Компьютерные вирусы

Компьютерный вирус - это небольшая программа, написанная программистом высокой квалификации, способная к саморазмножению и выполнению разных деструктивных действий. На сегодняшний день известно свыше 5 мил. компьютерных вирусов.

Существует много разных версий относительно даты рождения первого компьютерного вируса. Однако большинство специалистов сходятся на мысли, что компьютерные вирусы, как таковые, впервые появились в 1986 году, хотя исторически возникновение вирусов тесно связано с идеей создания самовоспроизводящихся программ. Одним из "пионеров" среди компьютерных вирусов считается вирус "Brain", созданный пакистанским программистом по фамилии Алви. Только в США этот вирус поразил свыше 18 тыс. компьютеров. В начале эпохи компьютерных вирусов разработка вирусоподобных программ носила чисто исследовательский характер, постепенно превращаясь на откровенно вражеское отношение к пользователям безответственных, и даже криминальных "элементов". В ряде стран уголовное законодательство предусматривает ответственность за компьютерные преступления, в том числе за создание и распространение вирусов.

Вирусы действуют только программным путем. Они, как правило, присоединяются к файлу или проникают в тело файла. В этом случае говорят, что файл заражен вирусом. Вирус попадает в компьютер только вместе с зараженным файлом. Для активизации вируса нужно загрузить зараженный файл, и только после этого, вирус начинает действовать самостоятельно.

Некоторые вирусы во время запуска зараженного файла становятся резидентными (постоянно находятся в оперативной памяти компьютера) и могут заражать другие загружаемые файлы и программы. Другая разновидность вирусов сразу после активизации может быть причиной серьезных повреждений, например, форматировать жесткий диск. Действие вирусов может проявляться по разному: от разных визуальных эффектов, мешающих работать, до полной потери информации. Большинство вирусов заражают исполнительные программы, то есть файлы с расширением .EXE и .COM, хотя в последнее время большую популярность приобретают вирусы, распространяемые через систему электронной почты.

Следует заметить, что компьютерные вирусы способны заражать лишь компьютеры. Поэтому абсолютно абсурдными являются разные утверждения о влиянии компьютерных вирусов на пользователей компьютеров.

Основные источники вирусов:

- дискета, на которой находятся зараженные вирусом файлы;
- компьютерная сеть, в том числе система электронной почты и Internet;
- жесткий диск, на который попал вирус в результате работы с зараженными программами;
- вирус, оставшийся в оперативной памяти после предшествующего пользователя.

Основные ранние признаки заражения компьютера вирусом:

- уменьшение объема свободной оперативной памяти;
- замедление загрузки и работы компьютера;
- непонятные (без причин) изменения в файлах, а также изменения размеров и даты последней модификации файлов;
- ошибки при загрузке операционной системы;
- невозможность сохранять файлы в нужных каталогах;
- непонятные системные сообщения, музыкальные и визуальные эффекты и т.д.

Признаки активной фазы вируса:

- исчезновение файлов;

- форматирование жесткого диска;
- невозможность загрузки файлов или операционной системы.

Существует очень много разных вирусов. Условно их можно классифицировать следующим образом:

1) загрузочные вирусы или BOOT-вирусы заражают boot-секторы дисков. Очень опасные, могут привести к полной потере всей информации, хранящейся на диске;

2) файловые вирусы заражают файлы. Делятся на:

- вирусы, заражающие программы (файлы с расширением .EXE и .COM);
- макровирусы вирусы, заражающие файлы данных, например, документы Word или рабочие книги Excel;
- вирусы-спутники используют имена других файлов;
- вирусы семейства DIR искажают системную информацию о файловых структурах;

3) загрузочно-файловые вирусы способные поражать как код boot-секторов, так и код файлов;

4) вирусы-невидимки или STEALTH-вирусы фальсифицируют информацию прочитанную из диска так, что программа, какой предназначена эта информация получает неверные данные. Эта технология, которую, иногда, так и называют Stealth-технологией, может использоваться как в BOOT-вирусах, так и в файловых вирусах;

5) ретровирусы заражают антивирусные программы, стараясь уничтожить их или

сделать нетрудоспособными;

6) вирусы-черви снабжают небольшие сообщения электронной почты, так называемым заголовком, который по своей сути есть Web-адресом местонахождения самого вируса. При попытке прочитать такое сообщение вирус начинает считывать через глобальную сеть Internet свое 'тело' и после загрузки начинает деструктивное действие. Очень опасные, так как обнаружить их очень тяжело, в связи с тем, что зараженный файл фактически не содержит кода вируса.

Если не принимать меры для защиты от компьютерных вирусов, то следствия заражения могут быть очень серьезными. В ряде стран уголовное законодательство предусматривает ответственность за компьютерные преступления, в том числе за внедрение вирусов. Для защиты информации от вирусов используются общие и программные средства.

К общим средствам, помогающим предотвратить заражение и его разрушительных последствий относят:

- резервное копирование информации (создание копий файлов и системных областей жестких дисков);
- избежание пользования случайными и неизвестными программами. Чаще всего вирусы распространяются вместе с компьютерными программами;
- перезагрузка компьютера перед началом работы, в частности, в случае, если за этим компьютером работали другие пользователи;
- ограничение доступа к информации, в частности физическая защита дискеты во время копирования файлов с нее.

К программным средствам защиты относят разные антивирусные программы (антивирусы). Антивирус - это программа, выявляющая и обезвреживающая компьютерные вирусы. Следует заметить, что вирусы в своем развитии опережают антивирусные программы, поэтому даже в случае регулярного пользования антивирусов, нет 100% гарантии безопасности. Антивирусные программы могут выявлять и уничтожать лишь известные вирусы, при появлении нового компьютерного

вируса защиты от него не существует до тех пор, пока для него не будет разработан свой антивирус. Однако, много современных антивирусных пакетов имеют в своем составе специальный программный модуль, называемый эвристическим анализатором, который способен исследовать содержимое файлов на наличие кода, характерного для компьютерных вирусов. Это дает возможность своевременно выявлять и предупреждать об опасности заражения новым вирусом.

Различают такие типы антивирусных программ:

1) программы-детекторы: предназначены для нахождения зараженных файлов одним из известных вирусов. Некоторые программы-детекторы могут также лечить файлы от вирусов или уничтожать зараженные файлы. Существуют специализированные, то есть предназначенные для борьбы с одним вирусом детекторы и полифаги, которые могут бороться с многими вирусами;

2) программы-лекари: предназначены для лечения зараженных дисков и программ. Лечение программы состоит в изъятии из зараженной программы тела вируса. Также могут быть как полифагами, так и специализированными;

3) программы-ревизоры: предназначены для выявления заражения вирусом файлов, а также нахождение поврежденных файлов. Эти программы запоминают данные о состоянии программы и системных областей дисков в нормальном состоянии (до заражения) и сравнивают эти данные в процессе работы компьютера. В случае несоответствия данных выводится сообщение о возможности заражения;

4) лекари-ревизоры: предназначены для выявления изменений в файлах и системных областях дисков и, в случае изменений, возвращают их в начальное состояние.

5) программы-фильтры: предназначены для перехвата обращений к операционной системе, которые используются вирусами для размножения и сообщают об этом пользователя. Пользователь может разрешить или запретить выполнение соответствующей операции. Такие программы являются резидентными, то есть они находятся в оперативной памяти компьютера.

6) программы-вакцины: используются для обработки файлов и boot-секторов с целью предупреждения заражения известными вирусами (в последнее время этот метод используется все чаще).

Следует заметить, что выбор одного "наилучшего" антивируса крайне ошибочное решение. Рекомендуется использовать несколько разных антивирусных пакетов одновременно. Выбирая антивирусную программу следует обратить внимание на такой параметр, как количество распознающих сигнатур (последовательность символов, которые гарантированно распознают вирус). Второй параметр - наличие эвристического анализатора неизвестных вирусов, его присутствие очень полезно, но существенно замедляет время работы программы. На сегодняшний день существует большое количество разнообразных антивирусных программ. Рассмотрим коротко, распространенные в странах СНГ.

DRWEB

Один из лучших антивирусов с мощным алгоритмом нахождения вирусов. Полифаг, способный проверять файлы в архивах, документы Word и рабочие книги Excel, выявляет полиморфные вирусы, которые в последнее время, получают все большее распространение. Достаточно сказать, что эпидемию очень опасного вируса OneHalf остановил именно DrWeb. Эвристический анализатор DrWeb, исследуя программы на наличие фрагментов кода, характерных для вирусов, разрешает найти почти 90% неизвестных вирусов. При загрузке программы, в первую очередь DrWeb проверяет самого себя на целостность, после чего тестирует оперативную память. Программа может работать в диалоговом режиме, имеет удобный настраиваемый интерфейс пользователя.

ADINF

Антивирус-ревизор диска ADINF (Avanced DiskINFoscope) разрешает находить и уничтожать, как существующие обычные, stealth- и полиморфные вирусы, так и совсем новые. Антивирус имеет в своем распоряжении лечащий блок ревизора ADINF - Adinf Cure Module - что может обезвредить до 97% всех вирусов. Эту цифру приводит "Диалогнаука", исходя из результатов тестирования, которое происходило на

коллекциях вирусов двух признанных авторитетов в этой области - Д.Н.Лозинского и фирмы Dr.Solomon's (Великобритания).

ADINF загружается автоматически в случае включения компьютера и контролирует boot-сектор и файлы на диске (дата и время создания, длина, контрольная сумма), выводя сообщения про их изменения. Благодаря тому, что ADINF осуществляет дисковые операции в обход операционной системы, обращаясь к функциям BIOS, достигаются не только возможность выявления активных stealth-вірусів, но и высокая скорость проверки диска. Если найден boot-вирус, то ADINF просто восстановит предшествующий загрузочный сектор, который хранится в его таблице. Если вирус файловый, то здесь на помощь приходит лечащий блок Adinf Cure Module, который на основе отчета основного модуля о зараженных файлах сравнивает новые параметры файлов с предыдущими, хранящиеся в специальных таблицах. При выявлении расхождений ADINF восстанавливает предыдущее состояние файла, а не уничтожает тело вируса, как это делают полифаги.

AVP

Антивирус AVP (AntiVirus Program) относится к полифагам, в процессе работы проверяет оперативную память, файлы, в том числе архивные, на гибких, локальных, сетевых и CD-ROM дисках, а также системные структуры данных, такие как загрузочный сектор, таблицу разделов и т.д. Программа имеет эвристический анализатор, который, по утверждениям разработчиков антивируса способен находить почти 80% всех вирусов. Программа AVP является 32-разрядным приложением для работы в среде операционных систем Windows 98, NT и 2000, имеет удобный интерфейс, а также одну из самых больших в мире антивирусную базу. Базы антивирусов к AVP обновляются приблизительно один раз в неделю и их можно получить с Internet. Эта программа осуществляет поиск и изъятие разнообразнейших вирусов, в том числе:

- полиморфных, или самошифрующихся вирусов;
- стелс-вирусов, или вирусов-невидимок;
- новых вирусов для Windows;
- макровирусов, заражающих документы Word и таблицы Excel.

Кроме того, программа AVP осуществляет контроль файловых операций в системе в фоновом режиме, выявляет вирус до момента реального заражения системы, а также определяет неизвестные вирусы с помощью эвристического модуля.

Контрольные вопросы

Что такое компьютерный вирус?

Каким образом вирус заражает компьютер?

Каким образом действуют компьютерные вирусы?

Какие вы знаете источники заражения компьютерным вирусом?

По каким признакам можно обнаружить факт заражения компьютерным вирусом?

Какие вы знаете типы вирусов? Какие деструктивные действия они осуществляют?

Какие действия предпринимают для предотвращения заражения компьютерным вирусом?

Что такое антивирус? Какие типы антивирусов вы знаете?

Что такое эвристический анализатор? Какие функции он выполняет?

Приведите примеры антивирусных программ. Коротко охарактеризуйте их.