Выводы

Предлагаемая методология для аудиоданных, как показывают результаты исследований, позволяет решать на основе достаточно общей физической и математической модели ряд задач стегоанализа при выявлении скрытой информации на уровне наименее значимых младших бит. Она может служить методологической основой для оценки стойкости алгоритмов стеганографии аудиоданных. Для выявления ее сильных и слабых сторон требуются массовые экспериментальные исследования.

Список литературы

1. *Аграновский А. В., Девянин П. Н., Черемушкин А. В., Хади Р. А.* Основы стеганографии: учеб. Пособие для вузов. Ростов-на-дону, 2003, 152 с.

2. *Грибунин В. Г., Головачев В. Ю., Оков И. Н.. Турищев И. В. Конжев А. В.* Компьютерная стеганография, М. Солон-Р, 2002 – 240с.

3. *Конахович Г. Ф., Пузыренко А. Ю.,* Компьютерная стеганография. 'МК-Пресс", Киев, 2006. 283 с.

4. *Mandelbrot B.B.* Fractals, Form, Chance, and Dimension, San Francisco: Freeman. 1977.

5. *Mandelbrot B.B.* The Fractal Geometry of Nature, San Francisco: Freeman. 1982.

6. *Эммануил Айфичер, Барри Джервис* Цифровая обработка сигналов, Москва-Санкт-Петербург-Киев, 2004 г., 989 с.

7. *H. Ozer, B. Sankur, N. Memon, 'I. Avcıba.* Detection of audio covert channels using statistical footprints of hidden messages. www.elsevier.com/locate/dsp, 2005.

8. *H. Ozer, 'I. Avcıba, B. Sankur, N. Memon.* Steganalysis of audio based on audio quality metrics, in: SPIE Electronic Imaging Conf. on Security and Watermarking of Multimedia Contents, vol. V. Santa Clara, January 20–24, 2003, pp. 55–66.

Надійшла 15.12.2007р.

УДК 004.056.5 (076.5)

Корниенко Б.Я., Щербак Л.Н.

АНАЛИЗ ДЕЙСТВИЯ И МЕТОДОВ ПРОТИВОДЕЙСТВИЯ ИНФОРМАЦИОННЫМ УГРОЗАМ ТИПА «RISKWARE»

Введение

Одной из актуальных и важных научно-технических проблем функционирования информационных систем, которые в настоящее время все в большей мере развиваются и внедряются в разные отрасли народного хозяйства Украины, является защита информации. Возникшее в ходе развития информационных систем противоборство между защитниками нормального функционирования систем и всякого рода кибертеррористами по сути переросло в «информационную войну», которая в большей мере является интеллектуальной борьбой высокого уровня специалистов.

Даная работа посвящена Spyware - программному обеспечению, которое собирает информацию о пользователе, как правило без его ведома или согласия, и затем передает эти данные другим лицам. Таким образом это по сути в большинстве случаев шпионское программное обеспечение.

Также как и другие компьютерные вирусы, шпионское программное обеспечение имеет множество различных форм, но в отличие от вирусов большинство spyware совершенно легально передает информацию. Собранная информация, используется компаниями для того, чтобы показывать пользователям рекламные всплывающие окна, а также для отправки нежелательных писем.

Шпионские программы были выделены в отдельный класс, так как не попадают под определение вредоносных кодов и обычного полезного программного обеспечения. Они находятся где-то посредине шкалы такого программного обеспечения.

Термином «spyware» в подавляющем большинстве случаев называют целое семейство программ, в которое входят: программы дозвона, утилиты для закачивания файлов из Интернета, различные серверы (FTP, Proxy, Web, Telnet), IRC-клиенты, средства мониторинга, PSW-утилиты, средства удаленного администрирования, программы-шутки. Более подробно эти типы программ будут рассмотрены ниже.

Иногда в семейство spyware включают еще и рекламные коды (adware), которые могут демонстрировать рекламные сообщения, подменять результаты поиска и любыми доступными способами продвигать рекламируемый сайт.

Таким образом все вышеперечисленные типы программ следует называть «riskware». На русском языке это слово означает «условно опасные программы», то есть те, которые могут причинить вред информации пользователя.

Ранее для названия вредоносных программ использовались термины «greyware», «blackware» и «whiteware». Такая система именования строится на трех цветах: сером (grey), черном (black) и белом (white). Greyware в данном случае выступает полным аналогом riskware, blackware является классом откровенно вредоносных программ и whiteware выступает в роли легитимного программного обеспечения (то есть абсолютно законного и полезного). Тем не менее, пользоваться такой терминологией очень неудобно, так как для вредоносных программ (blackware) уже давно устоялся собственный термин, который по-английски звучит как «malware», а на русском языке таким и остается — «вредоносное программное обеспечение».

Распространяется spyware в Интернете либо путем обмана пользователя, либо через программные уязвимости. При первом варианте пользователь скачивает из Интернета какое-то полезное программное обеспечение, а как приложение получает шпионский модуль. Чаще всего носителями spyware являются разнообразные ускорители работы Интернета. Иногда создатели шпионского программного обеспечения платят разработчикам условно бесплатных программ за добавление в инсталлятор своего модуля, а порой просто объединяют шпионский дистрибутив с уже готовыми полезными программами.

Современные браузеры не позволяют «шпионам» самовольно загружаться с сайтов, однако иногда пользователь сам разрешает их установку, потому что загрузочную ссылку нередко маскируют под всплывающие окна, похожие на обычные опросы. Независимо от того, за какой вариант ответа пользователь голосует, своим нажатием он запускает установку spyware. С последними версиями Internet Explorer возможностей для таких манипуляций у распространителей шпионских программ стало гораздо меньше, однако актуальность этот способ заражения еще не потерял - ведь, несмотря на многочисленные предупреждения, старые версии браузеров стоят на множестве компьютеров.

Признаки заражения пользователи в основном замечают лишь тогда, когда операционная система просто кишит spyware-объектами. Работа резко замедляется из-за нехватки ресурсов, часто происходят системные или программные сбои, наблюдаются трудности с Интернет-соединением. Не имеющий в большинстве случаев никакого представления о spyware, пользователь ищет причины неудовлетворительной работы в аппаратном обеспечении, проблемах установки Windows или же полагает, что его компьютер заражен вирусом. Обычный результат «накопления» шпионского программного обеспечения - переустановка системы.

По данным компании Earthlink и сайта vnunet.com, программы, относящиеся к категории spyware, сегодня установлены почти на 90% компьютеров, подключенных к Сети [1]. Более того, выгоду от использования шпионских программ уже уяснили спамеры — они добавляют эти программы в свои письма, а также киберпреступники, которые создают все больше сайтов для новых жертв. От шпионских программ страдают и организации, несмотря на то, что 70 % из них используют антишпионские программы. Самый высокий уровень

распространения шпионских программ в Европе приходится на Великобританию — там на одном компьютере в среднем присутствует 30,5 шпионских программ. Среднеевропейский показатель равен 24,5 программам [2].

Самая агрессивная и навязчивая программа в их ассортименте по данным компании Webroot - Cool Web Search, имеющая более 107 вариантов. На сегодня эта разновидность spyware можно обнаружить на 8,2% компьютеров. Второе место занимает Gator, на чью долю приходится до 2,2% заражений и на третьем месте - 180Search с его 2%.

Постановка задачи

Целью данной статьи является проведение исследование современных условно опасных программ, анализ действия и методов противодействия информационным угрозам типа «riskware».

Виды условно опасных программ

Проведем классификацию ряда условно опасных программ, которые в руках злоумышленников из полезных утилит превращаются в опасные атакующие средства:

Программы дозвона (dialers). Сами по себе эти программы являются полезными прикладными утилитами, но в руках преступника превращаются в средства дозвона (с помощью модема пользователя) на заранее запрограммированный злоумышленником номер. Таким образом, пользователь рискует получить счет на оплату телефонных услуг, в который войдут расходы на международный разговор и оплата за предоставленные услуги. Однако программы дозвона можно вполне использовать и в законных целях, например, чтобы дозваниваться до поставщика услуг Интернета, вести статистику такого соединения, планировать задания и т.д. Это двоякое использование средств дозвона и привело к тому, что они попали в категорию spyware.

Программы для загрузки файлов из Интернета. Пользователи модемных соединений часто устанавливают эти утилиты, чтобы оптимизировать процесс скачивания данных и обеспечить возможность в случае разрыва соединения продолжить скачивание с текущей позиции. В руках злоумышленника такая программа может быть использована для того, чтобы в тайне от пользователя (в фоновом режиме) переписать на компьютер откровенно вредоносный код. Действие такой программы напоминает работу паразитов, известных как Trojan Downloader. Эти троянцы, попав на компьютер пользователя, могут переписать еще несколько вредителей и внедрить их в систему.

FTP-серверы. Полезность этих программ не вызывает сомнений, так как огромное количество файлов в Интернете находится именно на ftp-серверах. Однако если преступнику удастся скрытно установить ftp-сервер на компьютер пользователя, он сможет удаленно получить доступ ко всем его файлам, а также следить за всеми производимыми операциями. Это может привести к утечке личной информации, кражи паролей и кодов доступа, а также к полной потере всех файлов на жестком диске.

Серверы-посредники (proxy servers). Эти программы широко используются для того, чтобы скрыть внутреннее адресное пространство вычислительной сети компаний и организаций от всех внешних пользователей. Злоумышленник может незаметно установить такой сервер-посредник на чужом компьютере и в некотором смысле осуществить кражу личности. Дело в том, что все последующие незаконные действия преступник будет осуществлять через сервер-посредник, следовательно, все следы потом приведут к ни в чем неповинному пользователю, которого могут обвинить в рассылке спама, организации сетевых атак, взломе корпоративной сети и т.д.

Серверы telnet и web. Утилита telnet разработана для удаленного управления компьютером в режиме терминальной сессии (то есть с помощью консоли и командной строки), а web-сервер позволяет внешним пользователям получить доступ к web-страницам, расположенным в отведенном для этого месте файловой системы. Злоумышленник может получить управление над чужим компьютером, если незаметно внедрит туда сервер telnet, и файловой системой, если развернет на компьютере-жертве web-сервер.

IRC-клиенты. В легальных целях эти программы используются для получения доступа к IRC-каналам (в основном mIRC). Эти утилиты обладают встроенными средствами обработки программ, написанных на транслируемых языках. Такая функциональность востребована некоторыми троянцами и IRC-червями.

Программы мониторинга. В обычных условиях эти утилиты позволяют следить за теми или иными ресурсами компьютера, собирать внутреннюю статистику по сетевому трафику и активности в интернете и хранить всю эту информацию на компьютере пользователя. Преступники же часто используют программу-монитор, чтобы собирать те же самые полезные данные, но потом красть их и анализировать в личных целях. Таким способом можно, например, выявить предпочтения пользователей при работе с Интернетом вообще или конкретными страницами в частности.

PSW-утилиты. Легальные пользователи применяют эти инструменты для восстановления потерянных или забытых паролей, а злоумышленники с их помощью могут быстро получить доступ к паролям пользователя, а потом переписать их на свой компьютер.

Утилиты удаленного администрирования. С одной стороны, эти инструменты позволяют системному администратору удаленно управлять рабочим станциями в сети предприятия. С другой стороны, с помощью тех же самых утилит можно злонамеренно управлять компьютером невинного пользователя.

«Глупые шутки». К этой категории относятся программы, которые не причиняют прямого вреда пользователю или компьютеру, но, например, демонстрируют время от времени какое-нибудь сообщение. Чаще всего эти сообщения содержат информацию о том, что компьютер заражен вирусом, скоро этот вирус отформатирует жесткий диск и т.д. Только чувство юмора создателя ограничивает функционал этих программ.

Таким образом, если рассмотреть любой приведенный выше класс программ, то можно легко определить, что кроме, как к riskware, его отнести некуда. Например, программы дозвона. Они не размножаются и не заражают файлы на компьютере пользователя. Следовательно, это не вирусы. Эти программы строго выполняют заложенные в них функции (то есть, звонят по указанному номеру) и не маскируются под какие-нибудь другие утилиты. Следовательно, это не троянцы. Средства дозвона также не рассылают себя по электронной почте, так что назвать их червями тоже невозможно. Тем не менее, благодаря подобным в целом полезным инструментам злоумышленник может направить ничего не подозревающего пользователя к поставщику ненужных услуг и таким способом нанести серьезный финансовый ущерб пострадавшему. Аналогично работают и все остальные типы условно опасных программ. Именно поэтому они отнесены к данной категории программного обеспечения.

Методы борьбы с вредоносным программным обеспечением

В современном мире предполагается использование различных программных средств в едином комплексе. Например, типовая автоматизированная система документооборота организации состоит из операционной среды, средств идентификации и аутентификации пользователей, различных программных средств, управления базами данных, телекоммуникационных программ, антивирусных программ, текстовых редакторов, средств электронной подписи и так далее.

Одним из важнейших условий правильного функционирования таких систем является обеспечение целостности, доступности и конфиденциальности данных, что достигается за счет защиты от того программного обеспечения, присутствие которого в системе является явно нежелательным и более того, вредным. В числе такого вредоносного программного обеспечения можно назвать не только вирусы, но и так называемые программные закладки, а также прочее вредоносное программное обеспечение, иногда называемое общим термином SpyWare [3].

Защиту можно грамотно организовать, зная задачи которые пробует решить злоумышленник с помощью программных закладок. Программные закладки могут выполнять одно из нижеперечисленных действий:

- вносить произвольные искажения в коды программ, находящихся в оперативной памяти компьютера (программная закладка первого рода);
- переносить фрагменты информации из одних областей оперативной памяти в другие (программная закладка второго рода);
- искажать выводимую на внешние компьютерные устройства или в канал связи информацию, которая была получена в результате работы других программ (программная закладка третьего рода).

Основные группы деструктивных воздействий, которые могут осуществляться программами-закладками:

- копирование информации пользователя компьютерной системы (паролей, криптографических ключей, кодов доступа, конфиденциальных электронных документов), находящихся в оперативной или внешней памяти этой системы либо в памяти другой компьютерной системы, подключенной к ней через локальную или глобальную компьютерную сеть;
- изменение алгоритмов функционирования системных, прикладных и служебных программ (например, внесение изменений в программу разграничения доступа может привести к тому, что она разрешит вход в систему всем без исключения пользователям - вне зависимости от правильности введенного пароля);
- навязывание определенных режимов работы (например, блокировка записи на диск при удалении информации - при этом информация, которую требуется удалить, не уничтожается и может быть впоследствии скопирована хакером).

К первой группе программ закладок относится программное обеспечение, предназначенное для скрытого слежения за деятельностью пользователей персональных компьютеров. В последнее время оно получило широкое развитие.

Исходя из такого перечня угроз необходимо подбирать и методы защиты. Самый простой способ - вообще не подключаться к Интернет. Можно также установить на компьютере брандмауэр при условии, что сам брандмауэр не содержит программ-закладок. Однако такой подход не позволяет детектировать существование самих шпионских программ в системе. Весьма проблематично также, что он защитит вас от вредоносной работы уже проникших в систему и хорошо замаскировавшихся там шпионских модулей. Поэтому приведем ряд рекомендаций, которые помогут эффективно противодействовать вредоносному программному обеспечению.

Необходимо постоянно отслеживать программное обеспечение, установленное на компьютер. Зачастую «резиденты» обитают в freeware и условно-бесплатных приложениях, а также adware - бесплатном программном обеспечении, демонстрирующем баннеры во время работы в Интернет. Причем с юридической точки зрения проблем нет - все нюансы работы «шпионского» программного обеспечения обязательно, пусть и в завуалированной форме, оговариваются в лицензионном соглашении. Следует читать сообщения в ходе инсталляции программ - проверьте, нужен ли ускоритель Интернет или программа автозаполнения форм, которые дополнительно предлагают разработчики бесплатного продукта?

Рекомендуется устанавливать качественный брандмауэр и регулярно обновлять базы антивируса. Следует проводить жесткую настройку правил для каждого программного обеспечения, имеющего доступ в Интернет. Для всего остального программного обеспечения доступ в Интернет необходимо заблокировать.

Необходимо запустить специализированные antispyware-утилиты, основным заданием которых как раз и является охота и поимка вредоносного программного обеспечения на компьютере.

Для обнаружения и удаления мониторинговых программных продуктов, которые могут быть установлены без ведома пользователя компьютера, в настоящее время используются

программы различных типов, обеспечивающие эффективную защиту исключительно только против известных мониторинговых программ с помощью сигнатурного анализа. Примеры таких программ – eTrust PestPatrol, Anti-SpyWare (компания Computer Associates) Ad-aware (Lavasoft), расширенные базы антивируса Лаборатории Касперского, Microsoft Anti-SpyWare и другие [4].

Выводы

В статье были приведены результаты анализа наиболее часто встречающихся программ типов spyware. Основные результаты анализа можно изложить в следующем:

- Spyware - программное обеспечение, которое собирает информацию о пользователе, как правило без его ведома или согласия, и затем передает эти данные другим лицам;
- к классу «spyware» можно отнести целое семейство программ, в которое входят: программы дозвона, утилиты для закачивания файлов из интернета, различные серверы (FTP, Proxy, Web, Telnet), IRC-клиенты, средства мониторинга, PSW-утилиты, средства удаленного администрирования, программы-шутки;
- к основным методам борьбы со шпионским программным обеспечением можно отнести установку на компьютере антивирусов, брандмауэров, мониторинговых программ и настройку операционной системы.

Список литературы

1. «Шпионскими программами заражены 90 процентов компьютеров», http://anti-malware.ru/index.phtml?part=news1&newsid=112&arc=1
2. «Spyware — потенциально опасные программы», Алексей Доля, http://www.viruslist.com/ru/analysis?pubid=164453811
3. «Шпионские войны: spyware и борьба с ним», Родион Насакин, http://anti-malware.ru/index.phtml?part=survey&surid=spyware
4. http://www.vnunet.com/vnunet/specials/2127675/spyware.

Надійшла 17.12.2007р.

УДК 004.681.3

Чернышев А. Н.

ОБЗОР СОВРЕМЕННЫХ «СПАМ» ТЕХНОЛОГИЙ. МЕТОДЫ ФИЛЬТРАЦИИ СПАМА

Термин "спам", как анонимная массовая не запрошенная рассылка электронных сообщений адресату, стало для пользователей электронной почты привычным и повседневным. Как правило, с помощью спама продают товары и услуги мелкие фирмы, которые не имеют возможности прибегнуть к более традиционным (и более дорогостоящим) рекламным каналам.

С точки зрения теории коммуникации, спам, это средство влияния на поведение людей, его получающих. Обычно спам направлен на побуждение получателей приобрести какие-либо товары и услуги непосредственно у заказчика спама. Однако заказчик может извлечь выгоду и косвенным способом – призывая покупать или продавать акции, обращающиеся на внебиржевом рынке в электронных торговых системах (так называемый "инвестиционным спамом").

Кроме спама и целевых коммерческих предложений существует еще один вид почтовых сообщений, который часто путают со спамом. Это нежелательная почта. В некоторых случаях не запрошенное и ненужное сообщение спамом не является. Наиболее частыми примерами нежелательной почты являются: разного рода отчеты об ошибках (ошибки автоматических рассыльщиков); различная техническая корреспонденция (сообщения о недоставке письма); новые возможности общения и бизнеса (деловое письмо о новом сотрудничестве); личные письма от тех, с кем получатель никогда ранее не