Введение

Массовое применение персональных компьютеров, оказалось связанным с появлением самовоспроизводящихся программ-вирусов, препятствующих нормальной работе компьютера, разрушающих файловую структуру дисков и наносящих ущерб хранимой в компьютере информации.

На сегодняшний день известны десятки тысяч различных компьютерных вирусов. Несмотря на такое изобилие число типов вирусов, отличающихся друг от друга механизмом распространения и принципом действия, достаточно ограничено. Существуют и комбинированные вирусы, которые можно отнести одновременно к нескольким типам.

Несмотря на разработку специальных программных средств защиты от вирусов, количество новых программных вирусов постоянно растет. Это требует от пользователя персонального компьютера знаний о природе вирусов, способах заражения вирусами и защиты от них.

1. Компьютерные вирусы, их свойства и классификация

1.1 Свойства компьютерных вирусов

Сейчас применяются персональные компьютеры, в которых пользователь имеет свободный доступ ко всем ресурсам машины. Именно это открыло возможность для опасности, которая получила название компьютерного вируса. Что такое компьютерный вирус? Формальное определение этого понятия до сих пор не придумано, и есть серьезные сомнения, что оно вообще может быть дано. Но для конкретизации приведем определение, данное в толковом словаре по информатике.

Компьютерные вирусы - это класс программ способных к саморазмножению и самомодификации в работающей вычислительной среде и вызывающих нежелательные для пользователей действия. Действия могут выражаться в нарушении работы программ, выводе на экран посторонних сообщений или изображений, порче записей, файлов, дисков, замедлении работы ЭВМ и др.

Вирус - программа, обладающая способностью к самовоспроизведению. Такая способность является единственным средством, присущим всем типам вирусов. Но не только вирусы способны к самовоспроизведению. Любая операционная система и еще множество программ способны создавать собственные копии. Копии же вируса не только не обязаны полностью совпадать с оригиналом, но, и могут вообще с ним не совпадать! Вирус не может существовать в "полной изоляции": сегодня нельзя представить себе вирус, который не использует код других программ, информацию о файловой структуре или даже просто имена других программ. Причина понятна: вирус должен каким-нибудь способом обеспечить передачу себе управления.

1.2 Классификация компьютерных вирусов.

Вирусы можно разделить на классы по следующим основным признакам:

- среда обитания;
- операционная система;
- особенности алгоритма работы;
- деструктивные возможности.

По среде обитания вирусы можно разделить на:

- файловые;
- загрузочные;
- макро;
- сетевые.
- Файловые вирусы заражают выполняемые файлы (это наиболее распространенный тип вирусов), либо создают файлы-двойники (компаньон-вирусы), либо используют особенности организации файловой системы (link-вирусы).
- Загрузочные вирусы заражают загрузочные сектора дисков (boot-сектор), либо главную загрузочную запись (Master Boot Record), либо меняют указатель на активный boot-сектор.
- Макровирусы - разновидность файловых вирусов встраивающиеся в документы и электронные таблицы популярных редакторов.
- Сетевые вирусы используют для своего распространения протоколы или команды компьютерных сетей и электронной почты.

Существует большое количество сочетаний - например, файлово-загрузочные вирусы, заражающие как файлы, так и загрузочные сектора дисков. Такие вирусы,

как правило, имеют довольно сложный алгоритм работы, часто применяют оригинальные методы проникновения в систему. Другой пример такого сочетания - сетевой макровирус, который не только заражает редактируемые документы, но и рассылает свои копии по электронной почте.

Заражаемая операционная система (вернее, ОС, объекты которой подвержены заражению) является вторым уровнем деления вирусов на классы. Каждый файловый или сетевой вирус заражает файлы какой-либо одной или нескольких ОС.

Макро-вирусы заражают файлы форматов Word, Excel, Office16. Загрузочные вирусы также ориентированы на конкретные форматы расположения системных данных в загрузочных секторах дисков.

Среди особенностей алгоритма работы вирусов выделяются следующие пункты:

- резидентность;
- использование стелс-алгоритмов;
- самошифрование и полиморфичность;
- использование нестандартных приемов.
- Резидентный вирус при инфицировании компьютера оставляет в оперативной памяти свою резидентную часть, которая затем перехватывает обращения операционной системы к объектам заражения и внедряется в них. Резидентные вирусы находятся в памяти и являются активными вплоть до выключения компьютера или перезагрузки операционной системы. Нерезидентные вирусы не заражают память компьютера и сохраняют активность ограниченное время.
- Использование стелс - алгоритмов позволяет вирусам полностью или частично скрыть себя в системе. Наиболее распространенным стелс -алгоритмом является перехват запросов ОС на чтение/запись зараженных объектов. Стелс-вирусы при этом либо временно лечат их, либо «подставляют» вместо себя незараженные участки информации. В случае макро-вирусов наиболее популярный способ -- запрет вызовов меню просмотра макросов.
- Самошифрование и полиморфичность используются практически всеми типами вирусов для того, чтобы максимально усложнить процедуру детектирования вируса. Полиморфик - вирусы (polymorphic) - это достаточно трудно обнаружимые вирусы, не имеющие сигнатур, т.е. не содержащие ни одного постоянного участка кода. В большинстве случаев два образца одного и того же полиморфик - вируса не будут иметь ни одного совпадения. Это

достигается шифрованием основного тела вируса и модификациями программы-расшифровщика.

По деструктивным возможностям вирусы можно разделить на:

- безвредные, т.е. никак не влияющие на работу компьютера (кроме уменьшения свободной памяти на диске в результате своего распространения);
- неопасные, влияние которых ограничивается уменьшением свободной памяти на диске и графическими, звуковыми и пр. эффектами;
- опасные вирусы, которые могут привести к серьезным сбоям в работе компьютера;
- очень опасные, в алгоритм работы которых заведомо заложены процедуры, которые могут привести к потере программ, уничтожить данные, стереть необходимую для работы компьютера информацию, записанную в системных областях памяти, и даже, как гласит одна из непроверенных компьютерных легенд, способствовать быстрому износу движущихся частей механизмов - вводить в резонанс и разрушать головки некоторых типов винчестеров.

2. Пути проникновения вирусов в компьютер и механизм распределения вирусных программ. Признаки появления вирусов

2.1 Пути проникновения вирусов в компьютер и механизм распределения вирусных программ

Основными путями проникновения вирусов в компьютер являются съемные диски (гибкие и лазерные), а также компьютерные сети. Заражение жесткого диска вирусами может произойти при загрузке программы с дискеты, содержащей вирус. Такое заражение может быть и случайным, например, если дискету не вынули из дисковода А и перезагрузили компьютер, при этом дискета может быть и не системной. Заразить дискету гораздо проще. На нее вирус может попасть, даже если дискету просто вставили в дисковод зараженного компьютера и, например, прочитали ее оглавление. Вирус, как правило, внедряется в рабочую программу таким образом, чтобы при ее запуске управление сначала передалось ему и только после выполнения всех его команд снова вернулось к рабочей программе. Получив доступ к управлению, вирус прежде всего переписывает сам себя в другую рабочую программу и заражает ее. После запуска программы, содержащей вирус, становится возможным заражение других файлов. Наиболее часто вирусом заражаются загрузочный сектор диска и исполняемые файлы, имеющие

расширения EXE, COM, SYS, BAT. Крайне редко заражаются текстовые файлы. После заражения программы вирус может выполнить какую-нибудь диверсию, не слишком серьезную, чтобы не привлечь внимания. И наконец, не забывает возвратить управление той программе, из которой был запущен. Каждое выполнение зараженной программы переносит вирус в следующую. Таким образом, заразится все программное обеспечение.

2.2 Признаки появления вирусов

При заражении компьютера вирусом важно его обнаружить. Для этого следует знать об основных признаках проявления вирусов. К ним можно отнести следующие:

- медленная работа компьютера
- невозможность загрузки операционной системы
- исчезновение файлов и каталогов или искажение их содержимого
- изменение даты и времени модификации файлов
- изменение размеров файлов
- неожиданное значительное увеличение количества файлов на диске
- существенное уменьшение размера свободной оперативной памяти
- вывод на экран непредусмотренных сообщений или изображений
- подача непредусмотренных звуковых сигналов
- частые зависания и сбои в работе компьютера

Следует отметить, что вышеперечисленные явления необязательно вызываются присутствием вируса, а могут быть следствием других причин. Поэтому всегда затруднена правильная диагностика состояния компьютера.

3. Меры по защите и профилактике

Основными мерами защиты от вирусов считаются:

- резервирование (копирование FAT, ежедневное ведение архивов измененных файлов);
- Профилактика (раздельное хранение вновь полученных программ и эксплуатирующихся, хранение неиспользуемых программ в архивах, использование специального диска для записи новых программ);
- ревизия (анализ вновь полученных программ специальными средствами и их запуск в контролируемой среде, систематическая проверка BOOT-сектора используемых дискет и содержимого системных файлов (прежде всего

command.com) и др.);
- фильтрация (использование специальных сервисных программ для разбиения диска на зоны с установленным атрибутом read only,);
- вакцинация (специальная обработка файлов, дисков, каталогов, запуск специальных резидентных программ-вакцин, имитирующих сочетание условий, которые используются данным типом вируса для определения, заражена уже программа, диск, ЭВМ или нет, т.е. обманывающих вирус);
- лечение (дезактивацию конкретного вируса с помощью специальной программы или восстановление первоначального состояния программ путем удаления всех экземпляров вируса в каждом из зараженных файлов или дисков).

Наиболее важный принцип, которого следует придерживаться после обнаружения вируса и во время анализа зараженных им программ и действий по их очистке или восстановлению, состоит в следующем: все действия следует выполнять только с защищенной от записи системной дискеты и использовать антивирусные и другие программы предварительно записанные на ней.

Выполнение действий по анализу и восстановлению на зараженной операционной системе является грубой ошибкой и может иметь катастрофические последствия.

Для обнаружения, удаления и защиты от компьютерных вирусов разработано несколько видов специальных программ, которые позволяют обнаруживать и уничтожать вирусы. Такие программы называются антивирусными.

Антивирусные программы предназначены для предотвращения заражения компьютера вирусом и ликвидации последствий заражения. В зависимости от назначения и принципа действия различают следующие антивирусные программы:

- резидентные мониторы или фильтры - постоянно находятся в памяти компьютера для обнаружения попыток выполнить несанкционированные действия. В случае обнаружения подозрительного действия выводят запрос пользователю на подтверждение операций
- сторожа или детекторы - предназначены для обнаружения файлов зараженных известными вирусами, или признаков указывающих на возможность заражения.
- доктора или фаги - предназначены для обнаружения и устранения известных им вирусов, удаляя их из тела программы и возвращая ее в исходное состояние. Наиболее известными представителями являются Dr.Web, AidsTest,

Norton Anti Virus.

- ревизоры - они контролируют уязвимые и поэтому наиболее атакуемые компоненты компьютера, запоминают состояние служебных областей и файлов, а в случае обнаружения изменений сообщают пользователю.
- вакцины - имитируют заражение файлов вирусами. Вирус будет воспринимать их зараженными и не будет внедряться.

4. Использование антивирусных программ

Ни один тип антивирусных программ по отдельности не дает, к сожалению, полной защиты от вирусов. Однако совместное использование антивирусных программ дает неплохие результаты, так как они хорошо дополняют друг друга:

- Поступающие из внешних источников данные (файлы, дискеты и т.д.) проверяются программой-детектором. Если эти данные забыли проверить, и зараженная программа была запущена, ее может «поймать» программа-сторож. Правда, в обоих случаях надежно обнаруживаются лишь вирусы, известные этим антивирусным программам. Неизвестные вирусы детекторы и сторожа, не включающие в себя эвристический анализатор, не обнаруживают вовсе (пример -- программа Aidstest), а имеющие такой анализатор -- обнаруживают не более чем в 80-90% случаев;
- Сторожа могут обнаруживать даже неизвестные вирусы, если они очень нагло себя ведут, например, пытаются отформатировать жесткий диск или внести изменения в системные файлы или области диска на жестком диске. Впрочем, некоторые вирусы умеют обходить такой контроль. Более мелкие «пакости» вирусов (изменение программных файлов, запись в системные области дискет и т.д.) обычно не отслеживаются, так как эти действия выполняются не только вирусами, но и многими программами;

Как правило, программы-сторожа должны работать на компьютере постоянно, детекторы - использоваться для проверки поступающих из внешних источников данных (файлов и дискет), а ревизоры -- запускаться раз в день для выявления и анализа изменений на дисках. Поскольку функции детектора, ревизора и сторожа дополняют друг друга, то в современные антивирусные комплекты программ обычно входят компоненты, реализующие все эти функции. При этом часто функции детектора и ревизора совмещаются в одной программе.

Заключение

Компьютерный вирус - специально написанная программа, способная самопроизвольно присоединяться к другим программам, создавать свои копии и внедрять их в файлы, системные области компьютера и в вычислительные сети с целью нарушения работы программ, порчи файлов и каталогов, создания всевозможных помех в работе компьютера. В настоящее время известно более 5000 программных вирусов, число которых непрерывно растет. Основные виды вирусов: загрузочные, файловые, файлово-загрузочные. Наиболее опасный вид вирусов - полиморфные. Любая оригинальная компьютерная разработка заставляет создателей антивирусов приспосабливаться к новым технологиям, постоянно усовершенствовать антивирусные программы. Причины появления и распространения вирусов скрыты с одной стороны в психологии человека, с другой стороны - с отсутствием средств защиты у операционной системы. Основные пути проникновения вирусов - съемные диски и компьютерные сети. Для обнаружения, удаления и защиты от компьютерных вирусов разработано несколько видов специальных программ, называемых антивирусными, но ни одна из существующих антивирусных технологий не может обеспечить полной защиты от вирусов.

Список литературы

1. Технологии защиты от вирусов - Обеспечение информационной безопасности информационно-технологической инфраструктуры электронного правительства | Электронный ресурс: https://studbooks.net/2062771/informatika/tehnologii_zaschity_virusov
2. Методы и технологии защиты от вредоносных программ. Энциклопедия «Касперского». | Электронный ресурс: https://encyclopedia.kaspersky.ru/knowledge/malware-protection-methods-and-techniques/
3. НОУ ИНТУИТ | Лекция | Механизмы защиты информации | Электронный ресурс: https://intuit.ru/studies/courses/18857/1300/lecture/25505