Введение

Вредоносная программа – компьютерная программа или переносной код, предназначенный для реализации угроз информации, хранящейся в компьютерной системе, либо для скрытого нецелевого использования ресурсов системы, либо иного воздействия, препятствующего нормальному функционированию компьютерной системы.

К вредоносному программному обеспечению относятся сетевые черви, классические файловые вирусы, троянские программы, хакерские утилиты и прочие программы, наносящие заведомый вред компьютеру, на котором они запускаются на выполнение, или другим компьютерам в сети.

Независимо от типа, вредоносные программы способны наносить значительный ущерб, реализуя любые угрозы информации – угрозы нарушения целостности, конфиденциальности, доступности.

Местом глобального распространения вредоносных программ является, конечно же, Internet.

Интернет, без сомнения, вещь в наше время нужная, для кого-то просто необходимая. За небольшой отрезок времени можно найти нужную информацию, ознакомиться с последними новостями, а также пообщаться с множеством людейи все это не выходя из дома, офиса и т.д. Но не забывайте, что по этой «толстой трубе» хакеры легко могут влезть в ваш компьютер и получить доступ к вашей личной информации.

Хотя поставщики аппаратного и программного обеспечения, а также официальные лица в правительстве принимают позы защитников личной информации, в которую постороннее вторжение недопустимо, имеются серьезные основания опасаться, что наши путешествия по Internet не останутся без внимания чьих-то «внимательных» глаз, анонимность и безопасность не гарантируется. Хакеры могут легко читать послания по электронной почте, а Web-серверы протоколируют все и вся, включая даже перечень просматриваемых Web-страниц.

1. Эволюция вирусных систем

Первые вирусные программы

1949 год. Американский ученый венгерского происхождения Джон фон Науманн (John von Naumann) разработал математическую теорию создания самовоспроизводящихся программ. Это была первая теория создания компьютерных вирусов, вызвавшая весьма ограниченный интерес у научного сообщества.

В начале 60-х инженеры из американской компании Bell Telephone Laboratories – В.А. Высотский, Г.Д. Макилрой и Роберт Моррис – создали игру «Дарвин». Игра предполагала присутствие в памяти вычислительной машины так называемого супервизора, определявшего правила и порядок борьбы между собой программ-соперников, создававшихся игроками. Программы имели функции исследования пространства, размножения и уничтожения. Смысл игры заключался в удалении всех копий программы противника и захвате поля битвы.

Конец 60-х – начало 70-х годов. Появление первых вирусов. В ряде случаев это были ошибки в программах, приводивших к тому, что программы копировали сами себя, засоряя жесткий диск компьютеров, что снижало их продуктивность, однако считается, что в большинстве случаев вирусы сознательно создавались для разрушения. Вероятно, первой жертвой настоящего вируса, написанного программистом для развлечения, стал компьютер Univax 1108. Вирус назывался Pervading Animal и заразил только один компьютер – на котором и был создан.

Вредоносные программы в наше время

Проблема вредоносных программ – рекламных и шпионских – заслуживает повышенного внимания как одна из самых главных неприятностей, с которыми ежедневно сталкиваются современные пользователи компьютеров. Их пагубное воздействие проявляется в том, что они подрывают принцип надёжности компьютера и нарушают неприкосновенность личной жизни, нарушают конфиденциальность и разрывают отношения между защищёнными механизмами работы компьютера, посредством некоторых комбинаций шпионских действий. Подобные программы часто появляются без ведома получателя, и даже при обнаружении от них трудно избавиться. Заметное снижение производительности, беспорядочная смена пользовательских настроек и появление новых сомнительных панелей инструментов или аддонов являются лишь немногими страшными последствиями заражения «шпионом» или рекламной программой. «Шпионы» и другие вредоносные программы могут также прилаживаться к более незаметным режимам функционирования компьютера и глубоко внедряться в сложные механизмы работы операционной системы так, чтобы в значительной степени осложнить их обнаружение и уничтожение.

Снижение производительности является, наверное, самым заметным последствием вредоносных программ, так как напрямую влияет на работу

компьютера до такой степени, что даже непрофессионал может это обнаружить. Если пользователи не так настораживаются, когда то и дело всплывают рекламные окна, пусть компьютер и не подключён к Интернету, то снижение отзывчивости операционной системы, поскольку потоки вредоносного кода конкурируют с системой и полезными программами, явно говорит о появлении проблем. Меняются программные настройки, таинственным образом добавляются новые функции, необычные процессы появляются в диспетчере задач (иногда их бывает и десяток), или программы ведут себя так, будто их использует кто-то другой, а вы потеряли над ними контроль. Побочные эффекты вредоносных программ (будь то рекламная или шпионская программа) приводят к серьёзным последствиям, и, тем не менее, многие пользователи продолжают вести себя легкомысленно, открывая настежь дверь к своему компьютеру.

В современном Интернет в среднем каждое тридцатое письмо заражено почтовым червем, около 70% всей корреспонденции – нежелательна. С ростом сети Интернет увеличивается количество потенциальных жертв вирусописателей, выход новых операционных систем влечет за собой расширение спектра возможных путей проникновения в систему и вариантов возможной вредоносной нагрузки для вирусов. Современный пользователь компьютера не может чувствовать себя в безопасности перед угрозой стать объектом чей-то злой шутки – например, уничтожения информации на винчестере – результатов долгой и кропотливой работы, или кражи пароля на почтовую систему. Точно так же неприятно обнаружить себя жертвой массовой рассылки конфиденциальных файлов или ссылки на порно-сайт. Кроме уже ставших привычными краж номеров кредитных карт, участились случаи воровства персональных данных игроков различных онлайновых игр – Ultima Online, Legend of Mir, Lineage, Gamania. В России также зафиксированы случаи с игрой «Бойцовский клуб», где реальная стоимость некоторых предметов на аукционах достигает тысяч долларов США. Развитие получили и вирусные технологии для мобильных устройств. В качестве пути проникновения используются не только Bluetooth-устройства, но и обычные MMS-сообщения (червь ComWar).

2. Разновидности вредоносных программ

2.1 Компьютерный вирус

Компьютерный вирус – разновидность компьютерных программ, отличительной особенностью которой является способность к размножению (саморепликация). В дополнение к этому вирусы могут повредить или полностью уничтожить все файлы и данные, подконтрольные пользователю, от имени которого была запущена заражённая программа, а также повредить или даже уничтожить операционную систему со всеми файлами в целом.

Неспециалисты к компьютерным вирусам иногда причисляют и другие виды вредоносных программ, такие как трояны, программы-шпионы и даже спам. (Спам (англ. spam) – рассылка коммерческой, политической и иной рекламы или иного вида сообщений лицам, не выражавшим желания их получать. Легальность массовой рассылки некоторых видов сообщений, для которых не требуется согласие получателей, может быть закреплена в законодательстве страны. Например, это может касаться сообщений о надвигающихся стихийных бедствиях, массовой мобилизации граждан и т.п. В общепринятом значении термин «спам» в русском языке впервые стал употребляться применительно к рассылке электронных писем) Известны десятки тысяч компьютерных вирусов, которые распространяются через Интернет по всему миру, организуя вирусные эпидемии.

Вирусы распространяются, внедряя себя в исполняемый код других программ или же заменяя собой другие программы. Какое-то время даже считалось, что, являясь программой, вирус может заразить только программу – какое угодно изменение не программы является не заражением, а просто повреждением данных. Подразумевалось, что такие копии вируса не получат управления, будучи информацией, не используемой процессором в качестве инструкций. Так, например неформатированный текст не мог бы быть переносчиком вируса.

Однако позднее злоумышленники добились, что вирусным поведением может обладать не только исполняемый код, содержащий машинный код процессора. Были написаны вирусы на языке пакетных файлов. Потом появились макровирусы, внедряющиеся через макросы в документы таких программ, как Microsoft Word и Excel.

Некоторое время спустя взломщики создали вирусы, использующие уязвимости в популярном программном обеспечении (например, Adobe Photoshop, Internet Explorer, Outlook), в общем случае обрабатывающем обычные данные. Вирусы стали распространяться посредством внедрения в последовательности данных (например, картинки, тексты, и т.д.) специального кода, использующего уязвимости программного обеспечения.

2.2 Троян

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.

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.

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).

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

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.

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.

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.

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.

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.

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.

Antispyware 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.

2.4 Сетевые черви

Сетевой червь – разновидность самовоспроизводящихся компьютерных программ, распространяющихся в локальных и глобальных компьютерных сетях. Червь является самостоятельной программой.

История

Одни из первых экспериментов по использованию компьютерных червей в распределённых вычислениях были проведены в исследовательском центре Xerox в Пало Альто Джоном Шочем (John Shoch) и Йоном Хуппом (Jon Hupp) в 1978. Термин возник под влиянием научно-фантастических романов Дэвида Герролда «Когда ХАРЛИ исполнился год» и Джона Браннера «На ударной волне»

Одним из наиболее известных компьютерных червей является «Червь Морриса», написанный Робертом Моррисом (Robert Morris) младшим, который был в то время студентом Корнельского Университета. Распространение червя началось 2 ноября 1988, после чего червь быстро заразил большое количество компьютеров, подключённых к интернету.

Механизмы распространения

Черви могут использовать различные механизмы («векторы») распространения. Некоторые черви требуют определенного действия пользователя для распространения (например, открытия инфицированного сообщения в клиенте электронной почты). Другие черви могут распространяться автономно, выбирая и атакуя компьютеры в полностью автоматическом режиме. Иногда встречаются черви с целым набором различных векторов распространения, стратегий выбора жертвы, и даже эксплойтов под различные операционные системы.

Структура

Часто выделяют так называемые ОЗУ–резидентные черви, которые могут инфицировать работающую программу и находиться в ОЗУ, при этом не затрагивая жёсткие диски. От таких червей можно избавиться перезапуском компьютера (и, соответственно, сбросом ОЗУ). Такие черви состоят в основном из «инфекционной» части: эксплойта (шелл–кода) и небольшой полезной нагрузки (самого тела червя), которая размещается целиком в ОЗУ. Специфика таких червей заключается в том, что они не загружаются через загрузчик как все обычные исполняемые файлы, а значит, могут рассчитывать только на те динамические библиотеки, которые уже были загружены в память другими программами.

Также существуют черви, которые после успешного инфицирования памяти сохраняют код на жёстком диске и принимают меры для последующего запуска этого кода (например, путём прописывания соответствующих ключей в реестре Windows). От таких червей можно избавиться только при помощи антивируса или подобных инструментов. Зачастую инфекционная часть таких червей (эксплойт, шелл-код) содержит небольшую полезную нагрузку, которая загружается в ОЗУ и может «догрузить» по сети непосредственно само тело червя в виде отдельного

файла. Для этого некоторые черви могут содержать в инфекционной части простой TFTP-клиент. Загружаемое таким способом тело червя (обычно отдельный исполняемый файл) теперь отвечает за дальнейшее сканирование и распространение уже с инфицированной системы, а также может содержать более серьёзную, полноценную полезную нагрузку, целью которой может быть, например, нанесение какого–либо вреда (например, DoS-атаки).

Большинство почтовых червей распространяются как один файл. Им не нужна отдельная «инфекционная» часть, так как обычно пользователь–жертва при помощи почтового клиента добровольно скачивает и запускает червя целиком.

2.5 Руткиты

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.

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.

3. Признаки заражения компьютера вирусом. Действия при обнаружении заражения

Присутствие вирусов на компьютере обнаружить сложно, потому что они маскируются среди обычных файлов. В данной статье наиболее подробно описаны признаки заражения компьютера, а также способы восстановления данных после вирусной атаки и меры по предотвращению их поражения вредоносными программами.

Признаки заражения:

- вывод на экран непредусмотренных сообщений или изображений;
- подача непредусмотренных звуковых сигналов;
- неожиданное открытие и закрытие лотка CD-ROM-устройства;
- произвольный, без вашего участия, запуск на компьютере каких-либо программ;
- при наличии на вашем компьютере межсетевого экрана, появление предупреждений о попытке какой-либо из программ вашего компьютера выйти в интернет, хотя вы это никак не инициировали.

Если вы замечаете, что с компьютером происходит подобное то, с большой степенью вероятности, можно предположить, что ваш компьютер поражен вирусом.

Кроме того, есть некоторые характерные признаки поражения вирусом через электронную почту:

- друзья или знакомые говорят вам о сообщениях от вас, которые вы не отправляли;
- в вашем почтовом ящике находится большое количество сообщений без обратного адреса и заголовка.

Следует отметить, что не всегда такие признаки вызываются присутствием вирусов. Иногда они могут быть следствием других причин. Например, в случае с почтой зараженные сообщения могут рассылаться с вашим обратным адресом, но не с вашего компьютера.

Есть также косвенные признаки заражения вашего компьютера:

- частые зависания и сбои в работе компьютера;
- медленная работа компьютера при запуске программ;
- невозможность загрузки операционной системы;
- исчезновение файлов и каталогов или искажение их содержимого;
- частое обращение к жесткому диску (часто мигает лампочка на системном блоке);
- интернет-браузер «зависает» или ведет себя неожиданным образом (например, окно программы невозможно закрыть).

В 90% случаев наличие косвенных симптомов вызвано сбоем в аппаратном или программном обеспечении. Несмотря на то, что подобные симптомы с малой вероятностью свидетельствуют о заражении, при их появлении рекомендуется провести полную проверку вашего компьютера установленной на нем антивирусной программой

Действия при обнаружении заражения:

1. Отключите компьютер от интернета (от локальной сети).
2. Если симптом заражения состоит в том, что вы не можете загрузиться с жесткого диска компьютера (компьютер выдает ошибку, когда вы его включаете), попробуйте загрузиться в режиме защиты от сбоев или с диска аварийной загрузки Windows, который вы создавали при установке операционной системы на компьютер.
3. Прежде чем предпринимать какие-либо действия, сохраните результаты вашей работы на внешний носитель (дискету, CD-диск, флэш-накопитель и т.д.).
4. Установите антивирус, если на вашем компьютере не установлено никаких антивирусных программ.
5. Получите последние обновления антивирусных баз. Если это возможно, для их получения выходите в интернет не со своего компьютера, а с незараженного компьютера друзей, интернет-кафе, с работы. Лучше воспользоваться другим компьютером, поскольку при подключении к интернету с зараженного компьютера есть вероятность отправки вирусом важной информации злоумышленникам или распространения вируса по адресам вашей адресной книги. Именно поэтому при подозрении на заражение лучше всего сразу отключиться от интернета.
6. Запустите полную проверку компьютера.

4. Методы защиты от вредоносных программ

Стопроцентной защиты от всех вредоносных программ не существует: от эксплойтов наподобие Sasser или Conficker не застрахован никто. Чтобы снизить риск потерь от воздействия вредоносных программ, рекомендуется:

- использовать современные операционные системы, имеющие серьёзный уровень защиты от вредоносных программ;
- своевременно устанавливать патчи; если существует режим автоматического обновления, включить его;
- постоянно работать на персональном компьютере исключительно под правами пользователя, а не администратора, что не позволит большинству вредоносных программ инсталлироваться на персональном компьютере;
- использовать специализированные программные продукты, которые для противодействия вредоносным программам используют так называемые эвристические (поведенческие) анализаторы, то есть не требующие наличия сигнатурной базы;
- использовать антивирусные программные продукты известных производителей, с автоматическим обновлением сигнатурных баз;
- использовать персональный Firewall, контролирующий выход в сеть Интернет с персонального компьютера на основании политик, которые устанавливает сам пользователь;
- ограничить физический доступ к компьютеру посторонних лиц;
- использовать внешние носители информации только от проверенных источников;
- не открывать компьютерные файлы, полученные от ненадёжных источников;
- отключить автозапуск со сменных носителей, что не позволит запускаться кодам, которые находятся на нем без ведома пользователя (для Windows необходимо gpedit.msc->Административные шаблоны (Конфигурация пользователя)->Система->Отключить автозапуск->Включен «на всех дисководах»).

Современные средства защиты от различных форм вредоносных программ включают в себя множество программных компонентов и методов обнаружения «хороших» и «плохих» приложений. Сегодня поставщики антивирусных продуктов встраивают в свои программы сканеры для обнаружения «шпионов» и другого вредоносного кода, таким образом, всё делается для защиты конечного пользователя. Тем не менее, ни один пакет против шпионских программ не идеален. Один продукт может чересчур пристально относиться к программам, блокируя их при малейшем подозрении, в том числе «вычищая» и полезные утилиты, которыми вы регулярно пользуетесь. Другой продукт более лоялен к программам, но может пропускать некоторый шпионский код. Так что панацеи, увы, нет.

В отличие от антивирусных пакетов, которые регулярно показывают 100% эффективности по обнаружению вирусов в профессиональном тестировании, проводящемся такими экспертами, как «Virus Bulletin», ни один пакет против рекламных программ не набирает более 90%, а эффективность многих других продуктов определяется между 70% и 80%.

Это объясняет, почему одновременное использование, например, антивируса и антишпионской программы, наилучшим образом обеспечивает всестороннюю защиту системы от опасностей, которые могут прийти неожиданно. Практика показывает, что один пакет следует использовать в качестве постоянного «блокировщика», который загружается всякий раз при включении компьютера (например, AVP 6.0), в то время как ещё один пакет (или более) должен запускаться, по крайней мере, раз в неделю, чтобы обеспечить дополнительное сканирование (например, Ad-Aware). Таким образом, то, что пропустит один пакет, другой сможет обнаружить.

5. Классификация антивирусных программ

Виды антивирусных программ

Евгений Касперский в 1992 году использовал следующую классификацию антивирусов в зависимости от их принципа действия (определяющего функциональность):

- **Сканеры** (устаревший вариант – «полифаги») – определяют наличие вируса по базе сигнатур, хранящей сигнатуры (или их контрольные суммы) вирусов. Их эффективность определяется актуальностью вирусной базы и наличием эвристического анализатора (см.: Эвристическое сканирование).
- **Ревизоры** (класс, близкий к IDS) – запоминают состояние файловой системы, что делает в дальнейшем возможным анализ изменений.
- **Сторожа** (мониторы) – отслеживают потенциально опасные операции, выдавая пользователю соответствующий запрос на разрешение / запрещение операции.
- **Вакцины** – изменяют прививаемый файл таким образом, чтобы вирус, против которого делается прививка, уже считал файл заражённым. В современных (2007 год) условиях, когда количество возможных вирусов измеряется сотнями тысяч, этот подход неприменим.

Современные антивирусы сочетают все вышесказанные функции.

Антивирусы так же можно разделить на:

- Продукты для домашних пользователей:
- Собственно антивирусы;
- Комбинированные продукты (например, к классическому антивирусу добавлен антиспам, файрвол, антируткит и т.д.);

Корпоративные продукты:

- Серверные антивирусы;
- Антивирусы на рабочих станциях («endpoint»).

Современные антивирусные средства защиты и их основные функциональные особенности

BitDefender Antivirus Plus

Основные функциональные особенности:

- функция Heuristics in Virtual Environment – эмуляция виртуальной машины, с помощью которой проходят проверку потенциально опасные объекты с использованием эвристических алгоритмов;
- автоматическая проверка данных, передаваемых по протоколу POP3, поддержка наиболее популярных почтовых клиентов (MS Exchange, MS Outlook, MS Outlook Express, Netscape, Eudora, Lotus Notes, Pegasus, The Bat и другие);
- защита от вирусов, распространяющихся через файлообменные Peer-2-Peer сети;
- формирование личного спам-листа пользователя.

Eset NOD32

Основные функциональные особенности:

- эвристический анализ, позволяющий обнаруживать неизвестные угрозы;
- технология ThreatSense – анализ файлов для выявления вирусов, программ-шпионов (spyware), непрошенной рекламы (adware), phishing-атак и других угроз;
- проверка и удаление вирусов из заблокированных для записей файлов (к примеру, защищенные системой безопасности Windows библиотеки DLL);
- поверка протоколов HTTP, POP3 и PMTP.

Антивирус Касперского

Основные функциональные особенности:

- проверка трафика на уровне протоколов POP3, IMAP и NNTP для входящих сообщений и SMTP для исходящих, специальные плагины для Microsoft Outlook, Microsoft Outlook Express и The Bat!;
- предупреждение пользователя в случае обнаружения изменения как в нормальных процессах, так и при выявлении скрытых, опасных и подозрительных;
- контроль изменений, вносимых в системный реестр;
- блокирование опасных макросов Visual Basic for Applications в документах Microsoft Office.

McAfee VirusScan Pro

Основные функциональные особенности:

- защита от вирусов, макровирусов, троянов, Интернет-червей, spyware, adware, вредоносных элементов управления ActiveX и Java;
- автоматическая проверка входящей (POP3) и исходящей (SMTP) электронной почты;
- технологии ScriptStopper и WormStopper для блокирования вредоносной активности скриптов и червей.

Dr. Web

Основные функциональные особенности:

- защита от червей, вирусов, троянов, полиморфных вирусов, макровирусов, spyware, программ-дозвонщиков, adware, хакерских утилит и вредоносных скриптов;
- обновление антивирусных баз до нескольких раз в час, размер каждого обновления до 15 KB;
- проверка системной памяти компьютера, позволяющая обнаружить вирусы, не существующие в виде файлов (например, CodeRed или Slammer);
- эвристический анализатор, позволяющий обезвредить неизвестные угрозы до выхода соответствующих обновлений вирусных баз.

Заключение

Если вы до сих пор ни разу не сталкивались с компьютерными вирусами, то обязательно с ними встретитесь. Было время, когда антивирусные ПО только появлялись, а вирусы уже «орудовали по полной», принося каждый день убытки на миллионы долларов. Сегодня, конечно, вирусы тоже могут сделать нашу жизнь невыносимой, но в большинстве случаев даже обычный среднестатистический пользователь может очистить свой ПК от вредоносного ПО. А вот несколько лет назад приходилось полностью форматировать жесткий диск и начинать все с нуля. Но даже это не всегда приводило к желаемому результату.

Помните: для защиты вашего компьютера, на нем необходима установленная и обновленная антивирусная программа. Не попадайтесь на уловки мошенников, игнорируйте спам, будьте внимательны при установке на ваш ПК нелицензионных программ.