КОМПЬЮТЕРНЫЕ ВИРУСЫ

Содержание

Выполнила: ученица 9 класса «Г»
Пулатова Камила

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.[1] 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

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 , в общем случае обрабатывающем обычные данные. Вирусы стали распространяться посредством внедрения в последовательности данных использующего уязвимости программного обеспечения.

Ныне существует немало разновидностей вирусов, различающихся по способу распространения и функциональности. Если изначально вирусы распространялись на дискетах и других носителях, то сейчас доминируют вирусы, распространяющиеся через Интернет. Растёт и функциональность вирусов, которую они перенимают от других видов программ: руткитов, бэкдоров (создают «чёрный ход» в систему), кейлоггеров (регистрация активности пользователей), программ-шпионов (крадут пароли от банковских счётов и номера кредитных карт), ботнетов (превращают заражённые компьютеры в станции по рассылке спама или в часть компьютерных сетей, занимающихся спамом, DoS-атаками и прочей противоправной активностью).

Создание и распространение компьютерных вирусов и вредоносных программ преследуется в России согласно Уголовному Кодексу РФ (глава 28, статья 273).

Согласно доктрине информационной безопасности РФ, в России должен проводиться правовой ликбез в школах и вузах при обучении информатике и компьютерной грамотности по вопросам защиты информации в ЭВМ, борьбы с компьютерными вирусами, детскими порносайтами и обеспечению информационной безопасности в сетях

Происхождение термина

Компьютерный вирус был назван по аналогии с биологическими вирусами. По всей видимости, впервые слово вирус по отношению к программе было употреблено Грегори Бенфордом (Gregory Benford) в фантастическом рассказе «Человек в шрамах»[2], опубликованном в журнале Venture в мае 1970 года.

Термин «компьютерный вирус» впоследствии не раз открывался и переоткрывался — так, переменная в программе PERVADE (1975), от значения которой зависело, будет ли программа ANIMAL распространяться по диску, называлась VIRUS. Также, вирусом назвал свои программы Джо Деллинджер (англ. *Joe Dellinger*), и, вероятно, — это и был первый вирус, названный собственно «вирусом».

Классификация

В настоящее время не существует единой системы классификации и именования вирусов (хотя попытка создать стандарт была предпринята на встрече CARO в 1991 году). Принято разделять вирусы по поражаемым объектам (файловые вирусы, загрузочные вирусы, скриптовые вирусы, макро-вирусы, сетевые черви), по поражаемым операционным системам и платформам (DOS, Microsoft Windows, Unix, Linux), по технологиям, используемым вирусом (полиморфные вирусы, стелс-вирусы), по языку, на котором написан вирус (ассемблер, высокоуровневый язык программирования, скриптовый язык и др.).

Макро-вирусы

(Macro viruses) являются программами на языках (макро-языках), встроенных во многие системы обработки данных (текстовые редакторы, электронные таблицы и т. д.). Для своего размножения такие вирусы используют возможности макро-языков и при их помощи переносят себя из одного зараженного файла (документа или таблицы) в другие. Наибольшее распространение получили макро-вирусы для Microsoft Word, Excel и Office97. Существуют также макро-вирусы, заражающие документы Ami Pro и базы данных Microsoft Access.

Классификация файловых вирусов по способу заражения

По способу заражения файловые вирусы (вирусы, внедряющие свой код в исполняемые файлы: командные файлы, программы, драйверы, исходный код программ и др.) разделяют на перезаписывающие, паразитические, вирусы-звенья, вирусы-черви, компаньон-вирусы, а так же вирусы, поражающие исходные тексты программ и компоненты программного обеспечения (VCL, LIB и др.).

Перезаписывающие вирусы

Вирусы данного типа записывают своё тело вместо кода программы, не изменяя названия исполняемого файла, вследствие чего исходная программа перестаёт запускаться. При запуске программы выполняется код вируса, а не сама программа.

Вирусы-компаньоны

Компаньон-вирусы, как и перезаписывающие вирусы, создают свою копию на месте заражаемой программы, но в отличие от перезаписываемых не уничтожают оригинальный файл, а переименовывают или перемещают его. При запуске программы вначале выполняется код вируса, а затем управление передаётся оригинальной программе.

Возможно существование и других типов вирусов-компаньонов, использующих иные оригинальные идеи или особенности других операционных систем. Например, PATH-компаньоны, которые размещают свои копии в основном каталоге Windows, используя тот факт, что этот каталог является первым в списке PATH, и файлы для запуска Windows, в первую очередь, будет искать именно в нём. Данными способом самозапуска пользуются также многие компьютерные черви и троянские программы.

ФАЙЛОВЫЕ ЧЕРВИ

ФАЙЛОВЫЕ ЧЕРВИ СОЗДАЮТ СОБСТВЕННЫЕ КОПИИ С ПРИВЛЕКАТЕЛЬНЫМИ ДЛЯ ПОЛЬЗОВАТЕЛЯ НАЗВАНИЯМИ (НАПРИМЕР, GAME.EXE, INSTALL.EXE И ДР.) В НАДЕЖДЕ НА ТО, ЧТО ПОЛЬЗОВАТЕЛЬ ИХ ЗАПУСТИТ.

ВИРУСЫ-ЗВЕНЬЯ

КАК И КОМПАНЬОН-ВИРУСЫ, НЕ ИЗМЕНЯЮТ КОД ПРОГРАММЫ, А ЗАСТАВЛЯЮТ ОПЕРАЦИОННУЮ СИСТЕМУ ВЫПОЛНИТЬ СОБСТВЕННЫЙ КОД, ИЗМЕНЯЯ АДРЕС МЕСТОПОЛОЖЕНИЯ НА ДИСКЕ ЗАРАЖЁННОЙ ПРОГРАММЫ НА СОБСТВЕННЫЙ АДРЕС. ПОСЛЕ ВЫПОЛНЕНИЯ КОДА ВИРУСА УПРАВЛЕНИЕ ОБЫЧНО ПЕРЕДАЁТСЯ ВЫЗЫВАЕМОЙ ПОЛЬЗОВАТЕЛЕМ ПРОГРАММЕ.

Паразитические вирусы

Паразитические вирусы — это файловые вирусы, изменяющие содержимое файла, добавляя в него свой код. При этом заражённая программа сохраняет полную или частичную работоспособность. Код может внедряться в начало, середину или конец программы. Код вируса выполняется перед, после или вместе с программой, в зависимости от места внедрения вируса в программу.

Вирусы, поражающие исходный код программ

Вирусы данного типа поражают исходный код программы или её компоненты (.OBJ, .LIB, .DCU), а также VCL и ActiveX-компоненты. После компиляции программы

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 на многих современных компьютерах.

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 ранее было преимущественно обусловлено возможностью создания на накопителе специального файла autorun.inf, в котором можно указать программу, запускаемую Проводником Windows при открытии такого накопителя. В последней версии MS Windows под торговым названием Windows 7 возможность автозапуска файлов с переносных носителей была устранена. Флешки — основной источник заражения для компьютеров, не подключённых к Интернету.

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. В некоторых письмах могут содержаться действительно только ссылки, то есть в самих письмах может и не быть вредоносного кода, но если открыть такую ссылку, то можно попасть на специально созданный веб-сайт, содержащий вирусный код. Многие почтовые вирусы, попав на компьютер пользователя, затем используют адресную книгу из установленных почтовых клиентов типа Outlook для рассылки самого себя дальше.

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 Интернета ввиду наличия на страницах всемирной паутины различного «активного» содержимого: скриптов, ActiveX-компонент. В этом случае используются уязвимости программного обеспечения, установленного на компьютере пользователя, либо уязвимости в ПО владельца сайта (что опаснее, так как заражению подвергаются добропорядочные сайты с большим потоком посетителей), а ничего не подозревающие пользователи зайдя на такой сайт рискуют заразить свой компьютер.

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. Уязвимости — это ошибки и недоработки в программном обеспечении, которые позволяют удаленно загрузить и выполнить машинный код, в результате чего вирус-червь попадает в операционную системы и, как правило, начинает действия по заражению других компьютеров через локальную сеть или Интернет. Злоумышленники используют заражённые компьютеры пользователей для рассылки спама или для DDoS-атак.

Экономика

Некоторые производители антивирусов утверждают, что сейчас создание вирусов превратилось из одиночного хулиганского занятия в серьёзный бизнес, имеющий тесные связи с бизнесом спама и другими видами противозаконной деятельности.[9]

Также называются миллионные и даже миллиардные суммы ущерба от действий вирусов и червей.[10] К подобным утверждениям и оценкам следует относиться осторожно — суммы ущерба по оценкам различных аналитиков различаются (иногда на три-четыре порядка), а методики

История

Первые самовоспроизводящиеся программы

Основы теории самовоспроизводящихся механизмов заложил американец венгерского происхождения Джон фон Нейман, который в 1951 году предложил метод создания таких механизмов. Первой публикацией, посвящённой созданию самовоспроизводящихся систем, является статья Л. С. Пенроуз в соавторстве со своим мужем, нобелевским лауреатом по физике Р. Пенроузом, о самовоспроизводящихся механических структурах, опубликованная в 1957 году американским журналом Nature.[11] В этой статье, наряду с примерами чисто механических конструкций, была приведена некая двумерная модель подобных структур, способных к активации, захвату и освобождению. По материалам этой статьи Ф. Ж. Шталь (F. G. Stahl) запрограммировал на машинном языке ЭВМ IBM 650 биокибернетическую модель, в которой существа двигались, питаясь ненулевыми словами. При поедании некоторого числа символов существо размножалось, причём дочерние механизмы могли мутировать. Если кибернетическое существо двигалось определённое время без питания, оно погибало. В 1961 году В. А. Высотский, Х. Д. Макилрой (H. D. McIlroy) и Роберт Моррис (Robert Morris) из фирмы Bell Telephone Laboratories (США) изобрели необычную игру «Дарвин», в которой несколько ассемблерных программ, названных «организмами», загружались в память компьютера

. Организмы, созданные одним игроком (то есть принадлежащие к одному виду), должны были уничтожать представителей другого вида и захватывать жизненное пространство. Победителем считался тот игрок, чьи организмы захватывали всю память или набирали наибольшее количество очков.

Появление первых вирусов

Появление первых компьютерных вирусов зачастую ошибочно относят к 1970-м и даже 1960-м годам. Обычно упоминаются как «вирусы» такие программы, как Animal, Creeper, Cookie Monster и Xerox worm.

Юрген Краус

В феврале 1980 года студент Дортмундского университета Юрген Краус подготовил дипломную работу по теме «Самовоспроизводящиеся программы»[13], в которой помимо теории приводились так же и листинги строго самовоспроизводящихся программ (которые вирусами на самом деле не являются) для компьютера Siemens. Вполне очевидно, что все описанные примеры не являются компьютерными вирусами в строгом смысле, и хотя они и оказали существенное влияние на последующие исследования, первыми известными вирусами являются Virus 1,2,3 и Elk Cloner для ПК Apple II. Оба вируса очень схожи по функциональности и появились независимо друг от друга, с небольшим промежутком во времени, в 1981 году.

Первые вирусы

С появлением первых персональных компьютеров Apple в 1977 году и развитием сетевой инфраструктуры начинается новая эпоха истории вирусов. Появились первые программы-вандалы, которые под видом полезных программ выкладывались на BBS, однако после запуска уничтожали данные пользователей. В это же время появляются троянские программы-вандалы, проявляющие свою деструктивную сущность лишь через некоторое время или при определённых условиях.

ELK CLONER

В 1981 году Ричард Скрента написал один из первых загрузочных вирусов для ПЭВМ Apple II — ELK CLONER. Он обнаруживал своё присутствие сообщением, содержащим небольшое стихотворение

Первые антивирусы

Первые антивирусные утилиты появились зимой 1984 года. Анди Хопкинс (англ. *Andy Hopkins*) написал программы CHK4BOMB и BOMBSQAD. CHK4BOMB позволяла проанализировать текст загрузочного модуля и выявляла все текстовые сообщения и «подозрительные» участки кода (команды прямой записи на диск и др.). Благодаря своей простоте (фактически использовался только контекстный поиск) и эффективности CHK4BOMB получила значительную популярность. Программа BOMBSQAD.COM перехватывает операции записи и форматирования, выполняемые через BIOS. При выявлении запрещённой операции можно разрешить её выполнение.

[править] Первый резидентный антивирус

В начале 1985 года Ги Вонг (англ. *Gee Wong*) написал программу DPROTECT — резидентную программу, перехватывающую попытки записи на дискеты и винчестер. Она блокировала все операции (запись, форматирование), выполняемые через BIOS. В случае выявления такой операции программа требовала рестарта системы.

Первые вирусные эпидемии

Очередным этапом развития вирусов считается 1987 год. К этому моменту получили широкое распространения сравнительно дешёвые компьютеры IBM PC, что привело к резкому увеличению масштаба заражения компьютерными вирусами. Именно в 1987 вспыхнули сразу три крупные эпидемии компьютерных вирусов.

Brain и другие

Первая эпидемия 1987 года была вызвана вирусом Brain (также известен как Пакистанский вирус), который был разработан братьями Амджатом и Базитом Алви (Amdjat и Basit Faroog Alvi) в 1986 и был обнаружен летом 1987. По данным McAfee, вирус заразил только в США более 18 тысяч компьютеров. Программа должна была наказать местных пиратов, ворующих программное обеспечение у их фирмы. В программке значились имена, адрес и телефоны братьев. Однако неожиданно для всех The Brain вышел за границы Пакистана и заразил сотни компьютеров по всему миру. Вирус Brain являлся также и первым стелс-вирусом — при попытке чтения заражённого сектора он «подставлял» его незаражённый оригинал.

Вторая эпидемия, берущая начало в Лехайском университете (США), разразилась в ноябре. В течение нескольких дней этот вирус уничтожил содержимое нескольких сот дискет из библиотеки вычислительного центра университета и личных дискет студентов. За время эпидемии вирусом было заражено около четырёх тысяч компьютеров.

Последняя вирусная эпидемия разразилась перед самым Новым годом, 30 декабря. Её вызвал вирус, обнаруженный в Иерусалимском Университете (Израиль). Хотя существенного вреда этот вирус не принёс, он быстро распространился по всему миру.

В пятницу 13 мая 1988 сразу несколько фирм и университетов нескольких стран мира «познакомились» с вирусом Jerusalem — в этот день вирус уничтожал файлы при их запуске. Это, пожалуй, один из первых MS-DOS-вирусов, ставший причиной настоящей