**2.2 Троян**

**2.2.1 Вредоносное воздействие**

*Троянская программа (также - троян, троянец, троянский конь, трой) -*вредоносная программа, проникающая на компьютер под видом безвредной - кодека, скринсейвера, хакерского ПО и т.д.

"Троянские кони" не имеют собственного механизма распространения, и этим отличаются от вирусов, которые распространяются, прикрепляя себя к безобидному ПО или документам, и "червей", которые копируют себя по сети. Впрочем, троянская программа может нести вирусное тело - тогда запустивший троянца превращается в очаг "заразы".

Троянские программы крайне просты в написании: простейшие из них состоят из нескольких десятков строк кода на Visual Basic или C++.

Название "троянская программа" происходит от названия "троянский конь" - деревянный конь, по легенде, подаренный древними греками жителям Трои, внутри которого прятались воины, впоследствии открывшие завоевателям ворота города. Такое название, прежде всего, отражает скрытность и потенциальное коварство истинных замыслов разработчика программы.

Троянская программа, будучи запущенной на компьютере, может:

мешать работе пользователя (в шутку, по ошибке или для достижения каких-либо других целей);

шпионить за пользователем;

использовать ресурсы компьютера для какой-либо незаконной (а иногда и наносящей прямой ущерб) деятельности и т.д.

**2.2.2 Маскировка троянской программы**

Для того чтобы спровоцировать пользователя запустить троянца, файл программы (его название, иконку программы) называют служебным именем, маскируют под другую программу (например, установки другой программы), файл другого типа или просто дают привлекательное для запуска название, иконку и т.п. Злоумышленник может перекомпилировать существующую программу, добавив к её исходному коду вредоносный, а потом выдавать за оригинал или подменять его.

Чтобы успешно выполнять эти функции, троянец может в той или иной степени имитировать (или даже полноценно заменять) задачу или файл данных, под которые она маскируется (программа установки, прикладная программа, игра, прикладной документ, картинка). Схожие вредоносные и маскировочные функции также используются компьютерными вирусами, но в отличие от них, троянские программы не умеют распространяться самостоятельно.

**2.2.3 Распространение**

Троянские программы помещаются злоумышленником на открытые ресурсы (файл-серверы, открытые для записи накопители самого компьютера), носители информации или присылаются с помощью служб обмена сообщениями (например, электронной почтой) из расчета на их запуск на конкретном, входящем в определенный круг или произвольном "целевом" компьютере.

Иногда использование троянов является лишь частью спланированной многоступенчатой атаки на определенные компьютеры, сети или ресурсы (в том числе, третьи).

**2.2.4 Методы удаления**

Трояны обладают множеством видов и форм, поэтому не существует абсолютно надёжной защиты от них.

Для обнаружения и удаления троянов необходимо использовать антивирусные программы. Если антивирус сообщает, что при обнаружении трояна он не может удалить его, то можно попробовать выполнить загрузку ОС с альтернативного источника и повторить проверку антивирусом. Если троян обнаружен в системе, то его можно также удалить вручную (рекомендуется "безопасный режим").

Чрезвычайно важно для обнаружения троянов и другого вредоносного ПО, регулярно обновлять антивирусную базу данных установленного на компьютере антивируса, так как ежедневно появляется множество новых вредоносных программ.

**2.3 Шпионское программное обеспечение**

**2.3.1 Определение**

*Spyware (шпионское программное обеспечение) -*программа, которая скрытным образом устанавливается на компьютер с целью полного или частичного контроля за работой компьютера и пользователя без согласия последнего.

В настоящий момент существует множество определений и толкований термина spyware. Организация "Anti-Spyware Coalition", в которой состоят многие крупные производители антишпионского и антивирусного программного обеспечения, определяет его как мониторинговый программный продукт, установленный и применяемый без должного оповещения пользователя, его согласия и контроля со стороны пользователя, то есть несанкционированно установленный.

**2.3.2 Особенности функционирования**

Spyware могут осуществлять широкий круг задач, например:

собирать информацию о привычках пользования Интернетом и наиболее часто посещаемые сайты (программа отслеживания);

запоминать нажатия клавиш на клавиатуре (кейлоггеры) и записывать скриншоты экрана (screen scraper) и в дальнейшем отправлять информацию создателю spyware;

несанкционированно и удалённо управлять компьютером (remote control software) - бэкдоры, ботнеты, droneware;

инсталлировать на компьютер пользователя дополнительные программы;

использоваться для несанкционированного анализа состояния систем безопасности (security analysis software) - сканеры портов и уязвимостей и взломщики паролей;

изменять параметры операционной системы (system modifying software) - руткиты, перехватчики управления (hijackers) и пр. - результатом чего является снижение скорости соединения с Интернетом или потеря соединения как такового, открывание других домашних страниц или удаление тех или иных программ;

перенаправлять активность браузеров, что влечёт за собой посещение веб-сайтов вслепую с риском заражения вирусами.

Законные виды применения "потенциально нежелательных технологий"

Tracking Software (программы отслеживания) широко и совершенно законно применяются для мониторинга персональных компьютеров.

Adware может открыто включаться в состав бесплатного и условно-бесплатного программного обеспечения, и пользователь соглашается на просмотр рекламы, чтобы иметь какую-либо дополнительную возможность (например - пользоваться данной программой бесплатно). В таком случае наличие программы для показа рекламы должно явно прописываться в соглашении конечного пользователя (EULA).

Программы удалённого контроля и управления могут применяться для удалённой технической поддержки или доступа к собственным ресурсам, которые расположены на удалённом компьютере.

Дозвонщики (диалеры) могут давать возможность получить доступ к ресурсам, нужным пользователю (например - дозвон к Интернет-провайдеру для подключения к сети Интернет).

Программы для модификации системы могут применяться и для персонализации, желательной для пользователя.

Программы для автоматической загрузки могут применяться для автоматической загрузки обновлений прикладных программ и обновлений ОС.

Программы для анализа состояния системы безопасности применяются для исследования защищённости компьютерных систем и в других совершенно законных целях.

Технологии пассивного отслеживания могут быть полезны для персонализации веб-страниц, которые посещает пользователь.

**2.3.3 История и развитие**

Согласно данным AOL и National Cyber-Security Alliance от 2005 года 61% респондентных компьютеров содержали ту или иную форму spyware, из них 92% пользователей не знали о присутствии spyware на их машинах и 91% сообщили, что они не давали разрешения на инсталляцию spyware.

К 2006 году spyware стали одним из превалирующих угроз безопасности компьютерных систем, использующих Windows. Компьютеры, в которых Internet Explorer служит основным браузером, являются частично уязвимыми не потому, что Internet Explorer наиболее широко используется, но из-за того, что его тесная интеграция с Windows позволяет spyware получать доступ к ключевым узлам ОС.

До релиза Internet Explorer 7 браузер автоматически выдавал окно инсталляции для любого компонента ActiveX, который веб-сайт хотел установить. Сочетание наивной неосведомлённости пользователя по отношению к spyware и предположение Internet Explorer, что все компоненты ActiveX безвредны, внесло свой вклад в массовое распространение spyware. Многие компоненты spyware также используют изъяны в JavaScript, Internet Explorer и Windows для инсталляции без ведома и/или разрешения пользователя.

Реестр Windows содержит множество разделов, которые после модифицирования значений ключей позволяют программе исполняться автоматически при загрузке ОС. Spyware могут использовать такой шаблон для обхождения попыток деинсталляции и удаления.

Spyware обычно присоединяют себя из каждого местонахождения в реестре, позволяющего исполнение. Будучи запущенным, spyware контролирует периодически, не удалено ли одно из этих звеньев. Если да, то оно автоматически восстанавливается. Это гарантирует, что spyware будет выполняться во время загрузки ОС, даже если некоторые (или большинство) звенья в реестре автозапуска удалены.

**2.3.4 Spyware, вирусы и сетевые черви**

В отличие от вирусов и сетевых червей, spyware обычно не саморазмножается. Подобно многим современным вирусам, spyware внедряется в компьютер преимущественно с коммерческими целями. Типичные проявления включают в себя демонстрацию рекламных всплывающих окон, кражу персональной информации (включая финансовую, например, номера кредитных карт), отслеживание привычки посещения веб-сайтов или перенаправление адресного запроса в браузере на рекламные или порносайты.

**2.3.5 Телефонное мошенничество**

Создатели spyware могут совершать мошенничество на телефонных линиях с помощью программ типа "диалер". Диалер может перенастроить модем для дозвона на дорогостоящие телефонные номера вместо обычного ISP. Соединение с этими не вызывающими доверия номерами идёт по международным или межконтинентальным тарифам, следствием чего являются непомерно высокие суммы в телефонных счетах. Диалер не эффективен на компьютерах без модема или не подсоединённых к телефонной линии.

**2.3.6 Методы лечения и предотвращения**

Если угроза со стороны spyware становится более чем назойливой, существует ряд методов для борьбы с ними. Среди них программы, разработанные для удаления или блокирования внедрения spyware, также как и различные советы пользователю, направленные на снижение вероятности попадания spyware в систему.

Тем не менее, spyware остаётся дорогостоящей проблемой. Когда значительное число элементов spyware инфицировало ОС, единственным средством остаётся сохранение файлов данных пользователя и полная переустановка ОС.

**2.3.7 Антиspyware программы**

Программы, такие как Ad-Aware (бесплатно для некоммерческого использования, дополнительные услуги платные) от Lavasoft и Spyware Doctor от PC Tools (бесплатное сканирование, удаление spyware платное) стремительно завоевали популярность как эффективные инструменты удаления и, в некоторых случаях, препятствия внедрению spyware. В 2004 году Microsoft приобрела GIANT AntiSpyware, переименовав её в Windows AntiSpyware beta и выпустив её как бесплатную загрузку для зарегистрированных пользователей Windows XP и Windows Server 2003. В 2006 году Microsoft переименовал бета-версию в Windows Defender который был выпущен для бесплатной загрузки (для зарегистрированных пользователей) с октября 2006 года и включён как стандартный инструмент в Windows Vista.

**2.5 Руткиты**

**2.5.1 Определение**

*Руткит (Rootkit) -*программа или набор программ, использующих технологии сокрытия системных объектов (файлов, процессов, драйверов, сервисов, ключей реестра, открытых портов, соединений и пр) посредством обхода механизмов системы.

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

В системе Windows под термином руткит принято считать программу, которая внедряется в систему и перехватывает системные функции, или производит замену системных библиотек. Перехват и модификация низкоуровневых API функций в первую очередь позволяет такой программе достаточно качественно маскировать свое присутствие в системе, защищая ее от обнаружения пользователем и антивирусным ПО. Кроме того, многие руткиты могут маскировать присутствие в системе любых описанных в его конфигурации процессов, папок и файлов на диске, ключей в реестре. Многие руткиты устанавливают в систему свои драйверы и сервисы (они естественно также являются "невидимыми").

В последнее время угроза руткитов становится все более актуальной, т.к разработчики вирусов, троянских программ и шпионского программного обеспечения начинают встраивать руткит-технологии в свои вредоносные программы. Одним из классических примеров может служить троянская программа Trojan-Spy. Win32. Qukart, которая маскирует свое присутствие в системе при помощи руткит-технологии. Ее RootKit-механизм прекрасно работает в Windows 95, 98, ME, 2000 и XP.

**2.5.2 Классификация руткитов**

Условно все руткит-технологии можно разделить на две категории:

Руткиты работающие в режиме пользователя (user-mode)

Руткиты работающие в режиме ядра (kernel-mode)

Первая категория основана на перехвате функций библиотек пользовательского режима, вторая - на установке в систему драйвера, осуществляющего перехват функций уровня ядра.

Также, руткиты можно классифицировать по принципу действия и по постоянству существования. По принципу действия:

* Изменяющие алгоритмы выполнения системных функций
* Изменяющие системные структуры данных

**Логическая бомба**

Программа, которая запускается при определенных временных или информационных условиях для осуществления вредоносных действий (несанкционированного доступа к информации, искажения или её уничтожения). Срабатывает в определенных условиях дата Чернобыльской АЭС (вирус CIH). Логическая бомба может быть «заложена» внутрь вредоносных программ другого типа, вызывая их срабатывание в заданное время. Кроме того, логическая бомба может находиться и внутри обычных программ, вызывая прекращение их работы в заданное время. Логическая бомба может быть получена через электронную почту.

**Ботнет**

Компьютерная сеть, состоящая из некоторого количества хостов, с запущенными ботами (автономным программным обеспечением). Часто бот в составе ботнета является программой, скрытно устанавливаемой на устройство жертвы и позволяющей выполнять некие действия за счет ресурсов зараженного компьютера. Используется для рассылки спама и перебора паролей на удаленных системах,DDos атаки.

Для получения управления чужим компьютером необходимо установить на компьютер жертвы специального ПО. Также у этих ПО продуманна система самозащиты и автозапуска. Управление происходит через определенный порт , или IRC-чат(протокол прикладного уровня для обмена сообщениями в режиме реального времени).

Ботнеты являются товаром на нелегальном рынке.

По оценке создателя TCP/IP протокола около четверти всех компьютеров, подключенных к интернету, находятся в ботнете. Чаще всего подвержены заражению компьютеры на Windows XP c установленным Service Pack 2.