это совсем разные вещи (см. рис. 3). ●

Табл. 1. Результаты тестирования

Тест	DLP 1	DLP 2	DLP 3	DLP 4
Запрос подтверждения	✓	✓	✓	✓
«Потайные карманы»	✓	✓	✓	✓
Примитивная стеганография	✓	✓	✓	✓
«Игра» с кодировками	✓	✓	✓	✗
PRN-файл (печать в файл)	✓	✓	✓	✓
Снимки экрана (PrtSc)	✓	✓		
SFX-архив	✓	✓	✓	
Спец. цепочка архивов	✓	✓		

Рис. 3

[2] В настоящее время мы тестируем потенциальную возможность отправить на DLP-сервер заранее обработанный контейнер с логами, содержащий SQL-инъекцию. Продолжение следует...