КОМПЬЮТЕРНЫЕ ВИРУСЫ

Что это такое и как это начиналось?

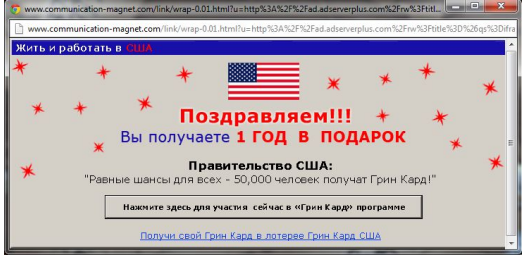
Составил учитель информатики
МОУ Путьоктябрьской СОШ
Горбачёв Сергей Александрович

Компьютерные вирусы

Основная отличительная характеристика компьютерного вируса — способность к самораспространению. Подобно биологическому вирусу для жизни и размножения он активно использует внешнюю среду - *память компьютера, операционную систему*.

- **Существует несколько определений компьютерных вирусов.**
- «**Компьютерный вирус** — это специально написанная, небольшая по размерам программа, которая может «приписывать» себя к другим программам («заражать» их), создавать свои копии и внедрять их в файлы, системные области компьютера и т. д., а также выполнять различные нежелательные действия на компьютере».
- «**Компьютерным вирусом** называется способная к самовоспроизводству и размножению программа, внедряющаяся в другие программы».
- «**Компьютерный вирус** - фрагмент исполняемого кода, который копирует себя в другую программу, модифицируя ее при этом. Дублируя себя, вирус заражает другие программы. Вирус выполняется только при запуске главной программы и вызывает ее непредсказуемое поведение, приводящее к уничтожению и искажению данных и программ».
- «**Компьютерный вирус** - программа, имеющая возможность создавать свои дубликаты и внедрять их в вычислительные сети и/или файлы, системные области компьютера и прочие объекты с целью искажения и уничтожения данных и программ. При этом дубликаты сохраняют способность к дальнейшему распространению. Такие программы, как правило, составляются на языке **ассемблера**, никаких сообщений на экран дисплея не выдают. Переносятся при копировании с диска на диск либо по сети Интернет.

Компьютерные вирусы и вредоносные программы

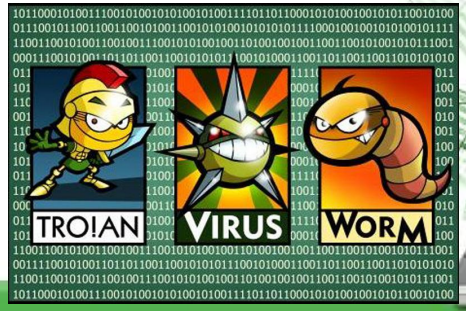


ОБЯЗАТЕЛЬНЫМ (НЕОБХОДИМЫМ) СВОЙСТВОМ КОМПЬЮТЕРНОГО ВИРУСА является возможность создавать свои дубликаты (не обязательно совпадающие с оригиналом) и внедрять их в вычислительные сети и/или файлы, системные области компьютера и прочие выполняемые объекты. При этом дубликаты сохраняют способность к дальнейшему распространению.

Определение **по ГОСТ Р 51188-98**

Вредоносная программа — компьютерная программа или переносной код, предназначенный для реализации угроз информации, хранящейся в КС, либо для скрытого нецелевого использования ресурсов КС, либо иного воздействия, препятствующего нормальному функционированию КС. К вредоносным программам относятся компьютерные **вирусы**, **трояны**, *сетевые* ***черви*** и др.

Компьютерные ***вирусы***, **трояны** и **черви** являются основными типами **вредоносных программ**.



Как это начиналось.

Изначально *компьютерные вирусы* были придуманы с совершенно иной целью.

Первые самораспространяющиеся программы не были вредоносными в понимаемом ныне смысле. Это были скорее программы-шутки либо последствия ошибок в программном коде, написанном в исследовательских целях. Сложно представить, что они были созданы с какой-то конкретной вредоносной целью.

История создания компьютерных вирусов начинается в **1983 году**, когда американский ученый **Фред Коэн** (Fred Cohen) в своей диссертационной работе, посвященной исследованию самовоспроизводящихся компьютерных программ впервые ввел термин - ***компьютерный вирус.***

Известна даже точная дата – **3 ноября 1983 года**, когда на еженедельном семинаре по компьютерной безопасности в Университете Южной Калифорнии (США) был предложен проект по созданию самораспространяющейся программы, которую тут же окрестили ***вирусом***. Для ее отладки потребовалось 8 часов компьютерного времени на машине ***VAX* 11/750** под управлением операционной системы Unix и ровно через неделю, 10 ноября состоялась первая демонстрация. **Фредом Коэном** по результатам этих исследований была опубликована работа "**Computer Viruses: theory and experiments**" с подробным описанием проблемы.

Первые вирусы

Pervading Animal (конец 60-х - начало 70-х) — так назывался первый известный ***вирус-игра*** для машины Univac 1108. С помощью наводящих вопросов ***программа*** пыталась определить имя животного, задуманного играющим. Благодаря наличию функции добавления новых вопросов, когда модифицированная ***игра*** записывалась поверх старой версии плюс копировалась в другие директории, через некоторое время ***диск*** становился переполненным.

Первый сетевой ***вирус*** **Creeper** появился в начале 70-х в военной компьютерной сети **Arpanet**, прототипе ***Интернет***. ***Программа*** была в состоянии самостоятельно выйти в сеть через модем и сохранить свою копию на удаленной машине. На зараженных системах ***вирус*** обнаруживал себя сообщением:

"I'M THE CREEPER: *CATCH* ME *IF* YOU *CAN*".

Для удаления назойливого, но в целом безобидного **вируса** неизвестным была создана ***программа*** **Reaper**. По сути это был ***вирус***, выполнявший некоторые функции, свойственные антивирусу: он распространялся по вычислительной сети и в случае обнаружения тела **вируса** Creeper уничтожал его.

Первые вирусы

Brain (1986 год) — первый ***вирус*** для ***IBM***-совместимых компьютеров, вызвавший глобальную эпидемию. Он был написан двумя братьями-программистами **Баситом Фарук** и **Амжадом Алви** из Пакистана с целью определения уровня пиратства у себя в стране: ***вирус*** заражал загрузочные сектора, менял метку диска на **"(c) Brain"** и оставлял сообщение с именами, адресом и телефоном авторов. Отличительной чертой его была ***функция*** подмены в момент обращения к нему зараженного сектора незараженным оригиналом. Это дает право назвать **Brain** первым известным **стелс-вирусом**.

В течение нескольких месяцев ***программа*** вышла за пределы Пакистана и к лету **1987 года** эпидемия достигла глобальных масштабов. Ничего деструктивного ***вирус*** не делал. В этом же году произошло еще одно знаменательное событие. Немецкий программист **Ральф Бюргер** открыл возможность создания программой своих копий путем добавления своего кода к выполняемым *DOS*-файлам формата *COM*. Опытный образец программы, получившей название **Virdem**, был продемонстрирован на форуме компьютерного андеграунда (**декабрь 1986 года, Гамбург, ФРГ**).

По результатам исследований **Бюргер** выпустил книгу ***"Computer Viruses. The Disease of High Technologies"***, послужившую толчком к написанию тысяч компьютерных **вирусов**, частично или полностью использовавших описанные автором идеи.

Первые вирусы

Lehigh (1987 год) — первый по-настоящему **вредоносный вирус**, вызвавший эпидемию в Лехайском университете (США), где в то время работал **Фред Коэн**. Он заражал только системные файлы ***COMMAND.COM*** и был запрограммирован на удаление всей информации на текущем диске. В течение нескольких дней было уничтожено содержимое сотен дискет из библиотеки университета и личных дискет студентов. Всего за время эпидемии было заражено около четырех тысяч компьютеров. Однако за пределы университета **Lehigh** не вышел.

Семейство резидентных ***файловых вирусов*** **Suriv (1987 год)** — творение неизвестного программиста из Израиля. Самая известная модификация, **Jerusalem**, стала причиной глобальной **вирусной** эпидемии. Действие **вирусов Suriv** сводилось к загрузке кода в ***память*** компьютера, перехватывании файловых операций и заражении запускаемых пользователем ***COM***- и/или **EXE**-файлов. Это и обеспечивало практически мгновенное распространение ***вируса*** по мобильным носителям. **Jerusalem** отличался от других программ дополнительной ***деструктивной функцией*** - уничтожением всех запускаемых программ **в пятницу, 13**. Такой черной датой стало **13 мая 1988 года**, когда в одночасье Перестали работать компьютеры многих коммерческих фирм, государственных Организаций и учебных заведений, в первую ***очередь*** **Америки, Европы и Ближнего Востока**.

Первые вирусные эпидемии

Возможности первых **вирусов** были сильно ограничены малой функциональностью существующих на тот момент вычислительных машин. Только в конце семидесятых, вслед за выпуском нового поколения персональных компьютеров Apple (Apple II) и в последствии ***IBM Personal Computer*** **(1981 год)**, стали возможны **вирусные** эпидемии. Появление ***BBS*** **(Bulletin *Board System*)** обеспечило быстрый ***обмен информацией*** между даже самыми отдаленными точками планеты.

Elk Cloner **(1981 год)** изначально использовал для распространения пиратских копий компьютерных игр. Поскольку жестких дисков тогда еще не было, он записывался в загрузочные сектора дискет и проявлял себя переворачиванием изображения на экране и выводом текста:

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!

Компьютерные черви

Червь Морриса (ноябрь 1988) — с ним связана первая эпидемия, вызванная **сетевым червем**. 60000-байтная ***программа***, написанная 23-летним студентом Корнельского университета (США) **Робертом Моррисом**, использовала ошибки в системе безопасности операционной системы **Unix** для платформ ***VAX* и *Sun* Microsystems**. С целью незаметного проникновения в вычислительные системы, связанные с сетью **Arpanet**, использовался подбор паролей (из списка, содержащего **481** вариант). Это позволяло маскироваться под задачу легальных пользователей системы. Однако из-за ошибок в коде безвредная по замыслу ***программа*** неограниченно рассылала свои копии по другим компьютерам сети, запускала их на выполнение и таким образом забирала под себя все сетевые ресурсы. **Червь Морриса** заразил по разным оценкам **от 6000 до 9000** компьютеров в США (включая Исследовательский центр *NASA*) и практически парализовал их работу на срок до пяти суток. Общие убытки были оценены в ***минимум*** 8 миллионов часов потери доступа и свыше миллиона часов прямых потерь на восстановление работоспособности систем. Общая ***стоимость*** этих затрат оценивается в 96 миллионов долларов. ***Ущерб*** был бы гораздо больше, если бы червь изначально создавался с разрушительными целями. 4 мая 1990 года впервые в истории состоялся **суд над автором компьютерного вируса**, который приговорил Роберта Морриса к **3 годам условно, 400 часам общественных работ и штрафу в 10 тысяч долларов США.**

Почтовые черви

Почтовые черви — **черви**, распространяющиеся в формате сообщений электронной почты.

Почтовый червь **Bagle** впервые был обнаружен **18 января 2004 года**. Для распространения он использовал собственный **SMTP-клиент**, код вируса пересылался во вложении с произвольным именем и расширением **.exe**. Рассылка производилась на адреса, найденные на зараженном компьютере. Также **Bagle** содержал встроенную **backdoor-процедуру**, открывающую ***порт*** **6777** на ***запуск*** команд и загрузку любых файлов.

Следующие модификации содержали процедуры распространения через ***P2P*-сети**, методы социальной инженерии, активно противодействовали антивирусному программному обеспечению.

Mydoom известен прежде всего массированной 12-дневной **DDoS-атакой** на **веб-*сайт*** компании ***SCO***, начавшейся **1 февраля 2004 года**. За пару часов работа сервера была полностью парализована и вернуться в нормальный режим www.sco.com смог только 5 марта.

Для распространения **Mydoom** использовал почтовую рассылку через собственный **SMTP-клиент**, а также ***P2P*-сети** (Kazaa).

Трояны

«Троянские кони»

«Троянские кони» — программы, предназначенные для перехвата данных на чужом компьютере или получения контроля над ним.

Троянские программы, попав на компьютер, глубоко проникают в систему, маскируются и ведут себя не совсем так, как другие типы вирусов.

Как правило, троянца сложнее обнаружить и удалить.

Содержание

Трояны

Троян (троянский конь) — тип вредоносных программ, основной целью которых является вредоносное воздействие по отношению к компьютерной системе. Трояны отличаются отсутствием механизма создания собственных копий. Некоторые **трояны** способны к автономному преодолению систем защиты КС, с целью проникновения и заражения системы. В общем случае, ***троян*** попадает в систему вместе с вирусом либо червем, в результате неосмотрительных действий пользователя или же активных действий злоумышленника. В силу отсутствия у ***троянов*** функций размножения и распространения, их жизненный цикл крайне короток - всего три стадии:

- **Проникновение на компьютер**
- **Активация**
- **Выполнение заложенных функций**

Это, само собой, не означает малого времени жизни ***троянов***.

Напротив, ***троян*** может длительное время незаметно находиться в памяти компьютера, никак не выдавая своего присутствия, до тех пор, пока не будет обнаружен антивирусными средствами.

Способы проникновения

Задачу проникновения на компьютер пользователя **трояны** решают обычно одним из двух следующих методов.

Трояны

Маскировка — ***троян*** выдает себя за полезное приложение, которое пользователь самостоятельно загружает из Интернет и запускает. Иногда пользователь исключается из этого процесса за счет размещения на Web-странице специального скрипта, который используя дыры в браузере автоматически инициирует загрузку и запуск **трояна**.

Кооперация с вирусами и червями — ***троян*** путешествует вместе с **червями** или, реже, с **вирусами**. В принципе, такие пары **червь-*троян*** можно рассматривать целиком как составного **червя**, но в сложившейся практике принято **троянскую** составляющую **червей**, если она реализована отдельным файлом, считать независимым **трояном** с собственным именем. Кроме того, **троянская** составляющая может попадать на компьютер позже, чем файл **червя**.

Активация – здесь приемы те же, что и у **червей**: ожидание запуска файла пользователем, либо использование уязвимостей для автоматического запуска.

Кто и почему создает вредоносные программы?

Основная масса вирусов и троянских программ в прошлом создавалась студентами и школьниками, которые только что изучили язык программирования, хотели попробовать свои силы, но не смогли найти для них более достойного применения. Отраден тот факт, что значительная часть подобных вирусов их авторами не распространялась и вирусы через некоторое время умирали сами вместе с дисками, на которых хранились. Такие вирусы писались и пишутся по сей день только для самоутверждения их авторов.

Вторую группу создателей вирусов также составляют молодые люди (чаще - студенты), которые еще не полностью овладели искусством программирования. Единственная причина, толкающая их на написание вирусов, это комплекс неполноценности, который компенсируется компьютерным хулиганством. Из-под пера подобных «умельцев» часто выходят вирусы крайне примитивные и с большим числом ошибок («студенческие» вирусы).

Став старше и опытнее, многие из подобных вирусописателей попадают *в* ***третью, наиболее опасную группу***, которая создает и запускает в

Кто и почему создает вредоносные программы?

мир «профессиональные» вирусы. Эти тщательно продуманные и отлаженные программы создаются профессиональными, часто очень талантливыми программистами. Такие вирусы нередко используют достаточно оригинальные алгоритмы проникновения в системные области данных, ошибки в системах безопасности операционных сред, социальный инжиниринг и прочие хитрости.

Отдельно стоит ***четвертая группа*** авторов **вирусов** — «исследователи», довольно сообразительные программисты, которые занимаются изобретением принципиально новых методов заражения, скрытия, противодействия антивирусам и т. д. Они же придумывают способы внедрения в новые операционные системы. Эти программисты пишут **вирусы** не ради собственно **вирусов**, а скорее ради исследования потенциалов «компьютерной фауны». Часто авторы подобных **вирусов** не распространяют свои творения, однако активно пропагандируют свои идеи через многочисленные интернет-ресурсы, посвященные созданию **вирусов**.

Интернет ресурс использованный при составлении презентации

- http://www.intuit.ru/studies/courses/1042/154/lecture/4275
- http://www.vr-online.ru/node?page=76
- http://www.2admina.net/tag/сетевой червь
- http://hd-pictures.ru/1280x800/компьютерный вирус/
- http://kachai-ca4ai.narod.ru/index/0 4
- http://albas.ru/page/
- (Словарь прикладной интернетики / Нехаев С.А., Кривошеин Н.В., Андреев И.Л., Яскевич Я.С.)

ВСЕМ ПОКА – ПОКА – ПОКА