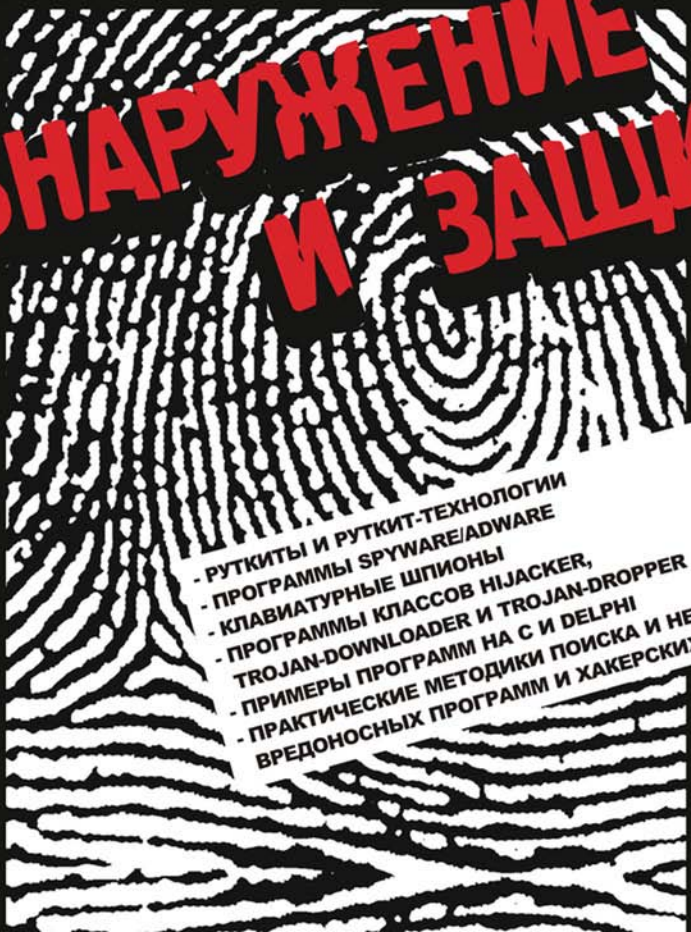
ОЛЕГ ЗАЙЦЕВ

ROOTKITS, SPYWARE/ADWARE, KEYLOGGERS & BACKDOORS

ОБНАРУЖЕНИЕ И ЗАЩИТА



- РУТКИТЫ И РУТКИТ-ТЕХНОЛОГИИ
- ПРОГРАММЫ SPYWARE/ADWARE
- КЛАВИАТУРНЫЕ ШПИОНЫ
- ПРОГРАММЫ КЛАССОВ HIJACKER, TROJAN-DOWNLOADER И TROJAN-DROPPER
- ПРИМЕРЫ ПРОГРАММ НА C И DELPHI
- ПРАКТИЧЕСКИЕ МЕТОДИКИ ПОИСКА И НЕЙТРАЛИЗАЦИИ ВРЕДОНОСНЫХ ПРОГРАММ И ХАКЕРСКИХ «ЗАКЛАДОК»

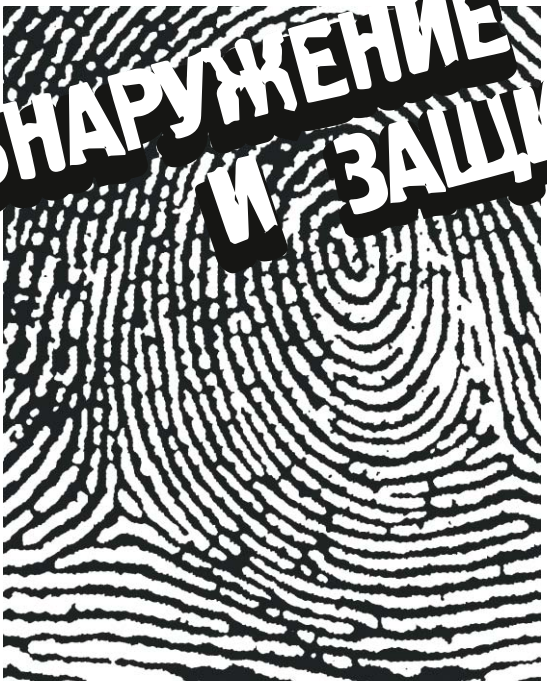
+cd

bhv

Олег Зайцев

ROOTKITS, SPYWARE/ADWARE, KEYLOGGERS & BACKDOORS

ОБНАРУЖЕНИЕ И ЗАЩИТА



Санкт-Петербург
«БХВ-Петербург»
2014

УДК 681.3.068
ББК 32.973.26-018.2
З-12

Зайцев О. В.

З-12 ROOTKITS, SPYWARE/ADWARE, KEYLOGGERS & BACKDOORS: обнаружение и защита. — СПб.: БХВ-Петербург, 2014. — 299 с.: ил.

ISBN 978-5-9775-1535-1

Рассмотрены технологии и методики, положенные в основу работы распространенных вредоносных программ: руткитов, клавиатурных шпионов, программ SpyWare/AdWare, BackDoor, Trojan-Downloader и др. Для большинства рассмотренных программ и технологий приведены подробные описания алгоритма работы и примеры кода на Delphi и C, демонстрирующие упрощенную реализацию алгоритма. Описаны различные утилиты, в том числе и популярная авторская утилита AVZ, предназначенные для поиска и нейтрализации вредоносных программ и хакерских "закладок". Рассмотрены типовые ситуации, связанные с поражением компьютера вредоносными программами. Для каждой из ситуаций описан процесс анализа и лечения. На прилагаемом компакт-диске приведены исходные тексты примеров, антивирусная утилита AVZ и некоторые дополнительные материалы.

Для системных администраторов, специалистов по защите информации, студентов вузов и опытных пользователей

УДК 681.3.068
ББК 32.973.26-018.2

Группа подготовки издания:

Главный редактор	*Екатерина Кондукова*
Зам. главного редактора	*Игорь Шишигин*
Зав. редакцией	*Григорий Добин*
Редактор	*Екатерина Капалыгина*
Компьютерная верстка	*Натальи Смирновой*
Корректор	*Наталия Першакова*
Дизайн обложки	*Инны Тачиной*
Зав. производством	*Николай Тверских*

"БХВ-Петербург", 190005, Санкт-Петербург, Измайловский пр., 29.

CD к книге выложен на FTP-сервер издательства по адресу:
ftp://ftp.bhv.ru/5941578687.zip

ISBN 978-5-9775-1535-1

Оглавление

Введение

Эта книга посвящена технологиям и методикам, применяемым в некоторых типах распространенных вредоносных программ. В частности, большое внимание уделено руткитам и клавиатурным шпионам.

Глава 1 содержит классификацию вредоносных программ, в которой особое внимание уделено AdWare и SpyWare. Данные программы являются условно вредоносными, поскольку не обладают присущей компьютерным вирусам способностью к размножению, не повреждают данные и не передают злоумышленникам конфиденциальной информации. Однако наличие AdWare на компьютере для пользователя неприятнее вируса — многие AdWare в процессе работы выводят рекламные окна с раздражающей частотой, подменяют стартовую страницу браузера и выполняют иные нежелательные действия.

В *главе 2* подробно рассмотрены технологии, применяемые современными вредоносными программами. В первую очередь внимание уделено руткитам и руткит-технологиям. Кроме того, подробно рассмотрены шпионские программы, осуществляющие слежение за клавиатурой и буфером обмена. Также описаны программы классов Hijacker, Trojan-Downloader и Trojan-Dropper, методики защиты от удаления, обхода Firewall и слежения за сетевым трафиком. Материалы *главы 2* рассчитаны в основном на опытного пользователя и системного администратора. Для большинства рассмотренных технологий приведены примеры на языках Delphi и C, поясняющие принципы работы и демонстрирующие особенности их реализации. Многие из примеров после небольшой доработки могут применяться для тестирования антивирусных программ и утилит.

Глава 3 посвящена различным утилитам, которые могут оказаться полезными для поиска и уничтожения вредоносных программ без применения антивирусов и антишпионов. Особое внимание уделено бесплатным программам, работающим без инсталляции. Все описанные программы разбиты по категориям (антируткиты, антикейлоггеры, утилиты мониторинга, диспетчеры процессов, менеджеры автозапуска, снифферы). Из описанных программ можно укомплектовать своеобразный набор инструментов, полезный для оперативного обследования компьютера. Помимо известных программ различных разработчиков в *главе 3* описана авторская утилита AVZ, предназначенная для полуавтоматического исследования компьютера. Данную утилиту с подробной документацией можно найти на прилагаемом к книге компакт-диске.

В *главе 4* рассмотрены практические примеры анализа компьютера с применением описанных в *главе 3* программ. Этот материал может быть интересен читателю с любым уровнем подготовки, так как демонстрирует базовые подходы к анализу компьютера. В качестве примеров анализа выбраны типовые ситуации, с которыми может столкнуться каждый пользователь, — примером такой ситуации является вывод посторонних окон с рекламной информацией или подмена стартовой страницы браузера.

Кому адресована эта книга

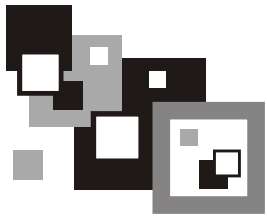
Книга предназначена для широкой аудитории читателей, интересующихся принципами работы вредоносных программ и методиками защиты от них. В частности, она может быть полезна:

- специалистам по защите информации;
- студентам, изучающим предметы по специальности "Информационная безопасность";
- системным администраторам;
- опытным пользователям, интересующимся принципами работы вредоносных программ и методиками защиты от них без применения антивируса.

Для изучения описанных в книге примеров желательно знание языков C и Delphi и общие познания в области системного программирования. Однако эти знания именно желательны, так как описание всех технологий в данной книге начинается с рассказа об алгоритмах и принципах их работы, а уже затем идут конкретные примеры, демонстрирующие данную технологию на практике. То же можно сказать по поводу описанных в книге утилит — для их применения не требуются специальные знания, как в случае использования отладчиков и дизассемблеров.

Благодарности

Я искренне благодарен Сергею Шерстневу за помощь, оказанную в подготовке и тестировании примеров к данной книге.



Глава 1

Классификация вредоносных программ

В настоящее время известно множество различных методик классификации вредоносных программ. В качестве классификационных признаков обычно выступает одно из свойств вредоносных программ.

- Методика заражения системы.
- Ущерб, наносимый системе в результате деятельности вредоносной программы.
- Некоторые технические признаки. Например, платформа, на которой может функционировать вредоносная программа (Win32, Linux, Java), или примененные в ходе создания средства разработки.

Классификация по методике заражения является одной из наиболее распространенных и универсальных.

Классификация по методике заражения системы

По методике заражения системы и файлов можно выделить ряд категорий.

- *Компьютерные вирусы.* Это вредоносные программы, обладающие способностью к заражению других программ. Под термином "заражение" в данном контексте понимается внедрение машинного кода вируса в тело поражаемой программы и модификация поражаемой программы таким образом, чтобы машинный код вируса получил управление в момент запуска зараженной программы или в процессе ее работы. Процедура удаления вируса (так называемое "лечение") в данном случае сводится к уда-

лению машинного кода вируса из тела программы и восстановлению ее работоспособности. Восстановление работоспособности приложения может быть как простым (состоящим, как правило, в восстановлении нескольких полей в заголовке исполняемого файла), так и очень сложным. Например, вирус может зашифровать фрагменты заражаемой программы, следовательно, для восстановления работы приложения потребуется их расшифровка.

- *Сетевые и почтовые черви.* Вредоносные программы данного типа не обладают способностью "заражать" другие приложения, но обладают алгоритмами, позволяющими рассылать им свои копии на другие компьютеры. Лечение червя сводится к поиску его компонентов на диске и их удалению.
- *Троянские программы.* Программы данной категории не обладают способностью заражать другие приложения или рассылать свои копии на другие компьютеры. Однако своей деятельностью они наносят вред пользователю тем или иным способом — например, передачей его конфиденциальных данных злоумышленнику, уничтожением информации, нарушением работы других приложений. Лечение троянской программы аналогично лечению червя — оно сводится к удалению файлов троянской программы.
- *AdWare/SpyWare.* Программы данного типа аналогичны троянским, т. е. они не могут заражать другие приложения или рассылать свои копии на другие компьютеры, но в отличие от троянских программ они не являются вредоносными. Однако их наличие на компьютере замедляет его работу, происходит ощутимый расход интренет-трафика, программа может осуществлять слежение за работой пользователя (например, фиксировать посещенные им URL) и доставлять массу беспокойства своей деятельностью. Часто подобные программы маскируют свое присутствие на компьютере и активно противодействуют своему удалению.

Стоит отметить, что известна масса вредоносных программ, которые можно отнести к нескольким категориям одновременно. Например, почтовый червь может выполнять функции троянской программы, а троянская программа, к примеру, может быть внедрена в одно из системных приложений по вирусному принципу. Кроме того, каждый из разработчиков антивирусных программ придерживается собственных критериев классификации. В результате один антивирус может вообще не детектировать некую вредоносную программу (поскольку аналитики не считают ее вредоносной), другой будет детектировать ее как AdWare, третий — как троянскую программу. Чаще всего подобные спорные моменты возникают именно для программ категорий AdWare и SpyWare, не являющихся вредоносными приложениями.

Классификация по наносимому ущербу

С другой стороны, можно классифицировать вредоносные программы по степени опасности для системы. В этом случае можно выделить следующие категории.

- *Безопасные.* Несмотря на то, что программы этой категории относятся к вредоносным, они не причиняют явного ущерба операционной системе и данным пользователя. В эту категорию попадают почти все AdWare- и SpyWare-программы. К безопасным также можно отнести Hoax, которые имитируют наличие вредоносной программы без нанесения ущерба.
- *Программы, уничтожающие и повреждающие данные.* Подобные деструктивные действия заложены в ряде компьютерных вирусов и троянских программ. Некоторые вредоносные программы производят обратимое повреждение информации (например, ее шифровку) с последующим требованием выкупа за восстановление информации, обычно после оплаты некоторой суммы разработчику.
- *Программы, собирающие и передающие третьим лицам конфиденциальную информацию.* Обычно это троянские программы, собирающие различные пароли, хранящиеся на компьютере пользователя.
- *Программы, организующие брешь в безопасности компьютера.* Это в первую очередь всевозможные backdoor и троянские программы, выполняющие создание посторонних учетных записей или выполняющие аналогичные операции, позволяющие злоумышленнику получить доступ к компьютеру пользователя
- *Программы, нейтрализующие или повреждающие специализированное программное обеспечение, применяемое для защиты компьютера.* В классификации лаборатории Касперского ряд таких программ выделен в категорию Trojan.Win32.KillAV.

Как и в случае с предыдущей классификацией, многие из вредоносных программ можно отнести к нескольким категориям одновременно. Например, троянская программа может воровать конфиденциальную информацию и одновременно с этим активно противодействовать Firewall и антивирусам.

Основные разновидности вредоносных программ

Рассмотрим подробнее несколько наиболее распространенных разновидностей современных вредоносных программ. Основное внимание уделим программам класса AdWare, SpyWare и Hoax, которые по своей многочисленно-

сти догнали и возможно уже перегнали вредоносные программы других типов. Кроме описания основных свойств программ формулируем критерии, по которым программу можно отнести к категории SpyWare или AdWare.

SpyWare (программы-шпионы)

Программой-шпионом (альтернативные названия — Spy, SpyWare, Spy-Ware, Spy Trojan) принято называть программное обеспечение, собирающее и передающее кому-либо информацию о пользователе без его согласия. Информация о пользователе может включать его персональные данные, конфигурацию его компьютера и операционной системы, статистику работы в сети Интернет.

Шпионское программное обеспечение применяется для ряда целей, из которых основными являются маркетинговые исследования и целевая реклама. В этом случае информация о конфигурации компьютера пользователя, используемом им программном обеспечении, посещаемых сайтах, статистика запросов к поисковым машинам и статистика вводимых с клавиатуры слов позволяет очень точно определить род деятельности и круг интересов пользователей. Поэтому на практике чаще всего можно наблюдать связку SpyWare + AdWare, т. е. "Шпион" + "Модуль показа рекламы". Шпионская часть собирает информацию о пользователе и передает ее на сервер рекламной фирмы. Там информация анализируется и в ответ высылается рекламная информация, наиболее подходящая для данного пользователя. В лучшем случае реклама показывается в отдельных всплывающих окнах, в худшем — внедряется в загружаемые страницы и присылается по электронной почте.

Однако собранная информация может использоваться не только для рекламных целей — например, получение информации о ПК пользователя может существенно упростить хакерскую атаку и взлом компьютера пользователя. А если программа периодически обновляет себя через Интернет, то это делает компьютер очень уязвимым — элементарная атака на DNS может подменить адрес источника обновления на адрес сервера хакера — такое "обновление" приведет к внедрению на ПК пользователя любого постороннего программного обеспечения.

Шпионское программное обеспечение может попасть на компьютер пользователя двумя основными путями.

- В ходе посещения сайтов Интернета. Наиболее часто проникновение шпионского ПО происходит при посещении пользователем хакерских и warez-сайтов, сайтов с бесплатной музыкой и порносайтов. Как правило, для установки шпионского ПО применяются ActiveX-компоненты или троянские программы категории TrojanDownloader по классификации лаборатории Касперского. Многие хакерские сайты могут выдать

"крек", содержащий шпионскую программу или Trojan-Downloader для ее загрузки.

- В результате установки бесплатных или условно-бесплатных программ. Самое неприятное состоит в том, что подобных программ существует великое множество, они распространяются через Интернет или на пиратских компакт-дисках. Классический пример — кодек DivX, содержащий утилиту для скрытной загрузки и установки SpyWare.Gator. Большинство программ, содержащих SpyWare-компоненты, не уведомляют об этом пользователя.

Точных критериев для занесения программы в категорию "SpyWare" не существует, и очень часто создатели антивирусных пакетов относят программы категорий "AdWare", "Hijacker" и "BHO" к категории "SpyWare" и наоборот.

Для определенности предлагается ряд правил и условий, при соблюдении которых программу можно классифицировать как SpyWare. В основу классификации положены проведенные автором исследования наиболее распространенных SpyWare-программ.

- Программа скрытно устанавливается на компьютер пользователя. Смысл данного пункта состоит в том, что инсталлятор обычной программы должен уведомить пользователя о факте установки программы (с возможностью отказа от установки), предложить выбрать каталог для установки и конфигурацию. Кроме того, после установки инсталлятор должен создать пункт в списке "Установка и удаление программ", вызов которого выполнит процесс деинсталляции. Шпионское программное обеспечение обычно устанавливается экзотическим способом (часто с использованием троянских модулей категории) скрытно от пользователя, при этом его деинсталляция в большинстве случаев невозможна. Второй путь инсталляции SpyWare — скрытная установка в комплекте с какой-либо популярной программой.
- Программа скрытно загружается в память в процессе загрузки компьютера. Стоит отметить, что разработчики современных SpyWare применяют rootkit-технологии для маскировки процесса в памяти и файлов на диске. Кроме того, становится популярным создание "неубиваемых" процессов (т. е. запуск двух процессов, которые перезапускают друг друга в случае остановки) и применение иных технологий, затрудняющих удаление SpyWare без применения специализированных средств. Такая технология, в частности, применяется в SpyWare.WinAd и многих других шпионских программах.
- Программа выполняет некоторые операции без указания пользователя — например, принимает или передает какую-либо информацию из Интернета.

- Программа загружает и устанавливает свои обновления, дополнения, модули расширения или иное ПО без ведома и согласия пользователя. Данное свойство присуще многим шпионским программам и чрезвычайно опасно, т. к. загрузка и установка обновлений и дополнительных модулей происходит скрытно и часто ведет к нестабильной работе системы. Более того, механизмы автоматического обновления могут быть использованы злоумышленниками для внедрения на ПК пользователя троянских модулей.
- Программа модифицирует системные настройки или вмешивается в функционирование других программ без ведома пользователя. Например, шпионский модуль может изменить уровень безопасности в настройках браузера или внести изменения в настройки сети.
- Программа модифицирует информацию или информационные потоки. Типовыми примерами являются разные расширения для программы Outlook Express, которые при отправке письма приписывают к нему свою информацию. Второй распространенный пример — модификация загружаемых из Интернета страниц (в страницы включается рекламная информация, некоторые слова или фразы превращаются в гиперссылки).

В данной классификации следует особо отметить тот факт, что программа категории SpyWare не позволяет удаленно управлять компьютером и не передает пароли и аналогичную им конфиденциальную информацию своим создателям — подобные действия специфичны другой категории программ — "Trojan" и "BackDoor". Однако по многим параметрам программы категории SpyWare являются родственниками троянских программ.

Рассказав о программах категории SpyWare, стоит акцентировать внимание на неявном слежении за пользователем. Предположим, что у пользователя установлена безобидная программа, загружающая рекламные баннеры один раз в час. Анализируя протоколы рекламного сервера, можно выяснить, как часто и как долго пользователь работает в Интернете, в какое время, через какого провайдера. Эта информация будет доступна даже при условии, что программа будет только загружать данные, не передавая никакой информации. Более того, каждая версия программы может загружать рекламу по уникальному адресу, что позволит узнать, какая именно программа загружает рекламу.

SpyWare cookies

Практически все программы для поиска программ AdWare/SpyWare детектируют и удаляют так называемые "SpyWare cookies" (в некоторых случаях их называют tracking cookies). В качестве теста автор проверил свой компьютер с помощью известной программы Ad-Aware SE Personal, и она обнаружила и

предложила удалить 164 "tracking cookies", причем большинство найденных cookies были созданы известными сайтами, в частности: rambler.ru, list.ru, hotlog.ru, downloads.ru. В результате часто в различных конференциях можно прочитать сообщения примерно такого содержания: "я лечил компьютер и нашел несколько сотен шпионов, которые пропустил мой антивирус/антишпион " — а затем анализ показывает, что речь шла о cookies.

По поводу cookies можно однозначно сказать, что это обычные текстовые файлы, которые не являются программами и не могут выполнять никаких шпионских или троянских действий на компьютере пользователя. Единственная "шпионская" операция, осуществимая с помощью cookies, состоит в возможности сайта сохранить на компьютере пользователя некоторые текстовые данные, которые будут переданы при последующем посещении сайта, сохранившего cookie. Рейтинги, счетчики и баннерные рулетки могут использовать cookie для своеобразной "пометки" пользователя.

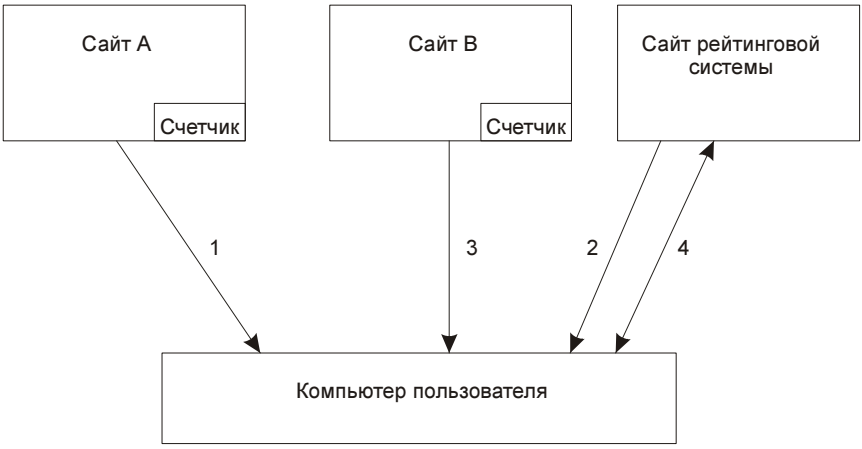


Рис. 1.1. Схема взаимодействия

Предположим, что пользователь посещает два сайта, содержащих на своих страницах счетчик одной и той же рейтинговой системы (рис. 1.1). При посещении сайта A произойдет минимум две операции — загрузка страницы с сайта A (шаг 1) и обращение к сайту рейтинговой системы (шаг 2). В заголовке HTTP ответа рейтинговой системы содержится поле, предписывающее браузеру сохранить cookie для сайта рейтинговой системы, — в результате браузер сохраняет cookie в своей базе данных. Затем пользователь посещает сайт B (шаг 3) и происходит повторное обращение к сайту рейтинговой системы (шаг 4), в ходе которого передается cookie, сохраненный на шаге 2.

Получив и проанализировав cookie, рейтинговая система опознает пользователя. Для этого, как правило, в cookie хранится присвоенный пользователю уникальный номер. В результате рейтинговая система может не просто фиксировать факт посещения сайта, но и отслеживать "траекторию" переходов по сайтам, страницы которых содержат счетчики этой рейтинговой системы. Кроме того, рейтинговая система может решить ряд интересных статистических задач — например, определить количество уникальных посетителей за определенный период, количество постоянных пользователей, периодичность посещения. Помимо статистических исследований идентификация пользователя с помощью cookie позволяет бороться с "накруткой" посещений или баннерных показов.

Важно отметить, что с помощью cookie любой сайт может регистрировать факт повторного посещения, но не может определить никаких персональных данных пользователя. Исключением является случай, когда пользователь сам передал серверу какие-либо данные, заполняя формы регистрации на сайте. Но даже в этом случае подобные данные очень редко хранятся непосредственно в cookie — обычно они вносятся в базу данных на стороне Web-сервера, а в cookie хранится идентификатор пользователя или сессии.

Таким образом, получается, что на взгляд автора опасность, которая приписывается "шпионским" cookie, существенно завышена. Internet Explorer всех версий позволяет отключить прием cookie, в версии 6.0 имеется возможность более тонкой настройки — все cookie делятся на основные (сохраняемые просматриваемой страницей) и сторонние (сохраняемые ресурсами, загружаемыми с других сайтов). Аналогичная возможность предусмотрена в альтернативных браузерах Mozilla Firefox и Opera.

AdWare-программы и модули

AdWare (синонимы AdvWare, Ad-Ware и т. п.) — это приложение, предназначенное для загрузки на ПК пользователя информации рекламного характера для последующей демонстрации этой информации пользователю. Можно выделить две категории AdWare-программ.

- Программы, распространяемые по AdWare-лицензии. Данные программы воспроизводят рекламу в качестве неявной оплаты за их использование, при этом реклама должна показываться только во время использования программы в контексте ее окон.
- Независимое приложение, предназначенное для воспроизведения рекламы. Такие программы, как правило, маскируются от обнаружения и удаления пользователем и могут существенно ему досаждать. Рекламная информация обычно выводится в виде всплывающих окон, хотя известны и широко применяются более экзотические методики демонстрации рек-

ламы — например, внедрение рекламной информации в рабочий стол в виде обоев или с использованием возможностей размещения Web-элементов на рабочем столе.

Можно сформулировать ряд правил, которых должна придерживаться корректная программа, распространяемая по AdWare-лицензии.

- При инсталляции на ПК программа должна предупредить пользователя о том, что является AdWare-приложением с разъяснением того, что конкретно понимается под термином "AdWare". При этом инсталлятор должен предусматривать возможность отказа от установки приложения (а еще лучше предлагать варианты установки — бесплатный AdWare-вариант или платный ShareWare-вариант). Типовым примером "правильной" инсталляции является менеджер закачек FlashGet, который честно предлагает два варианта установки — AdWare или ShareWare (FlashGet приведен в качестве примера не случайно — ряд программ анти-SpyWare по неизвестной причине считают его шпионским ПО и удаляют).
- AdWare-модуль должен быть или библиотекой, загружаемой AdWare-программой во время работы, или неразрывной частью AdWare-программы. При этом загрузка AdWare-модуля должна естественно происходить при запуске приложения, выгрузка и прекращение работы — при выгрузке приложения из памяти. Недопустимо внедрение AdWare-модулей в другие приложения или их установка на автозапуск.
- AdWare-модуль должен воспроизводить рекламную информацию только в контексте вызывавшего его приложения. Недопустимо создание дополнительных окон, запуск сторонних приложений, открытие неких Web-страниц.
- AdWare-модуль не должен выполнять действий, присущих программам категории SpyWare.
- AdWare-модуль должен деинсталлироваться вместе с установившим его приложением.

Как легко заметить, к AdWare-приложению в данной классификации предъявляются серьезные требования и практически ни один AdWare-модуль не удовлетворяет всем перечисленным требованиям.

Trojan-Downloader

Программы из категории Trojan-Downloader (сам термин "Trojan-Downloader" введен лабораторией Касперского) уже упоминались, поэтому следует дать определение для данной категории программ. Trojan-Downloader — это программа (модуль, ActiveX, библиотека и т. п.), основным назначением которой является скрытная несанкционированная загрузка программного обес-

печения из Интернета. Наиболее известными источниками Trojan-Downloader являются хакерские сайты. Сам по себе Trojan-Downloader как правило не несет прямой угрозы для компьютера — он опасен именно тем, что производит неконтролируемую загрузку программного обеспечения. Trojan-Downloader применяется в основном для загрузки вирусов, троянских и шпионских программ. Наиболее известными по статистике автора являются Trojan-Downloader.IstBar, Trojan-Downloader.Win32.Dyfuca, Trojan-Downloader.Win32.Agent и ряд других. Trojan-Downloader.Win32.IstBar и Trojan-Downloader.Win32.Agent поставили своеобразный рекорд по количеству различных модификаций и своей вредоносности — их появление на компьютере приводит к резкому росту трафика и появлению на ПК множества посторонних программ.

Все программы категории TrojanDownloader можно условно подразделить на две категории.

- Универсальные Trojan-Downloader — могут загружать любой программный код с любого сервера. Настройки могут храниться локально (в отдельном файле, реестре) или загружаться с определенного сайта.
- Специализированные Trojan-Downloader — предназначены для загрузки строго определенных типов троянских или шпионских программ. Адреса и имена файлов в таком случае жестко фиксированы и хранятся в теле программы.

Dialer

Программы категории Dialer (он же часто называется "порнозвонилка" от названия Porn-Dialer, присвоенного им в классификации лаборатории Касперского) достаточно широко распространены и предназначены для решения ряда задач, связанных с дозвоном до заданного сервера и установления с ним модемной связи. Применяются данные программы в основном создателями порносайтов, но страдают от них все — многие программы категории Dialer используют весьма изощренные способы установки (с использованием ActiveX, Trojan-Downloader), причем установка может быть инициирована при посещении практически любого сайта.

Организацию модемного соединения с сервером владельца Dialer может производить несколькими способами:

- набирать номер и устанавливать соединения своими средствами;
- создавать новое соединение удаленного доступа;
- изменять существующие соединения удаленного доступа.

В первых двух случаях Dialer, как правило, всячески привлекает внимание пользователя к себе и созданному им соединению — копирует себя во все

доступные места (в папки Program Files, Windows, Windows\System, Пуск и т. п.), создает ярлыки, регистрирует себя в автозапуске.

Часто кроме решения основной задачи программы типа Dialer выполняют задачи, свойственные программам других категорий (AdWare, SpyWare, Trojan-Downloader). Некоторые Dialer устанавливают себя на автозапуск, внедряются в другие приложения — например, автору известен Dialer, регистрирующий себя как расширение языка Basic и запускающийся при открытии любого приложения Microsoft Office, использующего скрипты.

Некоторые программы типа Dialer можно смело относить к троянским программам (а многие производители антивирусов считают Dialer троянской программой — на сайте производителей Norton Antivirus про Dialer говорится "троянская программа, предназначенная для..."), в классификации лаборатории Касперского есть специальная категория Trojan.Dialer.

Кроме утилит дозвонки к категории Dialer часто относят специализированные утилиты для просмотра порносайтов. Ведут они себя аналогично Dialer, только вместо модемного соединения соединяются с закрытими сайтами по Интернету.

> ***НА ЗАМЕТКУ***
>
> Не следует путать вредоносные Dialer с утилитами, предназначенными для автоматической дозвонки до провайдера. Они так же называются "Dialer", но в отличие от вредоносных программ устанавливаются пользователем и работают согласно его настройкам.

BHO (Browser Helper Object)

BHO (альтернативные названия — Browser Helper Object, Browser Plugin, Browser Bar, IE Bar, OE Bar и т. п., в классификации лаборатории Касперского есть подкатегория Toolbar, например, AdWare.Toolbar.Azesearch) — это расширение браузера или программы электронной почты, как правило, выполненное в виде дополнительной панели управления. У BHO есть ряд достаточно опасных особенностей.

- BHO не являются процессами системы — они работают в контексте браузера и не могут быть обнаружены в диспетчере задач.
- BHO запускаются вместе с браузером и могут контролировать события, связанные с работой пользователя в Интернете (по сути BHO для этого и предназначены).
- BHO обмениваются с сетью, используя API интеграции с браузером. Поэтому с точки зрения большинства персональных FireWall обмен с Интернетом ведет браузер. Как следствие, обнаружить такой обмен и воспрепятствовать ему очень сложно. Ситуация отягощается тем, что многие

BHO, входящие в категорию "SpyWare", передают информацию после запроса пользователя — это делает практически невозможным обнаружение постороннего обмена с Интернетом, т. к. он идет на фоне полезного трафика.

- Ошибки в работе BHO могут дестабилизировать работу браузера и приводить к трудно диагностируемым сбоям в его работе.

Несмотря на описанные особенности, BHO не обязательно является вредоносным приложением — например, существуют выполненные по BHO-технологии панели для IE, упрощающие работу с поисковыми системами (рис. 1.2).

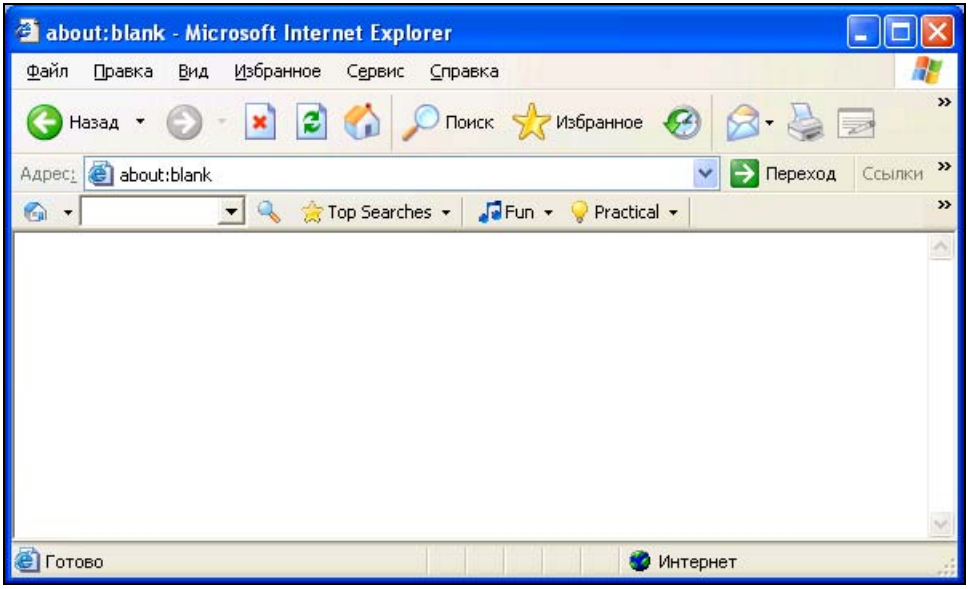


Рис. 1.2. Браузер с установленным BHO

Известен ряд универсальных BHO, представляющих собой конфигурируемую панель инструментов. Конфигурация, как правило, хранится в формате XML и может редактироваться пользователем или разработчиком.

Hijacker

Буквальный перевод этого термина звучит как "налетчик", "грабитель", "воздушный пират". Это программа, которая выполняет на компьютере пользователя нежелательные для него действия, преследуя цели своих разработчи-

ков. Производители многих антивирусных средств относят программы категории Hijacker к троянским программам.

Наиболее распространенной задачей программ класса Hijacker является перенастройка параметров браузера, электронной почты или других приложений без разрешения и ведома пользователя. В зарубежных источниках автору встречалось определение Hijacker, как утилиты, которая изменяет настройки браузера без ведома пользователя.

Чаще всего программы категории Hijacker применяются для изменения:

- стартовой страницы браузера — стартовая страница заменяется на адреса сайта создателей Hijacker;
- настройки системы поиска браузера (эти настройки хранятся в реестре). В результате при нажатии кнопки "Поиск" открывается адрес, установленный программой Hijacker;
- префиксов протоколов;
- уровней и настроек безопасности браузера;
- реакции браузера на ошибки. Например, известно несколько разновидностей Hijacker, заменяющих стандартные страницы Internet Explorer (в частности, описывающие ошибку с кодом 404) на собственные;
- списка адресов ("Избранное") браузера.

В чистом виде Hijacker встречается сравнительно редко, т. к. чаще всего по выполняемым действиям программа может быть отнесена кроме категории "Hijacker" к категориям "Trojan","Dialer" или "AdWare/SpyWare".

Trojan (троянская программа)

Троянская программа — это программа, которая выполняет действия, направленные против пользователя. Она собирает и передает владельцам конфиденциальную информацию о пользователе (эту категорию еще называют Trojan-Spy), выполняет несанкционированные или деструктивные действия. Из определения легко заметить, что троянская программа является "родственником" программ из категории SpyWare — разница, как правило, в том, что SpyWare не имеют выраженного деструктивного действия и не передают конфиденциальную информацию о пользователе. Однако вопрос об отнесении программы к той или иной категории достаточно спорный (часто получается, что одна антивирусная компания считает некий модуль AdWare, другая — троянской программой, третья — вообще игнорирует).

Backdoor

Backdoor — это программа, основным назначением которой является скрытное управление компьютером. Backdoor можно условно подразделить на следующие категории:

- Backdoor, построенные по технологии "клиент-сервер". Такой Backdoor состоит как минимум из двух программ — небольшой программы, скрытно устанавливаемой на поражаемый компьютер, и программы управления, устанавливаемой на компьютер злоумышленника. Иногда в комплекте идет еще и программа настройки;
- Backdoor, использующие для удаленного управления встроенный Telnet, Web или IRC-сервер. Для управления таким Backdoor не требуется специальное клиентское программное обеспечение. К примеру, известны Backdoor, которые подключаются к заданному IRC-серверу и используют его для обмена со злоумышленником.

Основное назначение Backdoor — скрытное управление компьютером. Как правило, Backdoor позволяет копировать файлы с пораженного компьютера и наоборот, передавать на пораженный компьютер файлы и программы. Кроме того, обычно Backdoor позволяет получить удаленный доступ к реестру, производить системные операции (перезагрузку ПК, создание новых сетевых ресурсов, модификацию паролей и т. п.). Backdoor по сути открывает атакующему "черный ход" на компьютер пользователя. Опасность Backdoor увеличилась в последнее время в связи с тем, что многие современные сетевые и почтовые черви или содержат в себе Backdoor-компонент, или устанавливают его после заражения ПК.

Hoax

Hoax — это относительно молодое развивающееся семейство вредоносных программ. Они получили широкое распространение в 2005 году, наблюдается устойчивая тенденция роста количества их разновидностей.

В буквальном переводе Hoax — "обман; ложь, мистификация, неправда", перевод термина достаточно точно отражает суть его работы. Идея Hoax — обман пользователя, чаще всего с целью получения прибыли.

Рассмотрим работу Hoax на примере. Наиболее типичным примером из данной категории является Hoax.Renos. Он состоит из единственного исполняемого файла, который после запуска скрытно загружает и инсталлирует "антишпионскую" программу SpywareNo объемом около 900 Кбайт и регистрирует ее в автозапуске. После этого Hoax.Win32.Renos портит обои на рабочем столе и делает недоступным меню смены обоев. Внешний вид рабочего стола показан на рис. 1.3.

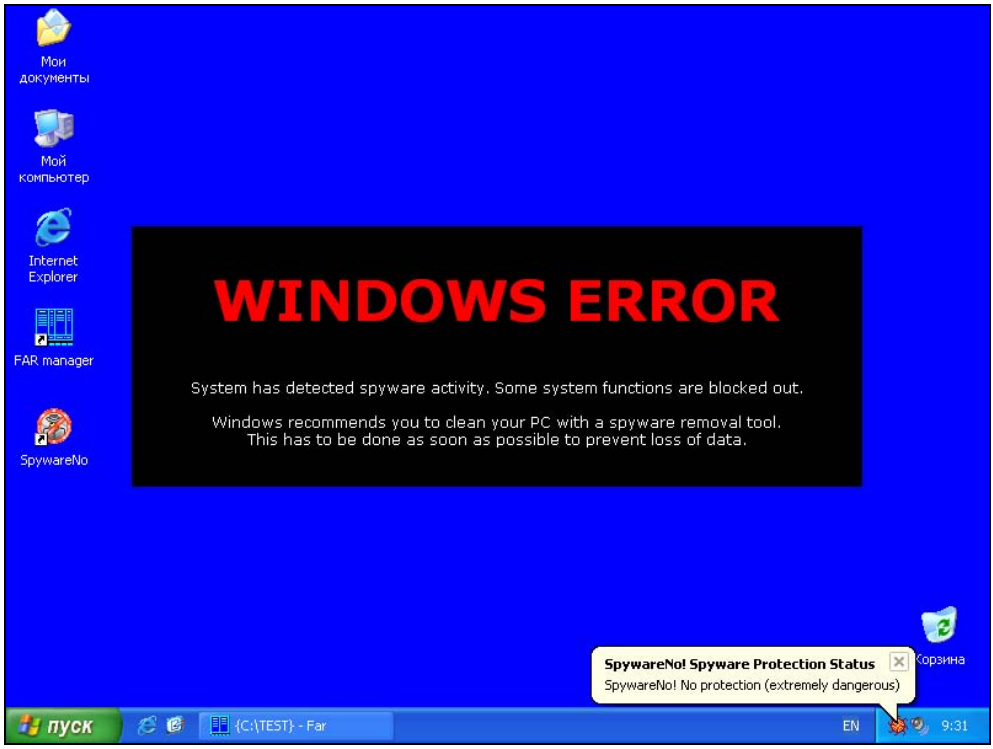


Рис. 1.3. Рабочий стол компьютера, пораженного Hoax.Win32.Renos

Установленная им программа SpywareNo, в свою очередь, отображает в трее иконку. При наведении на нее курсора мыши выводится всплывающее окно с сообщением "No protection" ("нет защиты") с указанием в скобках, что это чрезвычайно опасно для компьютера.

Щелчок по этой иконке открывает окно SpywareNo, в котором видны результаты "сканирования". Слово "сканирование" не случайно указано в кавычках, поскольку на эталонной лицензионной Windows XP этот сканер нашел 15 троянских программ (в том числе несколько клавиатурных шпионов, дропперов, флудеров). Напротив всех якобы найденных вредоносных программ в протоколе стояла пометка о том, что есть большой риск от их наличия на ПК пользователя (рис. 1.4).

Правда, есть одна тонкость — SpywareNo не показывает путь и имена найденных файлов, что не позволяет пользователю сразу разоблачить обман. Для лечения необходим лицензионный ключ, причем годичная лицензия стоит 38 евро. При получении бесплатного ключа на три дня данная программа вылечивает выдуманные ею вирусы и устраняет подмену картинки

рабочего стола, создавая видимость быстрого и эффективного лечения. Аналогов у Hoax.Renos в последнее время появилось достаточно много, но идея у всех одинаковая — имитация заражения ПК и реклама платного псевдоантивируса. Такая реклама естественно на порядок эффективнее простого AdWare, так как для пользователя искусственно создается ситуация, в которой ему необходим рекламируемый продукт.

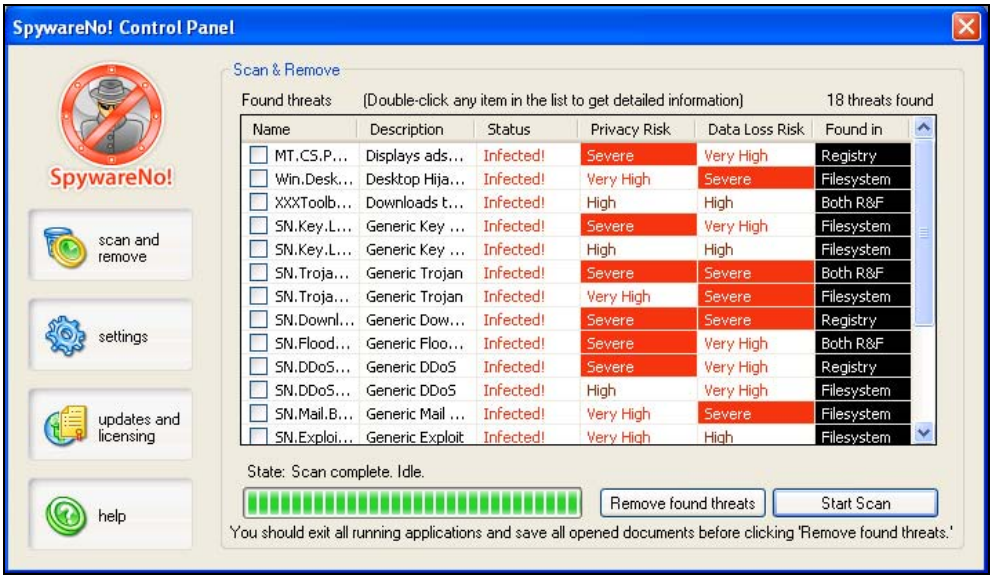


Рис. 1.4. "Антишпион" SpywareNo и найденные им "вирусы"

Другим направлением Hoax является прямой обман пользователя — например, программа может выдать себя за генератор кодов карт оплаты услуг сотовых операторов (чаще всего МТС или Beeline), программу для взлома электронных платежных систем. Особенностью всех программ данной разновидности является необходимость ввода пользователем номера неактивированной карты оплаты, номера кредитной карты или аналогичных параметров, которые затем передаются создателю данной программы и могут быть использованы им по своему усмотрению. По сути такую программу можно считать троянской, но с другой стороны она не маскирует своего присутствия и не ворует персональные данные, так как доверчивый пользователь сам запускает программу и вводит требуемую информацию.

Еще одной разновидностью Hoax можно назвать письма, в которых, как правило, сообщается об обнаружении в некоей платежной системе (чаще всего Webmoney) уязвимости, которая состоит в том, что если согласно опи-

санной в письме инструкции переслать некую сумму на указанный кошелек, то через некоторое время платеж вернется, но в удвоенном виде. Естественно, что никакой уязвимости в системе нет, и указанный в письмах кошелек принадлежит злоумышленнику. Тем не менее, доверчивые пользователи попадаются на данную уловку. Как и с другими видами Hoax, данные письма нельзя считать вредоносными (так как в них, собственно, даже программного кода нет).

Статистика распространенности различных видов вредоносного ПО

Рассмотрим статистику, собранную за 2005 год. В ее основу положены результаты анализа случаев заражения компьютеров и компьютерных сетей, изученных за год. По результатам можно построить диаграмму, отражающую процентный состав обнаруженных вредоносных программ (рис. 1.5).

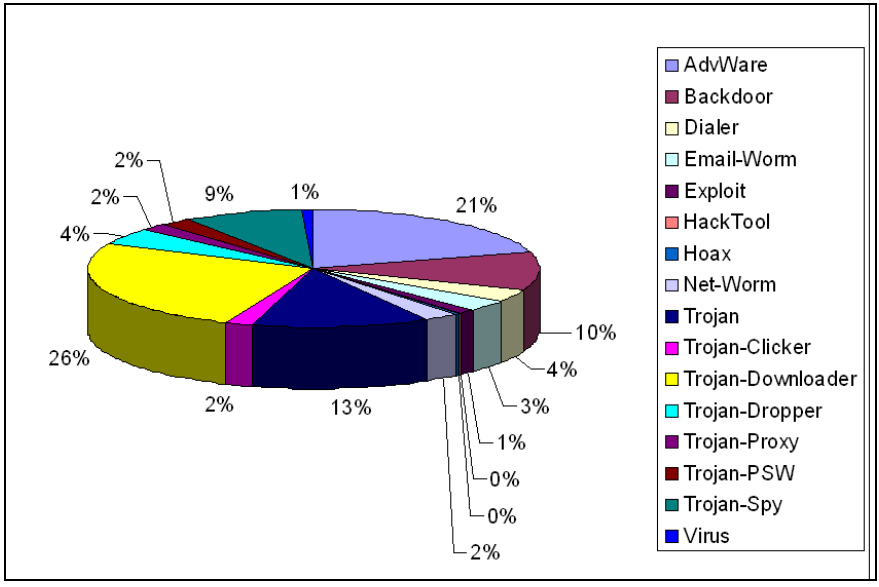


Рис. 1.5. Статистика за 2005 год, отражающая распространенность различных типов вредоносных программ

В данном случае рассматривается около 8 тысяч изученных программ, причем все образцы являются ITW (In-The-Wild, т. е. вредоносная программа, обнаруженная в реальных условиях на зараженных компьютерах пользовате-

лей). Следует заметить, что данная статистика отражает не количество зараженных компьютеров, а количество обнаруженных разновидностей вредоносных программ.

Как видно из статистики, самой распространенной категорией оказалась Trojan-Downloader (загрузчики вредоносных программ), далее идут AdWare, троянские и Backdoor-программы. Результат группировки по категориям показан на рис. 1.6.

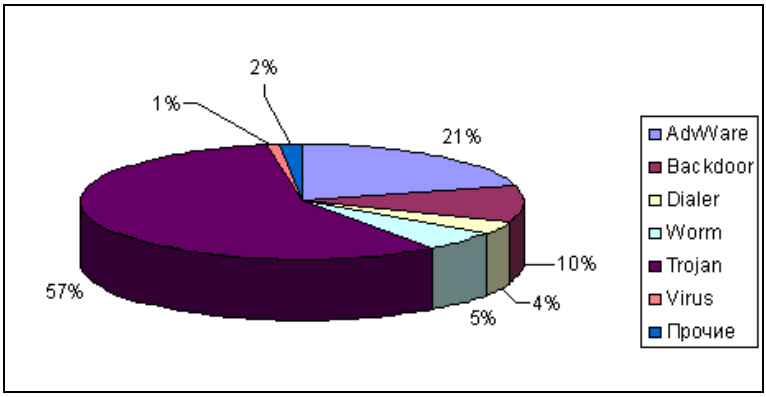


Рис. 1.6. Статистика с группировкой по категориям

Доля троянских программ различных видов составила 57% от изученных образцов, 21% — AdWare. Опираясь на эти цифры, можно утверждать, что за прошедший год обнаружено большое количество разновидностей вредоносных программ, не обладающих механизмами самораспространения. Большое количество разновидностей Trojan-Downloader подтверждает этот вывод и позволяет говорить об устойчивой тенденции заражения компьютера в несколько этапов:

1. Внедрение на компьютер-жертву небольшой программы класса Trojan-Downloader и ее запуск, который может осуществляться с помощью уязвимостей или социальной инженерии.
2. Trojan-Downloader скрытно загружает из Интернета и устанавливает на компьютере набор вредоносных компонентов — как правило, это или AdWare-программы, или Trojan/Backdoor.
3. При таком двухступенчатом поражении компьютера часто можно наблюдать "эффект снежного кома", связанный с тем, что загружаемые и устанавливаемые вредоносные программы сами являются Trojan-Downloader. Кроме того, некоторые Trojan-Downloader регистрируются в автозапуске

и восстанавливают загруженные ими троянские программы в случае их удаления пользователем или антивирусной программой, затрудняя тем самым лечение компьютера.

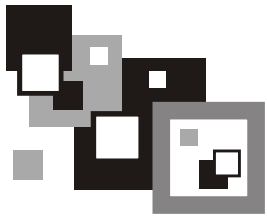
Тенденции развития вредоносных программ

Анализ вредоносных программ позволяет утверждать, что имеют место достаточно устойчивые тенденции.

- Повышается вредоносность троянских программ — многие из них нацелены на воровство паролей и иной конфиденциальной информации. Утечка подобной информации может нанести серьезный вред, причем во многих случаях сопряженный с потерей информации, утечкой конфиденциальных данных или финансовыми потерями.
- Явно прослеживается коммерческое применение троянских и Backdoor-программ. Лидерами являются так называемые *боты* — это гибриды троянской и Backdoor-программы, предназначенные для превращения зараженного компьютера в "зомби". Зараженные компьютеры могут применяться для решения различных задач, как правило, для проведения DDoS-атак или массовой рассылки спама.
- Разработчики вредоносных программ все чаще применяют экзотические методики автозапуска и внедрения в систему. Например, известны троянские программы, устанавливающиеся как монитор системы печати, провайдеры LSP/SPI, расширения проводника и Winlogon. Некоторые вредоносные программы применяют вирусные технологии, внедряя свой код в системные компоненты. Классическим примером может послужить Virus.Win32.Nsag, поражающий системную библиотеку wininet.dll. Это по сути не вирус, а небольшой троянский код, внедренный в wininet.dll по вирусному принципу.
- В ряде работающих с Интернетом и сетью вредоносных программ был обнаружен программный код, позволяющий нейтрализовать встроенный Firewall Windows. Основой методики является то, что настройки этого Firewall хранятся в реестре и модификацией реестра можно или отключить Firewall, или внести произвольное приложении в список доверенных.
- В ряде вредоносных программ был обнаружен код, предназначенный для обнаружения присутствия в системе средств мониторинга (REGMON, FILEMON) и отладчиков, запуска на виртуальном компьютере (чаще всего детектируется запуск на VMware).

- Для массовой рассылки троянских программ их разработчики начинают пользоваться услугами спамеров. В результате становится возможной рассылка вредоносной программы на большое количество компьютеров за небольшой интервал времени.

Помимо перечисленных тенденций можно отметить широкое распространение rootkit-технологий. Rootkit-технология достаточно проста в освоении, в Интернете можно найти массу исходных текстов готовых rootkit или заготовок и библиотек для их построения. Как следствие, разработчики вредоносных и шпионских программ берут rootkit-технологию на вооружение и применяют ее для маскировки присутствия своих программ на зараженном ПК и внедрения программного кода в другие процессы.



Глава 2

Технологии вредоносных программ и принципы их работы

В данной главе мы рассмотрим основные концепции и принципы, применяемые разработчиками вредоносных программ. Особое внимание будет уделено трем технологиям.

- Rootkit. Это технология, широко применяемая для защиты вредоносных программ от обнаружения и удаления, а также для шпионажа за пользователем.
- Клавиатурные шпионы и сопуствующие им технологии, предназначенные для скрытного слежения за работой пользователя.
- Прочие технологии, в частности, методики защиты программ от удаления, Trojan-Downloader и Trojan-Dropper, методики обхода Firewall и слежения за сетевой активностью.

Следует отметить, что в данной главе описываются наиболее распространенные методики, большинство из которых в том или ином виде встречается в ITW-образцах.

Rootkit

Термин "Rootkit" исторически пришел из мира UNIX, где под этим термином понимается набор утилит, которые хакер устанавливает на взломанном им компьютере после получения первоначального доступа. Это, как правило, хакерский инструментарий (снифферы, сканеры сети) и всевозможные троянские программы, работающие автономно или замещающие основные утилиты UNIX. Rootkit позволяет хакеру закрепиться во взломанной системе и скрыть следы своей деятельности.