Компью́терный ви́рус

Зайцев А.В

Основная цель вируса

- Основная цель вируса - его распространение. Кроме того, часто его сопутствующей функцией является нарушение работы программно-аппаратных комплексов — удаление файлов и даже удаление операционной системы, приведение в негодность структур размещения данных, блокирование работы пользователей и т. п. Даже если автор вируса не запрограммировал вредоносных эффектов, вирус может приводить к сбоям компьютера из-за ошибок, неучтённых тонкостей взаимодействия с операционной системой и другими программами. Кроме того, вирусы, как правило, занимают место на накопителях информации и потребляют ресурсы системы.

История компьютерных вирусов

- Основы теории самовоспроизводящихся механизмов заложил американец венгерского происхождения Джон фон Нейман, который в 1951 году предложил метод создания таких механизмов. С 1961 года известны рабочие примеры таких программ[2].
- Первыми известными вирусами являются Virus 1,2,3 и Elk Cloner для ПК Apple II, появившиеся в 1981 году.
  Зимой 1984 года появились первые антивирусные утилиты — CHK4BOMB и BOMBSQAD авторства Энди Хопкинса (англ. *Andy Hopkins*).
- В начале 1985 года Ги Вонг (англ. *Gee Wong*) написал программу DPROTECT —
  первый резидентный антивирус.

- специализированная программа для обнаружения компьютерных вирусов, а также нежелательных (считающихся вредоносными) программ и восстановления заражённых (модифицированных) такими программами файлов и профилактики — предотвращения заражения (модификации) файлов или операционной системы вредоносным кодом.

Антиви́русная програ́мма

Метод сканирования сигнатур

- основан на поиске в файлах уникальной последовательности байтов — **сигнатуры**, характерной для определенного вируса. Для каждого вновь обнаруженного вируса специалистами антивирусной лаборатории выполняется анализ кода, на основании которого определяется его сигнатура. Полученный кодовый фрагмент помещают в специальную базу данных вирусных сигнатур, с которой работает антивирусная программа. Достоинством данного метода является относительно низкая доля ложных срабатываний, а главным недостатком — принципиальная невозможность обнаружения в системе нового вируса, для которого отсутствует сигнатура в базе данных антивирусной программы, поэтому требуется своевременная актуализация базы данных сигнатур.

Метод контроля целостности

- основывается на том, что любое неожиданное и беспричинное изменение данных на диске является подозрительным событием, требующим особого внимания антивирусной системы. Вирус обязательно оставляет свидетельства своего пребывания (изменение данных существующих (особенно системных или исполняемых) файлов, появление новых исполняемых файлов и т. д.). Факт изменения данных — *нарушение целостности* — легко устанавливается путем сравнения контрольной суммы (дайджеста), заранее подсчитанной для исходного состояния тестируемого кода, и контрольной суммы (дайджеста) текущего состояния тестируемого кода. Если они не совпадают, значит, целостность нарушена и имеются все основания провести для этого кода дополнительную проверку, например, путем сканирования вирусных сигнатур. Указанный метод работает быстрее метода сканирования сигнатур, поскольку подсчет контрольных сумм требует меньше вычислений, чем операции побайтового сравнения кодовых фрагментов, кроме того он позволяет обнаруживать следы деятельности любых, в том числе неизвестных, вирусов, для которых в базе данных еще нет сигнатур.

Метод сканирования подозрительных команд

- основан на выявлении в сканируемом файле некоторого числа подозрительных команд и(или) признаков подозрительных кодовых последовательностей (например, команда форматирования жесткого диска или функция внедрения в выполняющийся процесс или исполняемый код). После этого делается предположение о вредоносной сущности файла и предпринимаются дополнительные действия по его проверке. Этот метод обладает хорошим быстродействием, но довольно часто он не способен выявлять новые вирусы.

Метод отслеживания поведения программ

- принципиально отличается от методов сканирования содержимого файлов, упомянутых ранее. Этот метод основан на анализе поведения запущенных программ, сравнимый с поимкой преступника «за руку» на месте преступления. Антивирусные средства данного типа часто требуют активного участия пользователя, призванного принимать решения в ответ на многочисленные предупреждения системы, значительная часть которых может оказаться впоследствии ложными тревогами. Частота ложных срабатываний (подозрение на вирус для безвредного файла или пропуск вредоносного файла) при превышении определенного порога делает этот метод неэффективным, а пользователь может перестать реагировать на предупреждения или выбрать оптимистическую стратегию (разрешать все действия всем запускаемым программам или отключить данную функцию антивирусного средства). При использовании антивирусных систем, анализирующих поведение программ, всегда существует риск выполнения команд вирусного кода, способных нанести ущерб защищаемому компьютеру или сети. Для устранения подобного недостатка позднее был разработан метод эмуляции (имитации), позволяющий запускать тестируемую программу в искусственно созданной (виртуальной) среде, которую часто называют песочницей (sandbox), без опасности повреждения информационного окружения. Использование методов анализа поведения программ показало их высокую эффективность при обнаружении как известных, так и неизвестных вредоносных программ.

Лжеантивирусы

- В 2009 году началось активное распространение лжеантивирусов — программного обеспечения, не являющегося антивирусным (то есть не имеющего реальной функциональности для противодействия вредоносным программам), но выдающим себя за таковое. По сути, лжеантивирусы могут являться как программами для обмана пользователей и получения прибыли в виде платежей за «лечение системы от вирусов», так и обычным вредоносным программным обеспечением.

Как избежать заражения компьютера вирусом

- 1)Не щелкайте по баннерам.
- 2)Остерегайтесь всплывающих окон.
- 3)Очистите кэш.
- 4)Не открывайте подозрительные сайты.
- 5)Не скачивайте не у проверенных сайтов