Компьютерные вирусы

Выполнили:
Жданова Екатерина
Верхотурцева Юлия
Студентки 221 группы

Компьютерный вирус

Компью́терные ви́русы — разновидность самовоспроизводящихся компьютерных программ, которые распространяются, внедряя себя в исполняемый код других программ или в документы специального формата, содержащие макрокоманды, например такие, как MS Word и Excel.

В общем словоупотреблении к компьютерными вирусами причисляют все вредоносные программы, такие как сетевые и файловые черви, троянские кони, программы-шпионы.

Этимология названия

Компьютерный вирус был назван по аналогии с биологическими вирусами за сходный механизм распространения. По-видимому, впервые слово «вирус» по отношению к программе было употреблено Грегори Бенфордом (Gregory Benford) в фантастическом рассказе «Человек в шрамах» опубликованном в журнале Venture в мае 1970 года.

- Термин «компьютерный вирус» впоследствии не раз «открывался» и переоткрывался. Так, переменная в подпрограмме PERVADE (1975), от значения которой зависело, будет ли программа ANIMAL распространяться по диску, называлась VIRUS. Также, вирусом назвал свои программы Джо Деллинджер и, вероятно, это и было то, что впервые было правильно обозначено как вирус.

Распространение

Через интернет, локальные сети и съемные носители.

Механизм

Вирусы распространяются, копируя своё тело и обеспечивая его последующее исполнение: внедряя себя в исполняемый код других программ, заменяя собой другие программы, прописываясь в автозапуск и другое. Вирусом или его носителем могут быть не только программы, содержащие машинный код, но и любая информация, содержащая автоматически исполняемые команды — например, пакетные файлы и документы Microsoft Word и Excel, содержащие макросы. Кроме того, для проникновения на компьютер вирус может использовать уязвимости в популярном программном обеспечении (например, Adobe Flash, Internet Explorer, Outlook), для чего распространители внедряют его в обычные данные (картинки, тексты и т. д.) вместе с эксплоитом, использующим уязвимость.

ПЕРВЫЙ КОМПЬЮТЕРНЫЙ ВИРУС

- Вирус который орудует в системе, это в первую очередь программа, которая способна к самовоспроизведению. Причём данная способность присущая практически всем типам вирусов. Вирус не может существовать в «полной изоляции» сам по себе. Вряд ли можно представить себе вирус, который не использует информацию о структуре файлов, код программ или просто действует под именем другой программы.
- Несмотря на распространённость таких понятий, как антивирусная защита, мало кто задумывался над тем, кем и когда был создан первый компьютерный вирус и к чему привели последствия его создания.

Первый компьютерный вирус

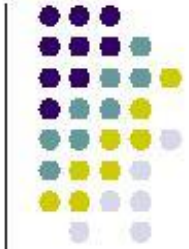
- Наверное, практически у каждого пользователя компьютера установлена антивирусная программа, и почти каждый хоть раз да слышал от нее тревожный сигнал: "Внимание! Обнаружена угроза!", но далеко не все знают, с чего это все началось.
- Впервые человечество столкнулось с тем, что позже назовут "вирусом", в 1972 году. Именно тогда, 19 апреля, в США, рухнули компьютерные сети, входившие в состав "Эйрпанет". Остановилась передача важной информации, выходили из строя компьютеры, ситуация затронула сотни тысячей пользователей и принесла миллионы долларов убытка. Что же послужило причиной?

- Причиной был всего лишь неудачный розыгрыш. Шутка. Студент-практикант, решив удивить и разыграть коллег, написал маленькую программу, в задачи которой входило самовоспроизводиться и передавать себя из компьютера в компьютер. Он, вероятно, и не предполагал, насколько велика будет скорость, с которой его детище начнет копировать себя, а главное не рассчитывал на то, что эта же программа начнет стремительно уничтожать данные в других компьютерах. Именно из-за скорости распространения вредоносной программы кто-то сравнил происходящее с эпидемией, а саму программу с вирусом. С тех пор и пошло это название.

- Как звали автора той программы, теперь уже никто не знает, но с последствиями его шутки, мы сталкиваемся до сих пор. Сбои компьютерных сетей могут приводить к серьезным проблемам и даже человеческим жертвам, как в случае поражения группой хакеров американских сетей, контролирующих электронные сигнальные системы. В результате этого поражения перестало работать значительное количество светофоров и произошло много автомобильных аварий.
- Написание вирусов превратилось в бизнес, как и создание антивирусных программ. Крупные корпорации, заботясь о сохранности своих данных, наряду с другими специалистами, специально нанимают хакеров для проверки надежности своей защиты. Написание программ-антивирусов стало огромной мощной отраслью, приносящей гигантскую прибыль. Вот что произошло после толчка, который устроил первый компьютерный вирус.

- Ежедневно и ежеминутно в сети появляются новые вирусы и пишутся обновления для антивирусов. И пока это приносит прибыль, ситуация не изменится. Большая часть пользователей компьютеров со всего земного шара будет, включая компьютер, созерцать обновление антивирусной системы, и время от времени слышать: "Внимание! Обнаружена вирусная угроза!

Классификация вирусов



Принято разделять вирусы по поражаемым объектам :

- файловые вирусы
- загрузочные вирусы
- скриптовые вирусы
- сетевые черви

По поражаемым операционным системам и платформам

- DOS
- Windows
- Unix
- Linux
- Java и другие

Классификация вирусов

По способу заражения файловые вирусы (вирусы, внедряющие свой код в исполняемые файлы: командные файлы, программы, драйверы, исходный код программ и др.)разделяют на

1. перезаписывающие
2. паразитические
3. вирусы-звенья
4. вирусы-черви
5. компаньон-вирусы
6. вирусы, поражающие исходные тексты программ и компоненты программного обеспечения (VCL, LIB и др.).

Перезаписывающие вирусы и Вирусы-звенья

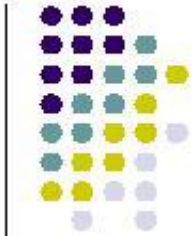
- Перезаписывающие вирусы

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

- Вирусы-звенья

  Как и компаньон-вирусы, не изменяют код программы, а заставляют операционную систему выполнить собственный код, изменяя адрес местоположения на диске зараженной программы, на собственный адрес. После выполнения кода вируса управление обычно передается вызываемой пользователем программе.

Вирусы-компаньоны и Файловые черви

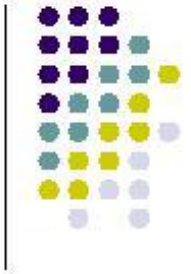


- Вирусы-компаньоны

  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 передается оригинальной программе.
- 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.

Паразитические вирусы и вирусы, поражающие исходный код программ



- Паразитические вирусы

  Паразитические вирусы — это файловые вирусы изменяющие содержимое файла добавляя в него свой код. При этом зараженная 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 или исходный код программы, либо её компоненты (OBJ-, LIB-, DCU- файлы) а так же VCL и ActiveX компоненты. После компиляции программы оказываются в неё встроенными. В настоящее время широкого распространения не получили.

Профилактика и лечение

- Не работать под привилегированными учётными записями без крайней необходимости. (Учётная запись администратора в Windows)
  Не запускать незнакомые программы из сомнительных источников.
  Стараться блокировать возможность несанкционированного изменения системных файлов.
  Отключать потенциально опасную функциональность системы (например, autorun-носителей в MS Windows, сокрытие файлов, их расширений и пр.).
  Не заходить на подозрительные сайты, обращать внимание на адрес в адресной строке обозревателя.
  Пользоваться только доверенными дистрибутивами.
  Постоянно делать резервные копии важных данных, желательно на носители, которые не стираются (например, BD-R) и иметь образ системы со всеми настройками для быстрого развёртывания.

Антивирусная программа

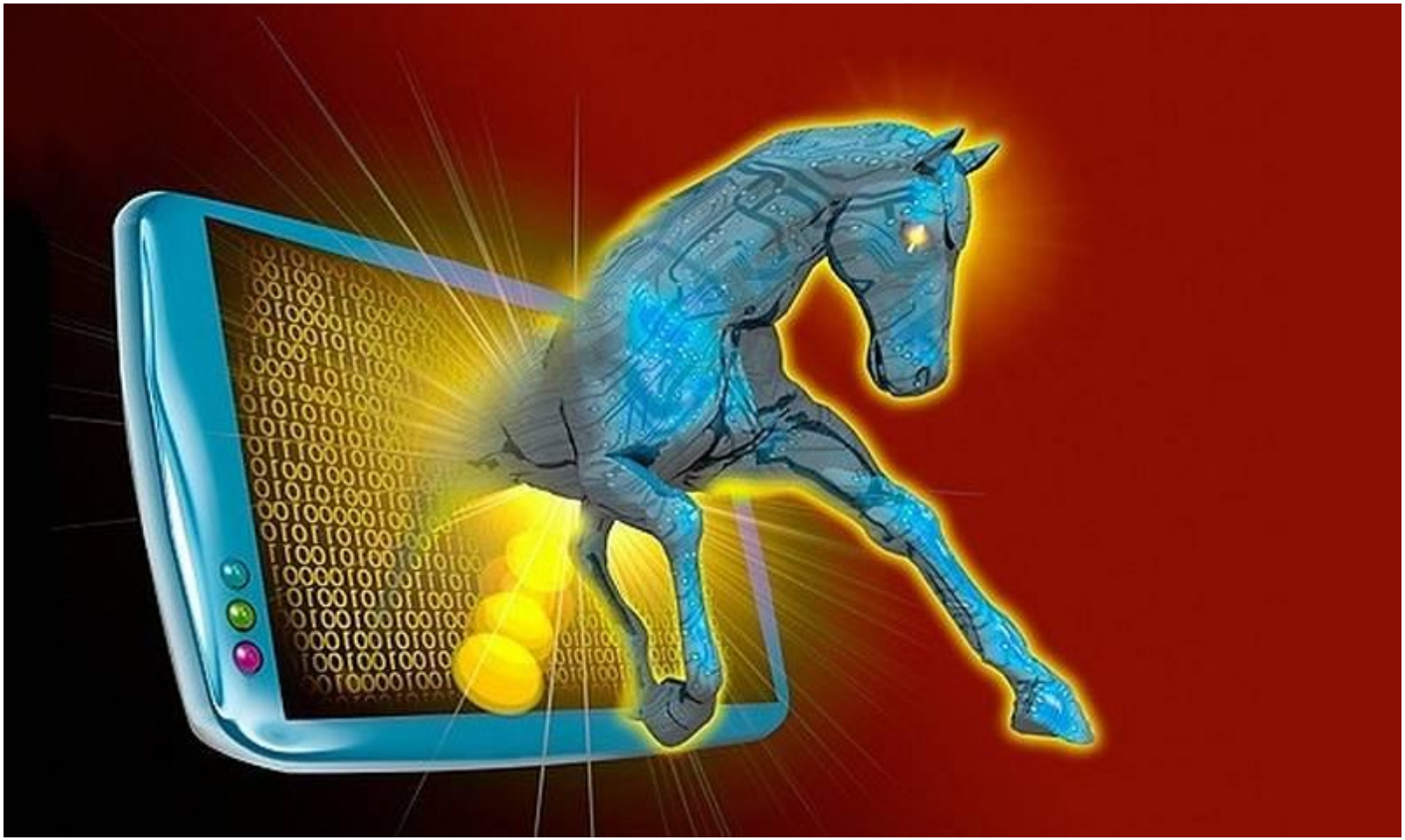
Антивирусная программа (антивирус) — программа для обнаружения и лечения программ, заражённых компьютерным вирусом, а также для предотвращения заражения файла вирусом (например, с помощью вакцинации).

Антивирусное программное обеспечение состоит из компьютерных программ, которые пытаются обнаружить, предотвратить размножение и удалить компьютерные вирусы и другие вредоносные программы.

Первые наиболее простые антивирусные программы появились почти сразу после появления вирусов. Сейчас разработкой антивирусов занимаются крупные компании. Как и у создателей вирусов, в этой сфере также сформировались оригинальные приёмы — но уже для поиска и борьбы с вирусами. Современные антивирусные программы могут обнаруживать десятки тысяч вирусов.

К сожалению, конкуренция между антивирусными компаниями привела к тому, что развитие идёт в сторону увеличения количества обнаруживаемых вирусов (прежде всего для рекламы), а не в сторону улучшения их детектирования (идеал — 100%-е детектирование) и алгоритмов лечения заражённых файлов.

Вирус троян



ВИРУС ТРОЯН

- Вирус троян – это обычный файл или программа, которые выглядят весьма безобидно до тех пор, пока их не активируют. Несмотря на относительно недавнее его появление, троян успешно упрочнился в современном компьютерном мире и представляет собой достаточно серьёзную угрозу безопасности. Далее мы более подробно расскажем, что такое троян, опишем некоторые из его видов и напомним, как с ним можно бороться.

Описание

- Многие из Вас наверняка слышали о таком понятии как вирус trojan, но не совсем представляют себе, что это такое. Можно сказать, что название это поистине историческое, которое берет начало ещё с семнадцатого столетия до нашей эры: с событий в легендарной Трое. Вы помните, что Троя была взята хитростью с использованием коня, в котором скрывались воины. Примерно по такому же принципу действует и вредоносная программа: внешне безопасное приложение таит в себе скрытые враждебные функции.
- Данный зловред представляет собой вредоносное ПО, при активации которого управление компьютером может переходить в руки злоумышленников. Без ведома владельца может быть получен доступ к его персональным данным, либо осуществляться слежение за действиями пользователя.
- Не совсем правы те пользователи, которые относят trojan к категории компьютерных вирусов. Это не совсем верно, поскольку действия именно этой программы являются целенаправленными. Чаще для кражи личной информации. К тому же в нём отсутствует механизм

Как избежать заражения

- Благодаря всевозможным ухищрениям данный вирус может попасть в систему, но одно Вы должны помнить наверняка: у трояна отсутствует механизм самокопирования! Поэтому, если Вы не активизируете файл, в котором он находится, вряд ли удастся причинить вред Вашему компьютеру. Очень важно на сегодняшний день проверять неизвестные файлы, не загружать сомнительное программное обеспечение из Интернета и не запускать программы с непроверенного flash накопителя.

Основные разновидности

- Приведем несколько наиболее распространенных видов данной программы, которые существуют на сегодняшний день:
- «Клавишные трояны» ведут запись абсолютно всего, что Вы набираете на клавиатуре, после чего успешно передают информацию злоумышленнику по почте;
- «Почтовики-трояны» передают всю информацию о Вашем компьютере по e-mail;
- «Трояны-насмешки» фактически не причиняют вреда Вашему компьютеру, только периодически отображают различные нудные всплывающие окна. Большинство этих окон подобны системным сообщениям, в которых содержатся предупреждения о необходимости установки той или иной программы;
- «Скрытые утилиты удалённого руководства» - фактически предоставляют возможность злоумышленнику удалённо управлять компьютером без Вашего ведома

ВИРУСЫ ШПИОНЫ!

- Шпионы не только вредят безопасности вашей информации, но также заметно снижают скорость Вашего компьютера. Когда Вы загружаете один из пакетов программ со шпионами, то эта программа автоматически устанавливается на вашем компьютере вне зависимости от вашего желания. Иногда, при инсталляции шпион просит Вас установить программное обеспечение спонсора. При установке шпионская программа стремиться установиться в системный реестр вашего компьютера и находится в нём до тех пор, пока вы полностью не удалите её оттуда.

- Шпион, пожирая потенциал компьютера, снижает работоспособность центрального процессора и памяти. В результате этого, ваш ПК снижает скорость работы или даже совсем перестает отвечать на запросы. Шпион не исчезнет сам по себе, а только будет вызывать все большую задержку, потому что Spyware продолжит собирать сведения Вашего компьютера. Существует три основных способа разрушения вашей системы программами- шпионами:

- 1. Есть шпионы, которые постоянно отслеживают все ваши покупки. Если вы используете свою кредитную карту, Вы можете в итоге не досчитаться своих финансов, программа - шпион узнает номер вашей кредитной карты, и даст возможность использовать её для покупок другими людьми. Вы можете об этом не узнать, пока не обнаружите нехватку денег.

  2. Хакеры (те, кто за кулисами) смогут получить доступ к вашему компьютеру и информации о нём. Они смогут узнать, какие клавиши вы используете в режиме реального времени, проникнуть в ваш компьютер, изменить настройки браузера, инсталлировать свои программы без вашего согласия. Кроме того, шпионы также могут собирать информацию об электронных адресах, паролях и даже номерах кредитных карт. Но эту проблему можно решить, но только просмотрите и внимательно изучите все имеющиеся программы по удалению шпионов, отзывы к ним, потому что некоторые из них могут причинить больше вреда, чем пользы.

  3. Программы - шпионы могут находить информацию о ваших адресах электронной почты. Если это произойдет, то вы столкнетесь с множеством проблем, одна из которых, Вас просто завалят рекламными письмами

- Если даже Вы простой пользователь, есть несколько способов, которые Вы можете легко сделать, чтобы быстро и надёжно увеличить скорость работы Вашего компьютера. Первый и самый доступный метод, который Вы должны обязательно сделать, заключается в дефрагментации дисков. "Мастер дефрагментации" на Вашем компьютере поможет её провести. Вы, возможно, хотели бы сделать это быстро, однако, это может занять много времени. Процесс не следует прерывать. При регулярной работе уже на следующую проверку уйдет меньше времени.

- Второй путь заключается в установке и применению хорошей программы по уничтожению программ-шпионов. Например, хорошо разбирается с ними Spyware Doctor.
  Далее можно программно в браузерах снизить период сохранения посещаемых страниц, если Вам это не нужно с одного месяца, как стоит по умолчанию до 1-2-х дней или на удаление их сразу после выхода со странички сайта.
  Когда Вы деактивируете свой рабочий стол, станет меньше нагрузка на оперативную память. А разницы в дизайне и работе не почувствуете.
  Убедитесь, что у Вас стоит хорошая антивирусная программа, используйте её постоянно. Если Вы удаляете вирусы и препятствуете их распространению, то этим Вы заметно ускоряете работу компьютера.
  Как только выполните эти простые правила, Вы будете поражены, насколько быстрее заработал компьютер, и сколько места на диске освободилось.

Заключение

Вирусы разных типов вредят данным на зараженных компьютерах, повреждают или стирают информацию. Приводят к неисправной работе программного обеспечения.Для защиты от вирусов существуют специальные программы – антивирусы. Они помогут вам обезопасить данные от повреждений.

Библиографический список

- http://www.itsmonline.ru/security/viruses/
- comodo.com
- www.avira.com
- www.esetnod32.ru/
- free.avg.com/
- www.drweb.com/
- www.kaspersky.ru/