Реферат

По теме: «Вирусология»

Предмет: Информатика

Учебное заведение: Лицей «Интеллект»

Класс: 10-В

Автор: Максим Юрьевич Михалёв

Донецк 1997

Вирус - это программа (как ни абсурдно это звучит, но некоторые до сих пор об этом не знают). И, следовательно, вредить она может лишь программно, но никак не аппаратно - страшные сказки о вирусах, убивающих и сводящих с ума пользователей при помощи вывода на экран смертельной цветовой гаммы, были и остаются всего лишь сказками. Далее - вирус является программой, способной к размножению. Мы совсем не случайно не упомянули о наносимом ущербе - существуют вирусы, которые не занимаются ничем, кроме самораспространения.

Все вирусы можно объединить в следующие основные группы.

Загрузочные вирусы - инфицируют загрузочные секторы жестких дисков и дискет.

Файловые вирусы - заражают файлы. Эта группа в свою очередь подразделяется на вирусы, инфицирующие исполняемые файлы (сом-, ехе-вирусы); файлы данных (макровирусы); вирусы-спутники, использующие имена других программ; вирусы семейства Dir, использующие информацию о файловой структуре. Причем два последних типа вообще не модифицируют файлы на диске.

Загрузочно-файловые вирусы - способны поражать как код загрузочных секторов, так и код файлов.

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.

В последнее время все большее распространение получают полиморфные вирусы, шифрующие свое тело и поэтому не имеющие неизменного набора символов, т. е. сигнатуры. Их появление поставило перед разработчиками антивирусов проблему создания совершенно нового алгоритма работы.

Stealth-вирусы фальсифицируют информацию, читаемую с диска, так, что активная программа получает неверные данные. Вирус перехватывает вектор прерывания int 13h и поставляет читающей программе ложную информацию, которая показывает, что на диске "все в порядке". Эта технология используется как в файловых, так и загрузочных вирусах.

Рeтровирусами называются обычные файловые вирусы, которые пытаются заразить антивирусные программы, уничтожая их или делая неработоспособными. Поэтому практически все антивирусы в первую очередь пверяют свои собственные размер и контрольную сумму.

Multipartition-вирусы могут поражать одновременно исполняемые файлы, boot-сектор, MBR, FAT и директории. Если они к тому же обладают пол и моренными свойствами и элементами невидимости, то становится понятно, что такие вирусы - одни из наиболее опасных.

В классификации вирусов Dr.Solomon's присутствуют также "троянские программы" (Trojans), которые производят вредоносные действия вместо объявленных легальных функций или наряду с ними. Они не способны на самораспространение и передаются только при копировании пользователем.

Интересное явление представляет собой вышедший из строя вирус - как результат порчи реального вируса либо просто плохого программирования со стороны вирусописателей. Такой вирус практически ничего не делает - или "зависает" при выполнении, или оказывается не в состоянии заражать файлы. Иногда происходит обратный процесс - вирус выполняет непредусмотренные действия, которые ведут к порче информации. Что поделаешь, среди авторов вирусов нередко встречаются слабые программисты.

Всего на сегодняшний день существуют тысячи пирусоп. нп только в нескольких десятках из них реализованы ориптппльные идеи, остальные являются лишь "вариациями на тему". Средства защиты от вирусов подразделяются на такие группы, как детекторы, фаги, ревизоры, сторожа и вакцины.

Детекторы (сканеры). Их задачей является постановка диагноза, лечением же будет заниматься другая антивирусная программа или профессиональный программист-"вирусолог".

Фаги (полифаги). Программы, способные обнаружить и уничтожить вирус (фаги) или несколько вирусов (полифаги). Современные версии полифагов, как правило, обладают возможностью проведения эвристического анализа файлов - они исследуют файлы на предмет наличия кода, характерного для вируса (внедрения части этой программы в другую, шифрования кода и т. п.).

Ревизоры. Этот тип антивирусов контролирует все (по крайней мере, все известные на момент выпуска программы) возможные способы заражения компьютера. Таким образом, можно обнаружить вирус, созданный уже после выхода программы-ревизора.

Сторожа. Резидентные программы, постоянно находящиеся в памяти компьютера и контролирующие все операции (не пользуются особой популярностью главным образом из-за большого количества ложных срабатываний, которые в отдельных случаях способны если не парализовать, то уж наверняка серьезно застопорить работу).

Вакцины. Используются для обработки файлов и загрузочных секторов с целью предотвращения заражения известными вирусами (в последнее время этот метод применяется все реже - вакцинировать можно только от конкретного вируса, причем некоторые антивирусы такую вакцинацию вполне могут спутать с самой болезнью, поскольку отличие вируса от вакцины на самом деле исчезающе мало).

Как известно, ни один из данных типов антивирусов не обеспечивает стопроцентной защиты компьютера, и их желательно использовать в связке с другими пакетами. Вообще, выбор только одного, "лучшего", антивируса крайне ошибочен.

Теперь о некоторых характеристиках антивирусных пакетов. Первое, на что пользователи обращают внимание, это количество распознаваемых сигнатур - последовательностей символов, однозначно определяющих вирус. Следует отметить, что производители применяют разные системы подсчета сигнатур: если у одних различные версии или близкие по характеристикам версии вирусов считаются за одну сигнатуру, то другие подсчитывают все вариации. Лучшие из пакетов определяют более 10 тысяч вирусов, что несколько меньше общего числа существующих сегодня вредоносных программ. Второй параметр - наличие эвристического анализатора неизвестных вирусов; его присутствие очень полезно, но существенно замедляет время работы программы.

Среди российских разработок наиболее известными являются комплект программ от "ДиалогНаука" и AntiViral Toolkit Pro by Eugene Kaspersky от НТЦ KAMI. Начнем обзор с продуктов "ДиалогНаука", поскольку эти программы уже стали некоторым стандартом, и подавляющее большинство компьютеров в нашей стране укомплектовано именно их антивирусами (мы не будем сейчас гадать, какое количество этих программ является лицензионным).

Литература:

1. «Компьютерное Обозрение» №108.—Киев: ООО «ITC», 1997.