Вряд ли стоит напоминать, что компьютеры стали настоящими помощниками человека и без них уже не может обойтись ни коммерческая фирма, ни государственная организация. Однако в связи с этим особенно обострилась проблема защиты информации.

Вирусы, получившие широкое распространение в компьютерной технике, взбудоражили весь мир. Многие пользователи компьютеров обеспокоены слухами о том, что с помощью компьютерных вирусов злоумышленники взламывают сети, грабят банки, крадут интеллектуальную собственность...

Сегодня массовое применение персональных компьютеров, к сожалению, оказалось связанным с появлением самовоспроизводящихся программ-вирусов, препятствующих нормальной работе компьютера, разрушающих файловую структуру дисков и наносящих ущерб хранимой в компьютере информации.

Все чаще в средствах массовой информации появляются сообщения о различного рода пиратских проделках компьютерных хулиганов, о появлении все более совершенных саморазмножающихся программ. Совсем недавно заражение вирусом текстовых файлов считалось абсурдом - сейчас этим уже никого не удивишь. Достаточно вспомнить появление "первой ласточки", наделавшей много шума - вируса WinWord. Concept, поражающего документы в формате текстового процессора Microsoft Word for Windows 6.0 и 7.0. Несмотря на принятые во многих странах законы о борьбе с компьютерными преступлениями и разработку специальных программных средств защиты от вирусов, количество новых программных вирусов постоянно растет. Это требует от пользователя персонального компьютера знаний о природе вирусов, способах заражения вирусами и защиты от них.

Компьютерные вирусы, их свойства и классификация

Свойства компьютерных вирусов

Сейчас применяются персональные компьютеры, в которых пользователь имеет свободный доступ ко всем ресурсам машины. Именно это открыло возможность для опасности, которая получила название компьютерного вируса.

Что такое компьютерный вирус? Формальное определение этого понятия до сих пор не придумано, и есть серьезные сомнения, что оно вообще может быть дано. Многочисленные попытки дать «современное» определение вируса не привели к успеху. Чтобы почувствовать всю сложность проблемы, попробуйте, к примеру, дать определение понятия «редактор». Вы либо придумаете нечто очень общее, либо начнете перечислять все известные типы редакторов. И то и другое вряд ли можно считать приемлемым. Поэтому мы ограничимся рассмотрением некоторых свойств компьютерных вирусов, которые позволяют говорить о них как о некотором определенном классе программ.

Прежде всего, вирус - это программа. Такое простое утверждение само по себе способно развеять множество легенд о необыкновенных возможностях компьютерных вирусов. Вирус может перевернуть изображение на вашем мониторе, но не может перевернуть сам монитор. К легендам о вирусах-убийцах, «уничтожающих операторов посредством вывода на экран смертельной цветовой гаммы 25-м кадром» также не стоит относиться серьезно. К сожалению, некоторые авторитетные издания время от времени публикуют «самые свежие новости с компьютерных фронтов», которые при ближайшем рассмотрении оказываются следствием не вполне ясного понимания предмета.

Вирус - программа, обладающая способностью к самовоспроизведению. Такая способность является единственным средством, присущим всем типам вирусов. Но не только вирусы способны к самовоспроизведению. Любая операционная система и еще множество программ способны создавать собственные копии. Копии же вируса не только не обязаны полностью совпадать с оригиналом, но, и могут вообще с ним не совпадать!

Вирус не может существовать в «полной изоляции»: сегодня нельзя представить себе вирус, который не использует код других программ, информацию о файловой структуре или даже просто имена других программ. Причина понятна: вирус должен каким-нибудь способом обеспечить передачу себе управления.

Классификация вирусов

В настоящее время известно более 5000 программных вирусов, их можно классифицировать по следующим признакам:

- среде обитания
- способу заражения среды обитания
- воздействию

- особенностям алгоритма

В зависимости от среды обитания вирусы можно разделить на сетевые, файловые, загрузочные и файлово-загрузочные. ***Сетевые вирусы*** распространяются по различным компьютерным сетям. ***Файловые вирусы*** внедряются главным образом в исполняемые модули, т. е. в файлы, имеющие расширения COM и EXE. Файловые вирусы могут внедряться и в другие типы файлов, но, как правило, записанные в таких файлах, они никогда не получают управление и, следовательно, теряют способность к размножению. ***Загрузочные вирусы*** внедряются в загрузочный сектор диска (Boot-сектор) или в сектор, содержащий программу загрузки системного диска (Master Boot Re-cord). ***Файлово-загрузочные*** вирусы заражают как файлы, так и загрузочные сектора дисков.

По способу заражения вирусы делятся на резидентные и нерезидентные. ***Резидентный вирус*** при заражении (инфицировании) компьютера оставляет в оперативной памяти свою резидентную часть, которая потом перехватывает обращение операционной системы к объектам заражения (файлам, загрузочным секторам дисков и т. п.) и внедряется в них. Резидентные вирусы находятся в памяти и являются активными вплоть до выключения или перезагрузки компьютера. ***Нерезидентные вирусы*** не заражают память компьютера и являются активными ограниченное время.

По степени воздействия вирусы можно разделить на следующие виды:

- ***неопасные***, не мешающие работе компьютера, но уменьшающие объем свободной оперативной памяти и памяти на дисках, действия таких вирусов проявляются в каких-либо графических или звуковых эффектах
- ***опасные*** вирусы, которые могут привести к различным нарушениям в работе компьютера
- ***очень опасные***, воздействие которых может привести к потере программ, уничтожению данных, стиранию информации в системных областях диска.

По особенностям алгоритма вирусы трудно классифицировать из-за большого разнообразия. ***Простейшие вирусы*** - паразитические, они изменяют содержимое файлов и секторов диска и могут быть достаточно легко обнаружены и уничтожены. Можно отметить ***вирусы-репликаторы***, называемые ***червями***, которые распространяются по компьютерным сетям, вычисляют адреса сетевых компьютеров и записывают по этим адресам свои копии.

Известны ***вирусы-невидимки***, называемые ***стелс-вирусами***, которые очень трудно обнаружить и обезвредить, так как они перехватывают обращения операционной системы к пораженным файлам и секторам дисков и подставляют вместо своего тела незараженные участки диска. Наиболее трудно обнаружить ***вирусы-мутанты***, содержащие алгоритмы шифровки-расшифровки, благодаря которым копии одного и того же вируса не имеют ни одной повторяющейся цепочки байтов. Имеются и так называемые ***квазивирусные*** или ***«троянские»*** программы, которые хотя и не способны к самораспространению, но очень опасны, так как, маскируясь под полезную программу, разрушают загрузочный сектор и файловую систему дисков.

Теперь поподробнее о некоторых из этих групп.

Троянские кони, программные закладки и сетевые черви

Троянский конь – это программа, содержащая в себе некоторую разрушающую функцию, которая активизируется при наступлении некоторого условия срабатывания. Обычно такие программы маскируются под какие-нибудь полезные утилиты. Вирусы могут нести в себе троянских коней или "троянизировать" другие программы – вносить в них разрушающие функции.

«Троянские кони» представляют собой программы, реализующие помимо функций, описанных в документации, и некоторые другие функции, связанные с нарушением безопасности и деструктивными действиями. Отмечены случаи создания таких программ с целью облегчения распространения вирусов. Списки таких программ широко публикуются в зарубежной печати. Обычно они маскируются под игровые или развлекательные программы и наносят вред под красивые картинки или музыку.

Программные закладки также содержат некоторую функцию, наносящую ущерб ВС, но эта функция, наоборот, старается быть как можно незаметнее, т.к. чем дольше программа не будет вызывать подозрений, тем дольше закладка сможет работать.

Если вирусы и «троянские кони» наносят ущерб посредством лавинообразного саморазмножения или явного разрушения, то основная функция вирусов типа «червь», действующих в компьютерных сетях, – взлом атакуемой системы, т.е. преодоление защиты с целью нарушения безопасности и целостности.

В более 80% компьютерных преступлений, расследуемых ФБР, "взломщики" проникают в атакуемую систему через глобальную сеть Internet. Когда такая попытка удается, будущее компании, на создание которой ушли годы, может быть поставлено под угрозу за какие-то секунды.

Этот процесс может быть автоматизирован с помощью вируса, называемого сетевой червь.

Червями называют вирусы, которые распространяются по глобальным сетям, поражая целые системы, а не отдельные программы. Это самый опасный вид вирусов, так как объектами нападения в этом случае становятся информационные системы государственного масштаба. С появлением глобальной сети Internet этот вид нарушения безопасности представляет наибольшую угрозу, т. к. ему в любой момент может подвергнуться любой из 40 миллионов компьютеров, подключенных к этой сети.

Пути проникновения вирусов в компьютер и механизм распределения вирусных программ

Основными путями проникновения вирусов в компьютер являются съемные диски (гибкие и лазерные), а также компьютерные сети. Заражение жесткого диска вирусами может произойти при загрузке программы с дискеты, содержащей вирус. Такое заражение может быть и случайным, например, если дискету не вынули из дисковода А и перезагрузили компьютер, при этом дискета может быть и не системной. Заразить дискету гораздо проще. На нее вирус может попасть, даже если дискету просто вставили в дисковод зараженного компьютера и, например, прочитали ее оглавление.

Вирус, как правило, внедряется в рабочую программу таким образом, чтобы при ее запуске управление сначала передалось ему и только после выполнения всех его команд снова вернулось к рабочей программе. Получив доступ к управлению, вирус, прежде всего, переписывает сам себя в другую рабочую программу и заражает ее. После запуска программы, содержащей вирус, становится возможным заражение других файлов.

Наиболее часто вирусом заражаются загрузочный сектор диска и исполняемые файлы, имеющие расширения EXE, COM, SYS, BAT. Крайне редко заражаются текстовые файлы.

После заражения программы вирус может выполнить какую-нибудь диверсию, не слишком серьезную, чтобы не привлечь внимания. И, наконец, не забывает возвратить управление той программе, из которой был запущен. Каждое выполнение зараженной программы переносит вирус в следующую. Таким образом, заразится все программное обеспечение.

Признаки появления вирусов

При заражении компьютера вирусом важно его обнаружить. Для этого следует знать об основных признаках проявления вирусов. К ним можно отнести следующие:

- прекращение работы или неправильная работа ранее успешно функционировавших программ
- медленная работа компьютера
- невозможность загрузки операционной системы
- исчезновение файлов и каталогов или искажение их содержимого
- изменение даты и времени модификации файлов
- изменение размеров файлов
- неожиданное значительное увеличение количества файлов на диске
- существенное уменьшение размера свободной оперативной памяти
- вывод на экран непредусмотренных сообщений или изображений
- подача непредусмотренных звуковых сигналов
- частые зависания и сбои в работе компьютера

Следует отметить, что вышеперечисленные явления необязательно вызываются присутствием вируса, а могут быть следствием других причин. Поэтому всегда затруднена правильная диагностика состояния компьютера.

Антивирусные программы

Kaspersky Internet Security – это программа для комплексной защиты ПК от вирусов и всех других типов вредоносных программ, а также от хакерских атак и спама.

Преимущества:

-Интегрированная защита от всех интернет-угроз

-Комплексная антивирусная защита:

1) проверка по базам сигнатур,

2) эвристический анализатор,

3) поведенческий блокиратор

-Проверка файлов, почты и интернет-трафика в режиме реального времени

-Персональный сетевой экран с системой IDS/IPS

-Предотвращение утечек конфиденциальной информации

-Родительский контроль

-Защита от спама и фишинга

-Автоматическое обновление баз.

Основные функции:

-Защита от вирусов, троянских программ и червей

-Защита от шпионского (spyware) и рекламного (adware) ПО

-Защита от всех типов клавиатурных шпионов

-Обнаружение всех видов руткитов

-Защита от вирусов при работе с ICQ и другими IM-клиентами

-Отмена нежелательных изменений на вашем компьютере

-Средства создания диска аварийного восстановления системы

Дополнительные возможности:

Отмена нежелательных изменений на вашем компьютере.
Самозащита антивируса от выключения или остановки.
Средства создания диска аварийного восстановления системы.
Бесплатная техническая поддержка.

NOD32 AntiVirus

NOD 32 Antivirus обеспечивает хорошо сбалансированную, современную защиту персональных компьютеров и корпоративных систем, работающих под управлением различных операционных систем.

Антивирус NOD32, разработка компании Eset, является обладателем большего количества наград Virus Bulletin 100% Award, чем любой другой антивирусный продукт.

Eset NOD32 - это комплексное антивирусное решение для защиты в реальном времени от широкого круга угроз.

Eset NOD32 обеспечивает надежную защиту от вирусов, а также от других угроз, включая троянские программы, черви, spyware, adware, phishing-атаки. Продукты Eset NOD32 предназначены как для защиты отдельных персональных компьютеров и рабочих станций, так и для защиты IT-инфраструктуры предприятий и организаций. Защита отдельных компьютеров может обеспечиваться комплектом Eset NOD32 Standard.

Для защиты корпоративной IT-инфраструктуры целесообразно использовать комплект Eset NOD32 Enterprise Edition, предусматривающий широкие возможности защиты серверов и централизованного управления:

• Поддержка централизованного управления до 10 000 рабочих мест

•Доведенные до совершенства возможности контроля событий, регистрации и отчетов

•Создание зеркал обновлений в сетях LAN/WAN

Dr.Web

Находит и удаляет:

*Почтовые черви * Сетевые черви * Файловые вирусы * Троянские программы * Стелс-вирусы * Полиморфные вирусы * Бестелесные вирусы * Макро-вирусы * Вирусы, поражающие документы MS Office *
Скрипт-вирусы * Шпионское ПО (Spyware) * Программы-похитители паролей * Клавиатурные шпионы* Программы-дозвонщики * Рекламное ПО (Adware) * Потенциально опасное ПО * Хакерские утилиты * Программы-люки * Программы-шутки * Вредоносные скрипты * Другие нежелательные коды *

Обновления вирусных баз выпускаются по мере добавления новых вирусных записей - до нескольких раз в час. "Горячие" обновления выпускаются по мере появления и анализа новых вирусов. Глобальная сеть вирусного мониторинга дает возможность оперативно получать новые образцы вирусов из всех регионов мира.

В Dr.Web - компактная вирусная база. Это позволяет быстрее сканировать файлы, экономит Ваше время и ресурсы компьютера, позволяет производить обновления молниеносно. Всего одна запись в вирусной базе Dr.Web позволяет определять десятки, а иногда и тысячи подобных вирусов.

Антивирус Dr.Web - один из самых нетребовательных к ресурсам компьютеров антивирусов и полностью совместим с версиями Microsoft Windows, от Windows 95 OSR2 и до Windows XP Professional. Дистрибутив антивируса Dr.Web имеет наименьший размер среди ведущих мировых антивирусов - около 9МБ, и всего 12-15МБ требуется на диске после установки! Dr.Web работает, не перегружая систему, что позволяет ему уверенно защищать даже маломощные компьютеры прежних поколений.

Антивирус Dr.Web очень прост в установке, с первых минут пользования не требует дополнительных настроек, удобен и понятен в обращении. «Поставил и забыл» - это об антивирусе Dr.Web! Обновления в Антивирусе Dr.Web полностью автоматизированы. При каждом подключении к Интернету программа сама обновляет вирусные базы.

Norton AntiVirus

Основные функции:

-Блокирует попытки кражи личной информации

-Находит и удаляет программы-шпионы

-Удаляет вирусы и интернет-червей

-Защищает от хакеров

-Автоматически распознает и блокирует вирусы, программы-шпионы и "червей"

-Улучшенная функция защиты от фишинга распознает и блокирует мошеннические веб-сайты

-Обнаруживает угрозы типа Rootkit и устраняет угрозы, скрытые в операционной системе

-Обучаемый брандмауэр блокирует хакеров и не позволяет программам-шпионам передавать информацию без вашего ведома

-Функция предотвращения вторжений автоматически исправляет новые уязвимости в системе защиты

-Функция защиты сети настраивает параметры безопасности при работе дома или в общедоступных сетях

-Полный осмотр системы позволяет провести тщательный анализ и удалить найденные вирусы, программы-шпионы и другие угрозы

-Компонент Norton™ Protection Center обеспечивает централизованное управление параметрами защиты

-Обновления средств защиты и новые компоненты продукта предоставляются в течение продляемого срока обслуживания

Panda AntiVirus

Антивирус Panda непрерывно и автоматически защищает Вас от атак всех типов вирусов и программ-шпионов. Он усиливает Вашу безопасность вторым уровнем защиты от новых вирусов и вторжений с помощью интеллектуальной технологии защиты TruPrevent.

Он также содержит брандмауэрную технологию, блокирующую атаки хакеров даже через Wi-Fi соединения; технологию защиты от фишинга и других онлайн мошенничеств.

Идеальный продукт для пользователей, которым требуется надежная, но простая в использовании защита: Panda AntiVirus объединяет в себе наиболее прогрессивные технологии, чтобы обеспечить домашних пользователей активной системой защиты от вредоносных кодов любого типа. Программа выявляет и уничтожает ошибки в программном обеспечении, установленном на Вашем компьютере, и проводит самодиагностику, чтобы гарантировать бесперебойную и продуктивную работу антивируса. Поэтому Ваш компьютер никогда не окажется беззащитным перед лицом вирусной атаки.

* Автоматически определяет и устраняет все типы вирусов и червей, пока Вы отправляете и принимаете почту, скачиваете файлы или работаете в Интернете

* Технология TruPreven. Самые разумные технологии, которые предлагают Вам гарантированную двойную защиту для борьбы с неизвестными вирусами и вторжениями

*Защита от программ-шпионов. Titanium 2006 отслеживает и устраняет программы-шпионы и другие раздражающие программы, которые устанавливаются на компьютер без Вашего ведома

*Блокирует вторжения хакеров и взломщиков даже через Wi-Fi соединения

*Защита от фишинга и других видов Интернет-мошенничеств

*Простота в использовании: установил и забыл о вирусах и программах-шпионах

*Максимальная скорость

*Техническая поддержка на русском языке

* Минимальные системные требования для установки