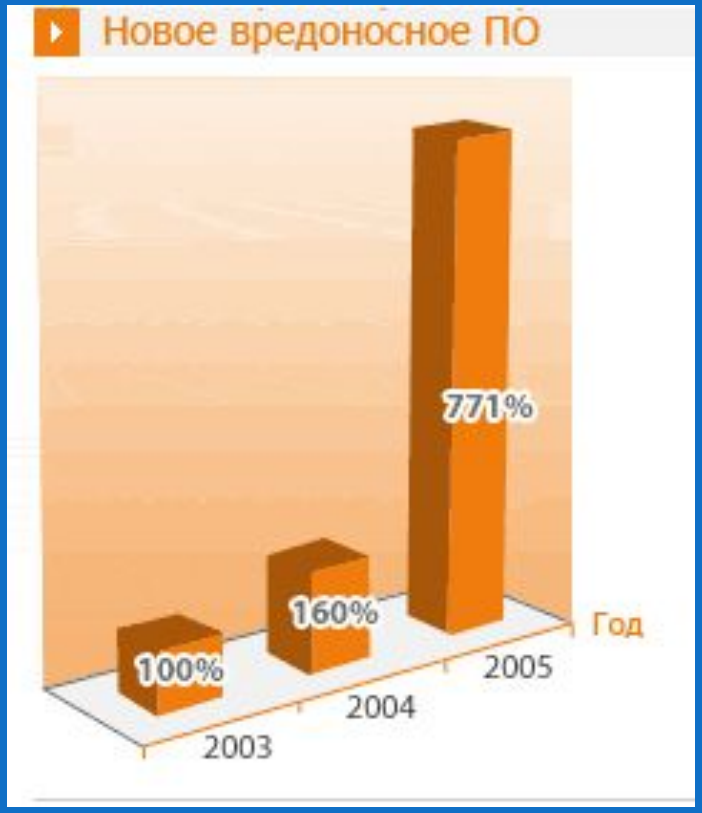
Вредоносные программы

Компьютерные вирусы

ВРЕДОНОСНЫЕ ПРОГРАММЫ

Вредоносные программы – это программы, наносящие вред данным и программам, хранящимся на компьютере.

За создание, использование и распространение вредоносных программ в большинстве стран предусмотрена уголовная ответственность



КОМПЬЮТЕРНЫЕ ВИРУСЫ

Компьютерные вирусы - это вредоносные программы, которые могут «размножаться» и скрытно внедрять свои копии в исполнимые файлы, загрузочные секторы дисков и документы.

После заражения компьютера вирус может начать выполнение вредоносных действий и распространение своих копий, а также заставлять компьютер выполнять какие-либо действия.

Активация компьютерного вируса может вызывать уничтожение программ и данных и может быть связана с различными событиями (наступлением определенной даты или дня недели, запуском программ, открытием документа и т.д.).

ПЕРВЫЕ ВРЕДОНОСНЫЕ И АНТИВИРУСНЫЕ ПРОГРАММЫ

Первый вирус, появившийся в июле 1982 г., был написан 15-летним школьником Ричем Скрента (Rich Skrenta) для платформы Apple II и относился к категории загрузочных. Он распространялся, заражая код загрузочных секторов дискет для операционной системы Apple II. При загрузке компьютера вирус оставался в памяти и заражал все дискеты, которые вставлялись в дисковод.

Жертвами вируса стали компьютеры друзей и знакомых автора, а также его учитель математики.

Как многие старые вирусы, Elk Cloner отличался визуальными проявлениями: при каждой 50-й загрузке он показывал короткое стихотворение («Elk Cloner - это уникальная программа. Она проникнет на все ваши диски, профильтрует ваши чипы. О да, это Cloner. Она приклеится к Вам, как клей. Программа способна изменить и RAM. Пустите к себе Cloner»).

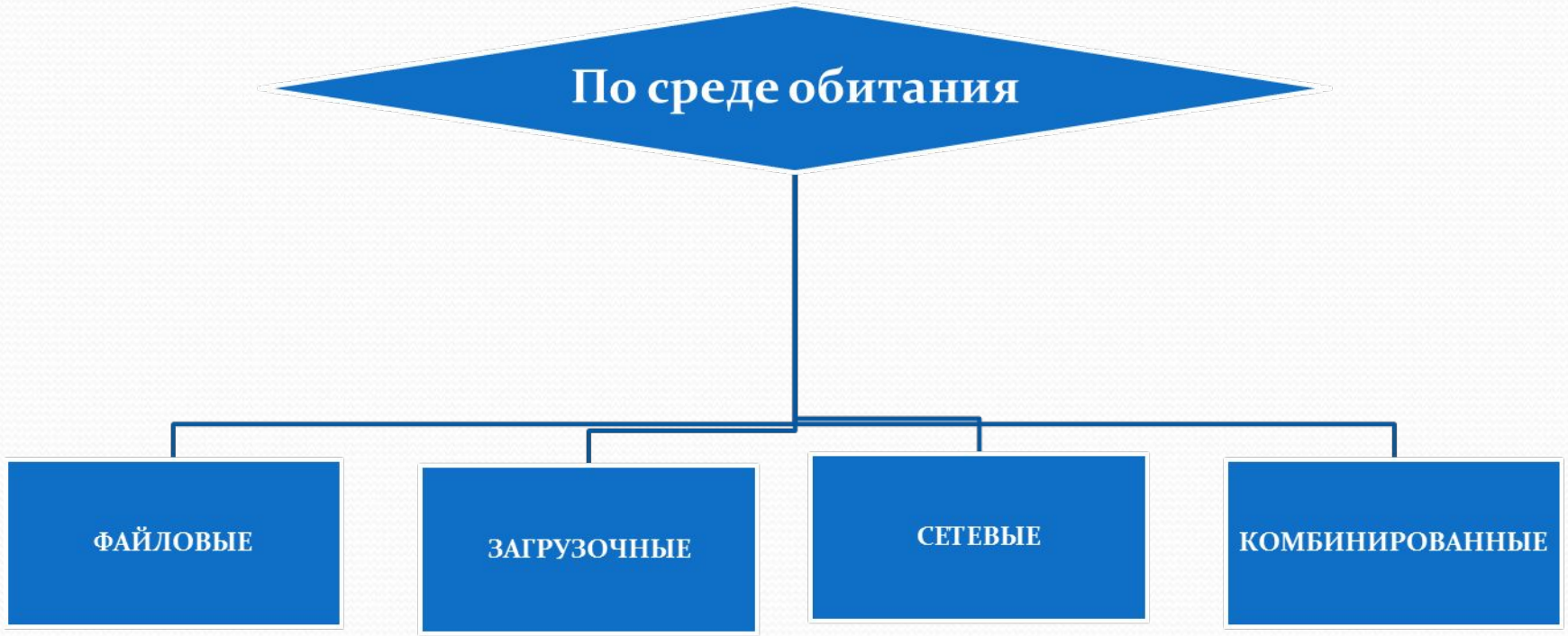
```
Elk Cloner:
The program with a personality

    It will get on all your disks
      It will infiltrate your chips
        Yes it's Cloner!

    It will stick to you like glue
      It will modify ram too
        Send in the Cloner!
```

Первый антивирус всего лишь на два года младше своего врага. В 1984 г. программист Анди Хопкинс (Andy Hopkins) написал утилиты, позволяющие перехватывать некоторые операции, выполняемые через BIOS, а также анализировать загрузочный модуль, что давало возможность бороться с некоторыми типами вирусов того времени.

Вирусы можно разделить на классы по следующим основным признакам:

- среда обитания;
- операционная система (ОС);
- особенности алгоритма работы (способ работы);
- деструктивные возможности (вредоносные воздействия).

Классификация компьютерных вирусов



КЛАССИФИКАЦИЯ ВИРУСОВ

По способу сохранения и исполнения своего кода:

- ЗАГРУЗОЧНЫЕ
- ФАЙЛОВЫЕ
- МАКРО-ВИРУСЫ
- СКРИПТ-ВИРУСЫ

Классификация компьютерных вирусов

КЛАССИФИКАЦИЯ ВИРУСОВ

ПО ДЕСТРУКТИВНЫМ ВОЗМОЖНОСТЯМ (ПО ВРЕДОНОСНОМУ ВОЗДЕЙСТВИЮ)

БЕЗВРЕДНЫЕ

НЕОПАСНЫЕ (последствия действия вирусов - уменьшение свободной памяти на диске, графические и звуковые эффекты)

ОПАСНЫЕ (последствия действия вирусов - сбои и «зависания» при работе компьютера)

ОЧЕНЬ ОПАСНЫЕ (последствия действия вирусов - потеря программ и данных форматирование винчестера и т.д.)

ЗАГРУЗОЧНЫЕ ВИРУСЫ

Загрузочные вирусы заражают загрузочный сектор гибкого или жесткого диска.

При заражении дисков загрузочные вирусы «подставляют» свой код вместо программы, получающей управление при загрузке системы, и отдают управление не оригинальному коду загрузчика, а коду вируса.

В 1986 году началась первая эпидемия загрузочного вируса. Вирус-невидимка «Brain» «заражал» загрузочный сектор дискет. При попытке обнаружения зараженного загрузочного сектора вирус незаметно «подставлял» его незараженный оригинал.

Профилактическая защита от таких вирусов состоит в отказе загрузки операционной системы с гибких дисков и установке в BIOS компьютера защиты загрузочного сектора от изменений.

ФАЙЛОВЫЕ ВИРУСЫ

Файловые вирусы внедряются в исполняемые файлы (командные файлы *.bat, программы *.exe, системные файлы *.com и *.sys, программные библиотеки *.dll и др.) и обычно активируются при их запуске.

После запуска зараженного файла вирус находится в оперативной памяти компьютера и является активным (т.е. может заражать другие файлы) вплоть до момента выключения компьютера или перезагрузки операционной системы.

По способу заражения файловые вирусы разделяют на перезаписывающие вирусы, вирусы-компаньоны и паразитические вирусы.

В 1999 году началась эпидемия файлового вируса Win95.CIH, названного «Чернобыль» из-за даты активации 26 апреля. Вирус уничтожал данные на жестком диске и стирал содержание BIOS.

Профилактическая защита от файловых вирусов состоит в том, что не рекомендуется запускать на исполнение файлы, полученные из сомнительного источника и предварительно не проверенные антивирусными программами.

МАКРО-ВИРУСЫ

Макро-вирусы заражают документы, созданные в офисных приложениях.

Макро-вирусы являются макрокомандами (макросами) на встроенном языке программирования Visual Basic for Applications (VBA), которые помещаются в документ.

Макро-вирусы являются ограниченно-резидентными, т.е. они находятся в оперативной памяти и заражают документ, пока он открыт.

Макро-вирусы заражают шаблоны документов.

В 1995 году началась эпидемия первого макро-вируса «Concept» для текстового процессора Microsoft Word. Макро-вирус «Concept» до сих пор широко распространен.

Профилактическая защита от макро-вирусов состоит в предотвращении запуска вируса (запрете на загрузку макроса).

СКРИПТ-ВИРУСЫ

Скрипт-вирусы – активные элементы (программы) на языках JavaScript или VBScript, которые могут содержаться в файлах Web-страниц.

Заражение локального компьютера происходит при их передаче по Всемирной паутине с серверов Интернета в браузер локального компьютера.

В 1998 году появился первый скрипт-вирус VBScript.Rabbit, заражающий скрипты Web-страниц, а в мае 2000 года грянула глобальная эпидемия скрипт-вируса «LoveLetter».

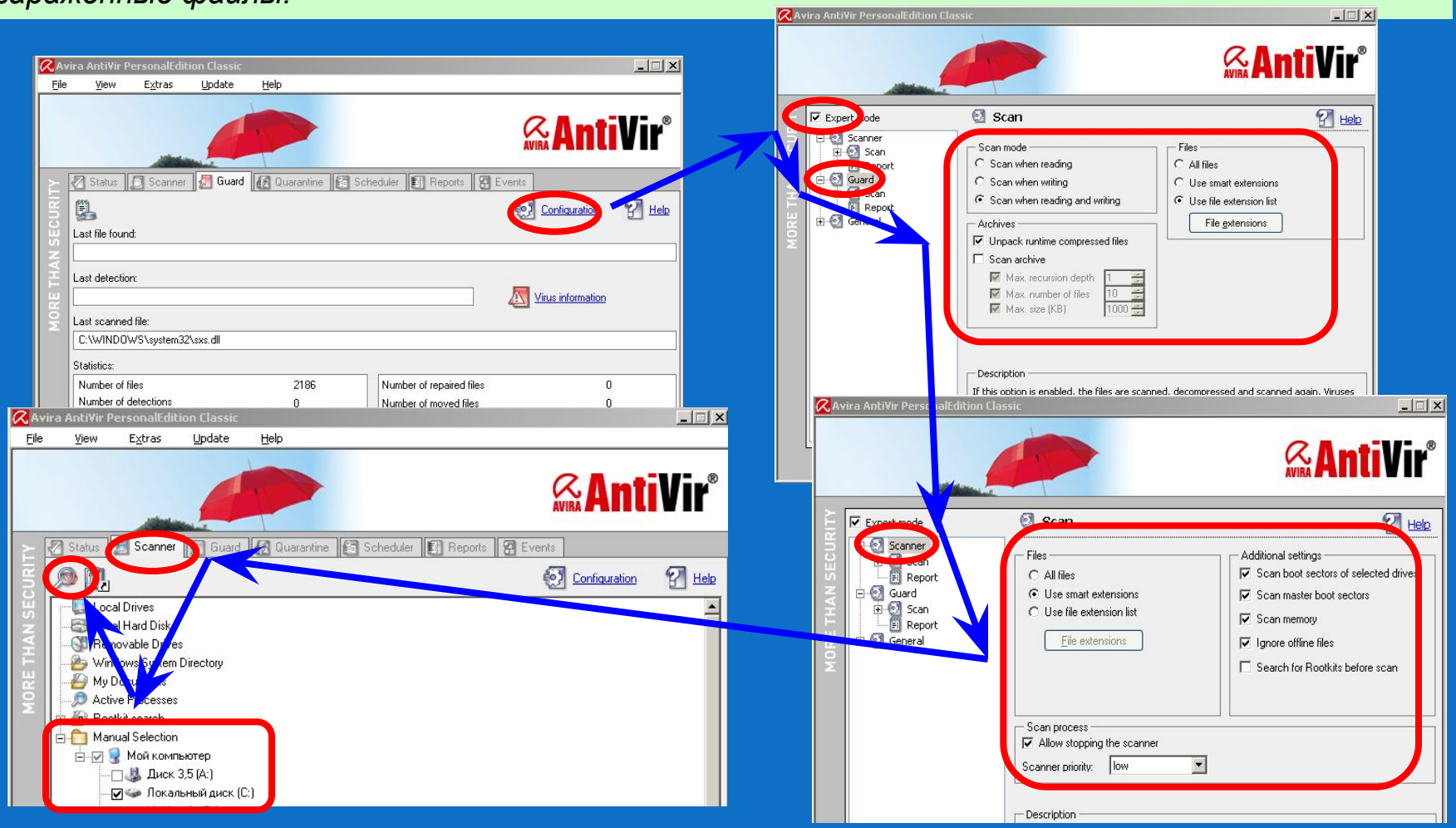
Профилактическая защита от скрипт-вирусов состоит в том, что в браузере можно запретить получение активных элементов на локальный компьютер.

Защита от компьютерных вирусов

*Задание. С помощью антивирусной программы **AntiVir Personal Edition**:*

***а) настроить параметры** антивирусного **монитора** (Guard) и антивирусного **сканера** (Scanner),*

***б) проверить компьютер на наличие вирусов** и при их обнаружении вылечить или удалить зараженные файлы.*

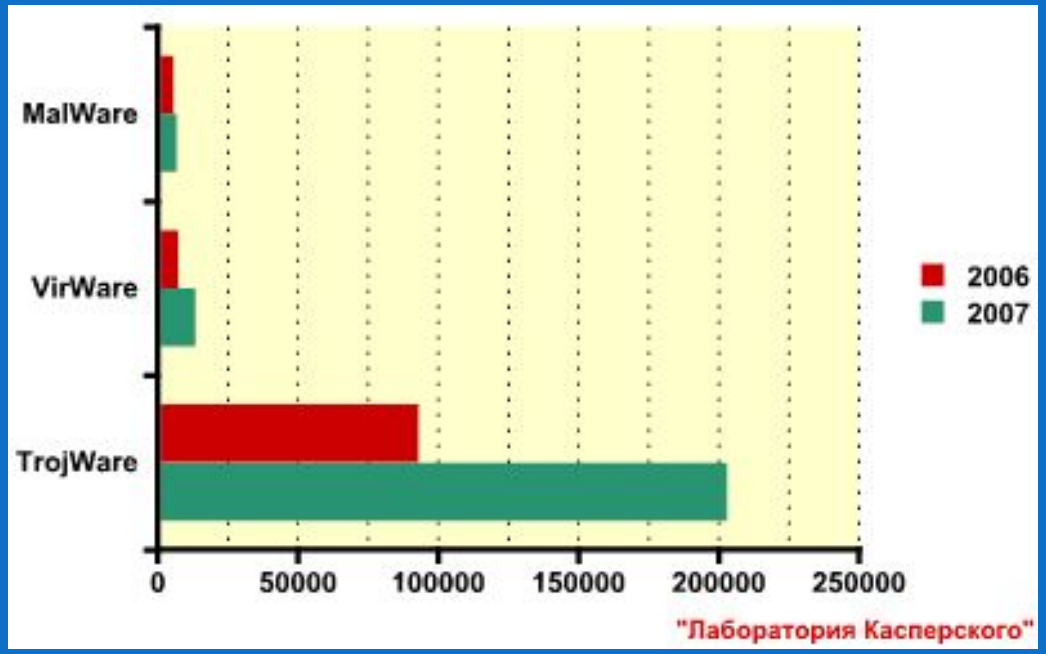


ТИПЫ ВРЕДОНОСНЫХ ПРОГРАММ

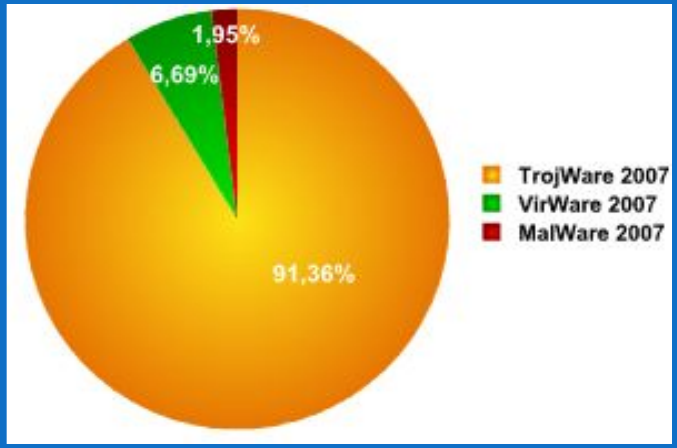
- КОМПЬЮТЕРНЫЕ ВИРУСЫ
- СЕТЕВЫЕ ЧЕРВИ
- ТРОЯНСКИЕ ПРОГРАММЫ
- ПРОГРАММЫ ПОКАЗА РЕКЛАМЫ (ADWARE)
- ПРОГРАММЫ-ШПИОНЫ (SPYWARE)
- ХАКЕРСКИЕ УТИЛИТЫ

ТИПЫ ВРЕДОНОСНЫХ ПРОГРАММ

Количество новых вредоносных программ, обнаруженных аналитиками «Лаборатории Касперского» в 2007 году



Распределение классов вредоносных программ (первое полугодие 2007 г.)



Согласно классификации «Лаборатории Касперского»:
TrojWare: различные троянские программы без возможности самостоятельного размножения (backdoor, rootkit и всевозможные trojan);
VirWare: саморазмножающиеся вредоносные программы (вирусы и черви);
Other MalWare: программное обеспечение, интенсивно используемое злоумышленниками при создании вредоносных программ и организации атак.

ПРИЗНАКИ ЗАРАЖЕНИЯ КОМПЬЮТЕРА

- Вывод на экран непредусмотренных сообщений или изображений
- Подача непредусмотренных звуковых сигналов
- Неожиданное открытие и закрытие лотка CD/DVD дисковода
- Произвольный запуск на компьютере каких-либо программ
- Частые «зависания» и сбои в работе компьютера
- Медленная работа компьютера при запуске программ
- Исчезновение или изменение файлов и папок
- Частое обращение к жесткому диску
- «Зависание» или неожиданное поведение браузера

ДЕЙСТВИЯ ПРИ НАЛИЧИИ ПРИЗНАКОВ ЗАРАЖЕНИЯ КОМПЬЮТЕРА

1. Сохранить результаты работы на внешнем носителе

2. Отключить компьютер от локальной сети и Интернета, если он к ним был подключен

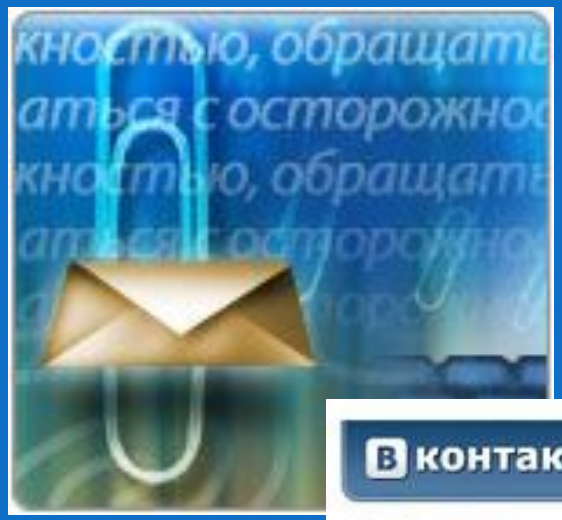
3. Загрузиться в режиме защиты от сбоев или с диска аварийной загрузки Windows (если компьютер выдает ошибку, когда вы его включаете)

4. Запустить антивирусную программу

Сетевые черви и защита от них

СЕТЕВЫЕ ЧЕРВИ

Сетевые черви - это вредоносные программы, которые проникают на компьютер, используя сервисы компьютерных сетей: Всемирную паутину, электронную почту, интерактивное общение, файлообменные сети и т.д.

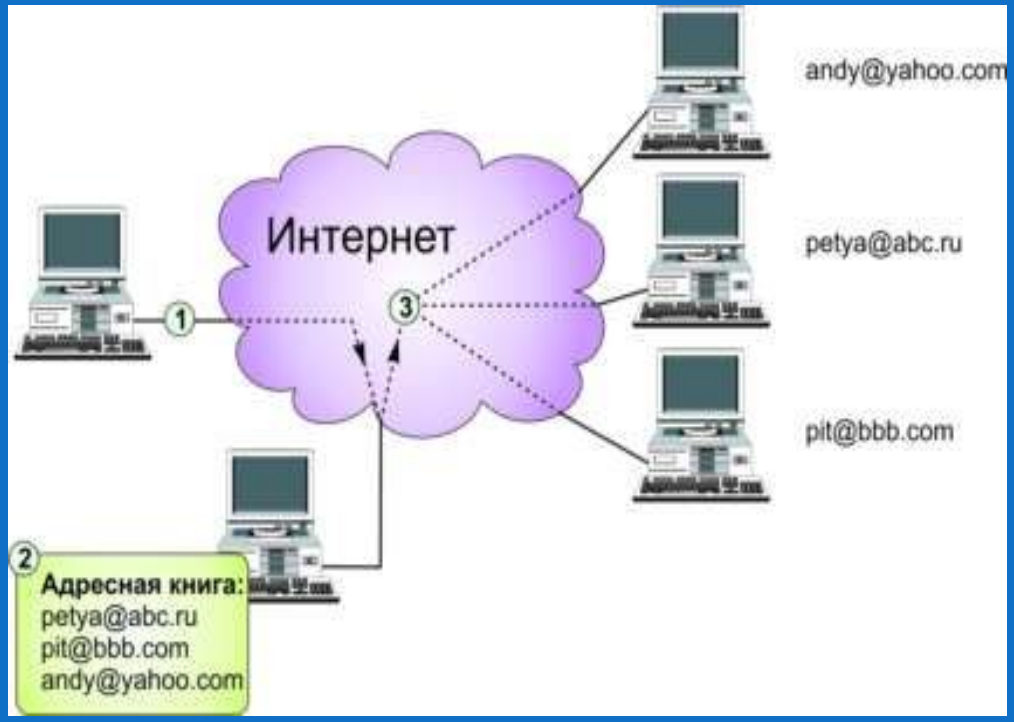


Многие сетевые черви используют более одного способа распространения своих копий по компьютерам локальных и глобальных сетей.

Активация сетевого червя может вызывать уничтожение программ и данных, а также похищение персональных данных пользователя.

ПОЧТОВЫЕ ЧЕРВИ

Почтовые черви для своего распространения используют электронную почту.



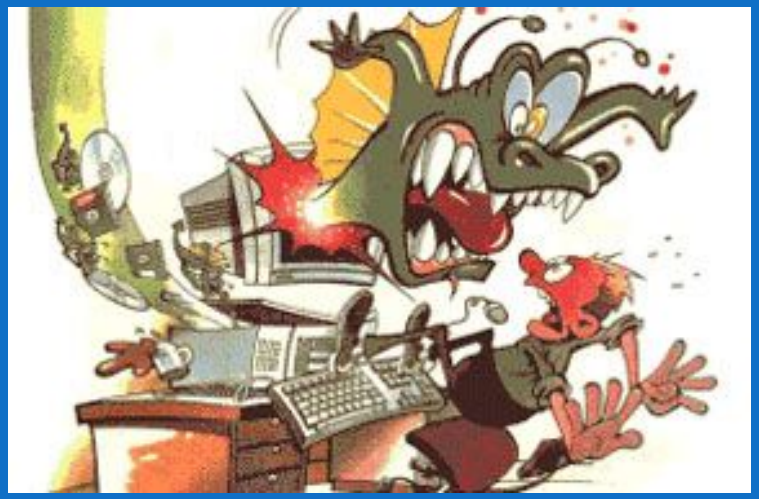
Червь отсылает либо свою копию в виде вложения в электронное письмо, либо ссылку на свой файл, расположенный на каком-либо сетевом ресурсе.

Код червя активируется при открытии (запуске) зараженного вложения или при открытии ссылки на зараженный файл.

Профилактическая защита от почтовых червей состоит в том, что не рекомендуется открывать вложенные в почтовые сообщения файлы, полученные из сомнительных источников.

ЧЕРВИ, ИСПОЛЬЗУЮЩИЕ «УЯЗВИМОСТИ» ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Червь ищет в сети компьютеры, на которых используются операционная система и приложения, содержащие уязвимости.



Червь посылает на компьютер специально оформленный сетевой пакет или запрос, в результате чего код (или часть кода) червя проникает на компьютер-жертву.

Если сетевой пакет содержит только часть кода червя, он затем скачивает основной файл и запускает его на исполнение на зараженном компьютере.

Профилактическая защита от таких червей состоит в том, что рекомендуется своевременно скачивать из Интернета и устанавливать обновления системы безопасности операционной системы и приложений.

ЧЕРВИ, ИСПОЛЬЗУЮЩИЕ ФАЙЛООБМЕННЫЕ СЕТИ

Для внедрения в файлообменную сеть червь копирует себя в папку обмена файлами на одном из компьютеров.

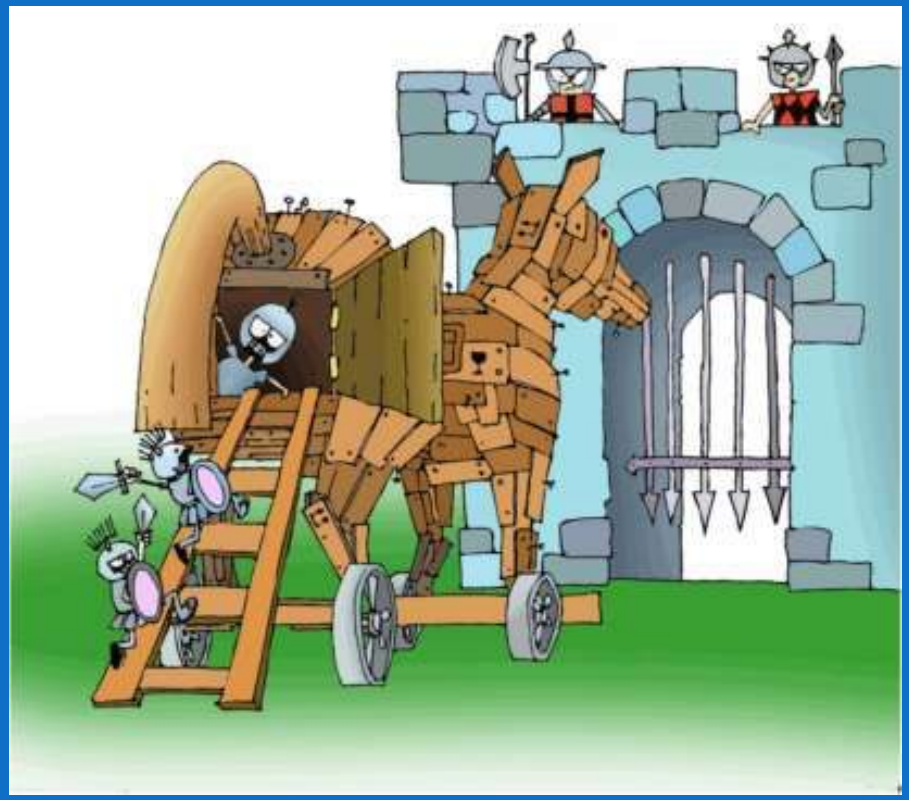
В 2001 году стал стремительно распространяться сетевой червь «Nimda», который атаковал компьютеры сразу несколькими способами: через сообщения электронной почты, через открытые ресурсы локальных сетей, а также используя уязвимости в системе безопасности операционной системы серверов Интернета.

Профилактическая защита от таких сетевых червей состоит в том, что рекомендуется своевременно скачивать из Интернета и обновлять антивирусную программу и вирусную базу данных.

Троянские программы и защита от них

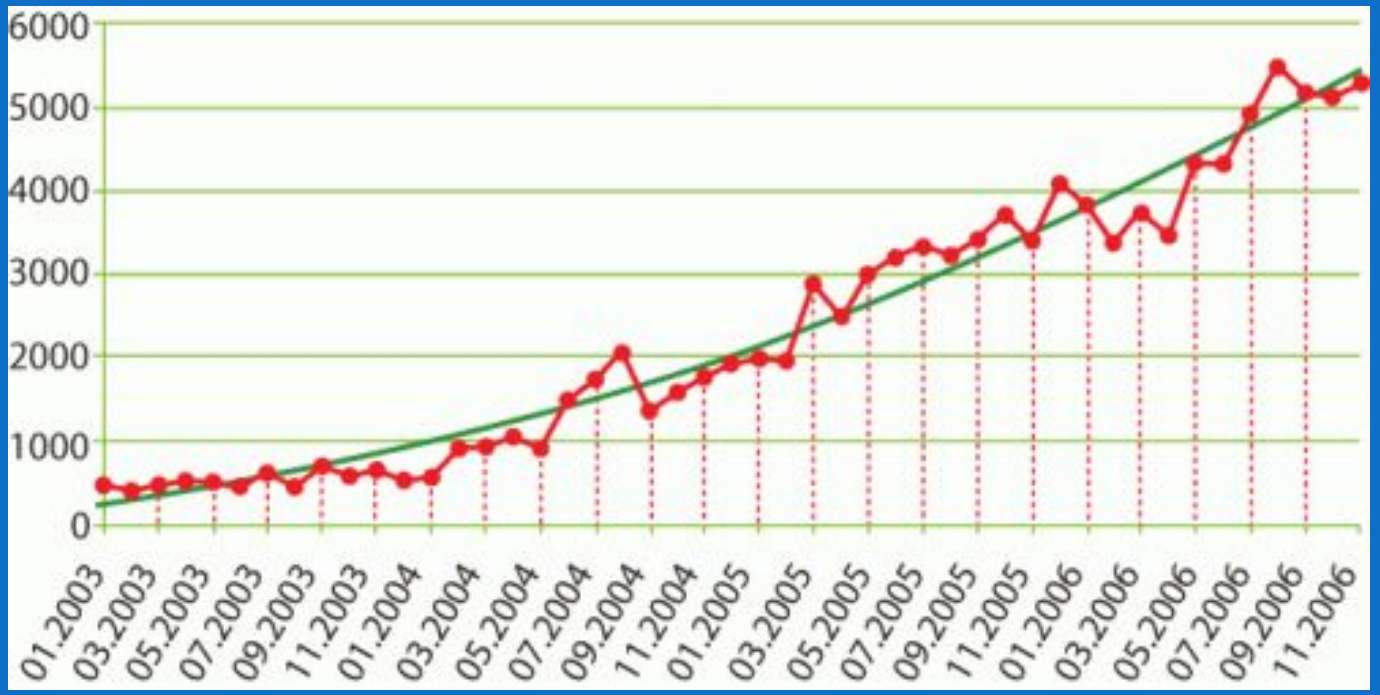
ТРОЯНСКИЕ ПРОГРАММЫ

Троянская программа, троянец (от англ. trojan) – вредоносная программа, которая выполняет несанкционированную пользователем передачу управления компьютером удаленному пользователю, а также действия по удалению, модификации, сбору и пересылке информации третьим лицам.



Троянские программы обычно проникают на компьютер как сетевые черви, а различаются между собой по тем действиям, которые они производят на зараженном компьютере.

ТРОЯНСКИЕ ПРОГРАММЫ



Количество обнаруживаемых аналитиками "Лаборатории Касперского" новых "троянских" программ

ТРОЯНСКИЕ УТИЛИТЫ УДАЛЕННОГО АДМИНИСТРИРОВАНИЯ

Утилиты скрытого управления позволяют принимать или отсылать файлы, запускать и уничтожать их, выводить сообщения, стирать информацию, перезагружать компьютер и т. д.

При запуске троянец устанавливает себя в системе и затем следит за ней, при этом пользователю не выдается никаких сообщений о действиях троянской программы в системе.

В 2003 году широкое распространение получила троянская программа Backdoor.Win32. BO, которая осуществляет следующие действия:

- высылает имена компьютера, пользователя и информацию о системе: тип процессора, размер памяти, версию системы, информацию об установленных устройствах;
- посылает/принимает, уничтожает, копирует, переименовывает, исполняет любой файл;
- отключает пользователя от сети;
- «завешивает» компьютер;
- читает или модифицирует системный реестр.

ТРОЯНСКИЕ ПРОГРАММЫ, ВОРУЮЩИЕ ИНФОРМАЦИЮ

Троянские программы ворующие информацию, при запуске ищут файлы, хранящие конфиденциальную информацию о пользователе (банковские реквизиты, пароли доступа к Интернету и др.) и отсылают ее по указанному в коде троянца электронному адресу или адресам.

Троянцы данного типа также сообщают информацию о зараженном компьютере (размер памяти и дискового пространства, версию операционной системы, IP-адрес и т. п.).

Некоторые троянцы воруют регистрационную информацию к программному обеспечению.

ТРОЯНСКИЕ ПРОГРАММЫ – ИНСТАЛЛЯТОРЫ ВРЕДОНОСНЫХ ПРОГРАММ

Троянские программы этого класса скрытно инсталлируют другие вредоносные программ и используются для «подсовывания» на компьютер-жертву вирусов или других троянских программ.

Загруженные без ведома пользователя из Интернета программы либо запускаются на выполнение, либо включаются троянцем в автозагрузку операционной системы.

ТРОЯНСКИЕ ПРОГРАММЫ - ШПИОНЫ

Данные троянцы осуществляют электронный шпионаж за пользователем зараженного компьютера: вводимая с клавиатуры информация, снимки экрана, список активных приложений и действия пользователя с ними сохраняются в каком-либо файле на диске и периодически отправляются злоумышленнику.

Троянские программы этого типа часто используются для кражи информации пользователей различных систем онлайновых платежей и банковских систем.

Троянские программы часто изменяют записи системного реестра операционной системы, поэтому для их удаления необходимо в том числе восстановление системного реестра.

Рекламные и шпионские программы и защита от них

РЕКЛАМНЫЕ ПРОГРАММЫ

Рекламные программы *(от англ. Adware: Advertisement - реклама и Software - программное обеспечение)* встраивают рекламу в основную полезную программу.

Часто рекламные программы входят в состав официально поставляемых условно бесплатных версий программного обеспечения.

Реклама демонстрируется пользователю в процессе работы основной программы в виде графических баннеров или бегущей строки.

Обычно после покупки и/или регистрации основной программы рекламная вставка удаляется и показ рекламы прекращается.

ШПИОНСКИЕ ПРОГРАММЫ

Шпионские программы *(от англ. Spyware: Spy - шпион и Software - программное обеспечение)* скрытно собирают различную информацию о пользователе компьютера и затем отправляют ее злоумышленнику.

Эти программы иногда проникают на компьютер под видом рекламных программ и не имеют возможности деинсталляции пользователем без нарушения функционирования использующей их программы.

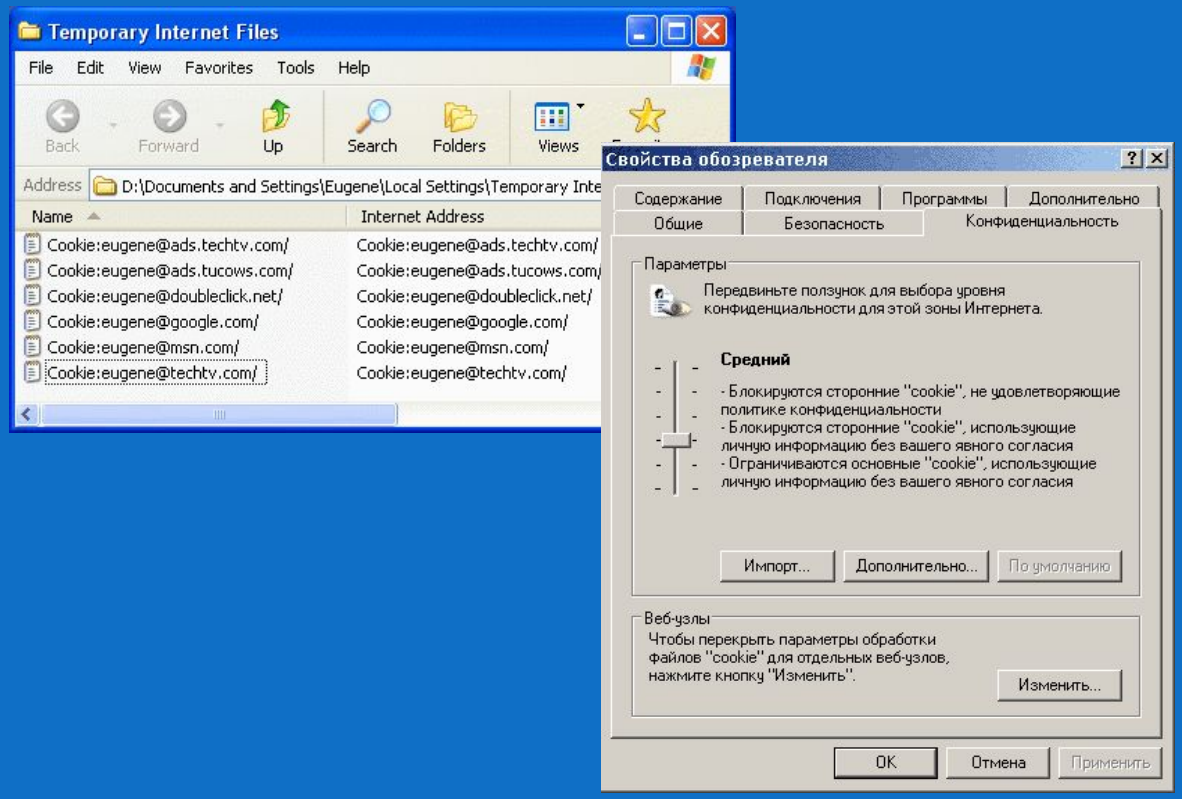
Иногда шпионские программы обнаруживаются в распространенных программных продуктах известных на рынке производителей.

В марте 2005 года под видом поисковой панели для браузера Internet Explorer начала распространяться рекламно-шпионская программа «mwsbar».

Программа регистрирует себя в системном реестре и добавляет в автозагрузку, что приводит к изменению настроек браузера и перенаправлению результатов поиска в Интернете на сайт злоумышленника.

КУКИ

Куки *(от англ. cookies - домашнее печенье)* - небольшой текстовый файл, помещаемый Web-сервером на локальный компьютер.



Файлы cookies могут храниться в оперативной памяти (сеансовые файлы cookies) или записываться на жесткий диск (постоянные файлы cookies).

Файлы cookies не могут быть использованы для запуска программного кода (запуска программ) или для заражения компьютера вирусами.

Браузеры позволяют включать и отключать использование файлов cookies, а также выполнять прием файлов cookies только после подтверждения со стороны пользователя.

Спам
и защита от него

СПАМ

Спам *(от англ. spam)* — это массовая автоматическая рассылка рекламных электронных сообщений, со скрытым или фальсифицированным обратным адресом.

Спам распространяется по компьютерным сетям с использованием электронной почты и систем интерактивного общения (типа ICQ), а также по мобильным сетям с использованием службы SMS-сообщений.

Спам приходит потому, что электронный адрес получателя стал известен спамерам (рассыльщикам спама).

Спамеры стремятся получить подтверждение, что почтовый адрес действительно используется (в этом случае поток спама может увеличиться многократно).

РЕКЛАМНЫЙ СПАМ

Рекламный спам используют некоторые компании, занимающиеся легальным бизнесом, для рекламы своих товаров или услуг.

Рассылку рекламного спама чаще заказывают компаниям (или лицам), которые на этом специализируются.

Привлекательность такой рекламы заключается в ее сравнительно низкой стоимости и большом охвате потенциальных клиентов.

С помощью спама часто рекламируют продукцию, о которой нельзя сообщить другими способами, например оружие, порнографию, лекарственные средства с ограничениями по обороту, ворованную информацию (базы данных), контрафактное программное обеспечение и т. п.

«НИГЕРИЙСКИЕ ПИСЬМА»

Иногда спам используется для выманивания денег у получателя письма. Наиболее распространенный способ получил название «нигерийские письма», потому что большое количество таких писем приходило из Нигерии.

«Нигерийское письмо» содержит сообщение о том, что получатель письма может получить большую сумму денег, а отправитель может ему в этом помочь. Затем отправитель письма просит перевести ему немного денег под предлогом, например, оформления документов или открытия счета.

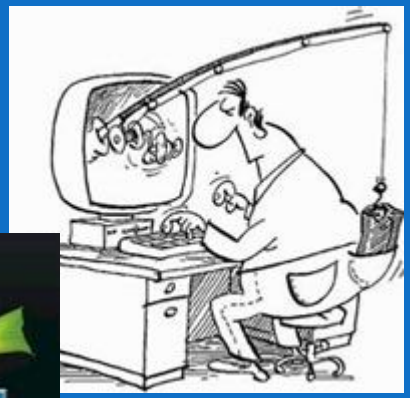
PLEASE READ VERY CAREFULLY / PROSHU VAS PROCHITAETE VNIMATELNO

Uvazjaemij.

Slediushe eto slov Mr.Anyanwu cherez svoj sinj Charles Anyanwu.
Mne nuzjno sposobnij chelovek dlya ochen ogromnij proekta!.
Koratko o proekte- zavod stali i splavov v Nigerij,-A.S.C.L postroiji kompanij ot bivshe sacz,V.O.Tyazhpromexport,rovno s 1979G do rovno 1999G
Vsevo dolzjnost k kompanij bilo v poryadok 2200 Million Dollarov!!
Kompanij poluchili rovno 1,300 Million dollarov do smerta president Nigeria tagda,General S.Abacha,ostalnij dengi rovno 900 Million Dollarov General Abacha cherez kompanij Mecosta Securities "ukral".
Vazjno shto s 1979 do 1998,vse dengi dlya plotezj glavnij kontrakorov kak V.O.Tyazhpromexport, a malo kontraktorov kak ne kotorij "Sovietskij" kompanij,bilo pod kontrolya kommittet-Debt Recconciliation and Contract review Committee-A.S.C.L.
Teper est summu 187,500,000.00 rovno,kotorij ostalis v scheet Kommitteta,a

ФИШИНГ

Фишинг *(от англ. fishing - рыбалка)* — выманивание у получателя письма данных, которые можно использовать для получения выгоды: номера его кредитных карточек или пароли доступа к системам онлайновых платежей.



Такое письмо обычно маскируется под официальное сообщение от администрации банка. В нем говорится, что получатель должен подтвердить сведения о себе, иначе его счет будет заблокирован, и приводится адрес сайта (принадлежащего спамерам) с формой, которую надо заполнить.

Для того чтобы жертва не догадалась об обмане, оформление сайта имитирует оформление официального сайта банка.

ЗАЩИТА ОТ СПАМА

В силу массового характера спамовые почтовые рассылки затрудняют работу информационных систем и ресурсов, создавая для них бесполезную нагрузку.

Для борьбы со спамом используются антиспамовые фильтры, которые могут быть установлены как на локальных компьютерах пользователей, так и на почтовых серверах провайдеров.

Антиспамовые фильтры анализируют содержание письма или пытаются опознать спамера по электронному адресу.

Для затруднения автоматической фильтрации спамовые сообщения часто искажаются, вместо букв используются похожие по начертанию цифры, русские буквы заменяются на латинские, а в случайных местах добавляются пробелы.

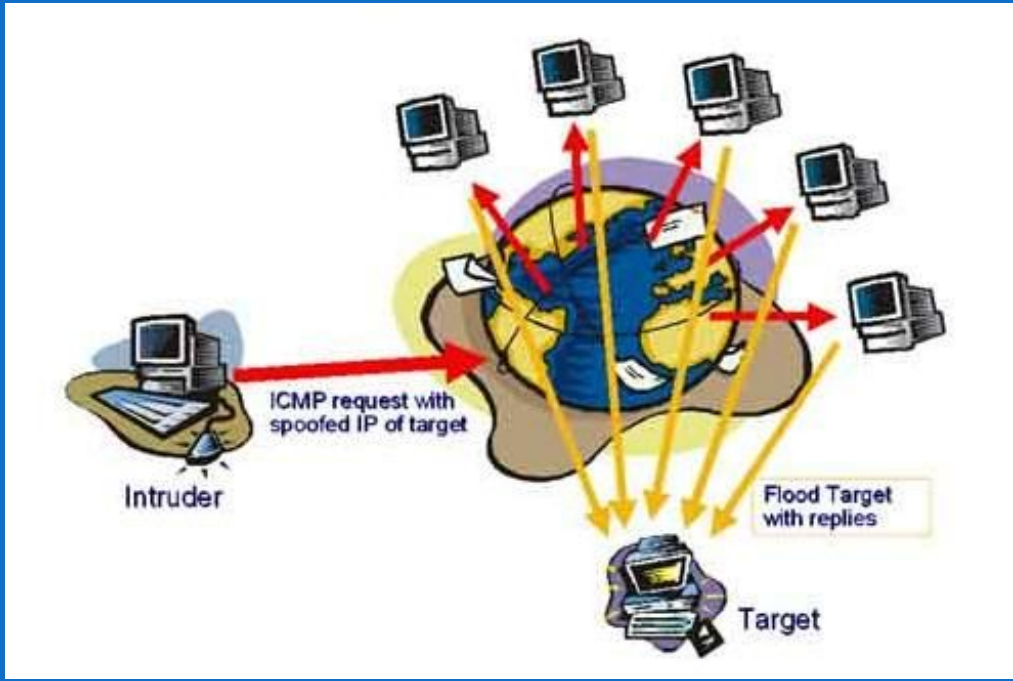
Хакерские утилиты и защита от них

СЕТЕВЫЕ АТАКИ

Сетевые атаки - направленные действия на удаленные сервера для создания затруднений в работе или утери данных

Сетевые атаки на удаленные серверы реализуются с помощью специальных программ, которые посылают на них специфические запросы. Это приводит к отказу в обслуживании («зависанию» сервера), если ресурсы атакуемого сервера недостаточны для обработки всех поступающих запросов.

СЕТЕВЫЕ АТАКИ

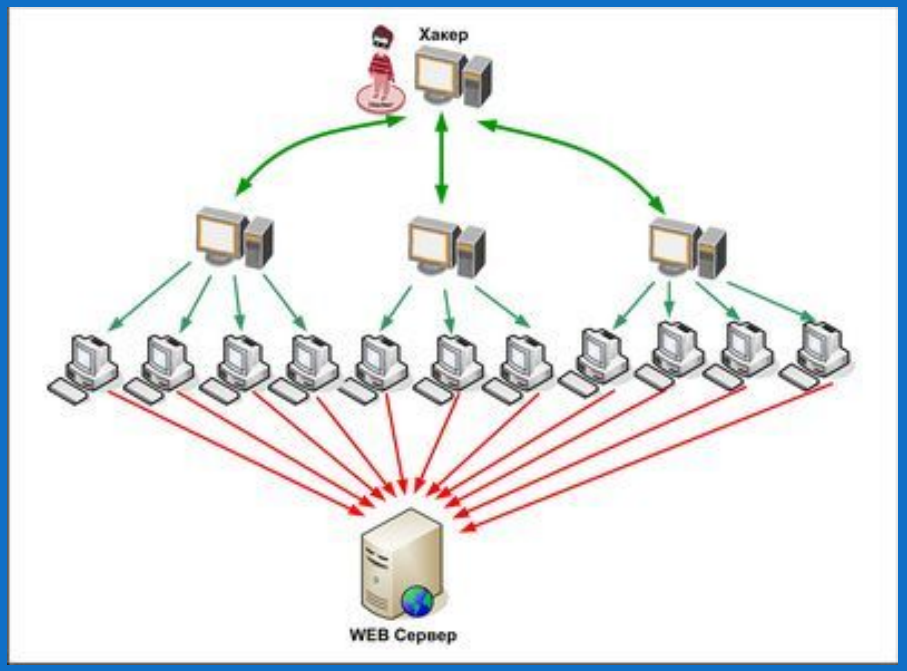


DoS-программы (от англ. Denial of Service – отказ в обслуживании) реализуют атаку с одного компьютера с ведома пользователя.

DoS-программы обычно наносят ущерб удаленным компьютерам и сетям, не нарушая работоспособность зараженного компьютера.

Некоторые сетевые черви содержат в себе DoS-процедуры, атакующие конкретные сайты. Так, червь «Codered» 20 августа 2001 года организовал успешную атаку на официальный сайт президента США, а червь «Mydoom» 1 февраля 2004 года «выключил» сайт компании – производителя дистрибутивов UNIX.

СЕТЕВЫЕ АТАКИ



Чаще всего при проведении DDoS-атак злоумышленники используют трехуровневую архитектуру

DDoS-программы *(от англ. Distributed DoS – распределенный DoS)* реализуют распределенные атаки с разных компьютеров, причем без ведома пользователей зараженных компьютеров.

Для этого DDoS-программа засылается на компьютеры «жертв-посредников» и после запуска в зависимости от текущей даты или по команде от хакера начинает сетевую атаку на указанный сервер в сети.

Некоторые хакерские утилиты реализуют фатальные сетевые атаки. Такие утилиты используют уязвимости в операционных системах и приложениях и отправляют специально оформленные запросы на атакуемые компьютеры в сети. В результате сетевой запрос специального вида вызывает критическую ошибку в атакуемом приложении, и система прекращает работу.

УТИЛИТЫ «ВЗЛОМА» УДАЛЁНЫХ КОМПЬЮТЕРОВ

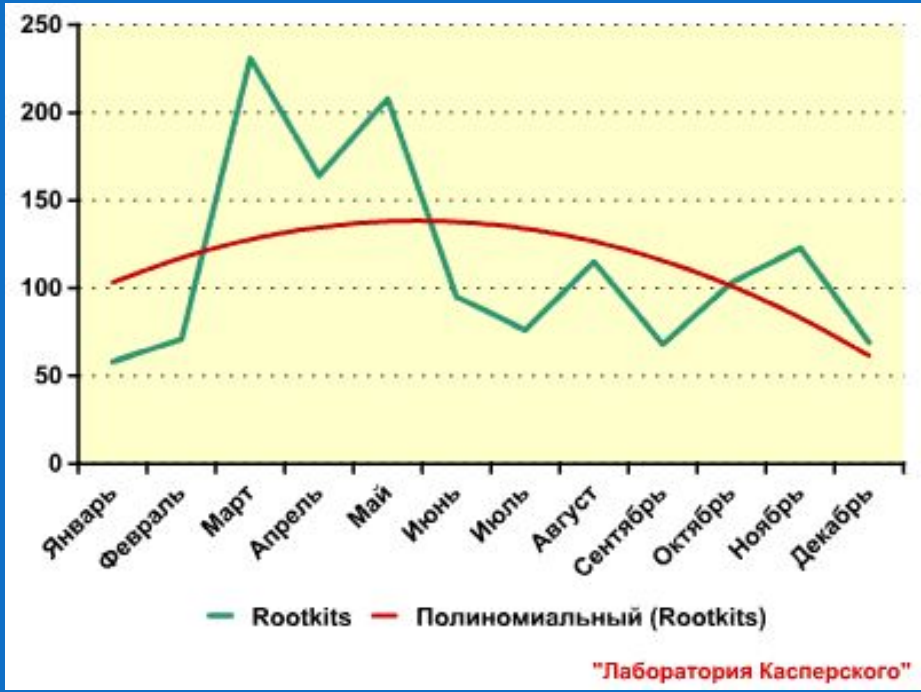
Утилиты «взлома» удаленных компьютеров предназначены для проникновения в удаленные компьютеры с целью дальнейшего управления ими (используя методы троянских программ типа утилит удаленного администрирования) или для внедрения во «взломанную» систему других вредоносных программ

Утилиты «взлома» удаленных компьютеров обычно используют уязвимости в операционных системах или приложениях, установленных на атакуемом компьютере.

Профилактическая защита от «взлома» состоит в своевременной загрузке из Интернета обновлений системы безопасности операционной системы и приложений.

РУТКИТЫ

Руткит *(от англ. root kit - «набор для получения прав root»)* - программа или набор программ для скрытного взятия под контроль «взломанной» системы.



Количество новых руткитов, обнаруженных аналитиками «Лаборатории Касперского» в 2007 году

В операционной системы UNIX под термином «rootkit» понимается набор утилит, которые хакер устанавливает на «взломанном» им компьютере после получения первоначального доступа.

В операционной системе Windows под rootkit принято подразумевать программу, которая внедряется в систему и перехватывает системные функции.

Многие rootkit устанавливают в систему свои драйверы и службы (они также являются «невидимыми»).

ЗАЩИТА ОТ ХАКЕРСКИХ АТАК И СЕТЕВЫХ ЧЕРВЕЙ

Защита компьютерных сетей или отдельных компьютеров от несанкционированного доступа может осуществляться с помощью межсетевого экрана, или брандмауэра *(от англ. firewall).*

Межсетевой экран позволяет:

- *блокировать хакерские DoS-атаки, не пропуская на защищаемый компьютер сетевые пакеты с определенных серверов (определенных IP-адресов или доменных имен);*
- *не допускать проникновение на защищаемый компьютер сетевых червей (почтовых, Web и др.);*
- *препятствовать троянским программам отправлять конфиденциальную информацию о пользователе и компьютере.*

Межсетевые экраны ZyXEL - защита сети от вирусов, спама, **сетевых атак**.

Межсетевой экран может быть реализован как аппаратно, так и программно.