Вирусы

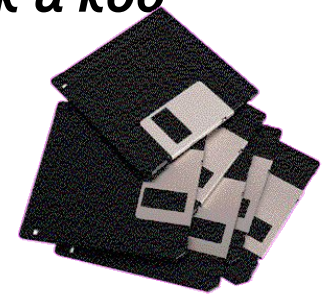
Работу выполнила
ученица 11 класса
Гибельгаус Таня.

Вирус

Под ***компьютерным вирусом*** принято понимать программы или элементы программ, несанкционированно проникшие в компьютер с целью нанесения вреда, отличительной особенностью которых является способность самотиражирования.

Все вирусы можно объединить в следующие основные группы:

- **Загрузочные вирусы (boot – вирусы)** — инфицируют загрузочные секторы жестких дисков и дискет, помещая в нем команды запуска на исполнение самого вируса, который находится где-то в другом месте компьютера.
- **Файловые вирусы** — заражают исполняемые файлы (с расширением .com, .exe, .sys), путем дописывания своей основной части («тела») в конец заражаемой программы, «головы» - в его начало. Вирус, находящийся в памяти, заражает все любой запущенный после этого исполняемый файл.
- **Загрузочно-файловые вирусы** способны поражать как код загрузочных секторов, так и код файлов.
- **Сетевые вирусы.**



Загрузочные вирусы (boot – вирусы)

- ***Макро-вирусы.***

Заражает файлы документов, например текстовые документы. После загрузки заражённого документа постоянно находится в оперативной памяти до закрытия документа.

- ***«Червь».***

это программа, которая тиражируется на жестком диске, в памяти компьютера и распространяется по сети.

- Особенностью червей, отличающих их от других вирусов, является то, что они не несут в себе ни какой вредоносной нагрузки, кроме саморазмножения, целью которого является замусоривание памяти, и как следствие, затормаживание работы операционной системы.

СЕТЕВЫЕ ЧЕРВИ

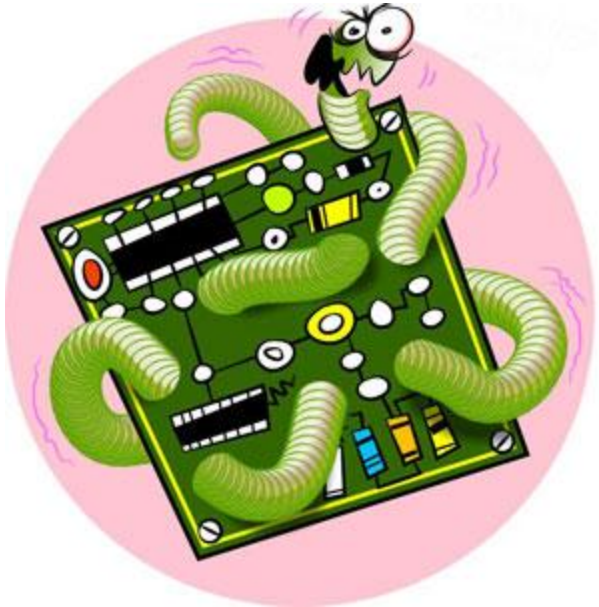
К данной категории относятся программы, распространяющие свои копии по локальным и/или глобальным сетям с целью:

1. ***проникновения на удаленные компьютеры;***
2. ***запуска своей копии на удаленном компьютере;***
3. ***дальнейшего распространения на другие компьютеры в сети.***

Для своего распространения сетевые черви используют разнообразные компьютерные и мобильные сети: электронную почту, системы обмена мгновенными сообщениями, файлообменные (P2P) и IRC-сети, LAN, сети обмена данными между мобильными устройствами (телефонами, карманными компьютерами) и т. д.

Большинство известных червей распространяется в виде файлов: вложение в электронное письмо, ссылка на зараженный файл на каком-либо веб- или FTP-ресурсе в ICQ- и IRC-сообщениях, файл в каталоге обмена P2P и т. д.

Некоторые черви (так называемые «бесфайловые» или «пакетные» черви) распространяются в виде сетевых пакетов, проникают непосредственно в память компьютера и активизируют свой код.



В дополнение к этой классификации отметим еще несколько отличительных особенностей, характеризующих некоторые файлово - загрузочные вирусы.

Полиморфизм.

Большинство вирусов, созданных в прежние годы, при саморазмножении никак не изменяются, так что «потомки» являются абсолютно точной копией «прародителя», что и позволяет легко их обнаруживать по характерной для каждого последовательности байтов

«Стелс» - технология.

Этот термин появился по аналогии с названием технологии разработки американского бомбардировщика, невидимого на экране радара. Стелс-вирус, находясь в памяти компьютера, перехватывает почти все векторы прерываний . В результате при попытке контроля длины зараженного файла ДОС выдает старую, «правильную» длину вместо истинной, а при просмотре коды вируса исключаются им из рассмотрения.

«Логические бомбы».

кая программа добавляется к какой-либо полезной программе и «дремлет» в ней до определенного часа. Когда же показания системного счетчика времени данного компьютера станут равными установленному программистом значению часов, минут и секунд (или превысят их), производится какое-либо разрушающее действие, например, форматирование винчестера. Это один из распространенных вариантов мести обиженных программистов своему руководству.

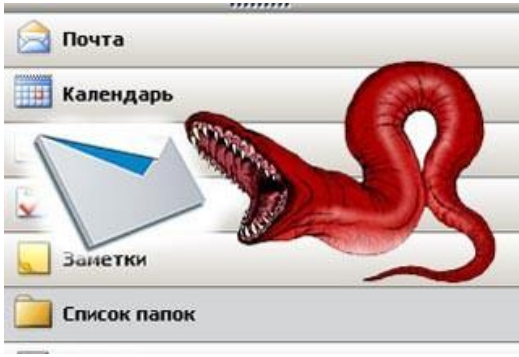
Программы-вандалы.

Самый простой способ напакостить всем и вся. Пишется программа-разрушитель (например, все тот же форматировщик винчестера), ей дается название, такое же, как у другой, полезной программы, и она размещается в качестве «обновленной версии». Ничего не подозревающий пользователь обрадовано «скачивает» ее на свой компьютер и запускает, а в результате - лишается всей информации на жестком диске.

Сетевые вирусы.

- **«Логические бомбы» - скрипты и апплеты**.

И хотя основные функции доступа к содержимому вашего диска здесь отключены, некоторые мелкие неприятности это может доставить. Кстати, в последнее время создатели некоторых сайтов (как правило, из разряда «только для взрослых») освоили любопытный вариант скриптов (на базе JavaScript), способных при открытии такой Web-страницы не только «прописать» адрес данного сайта в качестве «домашнего» (естественно, не спрашивая у посетителя разрешения), но и внести его непосредственно в системный реестр Windows в качестве «базового».



- **«Троянские кони».**

Это модули, присоединяемые к каким-либо нормальным программам, распространяемым по сети, или «забрасываемые» в ваш компьютер несанкционированным способом.

Цель «троянского коня» - воровать ценную информацию (пароли доступа, номера кредитных карточек и т. п.) и передавать ее тому, кто этого «коня» запустил.

- **Почтовые вирусы**.

Чаще всего заражение начинается с получения неизвестно от кого письма, содержащего исполняемую программу-«зародыш» . Когда ничего не подозревающий пользователь запустит такую программу на исполнение, содержащийся в ней вирус «прописывается» в системе и, обращаясь к содержимому адресной книги, начинает тайком от вас рассылать всем абонентам свои копии-зародыши в качестве вложений.

Вирусы делятся также на резидентные и нерезидентные

— первые при получении управления загружаются в память и могут действовать, в отличие от нерезидентных, не только во время работы зараженного файла.

Дополнительные типы вирусов

- ***Зомби***

Зомби (Zombie) - это программа-вирус, которая после проникновения в компьютер, подключенный к сети Интернет управляется извне и используется злоумышленниками для организации атак на другие компьютеры. Зараженные таким образом компьютеры-зомби могут объединяться в сети, через которые рассылается огромное количество нежелательных сообщений электронной почты, а также распространяются вирусы и другие вредоносные программы.

Шпионские программы

Шпионская программа (Spyware) - это программный продукт, установленный или проникший на компьютер без согласия его владельца, с целью получения практически полного доступа к компьютеру, сбора и отслеживания личной или конфиденциальной информации.

Эти программы, как правило, проникают на компьютер при помощи сетевых червей, троянских программ или под видом рекламы

Одной из разновидностей шпионских программ являются :

Фишинг (Phishing) - это почтовая рассылка имеющая своей целью получение конфиденциальной финансовой информации. Такое письмо, как правило, содержит ссылку на сайт, являющейся точной копией интернет-банка или другого финансового учреждения.

Фарминг – это замаскированная форма фишинга, заключающаяся в том, что при попытке зайти на официальный сайт интернет банка или коммерческой организации, пользователь автоматически перенаправляется на ложный сайт, который очень трудно отличить от официального сайта.

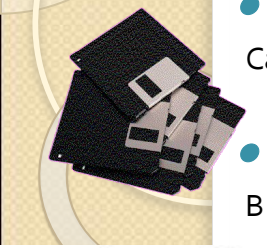
основной целью злоумышленников, использующих Фарминг, является завладение личной финансовой информацией пользователя. Отличие заключается только в том, что вместо электронной почты мошенники используют более изощренные методы направления пользователя на фальшивый сайт.

Хакерские утилиты и прочие вредоносные программы

К данной категории относятся:

- утилиты автоматизации создания вирусов, червей и троянских программ (конструкторы);
- программные библиотеки, разработанные для создания вредоносного ПО;
- хакерские утилиты скрытия кода зараженных файлов от антивирусной проверки (шифровальщики файлов);
- «злые шутки», затрудняющие работу с компьютером;
- программы, сообщающие пользователю заведомо ложную информацию о своих действиях в системе;
- прочие программы, тем или иным способом намеренно наносящие прямой или косвенный ущерб данному или удалённым компьютерам.

Каналы распространения



- ***Дискеты***

Самый распространённый канал заражения в 1980-90 годы. Сейчас практически отсутствует из-за появления более распространённых и эффективных каналов и отсутствия флоппи-дисководов.

- ***Флеш-накопители (флешки)***

В настоящее время USB-флешки заменяют дискеты и повторяют их судьбу — большое количество вирусов распространяется через съёмные накопители, включая цифровые фотоаппараты, цифровые видеокамеры, цифровые плееры (MP3-плееры), сотовые телефоны. Использование этого канала преимущественно обусловлено возможностью создания на накопителе специального файла ***autorun.inf,*** в котором можно указать программу, запускаемую Проводником Windows при открытии такого накопителя. Флешки — основной источник заражения для компьютеров, не подключённых к сети Интернет.

- ***Электронная почта***

Сейчас один из основных каналов распространения вирусов. Обычно вирусы в письмах электронной почты маскируются под безобидные вложения: картинки, документы, музыку, ссылки на сайты.

- ***Системы обмена мгновенными сообщениями***

Так же распространена рассылка ссылок на якобы фото, музыку либо программы, в действительности являющиеся вирусами, по ICQ и через другие программы мгновенного обмена сообщениями.

- ***Веб-страницы***

Возможно также заражение через страницы Интернет ввиду наличия на страницах всемирной паутины различного «активного» содержимого: скриптов, ActiveX-компоненты, Java-апплетов

- ***Интернет и локальные сети (черви)***

Черви — вид вирусов, которые проникают на компьютер-жертву без участия пользователя. Черви используют так называемые «дыры» (уязвимости) в программном обеспечении операционных систем, чтобы проникнуть на компьютер.

Это интересно!!!

Мнений по поводу рождения первого компьютерного вируса очень много. Нам доподлинно известно только одно: на машине Чарльза Бэббиджа, считающегося изобретателем первого компьютера, вирусов не было, а на Univax 1108 и IBM 360/370 в середине 1970-х годов они уже были.

Несмотря на это, сама идея компьютерных вирусов появилась значительно раньше. Отправной точкой можно считать труды Джона фон Неймана по изучению самовоспроизводящихся математических автоматов. Эти труды стали известны в 1940-х годах. А в 1951 г. знаменитый ученый предложил метод, который демонстрировал возможность создания таких автоматов. Позднее, в 1959 г., журнал "Scientific American" опубликовал статью Л.С. Пенроуза, которая также была посвящена самовоспроизводящимся механическим структурам. В отличие от ранее известных работ, здесь была описана простейшая двумерная модель подобных структур, способных к активации, размножению, мутациям, захвату. Позднее, по следам этой статьи другой ученый - Ф.Ж. Шталь - реализовал модель на практике с помощью машинного кода на IBM 650.

Необходимо отметить, что с самого начала эти исследования были направлены отнюдь не на создание теоретической основы для будущего развития компьютерных вирусов. Наоборот, ученые стремились усовершенствовать мир, сделать его более приспособленным для жизни человека. Ведь именно эти труды легли в основу многих более поздних работ по робототехнике и искусственному интеллекту. И в том, что последующие поколения злоупотребили плодами технического прогресса, нет вины этих замечательных ученых.

В 1962 г. 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.

10 самых опасных вирусов в истории Интернета:

Brain

Этот вирус в сравнении с последователями практически безопасен. Передается он по загрузочным секторам дискет, а примечателен тем, что первым вызвал настоящую вирусную эпидемию. Его разработка на совести братьев Амджата и Базита Алви (Amdjat и Basit Faroog Alvi), которые запустили его в 1986 году, а обнаружен он был летом 1987 года. Есть информация, что только в США вирус заразил более 18 тысяч компьютеров. А ведь в основе разработки лежали исключительно благие намерения: программа должна была наказать местных пиратов, ворующих программное обеспечение у фирмы братьев. Вирус Brain ко всему прочему еще и первый стелс-вирус. Так, при попытке чтения зараженного сектора, он «подставлял» и его незараженный оригинал.

Jerusalem

Этот вирус был создан в 1988 году в Израиле - отсюда и основное имя. Второе его название «Пятница 13-е». Это первый вирус для MS-DOS, вызвавший грандиозную панику. Скачанный в любое время с дискеты, он активировался в момент наступления злополучного числа - пятницы 13-е - и удалял абсолютно все данные с жесткого диска. В те времена вообще мало кто верил в существование компьютерных вирусов. Антивирусных программ и вовсе почти не существовало, а потому пользователи были совершенно беззащитны перед ним.

Червь Морриса

Активность этого опасного вредителя пришлась на ноябрь 1988 года. Данный Интернет-вирус тогда был первым в рейтинге самых страшных. Компьютеры ударом ноги подобно своему знаменитому тезке, он, конечно же, не убивал. Что он делал? Парализовывал работу компьютеров своим хаотичным и бесконтрольным размножением. Из-за него-то и вышла из строя вся, тогда еще не слишком глобальная, Сеть. И хоть сбой длился совсем не долго, общие убытки оценили в 96 миллионов долларов.

Michelangelo («March6»)

Этот вирус в свое время сильно переоценили. Правда, он заслуженно считается одним из самых безжалостных. Проникая через дискеты на загрузочный сектор диска, он тихо сидел там, не напоминая о своем существовании до 6 марта. А в этот день «счастливчики», получившие «Микеланджело» на свой компьютер, обнаруживали, что все данные с их жесткого диска стерты. Лютовал этот вирус в 1992 году. Зато он сильно сыграл на руку компаниям, производящим антивирусы. Пользуясь случаем, бизнесмены раздули истерию до невиданных масштабов, в то время как на деле от него пострадали всего около 10000 машин.

Чернобыль (CIH)

Один из самых знаменитых вирусов мира. Создан в 1998 году тайваньским студентом, по инициалам которого и назван. Через Интернет, электронную почту и диски вирус попадал в компьютер, прятался внутри других программ, а в определенный момент (26 апреля) вирус активировался, стирая содержимое жесткого диска и нанося вред аппаратной части компьютера. Эпидемия «Чернобыля» пришлась на апрель 1999 года. Тогда из строя было выведено более 300 тысяч компьютеров, в основном в Восточной Азии. Причем в течение нескольких последующих лет 26 апреля вирус продолжал свое черное дело, что по итогам нанесло урон огромному количеству компьютеров во всем мире.

Melissa

Создан в 1999 году. Первый всемирно известный почтовый червь. Он заражал файлы документов MS Word и рассылал свои копии в сообщениях электронной почты при помощи MS Outlook. Вирус распространялся с бешеной скоростью, а потому сумма нанесенного им ущерба оценивается более чем в $100 млн.

ILOVEYOU («Письмо счастья»)

Создан в 2000 году и примечателен тем, что придуман он довольно хитро. Пользователю на почту приходило сообщение «I LOVE YOU» с вложенным файлом. Доверившись столь милой оболочке, пользователь скачивал его и получал скрипт, который отсылал письма в невероятных количествах, а также удалял важные файлы на ПК. Результаты шокируют до сих пор: 10% всех существовавших на тот момент компьютеров были инфицированы, что нанесло ущерб в размере $5,5 миллиардов.

Nimda. 2001 год

Название представляет собой слово «admin», только наоборот. Вирус, попадая на компьютер, мгновенно «выписывал себе» права администратора. После чего изменял и нарушал конструкцию сайтов, блокировал доступ на хосты, IP-адреса и т.д. А проникал на компьютеры он столь виртуозно и эффективно, что уже через 22 минуты после своего создания он стал самым распространенным в сети Интернет.

My Doom. 2004 год

Самый быстрый вирус электронной почты. Работал он по нарастающей: каждый следующий компьютер отправлял спама еще больше, чем предыдущий. Кроме того, он модифицировал операционную систему, блокируя доступ к сайтам многих антивирусных компаний, новостным лентам и различным разделам сайта компании Microsoft. На его счету даже DDOS-атака на сайт Microsoft.

Conficker. 2008 год

Самый последний из всемирно распространившихся вирусов имеет славу опаснейшего из известных компьютерных червей. Атакует он операционные системы семейства Microsoft Windows. Вирус поразил более 12 миллионов компьютеров во всем мире. Принцип действия: червь находит уязвимости Windows, связанные с переполнением буфера, и при помощи обманного RPC-запроса выполняет код, отключая сервисные службы и обновление Windows, а также блокируя доступ к сайтам ряда производителей антивирусов.

Тест: Компьютерные вирусы

1. Заражение компьютерными вирусами может произойти в процессе ...

работы с файлами
форматирования диска
выключения компьютера
печати на принтере

2. Что необходимо иметь для проверки на вирус жесткого диска?

защищенную программу
загрузочную программу
файл с антивирусной программой
антивирусную программу, установленную на компьютер

3.Какая программа не является антивирусной?

AVP
Defrag
Norton Antivirus
Dr Web

4.Какие программы не относятся к антивирусным?

программы-фаги
программы сканирования
программы-ревизоры
программы-детекторы

5.Как вирус может появиться в компьютере?

при работе компьютера в сети
при решении математической задачи
при работе с макросами
самопроизвольно

6. Как происходит заражение «почтовым» вирусом?

при открытии зараженного файла, присланного с письмом по e-mail
при подключении к почтовому серверу
при подключении к web-серверу, зараженному «почтовым» вирусом
при получении с письмом, присланном по e-mail, зараженного файла

7. Компьютерным вирусом является ...

программа проверки и лечения дисков

любая программа, созданная на языках низкого уровня

программа, скопированная с плохо отформатированной дискеты

специальная программа небольшого размера, которая может приписывать себя к другим программам, она обладает способностью "размножаться"

8.Заражению компьютерными вирусами могут подвергнуться ...

графические файлы

программы и документы

звуковые файлы

все программы и вирусы

9.К категории компьютерных вирусов НЕ относятся

загрузочные вирусы

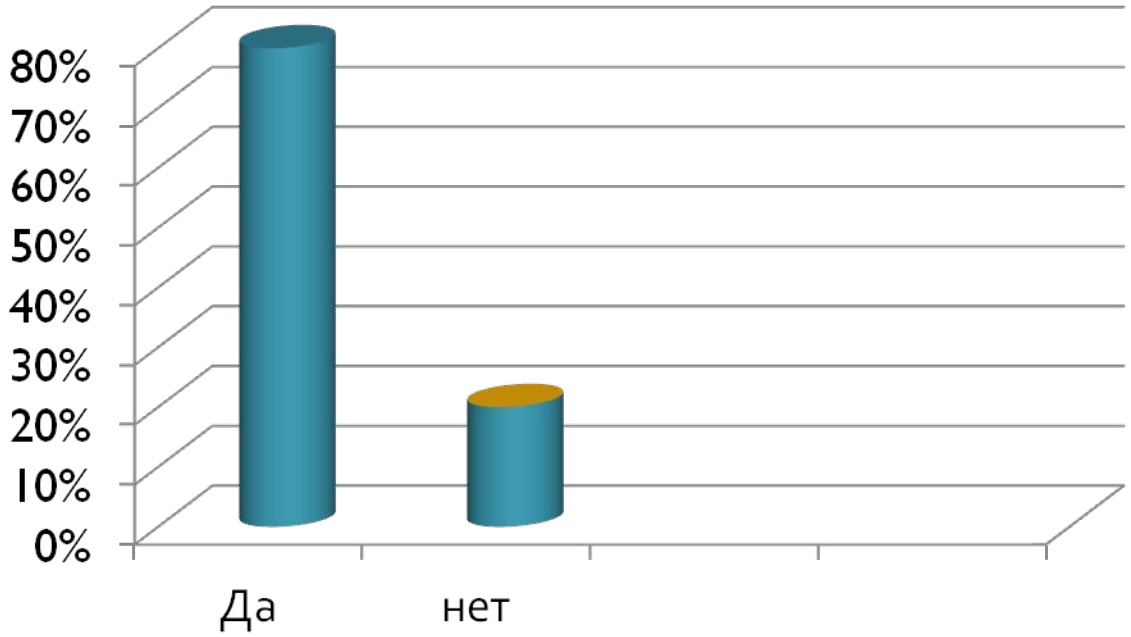
type-вирусы

сетевые вирусы

файловые вирусы

Анкетирование

Вопрос: Страдал ли ваш компьютер от вирусов?



Каким антивирусом вы пользуетесь?