Министерство образования Российской Федерации
Омский государственный университет
Лаборатория программного обеспечения
и компьютерных сетей

С.А. Белоусов, А.К. Гуц, М.С. Планков

Троянские кони

Принципы работы и методы защиты

Омск - 2003

Белоусов С.А., Гуц А.К., Планков М.С. Троянские кони. Принципы работы и методы защиты: Учебное пособие. – Омск: Издательство Наследие. Диалог-Сибирь, 2003. – 84 с.

ISBN 5-8239-0127-5

В данной книге сделана попытка собрать информацию о таком виде компьютерного зла, как троянские кони. Известно, что в Древней Греции пользы от троянского коня для защитников Трои было немного, а вот вреда более чем достаточно. С тех времён смысл названия изменился незначительно. Только поле битвы переместилось с полей Древней Греции в компьютерные сети.

В книге приводится некоторая классификация программ, отнесённых к троянским коням, показываются их основные отличия от вирусов, принципы функционирования, а также рекомендации по защите и борьбе с вредоносными приложениями. Приведены примеры троянских коней и программы по защите от них.

Художник
В.В. Коробицын

ISBN 5-8239-0127-5

СОДЕРЖАНИЕ

Безопасность – это не продукт, а процесс.

Брюс Шнейер

Самое дорогое на свете – глупость. Потому что за нее приходится платить дороже всего.

В. Шарапов,
Фильм «Место встречи изменить нельзя»

Введение

В настоящее время всё большее значение приобретает информация. Основой процветания, доходности любого предприятия являются новые технология и знания, полученные в ходе длительных и дорогостоящих исследований. Добытая информация и возможность её использования дорого ценятся. А раз так, то всегда найдутся люди, желающие получить её бесплатно. Очевидно, что это вызывает беспокойство у законных владельцев информационных ресурсов.

Попытки незаконно приобрести электронную информацию могут быть разнообразными. Выделим два основных варианта:

1) приобретение информации у лиц или организаций, не имеющих права на ее распространение;

2) хищение.

Именно при хищении убытки являются максимальными, так как скрывается обычно наиболее важная и дорогая информация. Владелец может даже не подозревать до поры до времени о том, что он уже ограблен. Примером хищений может быть промышленный шпионаж. Результатом его для предприятия могут стать огромные финансовые потери, а иногда и банкротство. По данным, опубликованным в сети Internet, общие потери от несанкционированного доступа к информации в компьютерных системах в 1997 году оценивались в 20 миллионов долларов, а уже в 1998 году в 53,6 миллиона долларов [6]. Конечно, нельзя утвер-

ждать, что эти цифры точны, но представить себе размеры потерь можно даже по ним. Поэтому всегда, а особенно в последнее время, проблема защиты информации является «вопросом жизни и смерти».

Наше время часто называют веком электроники. Большая часть информации хранится на компьютерах, так как этот способ хранения удобен и легче подвержен обработке. Поэтому наибольшее число хищений информации производится именно с компьютеров.

Для пресечения попыток воровства информации можно использовать множество методов. Первый и самый главный способ – это законодательная защита информации и её владельцев от посягательств злоумышленников. Второй – ограничение доступа посторонних лиц к тем компьютерам, на которых хранится информация; осуществление периодической проверки сотрудников «на чистоплотность», установка различных паролей и тому подобное.

Но дело значительно осложняется, если компьютер работает в сети. В этом случае запретить доступ к компьютеру полностью невозможно, так как основной принцип функционирования сети – это общение и обмен информацией. Вот тут и возникает соблазн для всевозможных взломщиков и просто любопытных воспользоваться наличием окна, через которое можно пробраться к «желанному» компьютеру.

Основным удобством для сетевого «информационного грабителя» является возможность длительное время пытаться взламывать систему защиты, не боясь при этом быть обнаруженным. Не следует надеяться на то, что будет найдена универсальное решение по защите сети, поскольку происходит дальнейшее увеличение размеров сетей и их объединение. Есть ещё несколько других причин, по которым взломщикам не стоит опасаться потери работы. Программное обеспечение всё более усложняется. При этом неизбежны ошибки и недоработки, которыми может воспользоваться достаточно подготовленный человек. Сбоям в системе защиты информации способствует и то, что в работе современных предприятий происходит дальнейший переход с бумажного документооборота на электронный. Ещё одной немаловажной причиной утечки информации является отсутствие культуры её охраны и сбережения.

Однако для конкретной организации создание эффективной и работоспособной системы защиты информации является реальной и выполнимой задачей. Дело в том, что на любом предприятии возможны локализация компьютеров и других устройств, содержащих конфиденциальную информацию, и сокращение доступа к ним посторонних людей и

персонала. При этом встаёт вопрос об эффективности вводимых ограничений, так как чрезмерное сокращение доступа к информации влечёт за собой увеличение потерь времени при работе с данными, а также материальных потерь. Поэтому следует решить и вопрос о зависимости важности информации и степени её защиты. Помимо ограничения доступа есть иной способ защиты – установление различных защитных программ, так называемых сетевых экранов и фильтров, а также программ, защищающих от вирусов и троянских коней, о которых будет сказано ниже.

1. Общие сведения о защите информации

Проблема защиты электронной информации назрела давно. Технологии опережают в своём развитии негласные нормы и правила поведения при работе с электронными источниками данных, а также процесс совершенствования законодательной базы. Возникает как бы культурное запаздывание в области информационных технологий, когда объект уже есть, а как вести себя по отношению к нему – неизвестно.

В сложившейся ситуации каждому владельцу более или менее ценных данных впору впасть в отчаяние. Может даже возникнуть впечатление, что «сопротивление бесполезно» и лучше хранить всё по старинке на бумаге, так, как делали это наши предки много веков подряд.

Но оставаться в зависимости от бумаги не только невыгодно, но уже невозможно. Человек (организация) не является одиноким в этом мире. Передача информации крайне необходима. При этом остро встаёт вопрос о скорости её передачи. Если много веков назад вполне приемлемой была передача корреспонденции со скороходом, то теперь даже пересылка информации с помощью авиаперевозок не соответствует ритму жизни современного предприятия. Передача же информации с помощью электронных сетей имеет большие и при этом жизненно необходимые преимущества. Так что, хотим мы того или нет, переход на новые средства передачи данных неизбежен, и поэтому становится актуальной потребность в защите информации в электронном виде. При этом важно отметить, что специалисты со всей ответственностью утверждают, что «создание полноценной и работоспособной системы защиты информации является не выдумкой, а реальностью».

Прежде всего следует осознать простую истину: «Никто не сделает твою работу за тебя». Защита информации – это прежде всего забота самого владельца, а не каких-либо организаций, работающих в данной сфере. Они могут быть лишь помощниками, советчиками, но вся ответственность полностью лежит на владельце. Именно он будет принимать окончательное решение, касающееся охраны информации, а в случае неудачи нести потери.

Таким образом, первый принципиальный момент – это решение проблемы по разграничению ответственности и прав доступа к информации. Каждый сотрудник должен иметь чётко определённые права и обязанности. Процедура доступа должна быть строго фиксированной. Лучше потерять немного времени, чем потом каяться в том, что из-за желания сделать всё быстрее случилась неприятность.

Однако при этом надо отдавать себе отчет в том, что чрезмерное усложнение процедуры доступа может значительно снизить производительность работы, а то и вовсе её заблокировать. Следовательно, владельцу информации необходимо принять разумное и взвешенное решение.

И таких принципиальных вопросов, для решения которых нет необходимости погружаться в море проблем, связанных непосредственно с техникой, обрабатывающей информацию, довольно много. Только когда все они будут решены, можно приступать к технической стороне дела.

При решении технических проблем важно определить необходимую степень ограничения свободы действий пользователей. Разнообразные сетевые экраны, «запирающие» те или иные программы, сканеры и антивирусные программы, как бы они ни были хороши, могут сильно и неоправданно ограничить права и возможности сотрудников. Избыточная защита хоть и даёт ощущение безопасности, часто не является жизненно необходимой, а иногда и вредит работе, так же как и жесткая бюрократия.

Итак, основной вывод из всего сказанного: «Разумность должна быть во всём». Оправданная необходимость, и только она, должна приниматься в расчет при защите информации. Создать же систему безопасности вполне реально, если подходить к вопросу грамотно. Поэтому паники по поводу собственной незащищённости быть не должно. Необходимо просто постоянно работать над совершенствованием системы информационной безопасности.

2. Статьи Уголовного кодекса Российской Федерации, относящиеся к преступлениям в сфере компьютерной информации

В Уголовном кодексе Российской Федерации имеется глава 28-я, содержащая статьи 272, 273, 274, предусматривающие ответственность за преступления в сфере компьютерной информации (приняты Государственной Думой 24 мая 1996 года). Авторы советуют читателю ознакомится с ними прежде, чем перейти к чтению этой книги.

Итак:

ГЛАВА 28. ПРЕСТУПЛЕНИЯ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ.

Статья 272. Неправомерный доступ к компьютерной информации.

1. Неправомерный доступ к охраняемой законом компьютерной информации, то есть информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети, – наказывается штрафом в размере от двухсот до пятисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от двух до пяти месяцев, либо исправительными работами на срок от шести месяцев до одного года, либо лишением свободы на срок до двух лет.

2. То же деяние, совершенное группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, а равно имеющим доступ к ЭВМ, системе ЭВМ или их сети, – наказывается штрафом в размере от пятисот до восьмисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от пяти до восьми месяцев, либо исправительными работами на срок от одного года до двух лет, либо арестом на срок от трех до шести месяцев, либо лишением свободы на срок до пяти лет.

Статья 273. Создание, использование и распространение вредоносных программ для ЭВМ.

1. Создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, а равно использование либо распространение таких программ или машинных носителей с такими программами – наказываются лишением свободы на срок до трех лет со штрафом в размере от двухсот до пятисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от двух до пяти месяцев.

2. Те же деяния, повлекшие по неосторожности тяжкие последствия, – наказываются лишением свободы на срок от трех до семи лет.

Статья 274. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети.

1. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим доступ к ЭВМ, системе ЭВМ или их сети, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ, если это деяние причинило существенный вред, – наказывается лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет, либо обязательными работами на срок от ста восьмидесяти до двухсот сорока часов, либо ограничением свободы на срок до двух лет.

2. То же деяние, повлекшее по неосторожности тяжкие последствия, – наказывается лишением свободы на срок до четырех лет.

Глава 1

ТРОЯНЦЫ XXI ВЕКА

1.1. Троянские кони и их отличия от вирусов и червей

Что понимается под троянскими конями в компьютерных науках?

Определение 1.1. *Троянский конь – это программа, предназначенная для выполнения определенных функций, преднамеренно скрывающая свои действия от владельца компьютера.*

Итак, данная программа делает всё возможное для того, чтобы владелец до поры до времени не заметил её пребывания на своей машине. Как правило, изначально она не регистрирует себя в реестре. Вот здесь и возникает первое отличие троянского коня от вируса.

Определение 1.2. *Троянский конь не делает своих копий даже после активизации. Действует только тот экземпляр, который вам «подарили».*

Создают свои копии, тиражируют себя на жестком диске компьютера, в его памяти и по сети, загружая тем самым ресурсы системы, другие вредоносные программы — вирусы и *черви*. «Червь отличается от вируса тем, что не несет в себе никакой «логической бомбы»[1], его единст-

[1] *Логическая бомба* — программа, содержащая код, переключающийся в режим атаки при определенных условиях. Например, логическая бомба может

венное назначение — самотиражирование. Некоторые черви распространяются через сообщения электронной почты» [9].

Несмотря на то что определения 1.1 и 1.2 не являются точными и исчерпывающими (под них, например, попадают некоторые программы, не являющиеся троянами), они в целом характеризуют понятие троянского коня. Уместно заметить, что неоднократно поднимался вопрос о том, что коммерческое программное обеспечение удаленного администрирования системы, содержащее функции скрытой установки, может быть причислено к троянам[2].

Условно всех троянов делят на четыре подкласса [8,10,11]:

1. **PSW-троянцы**, занимающиеся хищением и отправкой конфиденциальной информации жертвы по определенному адресу. В классификации AVP их называют PSW-троянскими конями (Password-Stealing-Ware).

2. **Backdoor** – предназначены для скрытого удаленного администрирования компьютера в сети. Эти троянцы обеспечивают полный доступ к ресурсам атакованной системы. Функции, заложенные в «продвинутые» трояны этого типа, исчисляются десятками. Являются самыми высокотехнологичными из троянцев и наиболее потенциально опасными. Используется технология «клиент-сервер», в связи с чем процесс их обнаружения более легок, чем PSW-троянов.

3. **Логические бомбы**. Это программы, совершающие какие-либо разрушительные действия. В зависимости от определённых условий они при каждом запуске уничтожают информацию на дисках, «подвешивают» систему и т.п.

4. **Дропперы** (носители). Это зараженные программы. Их код подправлен таким образом, что известные версии антивирусных

уничтожить все файлы 5 декабря. В отличие от вирусов логические бомбы не делают своих копий.

[2] Будем использовать для троянских коней следующие наименования: трояны, троянцы, кони.

программ не определяют в них троянца. Дроппер является одновременно программой-инсталятором самого троянца.

Размеры троянцев варьируются от 1Kb до 150Kb. Больший размер практически не используется потому, что перемещение коня на машину жертвы становится слишком заметным, что невыгодно для взломщика.

После приведенной классификации становится очевидной опасность, связанная с троянскими конями. Прежде всего по чисто материальным соображениям: мало кто захочет добровольно оплачивать использование Internet за какого-то довольно шустрого собрата по увлечению (не в смысле установки коней, а в смысле использования сети). Но это ещё самый безобидный вариант. Куда более мрачное будущее может ожидать компанию, предприятие или организацию, занимающихся разработкой продуктов, ценность которых заключается в их секретности и недоступности для конкурентов. Ведь после того как троянский конь сделал своё чёрное дело и отправил информацию о разработке конкурентам или тем, кому не предполагалось, остаётся только подсчитывать убытки.

Как видим, **вирусы** можно считать безобидной шалостью потому, что они **портят информацию либо в худшем случае оборудование, но не открывают тайн тем, кто их не должен знать**. Тут же на поверхности лежит и самый простой способ защиты, а скорее предотвращения последствий действия коней – отключение машины от сети. Но для кого такая защита приемлема?

1.2. Некоторые троянцы

На сайте http://www.viruslist.com/ находится «Вирусная энциклопедия», в которой в разделе «Троянские кони» описываются наиболее известные троянцы. Воспользуемся ею и приведем в этом параграфе сведения о некоторых из них.

1.2.1. Backdoor.BO, aka Back Orifice Trojan

Троянский конь BO (Back Orifice) является утилитой удаленного администрирования компьютеров в сети. Back Orifice является системой

удаленного администрирования, позволяющей злоумышленнику контролировать чужие компьютеры при помощи обычной консоли или графической оболочки. Данная программа устанавливает свою *серверную* компоненту на компьютере жертвы, а *клиетскую* на компьютере, который находится в распоряжении злоумышленника. В локальной сети или через Интернет Back Orifice предоставляет злоумышленнику больше возможностей на удаленном Windows-компьютере жертвы, чем имеет сам владелец этого компьютера.

Эту программу классифицируют как вредную троянскую программу, поскольку она не дает предупреждения об инсталляции и запуске и не выдает никаких сообщений о своих действиях в системе. Более того, ссылка на троянца отсутствует в списке активных приложений. В результате компьютер открыт для удаленного управления, а владелец об этом даже не догадывается.

Троянец распространяется как пакет из нескольких программ и документации. Все программы написаны на C++ и компилированы Microsoft Visual C++. Все программы имеют формат Portable Executable и могут выполняться только в среде Win32.

Основной программой в пакете является BOSERVE.EXE – это главная «серверная» компонента троянца, которая ждет вызовов от удаленных «клиентов», т.е. злоумышленников.

Вторым файлом является BOCONFIG.EXE, конфигурирующая «сервер» и позволяющая «прикрепить» BOSERVE.EXE к каким-либо другим файлам (как это делают вирусы). При запуске таких приложений вирус «выкусывает» их из зараженного файла и запускает на выполнение без каких-либо побочных эффектов.

В пакете также присутствуют две «клиентские» утилиты (консоль и графический интерфейс), они позволяют «клиенту» (= злоумышленнику) управлять удаленным «сервером». Еще две программы являются утилитами компрессии/декомпрессии файлов – они используются для копирования файлов с/на удаленный «сервер».

При запуске троянец инициализирует сокеты Windows, создает файл WINDLL.DLL в системном каталоге Windows, определяет адреса нескольких Windiows API, ищет свою копию в памяти и выгружает ее из памяти, если таковая обнаружена (то есть обновляет свою версию). Затем троянец копирует себя в системный каталог Windows и регистрируется в реестре как автозапускаемый процесс в ключе

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices.

Затем троянец перехватывает один из сокетов Windows (по умолчанию – сокет 31337) и остается в памяти Windows как скрытое приложение (то есть без активного окна и ссылки в списке приложений). Основная процедура перехвата сообщений затем ждет команд от удаленного клиента. Сокеты команды передаются в зашифрованном виде.

В зависимости от команды троянец выполняет следующие действия: 1) высылает имена компьютера, пользователей и информацию о системе: тип процессора, размер памяти, версия системы, установленные устройства и т.п.; 2) разрешает удаленный доступ к дискам (sahre); 3) ищет файл на дисках; 4) посылает/принимает файл, так же как уничтожает, копирует, переименовывает, выполняет любой файл; 5) создает/уничтожает каталог; 6) упаковывает/распаковывает файл; 7) отключает текущего пользователя от сети; 8) завешивает компьютер; 9) высылает список активных процессов; 10) выгружает указанный процесс; 11) подключается к сетевым ресурсам; 12) получает и отправляет кешированные пароли (которые использовались владельцем в течение текущего сеанса), ищет пароль для ScreenSaver (расшифровывает и отправляет); 13) выводит MessageBox; 14) читает/модифицирует системный реестр; 15) открывает/перенаправляет другие сокеты TCP/IP; 16) поддерживает протокол HTTP и эмулирует Web-сервер (то есть троянцем можно управлять при помощи браузера); 17) проигрывает звуковые файлы; 18) перехватывает, запоминает и затем высылает строки, вводимые с клавиатуры в момент подсоединения компьютера к сети и т.д.

Троянец также позволяет расширить список своих функций при помощи подключаемых ресурсов (plug-in). Они могут быть переданы на «сервер» и инсталлированы там как часть троянца и в дальнейшем могут выполнять практически любые действия на пораженном компьютере.

1.2.2. Trojan.AOL.Buddy

Создан Алексеем Подрезовым, Data Fellows Ltd. Троянский конь «Trojan.Aol.Buddy» (другое имя – «PennyTools Trojan») ворует пароли входа в Internet у пользователей известного провайдера **America Online.**

Используются следующие способы внедрения на компьютеры, реализующие одновременно пять различных уловок для создания дополнительных трудностей при удалении троянца:

1. При помощи системного реестра Windows. Изменяется ключ RUN для запуска скрытого файла C:\COMMAND.EXE, содержащего в себе тело этого троянца.

2. При помощи изменения файла SYSTEM.INI. Добавляется в него ссылка на скринсэйвер C:\Windows\System\WINSAVER.EXE. Система заражается в момент запуска этого скринсэйвера.

3. При помощи изменения файла WIN.INI. Добавляется в него запуск скрытого файла C:\America Online 4.0\BUDDYLIST.EXE в строку "LOAD=". Интересно то, что между самим именем файла и строкой "LOAD=" троянец ставит ровно 80 символов, так чтобы пользователь (владелец) не смог сразу увидеть эту ссылку.

4. Также в файл WIN.INI добавляется запуск скрытого файла C:\Windows\System\NortonAntiVir\REGISTRYREMINDER.EXE в строку "RUN=".

5. В папку автозагрузки (\Windows\Start Menu\Programs\Startup) добавляется файл AIM REMINDER.EXE.

В каталоге \Windows\System создается файл VCLCNTL.DLL, содержащий отнюдь не DLL код, а определенные текстовые данные, необходимые самому троянцу. При запуске Windows он также запускается, используя один из описанных выше способов, и остается активным все время работы операционной системы.

Программа находит и посылает имя и пароль пользователя системы **America Online** на адреса электронной почты

qware4019@hotmail.com или ha015312@hotmail.com.

1.2.3. Macro.Word97.Trojan.Tvangeste [8]

Макрос относят к троянским коням. Он добавляет в конец файла autoexec.bat команды, удаляющие все данные на дисках C:,D:,E:, и затем выводит на экран сообщения:

World War starting now!
Tvangeste v 1.0
3rd World War.

Затем макрос входит в бесконечный цикл, в котором выводит на экран сообщение:

3rd World War.

Tvangeste.b

Сохраняет копию зараженного документа под именем

"C:\Program Files\Microsoft Office\Шаблоны\kafeln.dot"

и добавляет в конец файла autoexec.bat команды:

```
cd C:\Program Files\Microsoft Office\Шаблоны  del normal.dot
                ren kafeln.dot normal.dot.
```

Таким образом, макрос пытается заменить шаблон «по умолчанию» на зараженный шаблон, но это работает только в том случае, если в MS Word установлен каталог шаблонов ("C:\Program Files\Microsoft Office\ Шаблоны\").

В файл autoexec.bat добавляются команды:

```
 md c:\atp_tour
md c:\atp_tour\kafelnik.001
md c:\atp_tour\sampras.002
md c:\atp_tour\corretja.003
md c:\atp_tour\rafter.004
md c:\atp_tour\moya.006
md c:\atp_tour\henman.007
md c:\atp_tour\rios.008
md c:\atp_tour\philipou.009
```

```
md c:\atp_tour\kucera.010
md c:\atp_tour\krajicek.005
subst k: c:\atp_tour >nul
```

Затем макрос выводит на экран сообщения:

```
3 мая 1999 года Кафельников - номер 1!!!!!!!!
3 мая 1999 года Кафельников - номер 1!!!!!!!!
Tvangeste v 2.0
Kafelnikov.
```

1.2.4. Trojan.Spy.KIM [8]

Это троянский конь, работающий в системе Windows и скрытно записывающий в файл заголовки всех открываемых окон и название кнопок, которые были нажаты в этих окнах.

При запуске устанавливает в систему три файла:

```
%WinDir%\System\Krnl40.dll
%WinDir%\heak.exe
%WinDir%\ki.ini .
```

Лог-файл с именем "key.dl" создается в каталоге, где установлена Windows (%WinDir%).

1.2.5. Trojan.PKZ300b [12]

Представляет собой самораспаковывающийся архив (Zip2Exe) с именем PKZ300B.EXE и длиной 178,981 байт. Внутри архива – 5 файлов:

PKZINST.EXE	5,328	сам троянец
WHATSNEW.300	2,417	WhatsNew из PkZip 2.04c, все строки 2.04c заменены на 3.0
COMPRESS.000	124,005	ARJ 2.41, плюс экстраданные

COMPRESS.001 116,260 ARJ 2.41 сам по себе

FILE_ID.DIZ 101 DOC-файл, говорит про этот архив,

что он – Pkzip 3.00b.

Троянцем является единственный файл – PKZINST.EXE. Написан он на Турбо-Паскале. При запуске выводит текст

PKZIP Install Utility Version 3.00b 4-05-950

Copr. 1989-1995 Pkware Inc. All Rights Reserved.

Pkzip Reg. U.S. Pat. and Tm. Off.

Initializing, this may take a few minutes....

и выполняет две команды:

COMMAND.COM /C Format c: NULL

COMMAND.COM /C deltree /y c: \ NULL.

К счастью, автору троянца не хватило ума сделать его без ошибок, и он на первой же команде – DOS ждет ответа на стандартный запрос

WARNING: ALL DATA ON NON-REMOVABLE DISK DRIVE C:
WILL BE LOST!

Proceed with Format (Y/N)?

Причем самого этого запроса на экране не видно. **При нажатии клавиши Y пойдет форматирование диска C, а если нажать N, то сработает DELTREE**. Однако естественно желание при виде «заснувшей» программы – нажать Reset или [Ctrl]+[Break]. В обоих случаях троянец отключается безо всякой потери данных; а если выход произошел по [Ctrl]+[Break], то он еще говорит напоследок Thanks for waiting, moron. You shouldn't have fucked with us и покидает DOS. Так что благодаря этой ошибке пользователь может спать спокойно и не бояться новых версий PKZip.

В этом троянце есть еще одна ошибка. Перенаправление NULL создает на диске файл NULL, а автор троянца, видимо, хотел отключить посторонний вывод на экран перенаправлением NUL. Судя по всему, это юное дарование читает DOS User's Guide и еще не дошло до буквы N в алфавитном списке команд DOS.

AVP ловит этого троянца под именем Trojan.PKZ300b как в распакованном файле, так и в архиве.

1.2.6. mIRC SCRIPT.INI [13]

SCRIPT.INI является скриптом mIRC (популярного IRC-клиента для Windows), распространение которого в настоящее время в большинстве крупных IRC-сетей принимает масштаб эпидемии. Скрипт запрограммирован таким образом, что позволяет другим людям управлять вашей IRC-сессией, просматривать ваши диалоги, читать ваши файлы и вмешиваться в работу IRC.

Для распространения скрипт использует возможности mIRC, представляющих потенциальную. угрозу безопасности: автоматический прием файлов по DCC и автоматическое выполнение файла SCRIPT.INI в каталоге mIRC.

Для того чтобы обезопасить себя от данного троянца, надо просто посмотреть, не присутствует ли в каталоге mIRC файл SCRIPT.INI, или запустить программу поиска подобных файлов по диску. SCRIPT.INI представляет для вас опасность **только в том случае**, когда находится в каталоге, откуда mIRC берет стартовые файлы (например **C:\MIRC**). Если для dcc-файлов используется что-нибудь вроде **C:\DOWNLOAD**, то вы в безопасности.

1.3. Троянцы на основе технологии Active X

Для начала несколько слов о самой технологии Active X. В основу концепции Active X положено две основных идеи Microsoft: объектная компоновка – OLE (Object Linking and Embedding) и компонентная объектная модель – COM (Component Object Model).

Можно считать (а именно так считает сама Microsoft), что Active X – это продолжение, некая модернизация OLE применительно к Internet. Да, во многом сходство есть. Active X так же, как и OLE, созданы для интеграции одних приложений в другие. Так, можно вставлять Excel-таблицы в документы Word. В принципе почти ничто не препятствует применению старой технологии OLE в случае использования в сетях. Почти, но не всё. OLE-объект получается слишком сложным и громоздким для того, чтобы работать с ним в условиях, когда информация передаётся по сети. Ведь нам придётся подкачивать данные с сервера, который может находиться очень далеко от точки, в которой необходимо запустить нужное приложение. Чересчур много лишних действий.

Поэтому идеи переработаны, объекты упрощены и модернизированы, а также объединены в одну общую платформу.

Как утверждает корпорация Microsoft, на данный момент существует более 1000 объектов данного типа. Не вдаваясь в тонкости классификации, которая будет дана ниже, сразу перейдём к принципам работы данной технологии.

Все элементы Active X, за исключением тех, что написаны с использованием Java, хранятся в файлах с расширением .OCX. В web-документ данные объекты встраиваются с помощью дескриптора OBJECT. Здесь же указывается то место, откуда в случае необходимости система должна будет загрузить код запускаемого элемента.

Итак, пользователь решил обратиться к Active X (например, возникло желание прослушать некоторый прикреплённый звуковой файл). Система обращается к системному реестру, делая запрос по поводу наличия кода данного объекта на жёстком диске машины. Если данный код на диске присутствует, то в оперативную память он выгружается сразу с диска. А если нет? Вот тогда и начинается выкачивание всей необходимой информации из сети.

Тут-то и кроется подвох. Перечень возможностей Active X очень велик: от просмотра ролика до таких привилегированных действий, как прямое обращение к диску или запуск нового процесса. Следовательно, загружая web-страницу с элементами Active X, вы можете получить из сети неприятный «подарок».

Здесь, наверное, стоит дать классификацию элементов Active X.

В своем последнем воплощении (учитывая всю ее новейшую техническую терминологию) Active X состоит из пяти основных компонентов, охватывающих клиентскую и серверную стороны:

- Элементы управления *Active X* – выполняемые объекты размером с мини-программу (applet), встраиваемые в Web-страницу. Согласно Microsoft, на рынке сегодня имеется более 1000 таких элементов (многие из них существовали ранее в виде объектов OLE). Их можно разрабатывать с помощью разнообразных инструментальных средств и языков программирования, включая C/C++, Visual Basic, Delphi и даже Java. Об инструментах для разработки *Active X* мы еще скажем.
- Документы *Active X* обеспечивают возможность просмотра в Web-браузере документов, не удовлетворяющих спецификации HTML (например файлы Word и Excel).
- Active Scripting – языки сценариев, включая VBScript на основе Visual Basic и JScript (собственную реализацию JavaScript корпорации Microsoft), с помощью которых можно компоновать вместе или интегрировать элементы управления *ActiveX* и активные объекты Java как на сервере, так и в браузере.
- Java Virtual Machine (VM) – созданная Microsoft собственная программно реализованная виртуальная машина, которая, по заявлениям компании, исполняет код Java лучше виртуальных машин Sun или Netscape. Кроме того, Java VM корпорации Microsoft допускает интеграцию элементов управления *Active X* и активных объектов Java.
- *Active X* Server Framework – серверная архитектура, обеспечивающая на Web-сервере такие функции, как защита и доступ к базам данных.

Как мы видим, возможностей очень много. При этом стоит учесть, что данные приложения постоянно разрабатываются (жизнь всё-таки не стоит на месте). И ничто в принципе не мешает под видом игрушки создать нечто вредоносное.

Microsoft попыталась решить эту проблему с помощью сертификатов Authenticode. Данные сертификаты дают «знак безопасности и благонадёжности» проверенным программам. Но были случаи, которые описаны в литературе [8], когда авторы получали сертификат на программы, действие которых можно назвать безвредным с большой натяжкой. Например, некто Fred McLain в 1996 году получил подтверждение безопасности на программу Internet Exploder, которая просто корректно (обратим внимание, что в этом случае ещё корректно) завершала работу компьютера, если на нём была установлена Windows 95 с улучшенной

системой электропитания. Необходимо заметить, что сертификат был получен официально, автор не скрывал того, что делает его программа, а также позаботился о том, чтобы работа прекращалась корректно. Но можно ли быть уверенным в том, что кому-нибудь не захочется ввести в заблуждение пользователя? Хотелось бы, но нельзя быть излишне доверчивым.

Конечно, в данном случае после того, как автор выложил созданную и сертифицированную программу на своём сайте, Microsoft заметила это и лишила новый элемент сертификата, ссылаясь на то, что программист обманул ожидания компании. Тем не менее стоит лишний раз подумать, прежде чем разрешать на своей машине загружать элементы Active X.

Ещё одним способом, позволяющим обойти систему защиты, созданную компанией Microsoft, является установка на программе флага Safe for scripting (помеченный как безопасный).

Что происходит при выставлении такого флага? Ничего особенного, просто игнорируется процедура проверки элемента Active X на наличие у него сертификата безопасности. Заметим ещё раз: ЭЛЕМЕНТЫ ACTIVE X СПОСОБНЫ ОСУЩЕСТВЛЯТЬ МНОГИЕ ПРИВИЛЕГИРОВАННЫЕ ДЕЙСТВИЯ: ЗАПИСЬ НА ДИСК, ЗАПУСК НОВЫХ ПРОЦЕССОВ И Т.Д.

Как установить данный флаг? Для этого в реестре в ключе Implemented Categories для выбранного элемента следует задать дополнительный параметр 7dd95801-9882-11cf-9fa9-00aa006c42c4.

Отвлечёмся ненадолго от рассматриваемых элементов и вернёмся к троянским коням. Что необходимо для начала деструктивной деятельности программы? Активировать процесс. Почти все уловки злоумышленников направлены на то, чтобы обмануть владельца компьютера, скрыть от него факт установки программы и под каким-либо предлогом заставить его активировать троянца. Например, используются прикреплённые файлы «обновления программ», якобы рассылаемые производителем, письма, отправленные по адресам, находящимся в почтовых ящиках ваших знакомых. Мы видим не более чем один из новых способов обмана. Только обмана более технологичного. Закачка может быть разрешена по умолчанию (о способах предотвращения закачки ниже).

Проблема заключается ещё и в том, что технология Active X ещё довольно молода, к тому же бурно развивается. Поэтому постоянно находятся всё новые лазейки в системе безопасности, связанной с ней. Microsoft, конечно же, стремится постоянно заделывать обнаруженные бреши, периодически выпуская обновления своего программного обес-

печения. Но не все пользователи следят за этими новшествами, поэтому рядовую машину зачастую можно «вскрыть», не тратя на это много времени. Помимо всего прочего в Java, использующей новые элементы, есть свои недоработки, которыми может воспользоваться злоумышленник.

1.3.1. Способы защиты

Начнём с элементарного. Прежде всего следует отдавать себе отчёт в том, что всякое неразумное действие может повлечь за собой неблагоприятные последствия. Поэтому стоит задуматься, есть ли смысл заходить на сайты с сомнительными названиями, вскрывать письма от неизвестных вам людей и т.д.

Но это всё общие фразы. Теперь стоит рассказать о нескольких реальных способах противодействия разрушениям, приносимым с помощью Active X.

1. Использование зон безопасности компьютера

Существует четыре выделенные зоны безопасности, из которых может загружаться код или доставляться другие данные. Это:

1. Local Intranet (местная зона).
2. Trusted Sites (зона надёжных узлов).
3. Internet (зона Internet).
4. Restricted Sites (зона ограниченных узлов).

Есть ещё одна зона – Local machine, но в режиме пользователя она недоступна (доступ осуществляется через настройку с помощью средств администрирования IE Administration Kit).

К зоне Internet по умолчанию относятся все узлы, содержащие в своём адресе “.”, не включённые в другую зону. Во все остальные зоны узлы можно включать вручную. Когда производится попытка загрузить страницу с некоторого узла, находящегося в той или иной зоне, активизируется политика безопасности, установленная в ней. Кстати, Active X в данной политике безопасности проходят отдельным пунктом, и не одним.

Заметим, что к зоне Internet приписаны по умолчанию почти все узлы. Поэтому к политике безопасности в этой зоне необходимо отнестись наиболее серьёзно.

Несколько слов непосредственно о настройке параметров безопасности.

На панели управления выбирается вкладка Internet Properties, а на ней страница Security (рис.1.1).

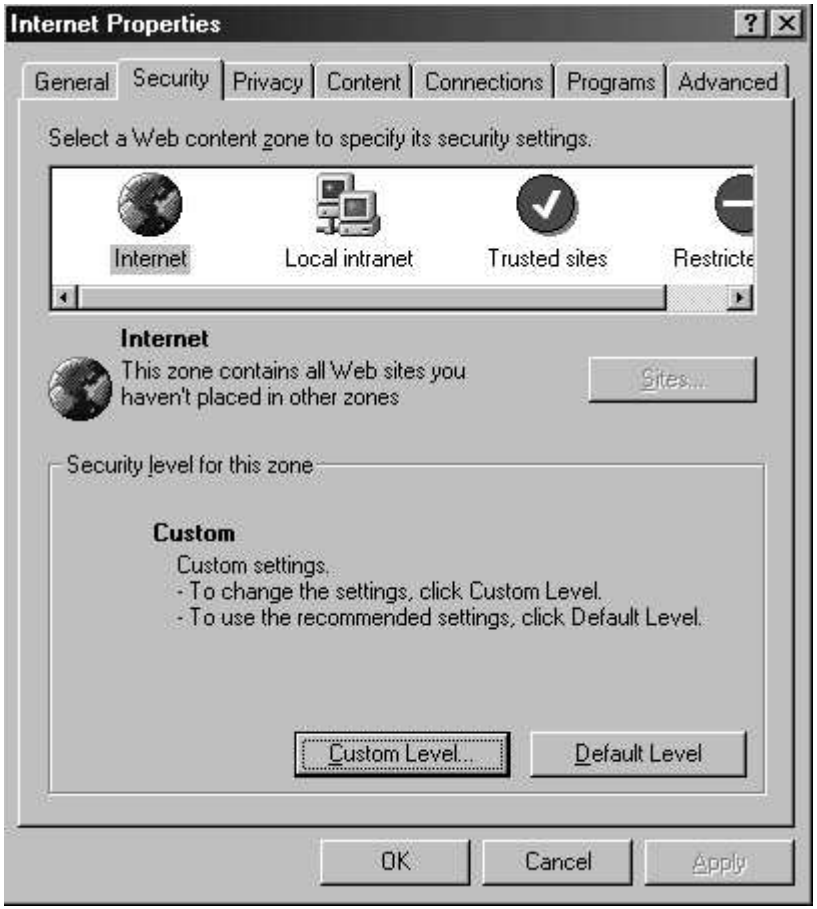

Рис.1.1. Вкладка зоны безопасности в меню **Настройка**

Затем выбирается зона Internet, а в ней Custom Level. После этого выпадает вкладка со множеством пунктов настройки, с которыми стоит разобраться (рис.1.2).

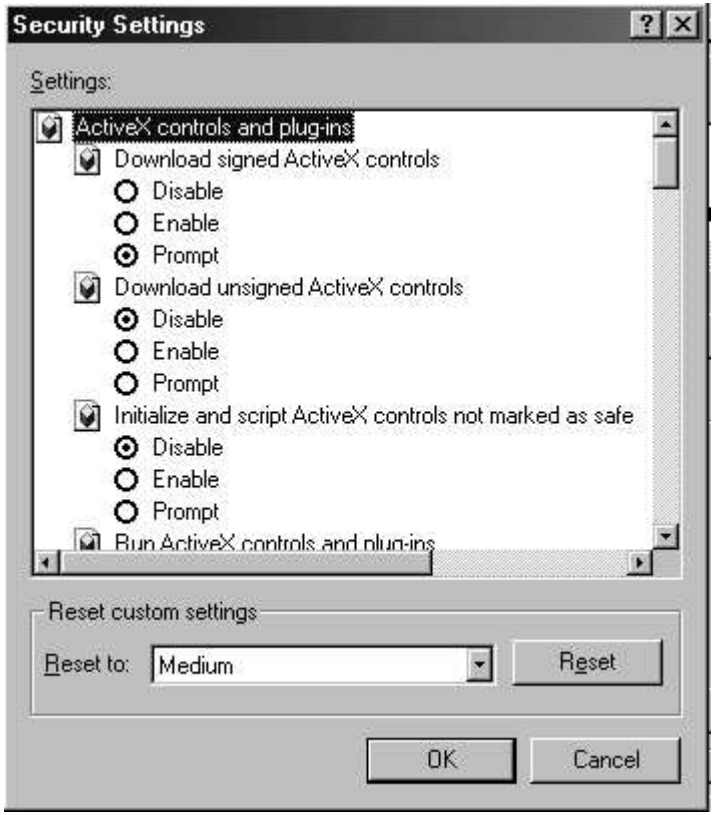

Рис.1.2. Вкладка **Настройка** уровня безопасности зоны Internet

Естественно, что сразу возникнет вопрос: «Как настроить?» Ответить на него каждый должен сам. Подписи на вкладке довольно доходчиво сообщают о том, что является следствием их выбора. Стоит только представлять себе, что, конечно, вы можете запретить использование элементов Active X. Но, с другой стороны, это означает отказ от преимуществ, которые даёт данная технология. Можно отгородиться от

всего мира, жить уединённо, но тогда жизнь может пройти мимо. Да и есть возможность при каждом случае, когда необходимо совершить манипуляции с данными элементами, запрашивать разрешение на исполнение операции у пользователя.

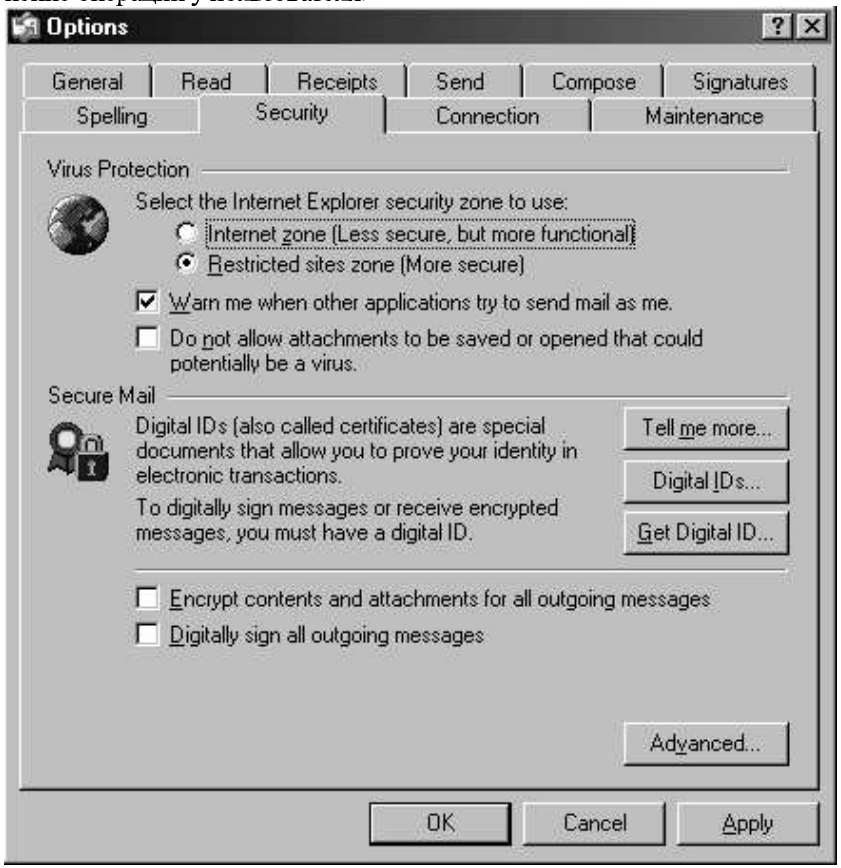

Рис.1.3. Настройка зон безопасности Outlook Express

Заметим, что помимо глобальной настройки уровня безопасности с помощью зон Internet возможна также отдельная настройка данных параметров для отдельных приложений. По сути довольно немногие программы нуждаются в регулярном использовании сети. Поэтому довольно логично, что их можно настраивать отдельно. Характерным приме-

ром служат почтовые программы. Рассмотрим подробнее приложение Outlook Express, так как именно эта программа используется как приложение для работы с электронной почтой по умолчанию.

Outlook является продуктом корпорации Microsoft, поэтому концепция разделения зон безопасности перекочевала и сюда. С помощью пункта в меню Tools → options → security можно получить доступ к странице, позволяющей настроить степень внимания к собственной безопасности (рис.1.3.).

Сразу обратим внимание на то, что доступны только две зоны: Internet и Restricted Sites.

Зайдя во вкладку Advanced, можно изменять установки для выбранной зоны, действующие по умолчанию. Обратим внимание, что активные элементы в почтовых сообщениях используются крайне редко, поэтому, если приходит письмо, богато сдобренное ими, стоит задуматься о его безопасности. Авторы считают, что отключение возможности использования Active X в электронных сообщениях не повлечёт за собой сколько-нибудь заметного ухудшения качества переписки.

В чём ещё заключается смысл ужесточения политики безопасности работы электронной почты? Вспомним один из базовых способов взлома. Вскрывается чей-либо почтовый ящик. Что скрывать, зачастую о безопасности собственной почты мы заботимся не слишком усердно. После этого составляется сообщение, в него добавляется вредоносная составляющая (вот тут-то и пригодился безобидный Active X), скрываемая от получателя до поры до времени либо маскируемая под полезную информацию. Самое интересное, что адрес отправителя знаком получателю сообщения, это его товарищ, коллега, родственник и т.д. Ничего не подозревая, он открывает письмо, и Active X автоматически, именно автоматически, начинает спокойно загружать себя. А уж что он загрузит, предугадать нельзя. Тут может быть и троян, и вирус, и просто глупая шутка. Как видим, раскрывать такие письма не совсем безопасно. С другой стороны, прочитать письмо без весёлой песенки на фоновом режиме вполне можно, при этом никакого волнения, а также обид на друзей. Однако это уже элементы системы защиты.

Следует заметить, что в данный момент большинство сайтов используют HTML, который исполняет задания непосредственно на сервере. Однако есть сайты, которые опираются на использование Active X.

В зону надёжных узлов можно включить официальные сайты интересующих вас организаций, а также те, к которым вы многократно обращались без негативных последствий. Хотя и здесь сохраняется опасность того, что сайт будет взломан и с него будет получен доступ к вашей машине. Правда, это уже из области навязчивых идей.

2. Флаг Safe for scripting

Основным способом защиты от опасности, скрывающейся в установке данного флага, является периодическая установка обновлений для своей операционной системы. Компания Microsoft, как создательница данной технологии, стремится всё глубже внедрить её в жизнь. Поэтому вопрос безопасности рассматриваемых элементов стоит для корпорации очень остро. Необходимо убедить потенциальных клиентов в безопасности своего продукта, из-за чего приходится постоянно выпускать обновления, отслеживающие и обезвреживающие вновь созданные небезопасные элементы Active X. Найти данные обновления можно по адресу

http://www.microsoft.com/technet/security/bulletin/ms99-32.asp

либо

http://officeupdate.microsoft.com/2000/downloadDetails/Uactlsec.htm .

Только нужно помнить, что постоянно создаются новые программы и обновления требуется устанавливать периодически.

Макросы Office можно защитить, изменив уровень безопасности на высокий в самой программе (каждая программа настраивается отдельно).

Ну и самый радикальный, при этом не самый лучший, метод – отказ от использования Active X. Но о всех прелестях данного решения вопроса было сказано выше.

1.4. Проникновение в систему

Теперь несколько слов о способе проникновения троянца на вашу машину. Конечно же, основной способ – это посылка электронного письма «неизвестно откуда». При этом конь может находиться где угод-

но и в какой угодно форме. Это может быть часть rar или zip архива, макрос в документе Word плюс всевозможные ActiveX-вещи и многое другое. Во-первых, засылка троянца в виде электронного письма гарантирует в отличие от распространения с компакт-дисками и другими носителями информации наличие подключения к сети, через которую можно будет отправлять информацию лицу, пославшему это письмо. Во-вторых, много людей очень часто рады прочитать «безобидное» письмо с заманчивым названием. Это только потом у них начинаются проблемы.

Приведем пример одного из таких посланий [1]. Оно не является письмом без отправителя, наоборот, вроде бы в нём сомневаться не приходится:

```
From: support@microsoft.ru
To: rik@microsoft.ru
Subject: Microsoft Corporation Update.

Добрый День!
   Вас приветствует менеджер по внешнеэкономической деятельности
и общих внешних связей Российского представительства корпорации
Microsoft Рик Киолски. По нашей информации, ваша система
Microsoft Windows, а конкретнее приложение Microsoft Internet
Explorer, отправила на наш локальный сервер 12 декабря 1999 года
запрос на аутенфикацию конкретного приложения. По нашим данным,
Ваш Microsoft Internet Explorer и библиотека Интернет работают
некорректно. Эта ошибка скорее всего вызвана при использованиим
версии WINSOCK.DLL -3.495.123.11a или ниже. Это может быть ошиб-
ка, отвечающая за безопасность операционной системы Windows,
подверженная атакам как локально, так и через Интернет. Это оз-
начает, что при использовании специального кода на javascript,
зайдя просто на какой-то сайт, Вы даже не заметите, как с Вашего
компьютера, благодаря ошибке Buffer Overflow (переполнение буф-
фера), пропадут многие файлы и работа ОС Windows в целом будет
нарушена.

ВАША ОС WINDOWS В ОПАСНОСТИ.

Для устранения этой ошибки мы предоставляем бесплатный патч, ко-
торый прикреплен к письму. Чем раньше Вы исправите эту ошибку -
тем больше шансов, что Ваша информация на жестких дисках и в се-
ти Вашей компании не подвергентся опасности. В целях Вашей безо-
пасности файл был проверен перед отправкой на наличие вирусов и
троянских коней антивирусной программой AVP последней версии.
Кроме того, чтобы предотвратить перехват файла между хостами
предоставляем его точное имя, размер и CRC32:patch-i386-win95-
win98-42332113.exe, 21645 Bytes, 312312A
```

Спасибо.

При получении такого письма стоит подумать: «Станет ли Microsoft рассылать такого рода программы?». Почему авторитетная и знаменитая фирма не объявила о неполадках официально? Почему она стала рассылать письма каждому пользователю по почте? Ответ очевиден – данный «подарок судьбы» является ловушкой. Но если вы не задумались и запустили прилагающуюся к письму программу, то вы заполучили троянского коня[3].

1.5. Обнаружение троянца

Итак, троянец уже на вашей машине. Как правило, данная программа сначала инициализирует сетевые каналы Windows. Иногда создаётся своя DLL. После этого программа обычно записывает себя в системный каталог, а потом регистрирует себя в реестре как автозапускаемый процесс, т.е. прописывает себя, например, в ключе

HKEY_LOCAL_MASHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices.

Так что если при очередном просмотре реестра вы заметили подключ с названием программы, которую вы вроде бы не устанавливали, то имеется повод задуматься и проверить, что это такое. В конце установки конь захватывает один или несколько сетевых каналов. Вот он и готов к действию.

У вас есть подозрения, будто что-то с вашей машиной не так. Например, она стала «тормозить» при загрузке сайтов (в 90% в этом виноват троян, приступивший к активной работе). Очень бы хотелось проверить, нет ли чего-нибудь лишнего. Как это сделать? Способов много. Приведем некоторые из них.

---

[3] Троянец **Trojan.WebMoney.Wmpatch** появляется в письме, говорящим, что пришла открытка: «Вы можете получить ее, щелкнув по ссылке: http://www.yahoo-greeting-cards.com/****/viewcard_680fe23d52.asp.scr ».

Способ 1. Можно установить антивирусную программу. Почти все из них отслеживают и вирусы, и коней. Желательно, чтобы антивирусная программа была резидентной (активной во время всей работы компьютера), так как в этом случае можно будет отследить момент попытки установки, а иногда узнать адрес «дарителя». Судя по откликам администраторов сетей (данные из сети), наиболее подходящим на эту роль является AVP лаборатории Касперского (см.§ 3.1).

Способ 2. Внимательно присмотритесь к названиям программ, загружающихся при запуске системы (прежде всего относится к Windows). Некоторые кони помещают себя в раздел автозагрузки, поэтому их можно заметить на данном этапе (при загрузке). Посмотрите "Пуск\ Программы\ Автозагрузка" и win.ini и system.ini (ключи run и load).

Способ 3. Реестр. Об этом уже кое-что говорилось. Если просмотреть ключи:

HKEY_LOCAL_MACHINE\ SOFTWARE\ Microsoft\ Windows\ CurrentVersion\ Run
HKEY_LOCAL_MACHINE\ SOFTWARE\ Microsoft\ Windows\ CurrentVersion\ RunOnce
HKEY_LOCAL_MACHINE\ SOFTWARE\ Microsoft\ Windows\ CurrentVersion\ Runservices
HKEY_LOCAL_MACHINE\ SOFTWARE\ Microsoft\ Windows\ CurrentVersion\ RunservicesOnce
HKEY_USERS\ .Default\ SOFTWARE\ Microsoft\ Windows\ CurrentVersion\ Run
HKEY_USERS\ .Default\ SOFTWARE\ Microsoft\ Windows\ CurrentVersion\ RunOnce
HKEY_USERS\ .Default\ SOFTWARE\ Microsoft\ Windows\ CurrentVersion\ Runservices
HKEY_USERS\ .Default\ SOFTWARE\ Microsoft\ Windows\ CurrentVersion\ RunservicesOnce,

то можно узнать очень много полезного. Например, если обнаружите строчку

Параметр: PATCH,
Значение: C:\ WINDOWS\ PATCH.EXE /nomsg,

то у вас прописался троян из серии BackDoor (см. список троянов в приложении 1 и список exe-файлов троянов в приложении 3).

Способ 4. Просматривайте панель работающих процессов. Для этого существует множество программ, например, в пакет Visual Studio входит программа Process Viewer Application. Вдруг вы заметите подозрительное приложение, имеющее приоритет выше, чем у Kernel32, или приложение имеет название, приведённое в приложениях 1,3. Может быть, стоит его проверить?

Способ 5. Проверяйте журнал удалённых подключений к вашей машине. Зачастую злоумышленник не удосуживается скрыть следы своего присутствия. Поэтому в журналах остаются адреса, с которых производилось подключение, а также login.

Способ 6. Используйте программы (см. §3.2), которые ведут слежение за сетевым трафиком. Данные приложения не пытаются предотвратить вторжение, но дают довольно много информации о том, с каких узлов производилось вторжение, о номерах используемых портов, а также информацию о пересылаемых пакетах. Минус тут один. Как уже говорилось, программа не препятствует взлому, а только ведёт журнал, поэтому приходится самостоятельно следить за трафиком и заботиться о своей безопасности. Но, согласитесь, дополнительная информация никогда не будет лишней.

Есть ещё несколько проблем, связанных с обнаружением вредоносных троянов. Во-первых, существует такая разновидность коней, которую очень трудно, а порой невозможно обнаружить антивирусными программами. Это так называемые *дропперы*. В чём причина их неуязвимости? Она до банальности проста. Любая антивирусная программа работает по принципу сравнения любой программы с программой-вредителем по имеющимся в базе данных признакам. Например, номер используемого порта. Но стоит только немного подкорректировать код вредителя, как он сразу станет невидимым. При этом не стоит принципиально менять действие программы. Достаточно самых минимальных изменений.

Авторы проверили это следующим образом. Взяли программу Alps6 и поменяли только номер используемого порта. Результатом стало то, что антивирусник Касперского молчал, когда программа работала, и не выказывал никаких признаков того, что она ему подозрительна, хотя начальную версию распознавал моментально. А портов, как известно, на машине очень много.

Существуют и другие варианты скрыть программу от антивирусных приложений. Это использование редких архиваторов. Многие авторы, пишущие по этому поводу статьи в сети Internet, утверждают, что результат будет тот же. Так как с архиваторами такого рода работать не приходилось, подтвердить этого нет возможности, как нет возможности и опровергнуть.

1.6. Удаление троянцев

Приведем некоторые способы удаления троянцев.

1. Если антивирусная программа обнаружила троянца, но не удалила его, то, во всяком случае, становится известной директория, в которой он находится. Попытка удалить его вручную ни к чему не приводит. Попытайтесь удалить директорию, в которой находится троян (предварительно скопировав незараженные файлы). Затем в свойствах корзины выбираем емкость, равную 0%, и нажимаем ОК. Троян удален. Однако хотя трояна нет на диске, он присутствует в ОЗУ. Чтобы удалить его, достаточно нажать кнопку RESET [14].

2. Если антивирусная программа не обнаружила троянца, а вы уверены, что он есть, то необходимо иметь в виду следующее. Новые троянцы и вирусы прописывают себя в **autoexec.bat** и запускаются при каждом включении машины. Хорошо, если вы помните, что у вас там было прописано до того, как подхватили троянца на диск. Тогда посмотрите, что вам незнакомо, и запомните, где оно находится на диске. Затем сотрите и сохраните изменения. Перезагрузитесь. Затем уничтожьте троян. Не советуем оставлять его в надежде потом посмотреть его исходник и т.д. Почему? Потому что вы можете ненароком его запустить, и все придется повторять сначала.

А если вы autoexec.bat до сей поры не видели, то стирайте в нем все кроме

```
mode con codepage prepare=((866) c:/windows/command/ega3.cpi)
mode con codepage selest=866
key ru,,c:/windows/command/keybrd3.sys .
```

Это для Windows 98. Далее действуйте согласно вышеизложенному [14].

3. Удалите в ключах реестра, приведенных в § 1.5, строчки с троянцами.

1.7. Техника безопасности

Теперь, после того как стало кое-что известно о работе троянцев, поговорим ещё раз о технике безопасности. Воспользуемся некоторыми пунктами из правил «Веб Плас».

Правило 1. Не запускайте у себя на компьютере программ из ненадежных источников и не открывайте приложения к письмам, даже если письмо пришло от вашего хорошего знакомого – в них могут быть спрятаны вирусы или троянские кони. Сначала сохраните это приложение и проверьте его антивирусной программой.

Правило 2. Если вы получили письмо от незнакомого человека или организации, то знайте, что скорее всего это спам – назойливые рекламные письма, и письмо попало в ваш ящик не по ошибке, а специально. Чтобы не получать письма от этого адресата впредь, нужно написать жалобу администратору сети, откуда прислано это письмо. Если же это не помогает, внесите адрес отправителя спама в список фильтруемых адресов.

Правило 3. Обязательно установите на свою машину антивирусную программу (предпочтение следует отдать AVP). Не реже 1 раза в месяц следует обновлять вирусные базы, иначе эффективность антивирусной программы резко снижается.

Правило 4. Не реже одного раза в месяц меняйте свой пароль, так как на данный момент даже без засылки троянца пароль можно определить в довольно непродолжительные сроки.

Правило 5. Лучше заранее позаботиться о резервных копиях системных файлов, хранящихся не на данной машине, на случай повреждения их в результате атаки извне.

Правило 6. Установите пакетный фильтр (программа отслеживает поступающие из сети пакеты и бракует подозрительные). Рекомендуются (данные из Internet): «Сфера», Tiny Personal Firewall, AtGuard[4]. Эти программы распространяются бесплатно.

Правило 7. Также можно использовать шифровальщики переписки, например PGP.

Правило 8. Периодически запускайте программу-трассировщик[5] (см. §3.2). Это позволит вам увидеть, с какими узлами «общается» ваш компьютер и через какие порты.

И самое главное, повторим ещё раз, не доверяйте программам из непроверенных источников.

[4] Настройка AtGuard описана на сайте http://home.ural.ru/~guard/atguard.htm
[5] Можно использовать программу netstat.exe с параметром «-a» или «-n».

Глава 2

ПРОГРАММА BelPL ПО ЗАЩИТЕ ОТ ТРОЯНЦЕВ

2.1. Описание программы типа «Троянский конь»

Рассмотрим более подробно программу-вредитель, работающую по принципу троянского коня. Пример подобной программы можно найти в сети Internet [1], и называется она Alps6.

Авторы предупреждают читателя от использования сведений, приводимых ниже, в незаконных целях.

Если говорить совсем кратко, то действие данной программы заключается в следующем. При активизации приложение устанавливается на машину, в системный каталог, инициирует подключение сети, узнает login-ы и пароли пользователей, работающих на данном компьютере, и отправляет информацию владельцу через каналы, открытые самостоятельно. При этом процесс не виден на панели задач, работает из системной области, и обнаружить его можно лишь с помощью специальных приложений, таких как Process Viewer, поставляемый в пакете Visual Studio.

2.1.1. Этапы работы программы Alps6

Предположим, что программа-троянец был запущена из некоторого каталога компьютера ничего не подозревающим владельцем. Чтобы преждевременно не обнаружить себя, после запуска троянца на компьютере эта программа перемещает себя в системный каталог и перезапускается оттуда. Для этого она:

1. Узнает имя системной директории.
2. Копирует в неё файл с программой.
3. Запускает свою копию.

Замечание. Как только копия запущена из системной директории, действие текущего приложения завершается.

Далее:

1. Для длительной работы программы, в том числе и после перезагрузок, она может установить VXD-файл.
2. Открывается сокет.
3 Начинается сбор информации о сервере. Прежде всего определяется IP-адрес сервера.
3. Как только он получен, делается попытка выйти в Internet. Если она удачна, то по заданному злоумышленником адресу высылается информация о сервере, логинах и многом другом. Например, отправляются адреса посещаемых владельцем страниц в Сети, а также адреса, по которым владелец отсылал свои письма.
4. Самым ответственным моментом является определение паролей. Для этого троянец загружает библиотеку MPR.dll, внутреннее действие которой состоит в перехватывании нажатий клавиш при входе в систему. Отсылается и эта информация, после чего соединение завершается.
5. Сделав свою «работу», троянец Alps6 самоуничтожается. Для этого он использует функцию отложенного удаления, так как файл действующего приложения удалить нельзя.

В итоге программа не оставляет следов своей деятельности, вреда системе она не нанесла, а лишь «позаимствовала информацию». Про-

грамму можно обнаружить только во время её работы, т.е. необходимо следить за работой системы в резидентном режиме.

Данное описание работы программы очень краткое, но оно содержит ключевые моменты ее функционирования. И главное, после описания действия программы становится очевидно, что, в отличие от вирусов, основным результатом присутствия которых на машине является разрушение программ и данных, приложения данного вида деструктивных действий не осуществляют. Поэтому программе часто удаётся «уйти незамеченной». А последствия от утери данных могут быть на порядок опасней последствий деятельности обычного вируса или червя. И именно для предотвращения подобных опасностей существуют сетевые экраны (правда, их зона деятельности намного шире), резидентные антивирусные программы, например AVP, а также следующая программа, разработанная авторами в целях самообучения.

2.2. Описание программы BelPL по защите от троянских коней

Программа BelPL, которая будет описана ниже, является пробной. Действие её основывается на принципах, описанных в предыдущих главах. Программа работает в операционных системах Windows NT 4.0, 2000, XP. Программа предназначена для предотвращения попыток взлома машины из сети Internet (подразумевается установка так называемых троянских коней) и при необходимости сообщения об этом администратору.

Суть работы программы заключается в постоянном отслеживании параметров работы машины и, в случае обнаружения подозрительной ситуации, сообщении администратору об этом. Отслеживаются следующие параметры:

1. Системный реестр.
2. Файловая структура системы.
3. Действующие процессы.
4. Сетевой трафик.

2.2.1. Описание работы программы BelPL

Реестр. Во-первых, опишем, как и для чего отслеживается системный реестр. Как говорилось выше, троянские кони, ворующие информацию и отсылающие её по сети, находятся на машине длительное время. В связи с этим им необходимо регистрироваться в реестре, обычно в разделе автозагрузки (подробнее принцип действия уже был описан выше) для того, чтобы активизироваться при каждой загрузке. Таким образом, отслеживая изменения реестра, можно пресечь попытку установки троянца, предназначенного для длительной работы. Программа устанавливает попытку записи в реестр непосредственно в момент записи. При этом возможно либо отслеживать все изменения, либо только запись программ с подозрительными именами.

Файловая система. Идея отслеживать файловую структуру тоже оправданна. Прежде всего, как и любая информация, троянский конь должен быть помещён на диск. При этом он может попытаться тайно скопировать себя в системный каталог или любое другое место. Таким образом, отслеживая все изменения файловой структуры, можно определить момент установки опасной программы, а также место, куда она записана. Оценивается состояние файловой структуры постоянно в реальном режиме, что позволяет своевременно заметить попытку несанкционированного доступа. При этом, так как функции, отслеживающие данный аспект работы компьютера, «висят на петле сообщений системы» и не загружают чересчур процессор, больших перегрузок системы из-за данного слежения нет.

Действующие процессы. Польза слежения за активными процессами очевидна. Троянский конь, как и любая исполняющаяся программа, – это активный процесс. Скрыть действующий процесс в системе невозможно. Его может быть не видно на панели задач, но он всегда регистрируется в системе, так как распределением процессорного времени руководит операционная система. Существуют функции, с помощью которых можно отслеживать активные процессы, определять их приоритеты и, при необходимости, экстренно завершать их. Проблема здесь состоит в следующем. Как указано выше, зачастую процессы вредоносных программ имеют высокий приоритет, а также общеизвестное имя. Таким образом, при запуске нового процесса есть вероятность сразу

обнаружить вредоносную программу. Если же это сделать не удается, то, отслеживая дальнейшие действия данного процесса (вплоть до его завершения), всегда известно, какой процесс занимается подозрительной деятельностью.

Порты. Теперь несколько слов об открытых портах. При передаче информации программа-вредитель использует отдельный порт. Она сама его открывает, а после этого передаёт через него информацию. Таким образом, сразу возникает мысль о том, чтобы отслеживать состояние портов. При попытке открытия порта следует установить программу, которая делает это, и проверить, должна ли данная программа выходить в сеть. После этого, если доступа быть не должно, следует сообщить об этом администратору и прервать процесс, открывавший порт. Как правило, администратор знает, какие программы должны иметь возможность передавать данные по сети, а какие нет. Поэтому необходимо предоставить ему право разрешать или запрещать выход программы в сеть, а не хранить данные о подозрительных программах постоянно. Другой способ – использование списка «проверенных программ», которым разрешен выход в сеть; всем остальным программам отказывается в доступе к сети. При необходимости добавления к этому списку делаются вручную.

2.2.2. Системные требования программы BelPL

Для нормальной работы данной программы требуются:

Операционная система: **Windows NT 4.0**, **2000, XP**.
Процессор: **166MHz.**
Оперативная память: **32 Mb,** желательно **64Mb.**

2.2.3. Описание пользовательского интерфейса

Итак, основные принципы работы описаны, теперь перейдём к пользовательскому интерфейсу.

При обычной установке программа работает в реальном времени, активизируется при запуске операционной системы (находится в разделе

autorun). При этом на таскбаре появляется стилизованное изображение змейки красного цвета (рис.2.1).

Рис.2.1.

Развёрнутое окно приложения имеет следующий вид (рис.2.2):

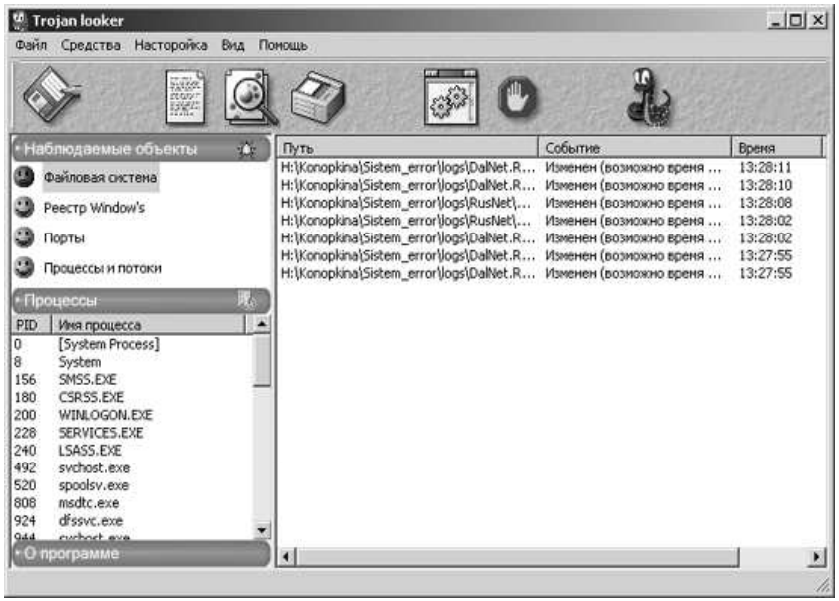

Рис.2.2. Окно программы BelPL.

В левой части окна находится дерево разделов, за которыми ведётся наблюдение. При нажатии на один из разделов в правой части окна появляются сообщения о результатах слежения за данным разделом. При желании можно убирать или восстанавливать дерево разделов.

При необходимости программу можно выгрузить, развернуть на весь экран и постоянно следить за состоянием системы либо продолжать наблюдение в фоновом режиме, а при необходимости временно прекращать слежение, что можно сделать не выгружая программу. В случае обнаружения опасной ситуации на экране появляется messagebox следующего вида – рис.2.3.

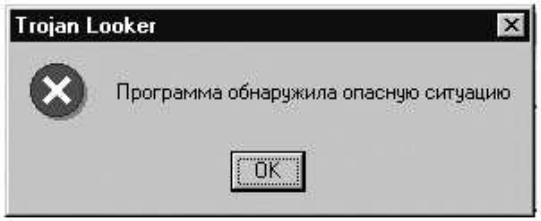

Рис.2.3. Программа BelPL. Предупреждение об опасности.

Пользователь после получения сообщения о потенциальной или явной опасности может сам принимать решение о последующих действиях. Однако в случае необходимости немедленного предотвращения попытки взлома программа может сама сначала принять меры, уже потом сообщить об этом администратору (существует два режима работы программы: с автоматическим решением проблем и запросом на решение у администратора). Примером такой ситуации может служить установка программы с именем, совпадающим с именем одной из программ – троянских коней, хранящихся в списке таких приложений в самой программе.

Для определения поведения программы в данной ситуации, а также для иных настроек работы приложения существует вкладка «Настройка», находящаяся на toolbar и в меню. Данная вкладка представляет со-

бой propertysheet, содержащий в себе окна с настройками параметров слежения.

В диалоге настроек устанавливаются следующие параметры наблюдения:

1. Включение и отключение слежения за следующими параметрами работы системы (файловая структура, реестр, процессы, порты (каждый подключается в своей вкладке).

2. Конкретные параметры работы с различными разделами.

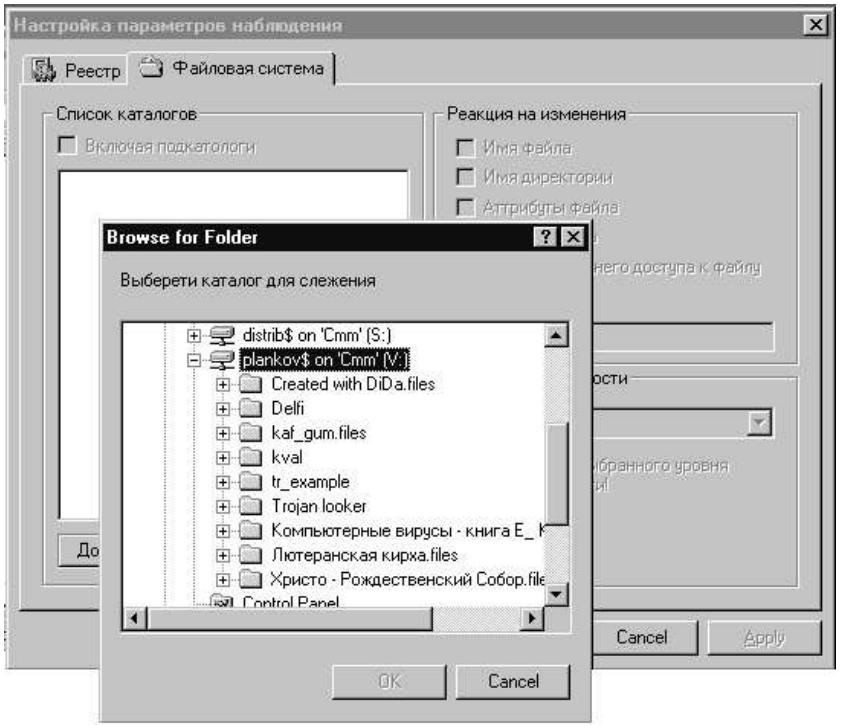

Рис.2.4. Программа BelPL. Настройки работы с файловой системой.

Теперь несколько слов о внутренних настройках каждого пункта слежения. Начнём с файловой системы.

Диалог настройки работы с файловой системой представлен на рис.2.4.

В левой части (рис.2.4) – список каталогов, находящихся под контролем программы. Возможно добавлять новые или удалять те, за которыми слежение уже ведётся.

ВНИМАНИЕ! По умолчанию при запуске программы слежение за файловой системой отключено, следовательно, и разделов, за которыми ведётся слежение, в списке нет. После выбора каталога необходимо подтвердить своё действие, включив его в область проверки. Так же регулируется, просматриваются подкаталоги или нет.

В правой части (рис.2.4) указаны действия, на которые следует реагировать программе. Это изменение имени файла, изменение названия директории, изменение атрибутов файла, его размера, а также времени последнего доступа к нему. При этом могут устанавливаться маски файлов, за которыми необходимо следить.

Помимо перечисленных параметров возможна также настройка уровня экстренности сообщений. На первом уровне сообщение выводится только в рабочую область программы. Таким образом, если программа находится в режиме наблюдения на фоновом уровне, то сообщение останется незамеченным. На втором уровне, помимо выведения сообщения в рабочую область программы, выводится системное сообщение о произошедшем событии, что будет заметно даже в том случае, когда программа находится в фоновом режиме.

Замечание. Несколько слов о настройке параметров слежения за файловой структурой. Как уже говорилось выше, опасные программы, как правило, записывают себя в системные папки, поэтому искать их и ждать установки в несистемные папки, а тем более разделы, где хранятся архивные и малоиспользуемые файлы, малоэффективно. К тому же каждый новый пункт слежения добавляет нагрузку на программу и, если число таких разделов неразумно велико, замедляет работу не только программы, но и системы в целом. Поэтому рекомендуется включать в слежение в основном системные папки, а также разделы, наиболее часто используемые.

Теперь о вкладке **Реестр**. Сделана она аналогично предыдущей (рис.2.5).

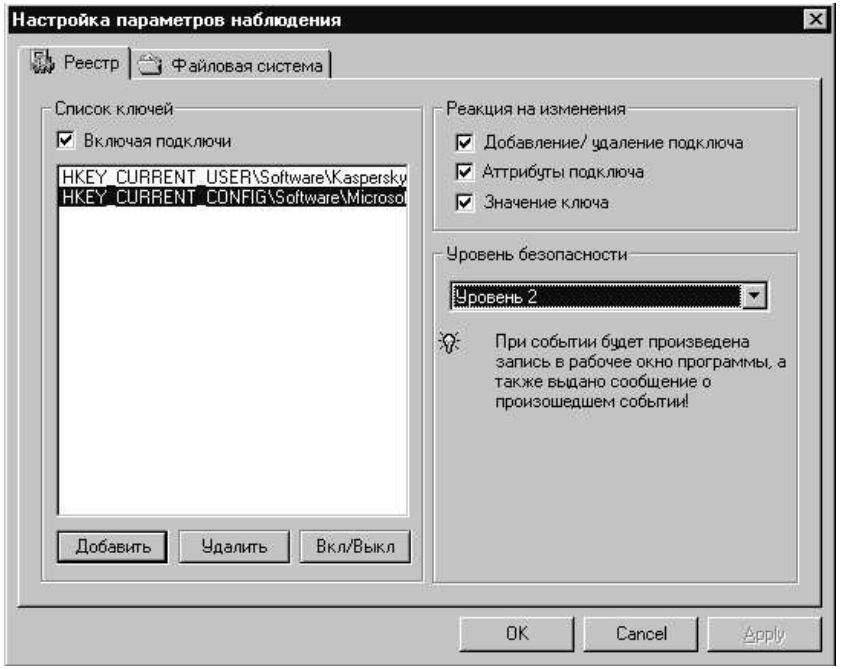

Рис.2.5. Программа BelPL. Вкладка **Реестр.**

Изначально также нет ключей, подверженных слежению по умолчанию. Поэтому для активизации режима слежения необходимо выбрать необходимые ключи и включить слежение. Выбираются также варианты отслеживания подключей либо только указанных.

Подключаются изменения, на которые необходимо реагировать. Это добавление и удаление ключа, изменение атрибутов ключа, а также значения ключа. Так же, как и в файловой структуре, возможны два варианта слежения: с выводом сообщения только в рабочую область программы либо с сообщением «на экран».

Замечание. При попытке выбора ключа возможна некоторая задержка перед выведением структуры реестра. Это связано с необходимостью загрузки файла, содержащего данные о реестре. В дальнейшем эта задержка должна быть устранена. Ключи, наиболее часто подвергающиеся изменению программами-вредителями:

HKEY_LOCAL_MASHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices

HKEY_CURRENTUSER\Software\Microsoft\CurrentVersion\Run

HKEY_LOCAL_MASHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run и др.

Иногда бывает, что программа прописывает себя сразу в нескольких ключах. Это связано со структурой реестра. Некоторые его разделы не являются независимыми, пересекаются, а иногда и включают друг друга. Поэтому бывает достаточно отметить один из разделов «группы» в список наблюдаемых.

Вкладка **Процессы** дана на рис.2.6.

В данной вкладке в списке процессов находятся не те процессы, за которыми программа следит, а перечень наиболее часто встречающихся приложений «троянской направленности». Пользователь может сам обновлять этот список либо удалять имена процессов, которые, по его мнению, безопасны. Данный пункт работы в отличие от остальных разделов является активным, используется список процессов, имеющийся в программе изначально.

Теперь об изменениях, на которые должна реагировать программа. Они настраиваются в правой части диалога. Это могут быть: запуск процесса из «чёрного списка» (включён по умолчанию), запуск любого процесса, появление процесса с неожиданно высоким приоритетом. Уровней безопасности здесь не два, как в предыдущих частях, а три. Первые два – стандартные. Третий уровень – уничтожать процесс сразу после обнаружения и только потом сообщать об этом администратору (это связано с тем, что очень часто промедление в этой ситуации может привести к необратимым последствиям.)

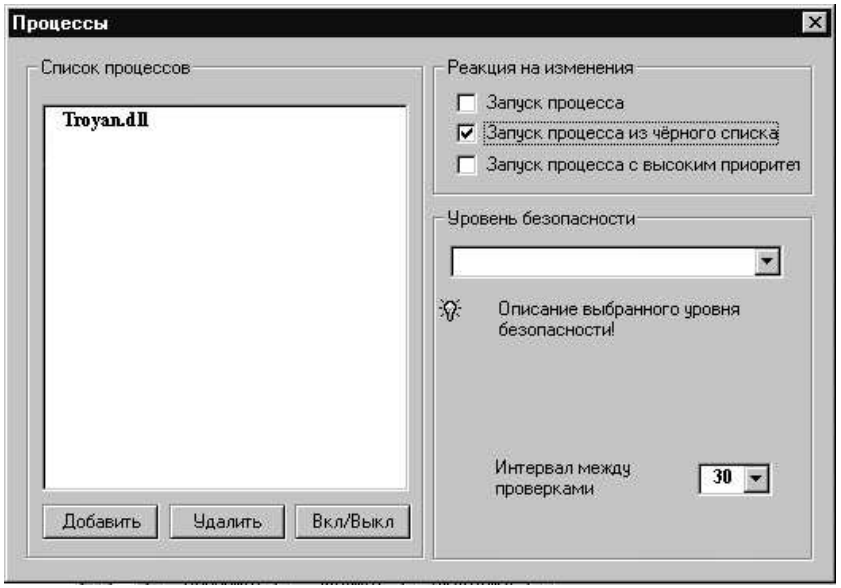

Рис.2.6. Программа BelPL. Вкладка **Процессы.**

Ещё один пункт настройки – интервалы, через которые необходимо проверять список активных процессов. В системе Windows наблюдение за процессами в реальном режиме времени невозможно, реально лишь периодически получать от системы список активных процессов. По умолчанию этот интервал – 30 секунд.

Замечание. Во-первых, обращаться с «чёрным списком» нужно осторожно. Это связано с тем, что в случае неправильного удаления возможны варианты, когда вредоносные процессы не будут замечены. В случае же добавления в список безопасных процессов, к тому же при установке третьего уровня безопасности, нормальная работа ставится под угрозу. Это связано с тем, что будет невозможно запустить полезные приложения, по тем или иным причинам занесённые в «чёрный список». Таким образом, при отсутствии твёрдой уверенности в правильности своих действий менять данный список **не следует!**

Несколько слов о периодичности проверок. Избыточное уменьшение интервала между проверками может привести к перегрузке процессора. Поэтому следует обратить особое внимание на этот пункт настроек.

Вкладка **Порты** – см. рис.2.7.

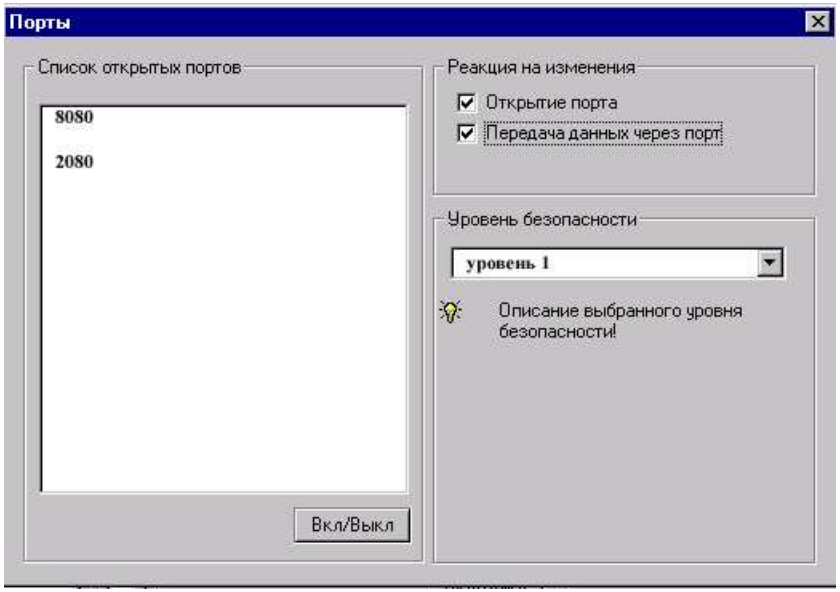

Рис.2.7. Программа BelPL. Вкладка **Порты.**

Здесь в списке находятся открытые в данный момент порты. Очевидно, что вносить изменения в данный список невозможно.

Данный раздел слежения при запуске программы неактивен, его следует запускать при необходимости вручную.

Изменения, на которые реагирует программа, следующие: открытие порта и передача через этот порт данных. Уровней безопасности два, аналогичных уровням безопасности для файловой структуры и реестра.

Замечание. Возможны отказы при попытке просмотреть список портов, что будет в скором времени исправлено.

Ещё одним видом настройки программы является настройка цветовой гаммы окна приложения, но она не имеет существенного значения, поэтому останавливаться на ней подробно не стоит.

Данная программа была описана на стадии разработки. В связи с этим возможны некоторые изменения интерфейса, не влияющие на основополагающие принципы работы приложения. Все коррективы будут направлены на увеличение удобств пользователя при работе с данной программой. Ухудшений в работе программы быть не может.

***

Программа BelPL разработана в научно-исследовательской лаборатории программного обеспечения и компьютерных сетей Омского государственного университета С.А. Белоусовым и М.С. Планковым. Для приобретения обращайтесь по адресу *cmm@univer.omsk.su*.

Глава 3

ДРУГИЕ ПРОГРАММЫ, ИСПОЛЬЗУЕМЫЕ ДЛЯ ПРЕДОТВРАЩЕНИЯ ВТОРЖЕНИЯ ТРОЯНЦЕВ

Теперь о других программах, традиционно применяющихся для защиты машин от внешних вторжений. Эти программы разделяются на несколько типов:

1. Программы, обнаруживающие неактивный вредоносный код.
2. Программы, отслеживающие подозрительный трафик.
3. Программы, предотвращающие передачу нежелательного трафика.

Рассмотрим эти программы более подробно.

3.1. Программы для обнаружения вредоносного кода

К данной категории можно отнести все антивирусные программы, потому что почти вся их деятельность направлена на обнаружение кода деструктивной программы среди «благонадёжных». У программы имеется некая база данных, содержащая примеры кодов вирусов и троянцев, которая для успешной работы программы должна периодически обновляться. Проверяемые данные сравниваются с элементами базы на предмет совпадения, и если таковое обнаруживается, то в зависимости от настроек антивирусника решается вопрос о дальнейшей судьбе данной

информации. С активными приложениями такие программы не борются. Таким образом, они являются неким подобием замка, висящего на дверях амбара с зерном. Чужаку трудно проникнуть внутрь, но мыши, живущие под его крышей, преспокойно могут поедать собранный урожай. Также следует обратить внимание на проблему, связанную с необходимостью периодических обновлений базы данных, в которой хранятся примеры кодов вирусных программ. Программы-вредители при относительно однотипных действиях могут незначительно различаться в своём коде, что иногда приводит к тому, что одну из них сканер обнаруживает, а другую – нет. Подобный пример был приведён в одной из предыдущих глав, он был связан с изменением номера порта, через который передаётся информация.

Однако при корректном использовании антивирусных программ вероятность вторжения многократно снижается.

Одним из наиболее ярких представителей семейства антивирусных сканеров является программа **AVP** (Antiviral Toolkin Pro) лаборатории Касперского.

Программа работает в резидентном режиме, запускаясь при каждом старте операционной системы. Последняя версия вообще работает как системная служба. При запуске на панели задач появляется значок приложения, говорящий о том, что антивирусная служба в действии.

В общую оболочку программы сведены следующие компоненты:

1. Сканер – часть программы, непосредственно проверяющая хранящуюся на жёстком диске информацию на наличие кода вирусов, троянцев и прочих деструктивных программ.
2. Монитор – составляющая, которая позволяет координировать действия остальных частей системы; это так называемый планировщик.
3. Центр обновления баз данных – компонента, отвечающая за обновление информации о существующих вирусах и троянцах.
4. Прочие утилиты – набор дополнительных средств, позволяющих усовершенствовать работу системы.

Принцип работы

Так как приложение действует по умолчанию постоянно, то фоновая деятельность осуществляется следующим образом: при обращении к некоторому файлу автоматически запускается сканер, проверяющий его содержимое на наличие опасного кода. Если таковой находится, то пользователю выводится сообщение об этом и в зависимости от настро-

ек системы выполняются операции по предотвращению разрушительных действий. Обычно к файлу запрещается доступ (подробнее о настройках системы ниже). Следует заметить, что иногда AVP может принять за вредную программу вполне безопасное приложение. Тут ничего не поделаешь, так как методы, используемые для взлома, вполне можно применять и в мирных целях. Поэтому некоторые данные система будет упорно укрывать от вас, ссылаясь на их опасность. Лучше перестраховаться, чем потом пожинать плоды своей безалаберности.

К тому же, если есть полная уверенность в безопасности обрабатываемой информации, то AVP- монитор можно просто отключить.

Настройки

Настройки центра управления и монитора в данном разделе неинтересны, так как направлены на решение задач диспетчеризации работы системы. Остановиться следует на настройках самого сканера.

При запуске AVP-сканера появляется следующее окно:

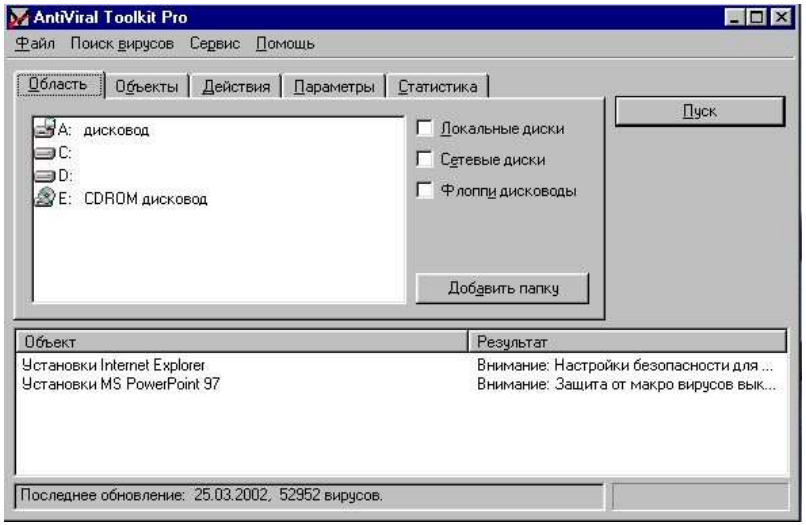

Рис. 3.1. Программа AVP. Вкладка **Сканер**

На первой странице указывается область, которая будет подвержена сканированию. Указываются либо диски, либо отдельные папки.

На странице «Объекты» указываются типы объектов, подвергаемых сканированию. Это могут быть текстовые файлы, почтовые файлы, архивы и т.д. Помимо этого указывается тип рассматриваемых файлов (признак объединения для обработки): маска, формат, расширение либо просто все файлы.

Вкладка «Действия». Здесь следует отметить дальнейшую судьбу объекта, оказавшегося заражённым или имеющего подозрение на заражение. О заражённых файлах система может либо просто сообщать, либо запрашивать разрешение на лечение, лечить сразу, удалять или перемещать в специальную папку, имя которой указывается. О подозрительных объектах или сообщается, или они перемещаются в специально отведённую папку.

Во вкладке «Параметры» указываются имя файла отчёта и некоторые особенности работы программы: избыточность сканирования, включение анализа кода и т.д.

В окне «Статистика» расположен индикатор сканирования и краткий отчёт о его течении: скорость сканирования, время сканирования, число обработанных файлов, количество инфицированных и т.д.

Как видно из пояснений, интерфейс программы сделан довольно удобным, понятным даже для неопытного пользователя и не требующим глубоких познаний в области защиты информации. Обновление баз также автоматизировано (для его проведения достаточно подключиться к сети либо указать путь к файлу обновления и запустить центр обновлений). В программу встроена подробная и удобная справочная система. При корректном использовании данного приложения степень безопасности вашей машины станет на порядок выше.

3.2. Программы, отслеживающие сетевой трафик (трассировщики)

Данные программы, именуемые иногда трассировщиками, предназначены для того, чтобы перехватывать сетевой трафик. Программы могут сохранять сетевой дамп и позволяют пользователю просмотреть его, получив при этом много полезной информации. Данные приложения не прерывают передачи, не блокируют её. Таким образом, они могут служить только для слежения за ситуацией. В отличие от них предот-

вращать нежелательную передачу могут брандмауэры, но о них будет сказано ниже.

Трассировщики позволяют просмотреть служебную информацию, связанную с переданными пакетами. Различаются они зачастую только степенью детализации данной информации. Как правило, отыскивается время передачи, направление трафика, название используемого интерфейса, размеры пакетов, адрес получателя или отправителя, используемый порт и т.д. В большинстве случаев, используя данную информацию, удаётся предотвратить вторжение. Но в отличие от программ, описанных в предыдущем разделе, для наиболее полного использования информации от данных приложений необходим достаточный опыт.

Рассмотрим одного из представителей данного класса – программу **TCPdump** и её версию для Windows – **Windump**. Данная программа распространяется бесплатно. Её дистрибутив и пояснительную информацию можно найти по адресу [15]. Программа состоит непосредственно из приложения и библиотеки wpcap.dll и работает в DOS-режиме. Следует заметить, что версия приложения, которая была получена нами для изучения, работала не совсем корректно. То есть работу программы нельзя назвать устойчивой. Прежде всего это относится к тому, что при некоторых запусках приложения система просто утрачивала свою работоспособность. Появлялся так называемый «Синий экран смерти». Скорее всего это связано с тем, что перенесение кода с Unix на NT было совершено не совсем корректно.

Фактически программа перехватывает весь входящий и исходящий трафик и выделяет из него служебную информацию. Конкретно это:

1. Время передачи или приёма.
2. Используемый интерфейс.
3. Направление трафика.
4. Адрес и порт отправителя.
5. Адрес и порт получателя.
6. Размер пакета.
7. Размер окна передачи и т.д.

Информация выдаётся дампами по каждому пакету. Так как пакет идентифицируется временем приёма или передачи, то последовательно отслеживать их нетрудно.

Итак, подробнее о формате данных. Ниже на рис.3.2 приведён кусок трассировки, выполненной на машине одного из авторов.

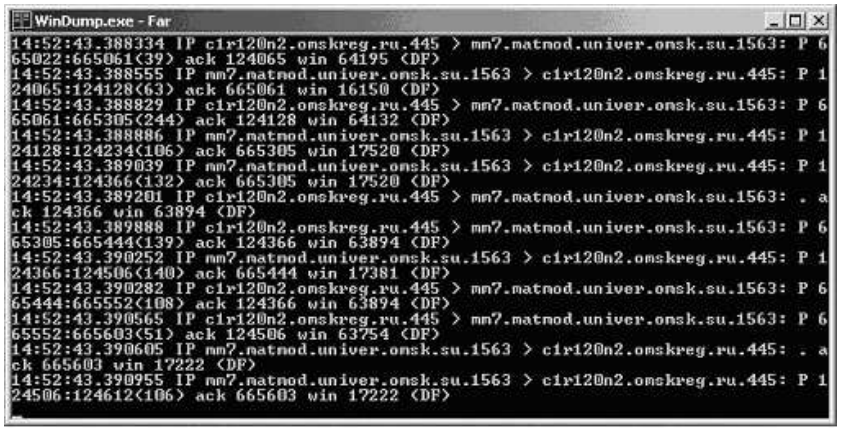

Рис. 3.2. Окно трассировки программы WinDump.

Разберёмся поподробнее с форматом информации, предоставляемой нам программой. Рассмотрим информацию о пакете, переданном в 14:52:43.388334.

Итак, формат данных:

1) 14:52:43.388334 – время, когда был распознан пакет. Значение после точки – дополнительный идентификатор пакета, так как за секунду может приходить большое число пакетов;
2) IP – используемый для передачи протокол;
3) c1r120n2.omskreg.ru.445 – адрес и порт получателя;
4) > – направление трафика (> – исходящий);
5) mm7.matmod.univer.omsk.su.1563 – адрес и порт отправителя пакета;
6) P – флаги (P – PSH - передача пакета в приложение при первой же возможности);
7) 665022:665061(39) – первый и последний номера байт в пакете, в скобках размер пакета в байтах. Используется для синхронизации при передаче;
8) ack 124065 – номер байта начала следующего пакета;
9) win 64195 – размер окна передачи в данный момент. Дело в том, что при передаче для предотвращения потери информации используется так называемый механизм скользящего окна. Без

подтверждения о получении от машины-получателя может передаваться только объём информации, равный размеру окна. В зависимости от числа байт, отправленных, но не подтверждённых, размер окна меняется;

10) DF – означает, что пакет передаётся без фрагментации (Don't Fragment). Если бы фрагментация была произведена, то здесь были бы указаны идентификатор и смещение фрагмента.

Замечание. В Tcpdump дополнительно перед информацией выводится поле с информацией о протоколе.

Как видно из описания, информация, предоставляемая программой, довольно полная и исчерпывающая. Например, по совпадению адреса отправителя у пакетов с различными портами получателя можно отловить процесс сканирования портов. Вообще, отслеживать вторжение по данным трассировки – целое искусство. Высококвалифицированные специалисты занимаются этой проблемой. Но и обычному думающему пользователю трассировка может дать информацию к размышлению. Причем если использовать трассировщики в комплексе с другими приложениями, то можно достичь больших успехов. Например, зная адрес, с которого идёт сканирование, или порт, через который уходит информация, их можно заблокировать с помощью брандмауэра.

3.3. Программы по установлению сетевой политики (брандмауэры)

Данные программы предназначены для блокирования нежелательного трафика.

Брандмауэры делятся на две категории:

– программы по фильтрации пакетов и
– программные посредники (application proxy).

Последние считаются более надёжными, но из-за их небольшой производительности зачастую выгоднее использовать первые, так как при правильной настройке они обеспечивают достаточную надёжность сети.

Итак, что делает брандмауэр? Приложение данного типа, как правило, отслеживает весь сетевой трафик, следующий через узел, за которым он следит. При этом на основе правил, установленных в программе пользователем, происходит отсеивание пропускаемой информации. Данные правила, например, закрывают определённые TCP или UDP-порты (при одинаковых номерах портов на самом деле порты для UDP и TCP будут разные, так как номер порта составляется как комбинация номера порта и протокола). Могут закрываться определённые сайты, может отсекаться реклама. Все правила сохраняются в конфигурационном файле и активизируются при запуске приложения. Само приложение обычно резидентно и работает как сервис. При этом при необходимости вся информация сохраняется в журналах, на основе которых можно отследить историю атак, их общие черты и откорректировать правила. Ещё одним достоинством брандмауэров является их способность запрещать ответ на ненужные запросы, что не позволяет взломщику собирать информацию о системе по её ответам на запросы. Некоторые приложения позволяют открыто трассировать весь трафик, из которого пользователь сам выбирает необходимую информацию.

Рассмотрим принципы работы брандмауэра на примере **Agnitum Outpost Firewall Pro**. Данная программа создана компанией Агнитум Лимитед. Приложение представляет собой систему фильтрации и блокирования сетевого трафика на основе правил, установленных пользователем.

Приложение работает как системная служба. Обычно запускается при старте работы операционной системы, однако при желании можно запускать его как обычную программу. Если программа работает, то на таскбаре отображается индикатор, характеризующий текущую активную политику.

Возможно использование следующих политик:

1. Режим бездействия, при котором приложение не ведёт никаких активных действий по поддержанию безопасности системы.
2. Режим разрешения – режим, при котором всем приложениям по умолчанию разрешается осуществлять все действия, если они отдельно не регламентированы правилами.

3. Режим обучения – в данном режиме создаются все правила, которые применяются сразу после создания без перезагрузки приложения.
4. Режим блокировки – при данной установке запрещаются действия всех приложений, которым правилами не было выдано отдельное разрешение.
5. Блокировать всё – происходит блокировка всех приложений.

Рассмотрим более подробно настройки и параметры данной системы. Приложение изначально запускается с базовой конфигурацией, которую легко просмотреть. Вообще вся система делится на две части: базовый сервис и подключаемые модули. Базовый сервис обслуживает систему правил, а подключаемые модули предоставляют пользователю дополнительные средства. При этом всегда можно подключить новый модуль или убрать существующий. Новый модуль должен быть динамической библиотекой. К тому же в программу встроена автоматическая система обновления, что позволяет периодически совершенствовать брандмауэр.

Теперь о настройках подробнее. Открывается окно настроек через панель инструментов или же через меню. Окно программы приведено на рис.3.3.

На первой вкладке настроек «Общие» устанавливается режим запуска и режим работы, устанавливается, если необходимо, пароль, настраиваются параметры журнала. Под параметрами журнала подразумеваются размер файла журнала и период, в течение которого будут сохраняться данные в журнале.

Следующая вставка «Приложения». Здесь указываются приложения, которым запрещается использовать сеть, приложения, которые должны получать разрешение на использование сети каждый раз, и приложения, находящиеся на доверии пользователя, которые могут беспрепятственно использовать сетевой трафик по умолчанию. Данные приложения добавляются и удаляются вручную.

Вкладка «Системные» – одна из самых важных. Здесь устанавливаются основные правила работы сети для данной машины. Тут устанавливаются параметры соединения через NetBIOS, ICMP, тип ответа (машина-невидимка или нет) и общие правила. С помощью общих правил открываются и закрываются TCP и UDP порты, запрещается доступ к определённым адресам в сети, определяются типы разрешённых прото-

колов, направления трафика и т.д. Можно либо редактировать имеющиеся правила, либо создавать новые.

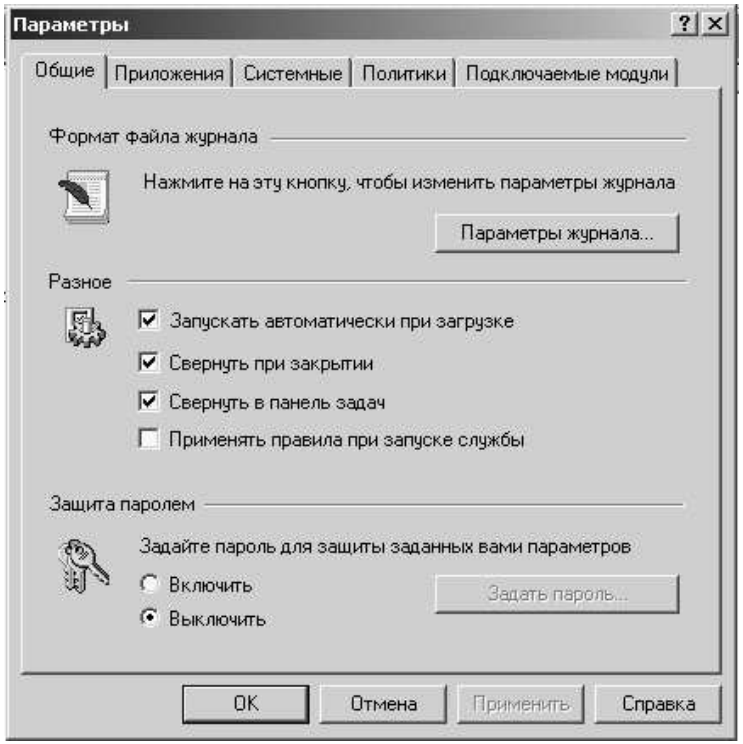

Рис.3.3. Вкладка **Параметры** программы Agnitum OutPost Firewall

Вкладка «Политики» – здесь устанавливается политика работы брандмауэра. О возможных вариантах данной политики было сказано выше. К тому же здесь можно указать зону проверенных адресов, с которых можно не опасаться получить вредоносные пакеты (это могут быть внутренние адреса сети либо адреса машин и серверов, которые проверены на безопасность и не могут послужить источником опасности).

Как было сказано выше, система помимо базовых средств защиты имеет средства, предоставляемые подключаемыми модулями. На по-

следней вкладке «Подключаемые модули» возможно добавить, удалить или настроить данные модули. Модули должны представлять собой динамические библиотеки. Стандартно поставляется модуль борьбы с излишней рекламой. Он позволяет отключать на странице баннеры, не даёт подгружаться изображениям определенного размера, которые могут представлять собой баннеры. Также с помощью включаемых модулей возможно установить попытку сканирования портов и пресечь её.

Таким образом, следует отметить, что программа довольно проста и удобна, позволяет подключать к себе дополнительные модули и под управлением ОС Win2k помогает контролировать доступ к портам, что разрешают делать очень немногие программы.

Приложение 1

Названия наиболее часто применяющихся троянских коней [7]

1. Acid Shivers
2. Antigen
3. Back End
4. Back Orifice
5. Back Door
6. Count2K
7. DeepThroat
8. Devil
9. Dmsetup
10. DoS.DieWar
11. EvilFTP
12. Executer 1
13. Executer 2
14. Flooder
15. Fore 1.0b
16. FTP99cmp
17. GateCrasher
18. Gjamer
19. Gina
20. GirlFriend
21. Hacker's Paradise
22. ICKiLLEr
23. ICQ Trojen
24. Invisible FTP
25. Kuang
26. Lamer's Death
27. Leave
28. Master's Paradise
29. Millenium
30. NetBus
31. Net Monitor

32. Netspy
33. NetSphere
34. Nuker
35. Pass Ripper
36. phAse zero
37. Phineas Phucker
38. PortalOfDoom
39. Priotrity
40. Prosiak 0.47
41. PSS
42. QAZ
43. Randon (Apher, порт 445)
44. Remote Grab
45. Ripper Pro
46. Remote windows shutdown
47. Silencer
48. ShockRave
49. Shtirlitz
50. Sivka-Burka
51. Sstrojg (Senna Spy Trojan Back Door Generator)
52. Sockets de Troje
53. Socket23
54. Socket25
55. StealthSpy Beta
56. Storm
57. SubSeven
58. Telecommando
59. TheSpy
60. TrojanCow
61. Voice
62. Vodoo
63. Ultimx
64. Win Crash
65. Wingate (Socks-Proxy)
66. Wrapper
67. Y3k

Приложение 2

Список возможностей нескольких (6-7) троянских коней (406 функций) [7]

1.Lists most of the commands (description of command)
2.Hide a task from control + alt + delete
3.Show a hidden task in control + alt + delete
4.List Contents of Current Directory
5.Change To Specified Directory/Drive
6.Clear Screen
7.Kill Process by PID (Shown in PS)
8.Shows Running Processes
9.Deletes Specified Files
10.Change Port Acid Shiver Listens on (Until Next Reboot)
11.Change to default Windows Desktop folder
12.Change to Windows Recent folder
13.Change to default WS_FTP folder
14.Show Version Number of Acid Shiver
15.Show physical, RAM, CD-ROM, and Network drives
16.Relay connection to host on port, Control + C to abort
17.Sendkeys to active window
18.Show ethernet stats and physical address
19.Rename the users computer
20.Shows DOS Environment variables
21.Beeps the specified number of times
22.Type 'CDROM' for more informationv - Terminate Acid Shiver
23.Rename a specified disk drive
24.Type 'Shutdown' for more information
25.Retrives information on specified drive
26.Disconnect a session by socket index show in 'STATUS'
27.Shows users current system time
28.Shows users current system date

29.Shows some general system information about host and user
30.Show the state of all sockets used since last reboot
31.Retrieve specified file
32.Retrieve specified file in hex form
33.Run the specified shell command
34.Run the specified command and display results (may lock up)
35.Make a new directory
36.Remove a directory and all files and subdirectories inside
37.Copy file1 to file2
38.Spawn a text based application on a tcp port.
39.Stops an application from listening for connections.
40.Lists the applications currently listening for connections.
41.Creates a directory.
42.Lists files and directory. You must specify a wildcard if you want more than one file to be listed.
43.Removes a directory.
44.Creates an export on the server.
45.Deletes an export.
46.Lists current shared resourses (name, drive, access, password).
47.Copys a file.
48.Deletes a file.
49.Searches a directory tree for files that match a wildcard specification.
50.Compresses a file.
51.Decompresses a file.
52.Views the contents of a text file.
53.Disables the http server.
54.Enables the http server.
55.Logs keystrokes on the server machine to a text file.
56.Ends keyboard logging. To end keyboard logging from the text client, use 'keylog stop'.
57.Captures video and audio (if available) from a video input device to an avi file.
58.Captures a frame of video from a video input device to a bitmap file.
59.Captures an image of the server machine's screen to a

bitmap file.
60.Lists video input devices.
61.Plays a wav file on the server machine.
62.Lists current incomming and outgoing network connections.
63.Disconnects the server machine from a network resource.
64.Connects the server machine to a network resource.
65.Views all network interfaces, domains, servers, and exports visable from the server machine.
66.Pings the host machine. Returns the machine name and the BO version number.
67.Executes a Back Orifice plugin.
68.Tells a specific plugin to shut down.
69.Lists active plugins or the return value of a plugin that has exited.
70.Terminates a process.
71.Lists running processes.
72.Runs a program. Otherwise it will be executed hidden or detached.
73.Redirects incomming tcp connections or udp packets to another ip address.
74.Stops a port redirection.
75.Lists active port redirections.
76.Creates a key in the registry.
77.Deletes a key from the registy.
78.Deletes a value from the registy.
79.Lists the sub keys of a registry key.
80.Lists the values of a registry key.
81.Sets a value for a registry key.
82.Resolves the ip address of a machine name relative to the server machine.
83.Creates a dialog box on the server machine with the supplied text and an 'ok' button.
84.Displays system information for the server machine.
85.Locks up the server machine.
86.Displays cached passwords for the current user and the screen saver password.
87.Shuts down the server machine and reboots it.
88.Connects the server machine and saves any data recieved

from that connection to the specified file.
89.Connects the server machine and sends the contents of the specified file, then disconnects.
90.Ejecting And Closing The CD-ROM Drive.
91.Sends a Msg Box To The Host.
92.Hide\Show Startbar.
93.Starts a FTP Server (On Port 21).
94.Captures the screen to a Jpeg around 80 Kb and sends it to you.
95.Sends Host to A Url Of Your Choice.
96.Turn Monitor On/Off.
97.Spawn Prog.
98.Spawns a program invisibly.
99.Reboot
100.Scan for Hosts with DT server running.
101.Sends a packet to see in host is Running the Server.
102.Host System info.
103.Open/Close CDROM
104.Send "Beep" Signal
105.Send text to Notepad
106.Send Message "Yche! Yche!" with interval
107.Send Applications Bomb
108.Notepad Flooder
109.Reboot
110.Windows Clean Up
111.ICQ Killer
112.Full FTP access
113.Destroy Mouse Double Click
114.Change All System Colors To Yellow
115.Hang Up All Connections
116.Disable CTRL+ALT+DEL Keys
117.Set Cursor Position To 0,0
118.Hide Windows TaskBar
119.Reboot Computer
120.Enable Jumping Mouse
121.Enable Mouse Double Click
122.Enable CTRL+ALT+DEL Keys
123.Show Windows TaskBar
124.Disable Jumping Mouse

125.Copy EXECUTER To C:\Windows\ Directory
126.Add EXECUTER To Windows StartUp
127.Show Message-'Hello'
128.Show Message-'Hello bitch!!!!!!!!!!!!!'
129.Show Message-'Do u ready to fuck your system??????!!!'
130.Show Message-'ShutUp bitch!!!!!!!!!!'
131.Show Message-'Get ready to start!!!!!!'
132.Show Message-'Thats All bitch!!!!!!!!!'
133.Delete C:\Logo.sys
134.Delete C:\Windows\Win.com
135.Delete C:\IO.sys
136.Delete C:\Windows\System.ini
137.Delete C:\Windows\Win.ini
138.Delete C:\Config.sys
139.Delete C:\Autoexec.bat
140.Enable Paiting On The Screen('DIE!!! DIE!!! DIE!!!')
141.Disable Paiting On The Screen('DIE!!! DIE!!! DIE!!!')
142.Enable Creating Of Many Forms With Caption('DIE!!! DIE!!! DIE!!!')
143.Disable Creating Of Many Forms With Caption('DIE!!! DIE!!! DIE!!!')
144.Execute File
145.Change Desktop Colors
146.Send Message
147.Hide/Show Taskbar
148.Open/Close CDROM
149.Mouse Double Click On/Off
150.Get Windows, System & Application Directory
151.Terminate Server
152.Reboot Computer
153."No Access" for server
154.Self Removing Server
155.List Dialup parameters (phone, passwords...)
156.List ICQ UIN
157.Process List
158.Start FTP Server
159.Hides the victims TaskBar
160.Shows the victims taskBar
161.Starts an Program on the victims computer, program

doesn't have to be an .EXE, it will start and file with it's default program too.
162. Opens the victims default Web Browser at the URL you specify
163. Opens the victims Control Panel
164. Opens the victims Date/Time Options
165. Opens the victims Appearence Options
166. Starts the victims Screen Saver
167. Closes the Server on the victims machine
168. Deletes a file you specify, from the victims machine
169. Reboots the victims computer
170. Deletes a WHOLE directory from the victims computer
171. Clears the victims recent folder (The Documents folder on the START menu)
172. Ends the current windows session
173. Forces a shutdown !
174. Loggs the victim off his/her current windows session
175. Reads from the victims floppy drive
176. Sends a ping to the Server
177. Sends a Message to the victim
178. Returns the victims WINDOWS directory
179. Returns the victims TEMP Directory
180. Returns the path that the server is installed on
181. Returns the victims Hard Disk Letter
182. Returns the victims LOCAL TIME
183. Returns the victims OPEN WINDOWS
184. Maximises a window on the victims computer that you specify
185. Sets the victims Computer Name
186. Makes the victims Mouse "CRAZY" and uncontolable
187. Returns the victims Mouse to normal
188. Returns the vitims ICQ#
189. Lists all the files and any directory
190. Formats and drive on the victims Computer
191. Closes any window on the vitims Computer
192. Serches for a File, or a Pattern, on the vistims Computer
193. Sets the name of Drive C:
194. Sets the victims Computer Name
195. Sends text to and active input box on the victims computer

196.Creats a file on the victims Computer that fills up the entire drive
197.Returns the Registered User of that Computer
198.Returns the Registered Organization of that Computer
199.Returns the amount of free space on any drive
200.Returns the Operating System of the victims Computer
201.Returns the Serial Number of any Disk
202.Opens an FTP Server on the victims computer, gives you; List, Read Write, Delete, Make Dir, Delete Dir and Execute
203.information as text, that "infected" user enters to any window containing password field.
204.information aspasswords, which "infected" user enters to password fields.
205.send "system" messages to remote PC.
206.play sounds.
207.show bitmaps (.bmp pictures).
208.run exe files.
209.send "victim" to any URL.
210.change server's port.
211.hide GF Client with BOSSKEY=F12.
212.scan subnet for infected servers.
213.save windows list.
214.work with files and folders using GF filemanager.
215.Shutdown Remote Computer
216.Restart Remote Computer
217.Log-Off Remote Computer
218.Restart Remote Computer in MS-DOS
219.Close Remote Computer Spy
220.Remove Remote Computer Spy
221.Open Remote Computer CD-ROM
222.Close Remote Computer CD-ROM
223.Disconnect Remote Computer
224.Disable Ctrl+Alt+Del On Remote Computer
225.Enable Ctrl+Alt+Del On Remote Computer
226.Hide Remote Computer Taskbar
227.Show Remote Computer Taskbar
228.Turn Caps Lock On On Remote Computer
229.Turn Caps Lock Off On Remote Computer

230.Turn Num Lock On On Remote Computer
231.Turn Num Lock Off On Remote Computer
232.Change Remote Computer Computer Name
233.Change Remote Computer Recycling Bin Name
234.Swap Remote Computer Mouse Buttons
235.Unswap Remote Computer Mouse Buttons
236.Set Remote Computer Cursor Position
237.Show Remote Computer Cursor
238.Hide Remote Computer Cursor
239.Get Mouse Double Click Speed Of Remote Computer
240.Set Mouse Double Click Speed Of Remote Computer
241.Get Remote Computer Windows Mode
242.Get Remote Computer Amount Of Mouse Buttons
243.Get Remote Computer Windows Run Time
244.Get Remote Computer Free Space On C:\
245.Get Current User Logged In On Remote Computer
246.Get Serial Number Of Drive C:\ On Remote Computer
247.Get Remote Computer Temp Directory
248.Get Remote Computer Windows Directory
249.Get Remote Computer Windows System Directory
250.Get Resolution Of Remote Computer
251.Set Resolution Of Remote Computer
252.Start Remote Computer Default Screen Saver
253.Set Remote Computer Start Menu Pop-up Speed
254.Add A Line To Remote Computer Autoexec.bat File
255.Get Percent Of Memory Used On Remote Computer
256.Get Number Of Bytes In Physical Memory Of Remote Computer
257.Get Available Bytes Of Physical Memory On Remote Computer
258.Get Total Memory Amount In Page File On Remote Computer
259.Get Available Memory Amount In Page File On Remote Computer
260.Get Total Amount Of Virtual Memory On Remote Computer
261.Get Available Amount Of Virtual Memory On Remote Computer
262.Pop-up Remote Computer Message

263. Delete Files
264. Copy Remote Computer Files
265. Rename Remote Computer Files
266. Create Remote Computer Files
267. Close Remote Computers Programs
268. Get List Of Running Remote Computer Programs
269. Set Spy Password On Remote Computer
270. Server Admin (set password, close server, restrict access)
271. Host Info (system info, cached passwords)
272. Message Manager
273. File Manager (create/delete folder, upload/download /delete file)
274. Window Manager
275. Registry Manager
276. Sound System Balance
277. Plugin Manager
278. Port Redirect
279. Application Redirect
280. File Actions (execute file, play sound, show image, open document, print document)
281. Spy Functions (keyboard listen, capture screen image, capture camera video, record sound)
282. Exit Windows (logoff, poweroff, reboot, shutdown)
283. Client chat
284. Open/Close CDROM
285. Keyboard (disable keys, key click, restore keys)
286. Mouse (swap buttons, resore buttons)
287. Go To URL
288. Send Text
289. Send message
290. Shutdown remote computer
291. Download files
292. Upload files
293. Delete files
294. Execute files
295. Create folders
296. Screeb capture
297. View process list
298. Kill process

299.tell the server to upload the specified local file via ftp to remote path
300.tell the server to download the specified remote file via ftp to local path
301.execute a file (show window, hide window)
302.change directory
303.list directory
304.create directory
305.remove directory
306.show current dir
307.copy file
308.move file
309.rename file
310.delete file
311.type the specified text file
312.shows an hexadecimal dump of the specified binary or text file
313.shows the specified message into a dialog box on the server
314.locks up the server
315.trashes the server and locks it up
316.create the specified registry key
317.deletes the specified registry key
318.deletes the specified registry value
319.determines if a key or a name exists
320.sets the currently open registry key
321.read the specified key's value
322.creates or updates the specified key and associated value
323.lists available keys in the currently open key
324.lists available values in the currently open key
325.terminates the current session only
326.terminates all connections and unloads the server
327.Log all of the Dial-Up Networking accounts on a remote computer
328.Capturing full-size screen
329.Kill any programm (window)
330.View help screen
331.Shutdown remote machine
332.Reboot remote machine

333.Logoff remote machine
334.Hide active window
335.Destroy active window
336.Kill window with matching title
337.List files in current directory
338.Change directory to [dir]
339.Execute DOS command
340.Launch application
341.Send message
342.Chat with remote
343.Enter notification mode
344.Sends some information - process list and more
345.Exits server
346.Disconnects you from server
347.Remove server from remote computer memory
348.Destroy the server autostart
349.Take rights on server
350.Change & delete password
351.Send dialog box with OK button
352.Send dialog box with Yes/No buttons
353.Change folder
354.Make new folder
355.Remove folder
356.Delete files
357.List Files
358.Get current directory
359.Get logical drives
360.Lock/Unlock desktop
361.Make a puzzle with remote desktop
362.Stars On/Off on remote desktop
363.Hide/Show Start button
364.Hide/Show Taskbar
365.Hide/Show Desktop
366.Execute application (Normal/Minimized/Maximized/ Hidden Status)
367.List/Kill 32 bit process
368.LogOff user
369.Reboot system
370.Shutdown system

371.Get user name
372.Get computer name
373.Get date & time
374.Keyboard Lights Bomb
375.Lock/Unlock Mouse
376.Move Mouse
377.Monitor On/Off
378.Flip Screen
379.Open/Close CD-ROM Drive
380.Flood Server Printer
381.System Keys ON/OFF
382.Clipboard Lock
383.Screen Saver Bomb
384.Hide/Show Taskbar
385.Hide/Show Start Button
386.Disable/Enable Start Button
387.Active the Screen Saver
388.Remove Desktop Wallpaper
389.Change Desktop Wallpaper
390.Modify Remote Date
391.Close Server EXE
392.Delete Server EXE
393.Lock Up the System
394.Close all Programs
395.Exit Windows
396.Shutdown Windows
397.MSG Box [Chat]
398.Send Text
399.Get Server Information
400.View Remote Passwords
401.View Remote Netstat
402.View Active Process
403.Open Server Hard Disk
404.Play Wav Files
405.Delete and Execute Files
406.Modify Remote Autoexec.bat

Приложение 3

Перечень исполняемых файлов троянцев

(в скобках размер файла)

1. ACiDShivers.exe (186368)
2. Agent.exe (293376)
3. Agent.exe (325632)
4. Agent.exe (327680)
5. antigen.exe (19456)
6. backdoor.exe (233472)
7. backdoor.exe (241664)
8. backdoor.exe (294912)
9. backdoor.exe (344064)
10. backend.exe (102912)
11. boclient.exe (57856)
12. boclient.exe (707072)
13. bogui.exe (284160)
14. boserve.exe (124928)
15. bug.exe (57344)
16. cfg95.exe (79242)
17. client.exe (164352)
18. Client.exe (180224)
19. client.exe (202240)
20. client.exe (334848)
21. client.exe (471552)
22. client.exe (54272)
23. Controller.exe (313856)
24. Controller.exe (340992)
25. control.exe (499200)
26. DeepBo.exe (530432)
27. Devil13.exe (95232)
28. dmsetup.exe (40188)
29. Exec.exe (231424)
30. Exec.exe (249344)
31. faxmgr.exe (27648)

32. FixIT.exe (23087)
33. foreclient.exe (482304)
34. foresvr.exe (309248)
35. FTP99cmp.exe (369185)
36. ftp.exe (402944)
37. gc.exe (221184)
38. GF.exe (425984)
39. GF.exe (454656)
40. gserver.exe (126976)
41. hs.exe (267264)
42. ICKiLLeR.exe (534016)
43. icqclient.exe (31744)
44. icqcrk.exe (50688)
45. ICQFlood.exe (24576)
46. ICQFuckerExtentitions.exe (182272)
47. icqnuke.exe (10240)
48. icqtrogen.exe (39424)
49. inet.drv (36864)
50. inet.hlp (98304)
51. KeyHook.dll (54272)
52. lame.exe (335872)
53. MSTConfig.exe (378880)
54. mustget.exe (527360)
55. NBSvr.exe (612864)
56. NetBus.exe (1114112)
57. NetBus.exe (494592)
58. NetBus.exe (567296)
59. NetBus.exe (599552)
60. NetMonitor.exe (205824)
61. netspy.exe (141312)
62. Paradise.exe (1096704)
63. Paradise.exe (1310208)
64. Paradise.exe (855552)
65. Paradise.exe (888320)
66. Paradise.exe (916480)
67. Paradise.exe (924672)
68. Patch.exe (494592)
69. Path.exe (472576)
70. phase.exe (301568)

71. Phineas.com (93250)
72. Phucker.exe (352768)
73. port.dat (94208)
74. port.doc (39424)
75. port.exe (40960)
76. procmom.exe (14848)
77. PSS-Client.exe (80384)
78. Readme.exe (102400)
79. Readme.exe (73728)
80. Readme.exe (77824)
81. Readme.exe (98304)
82. RemoteControl.exe (505344)
83. Rgrab.exe (258048)
84. RipClient.exe (305664)
85. RipServer.exe (211968)
86. RmtEwxC.exe (268800)
87. Server.exe (210432)
88. Server.exe (211456)
89. Server.exe (296448)
90. Server.exe (533013)
91. Setup.exe (14336)
92. Sockets23.exe (1082880)
93. Spyserver.exe (30720)
94. Spy.exe (48128)
95. SysEdit.exe (473088)
96. SystemPatch.exe (491008)
97. TeLeCoMMaNDo.exe (327276)
98. Telman.exe (137216)
99. Telserv.exe (235520)
100. Tserv.dll (82432)
101. uagent.exe (282624)
102. wave.dll (27648)
103. Wave.exe (38400)
104. win32cfg.exe (4128)
105. wincrash.exe (309248)
106. windll.exe (331264)
107. windll.exe (344064)

Приложение 4

Список TCP портов, используемых троянцами

31 - Master Paradise
121 - BO jammerkillahV
456 - Hackers Paradise
555 - Stealth Spy, Phase0, NeTadmin
666 - Attack FTP
1001 - Silencer, WebEx
1010 - Doly trojan v1.35
1011 - Doly Trojan
1015 - Doly trojan v1.5
1033 - Netspy
1042 - Bla1.1
1080 - Wingate
1170 - Streaming Audio Trojan
1243 - SubSeven
1245 - Vodoo
1269 - Maverick's Matrix
1492 - FTP99CMP
1509 - Psyber
1600 - Sivka Burka
1807 - SpySender
1981 - ShockRave
1999 - Backdoor
2001 - TrojanCow
2023 - Pass Ripper
2115 - Bugs
2140 - The Invasor
2283 - HVL Rat5
2300 - PC Xplorer v1.2
2565 - Striker
2583 - Wincrash2

2801 - Phineas
3791 - Total Eclypse 1.0
4950 - IcqTrojan
5000 - Blazer 5
5011 - OOTLT + OOTLT Cart
5031 - NetMetro 1.0
5321 - Firehotcker
5400 - BladeRunner 0.80, BackConstruction1.2
5521 - Illusion Mailer
5550 - Xtcp
5569 - RoboHack
5742 - Wincrash
6400 - The tHing
6669 - Vampire
6670 - Deep Throath 1,2,3.x
6883 - DeltaSource
6912 - ShitHeep
6969 - Gatecrasher
7306 - NetMonitor
7789 - ICQKiller
9400 - InCommand 1.0
9872 - PortalOfDoom
9989 - InIkiller
4567 - FileNail
6939 - Indoctrination
9875 - Portal of Doom
9989 - iNi-Killer
10101 - BrainSpy
10607 - Coma
11000 - Senna Spy Trojans
11223 - ProgenicTrojan
12076 - Gjamer
12223 - Hack¦99 KeyLogger
12346 - NetBus 1.x
12701 - Eclipse 2000
16969 - Priotrity
17300 - Kuang2 theVirus
20000 - Millenium
20034 - NetBus Pro

20331 - Bla
21554 - GirlFriend, Schwindler 1.82
22222 - Prosiak 0.47
23023 - Logget
23456 - WhackJob, UglyFtp, Evil ftp
29891 - The Unexplained
30029 - AOLTrojan1.1
30100 - NetSphere
30303 - Socket23
30999 - Kuang
31337 - BackOriffice, Chaplins Bo Spy v1.3, ExCulibar, Orc2
31339 - NetSpy
31787 - Hack'a'tack
33911 - Trojan Spirit 2001
34324 - Tiny Telnet Server, BigGluck
40412 - TheSpy
40423 - Master Paradise
50766 - Fore, Schwindler
53001 - Remote Windows Shutdown
54321 - SchoolBus v2.0
61466 - Telecommando
65000 - Devil 1.03

Литература

1. Тексты программ Alps6, BackDoor, PassCash. Сеть Internet. Сайт http://www.alguszone.ru
2. Статьи по описанию вредоносных программ в сети. Сеть Internet. Сайт http://www.viruslist.com
3. Романец Ю. В. Защита информации в компьютерных системах и сетях, 2001.
4. Лющарёв В.С., Ермаков К.В. и др. Безопасность компьютерных сетей на основе Windows NT. М.: Русская редакция, 1998.
5. Безопасность сетей Windows NT.
6. Зенковский А.К. Информация как объект защиты. Сеть Internet. Сайт http://www.info_sec.ru.
7. Сайт: http://www.hackzone.ru/articles/sweet.html.
8. Вирусная энциклопедия. Сайт http://www.viruslist.com/viruslist.html?id=3971.
9. Александер С. Вирусы, черви, троянские кони и зомби // ComputerWorld. 2000. N.19. - http://www.osp.ru/cw/2000/19/031_0.htm.
10. TROJANS. - http://kardinal.nn.ru/NT_HOLE/bkdoor-1.htm.
11. Прочие вредоносные программы.
    - http://lib.isystem.ru/Encyclopedia.Rus/1classi/z_bad_pr.htm.
12. Троянские кони.
    http://www.nestor.minsk.by/kg/kg98/kg9801/kg80105.htm.
13. Kolotsov V. mIRC SCRIPT.INI.
    - http://www.irc.portal.ru/script_ini.html.
14. Простой способ удалить вирус или троян.
    - http://alexhak.narod.ru/stat/antitrojan.html.
15. Сайт, посвященый троянам
    - http://alguszone.chat.ru/.

С.А. Белоусов, А.К. Гуц, М.С. Планков

Троянские кони
Принципы работы и методы защиты

Редактор Е.В. Брусницына

Подготовлена к печати
ООО «Издательство Наследие. Диалог-Сибирь»
Лицензия ЛР № 071680 от 04.06.98.

Подписано в печать 15.03.2003.
Формат 60x84 1.16. Печ. л. 5,39. Уч.-изд. л. 5,3.
Тираж 200 экз.

Полиграфический центр КАН
644050, г. Омск, пр. Мира 32, ком.11, тел. (381-2) 65-47-31
Лицензия ПЛД № 58-47 от 21.04.97 г.