Внимание Вирус

Классификация, методы борьбы

Автор Шлевис В.А.

Оглавление

Что такое компьютерный вирус?

- **Компьютерный вирус –** самораспростроняющаяся, самоорганизующаясяя программа несущая деструктивный код, способная создавать свои копии и внедрять их в различные объекты или ресурсы компьютерных систем без ведома пользователя.
- На сегодняшний день известно 6 основных типов вирусов:
  - файловые,
  - загрузочные,
  - STELS (невидимки),
  - скрипт-вирусы
  - макро-вирусы.
- Следует отличать вирусы от вредоносных кодов. К ним относятся:
  - Интернет-черви
  - программы - «Троянские кони».
- Основные симптомы вирусного поражения:
  - замедление работы некоторых программ,
  - увеличение размеров файлов (особенно выполняемых),
  - появление не существовавших ранее подозрительных файлов,
  - уменьшение объема доступной оперативной памяти (по сравнению с обычным режимом работы),
  - внезапно возникающие разнообразные видео и звуковые эффекты.

При всех перечисленных выше симптомах, а также при других странных проявлениях в работе системы (неустойчивая работа, частые самостоятельные перезагрузки и прочее) следует немедленно произвести проверку системы на наличие вирусов.

Зарождение компьютерных вирусов

- О появлении первого компьютерного вируса много разных мнений. Доподлинно только известно, что на машине Чарльза Бэббиджа, считающегося изобретателем первого компьютера, его не было, а на Univax 1108 и IBM 360/370, в середине 1970-х годов они уже были.

Интересно, что идея компьютерных вирусов появилась намного раньше самих персональных компьютеров.

- Точкой отсчета можно считать труды известного ученого Джона фон Неймана по изучению самовоспроизводящихся математических автоматов, о которых стало известно в 1940-х годах. В 1951 году он предложил способ создания таких автоматов. А в 1959 году журнал Scientific American опубликовал статью Л.С. Пенроуза, посвященную самовоспроизводящимся механическим структурам. В ней была описана простейшая двумерная модель самовоспроизводящихся механических структур, способных к активации, размножению, мутациям, захвату. Позднее другой ученый Ф.Ж. Шталь реализовал данную модель на практике с помощью машинного кода на IBM 650.

Пути проникновения вирусов в компьютер и механизм распределения вирусных программ

- Основными путями проникновения вирусов в компьютер являются съемные диски (гибкие, лазерные, флеш), а также компьютерные сети. Заражение жесткого диска вирусами может произойти при загрузке программы с диска, содержащего вирус. Такое заражение может быть и случайным, например, если дискету не вынули из устройства и перезагрузили компьютер, при этом диск может быть и не системным. Заразить съемный диск гораздо проще. На него вирус может попасть, даже если диск просто вставили в устройство чтения зараженного компьютера.
  - Естественно, что заразить можно только диск позволяющий запись. Заражение лазерного диска происходит в процессе подготовки и последующей записи на него зараженных файлов.
- Вирус, внедряясь в систему, перехватывает управление и заражает текущую или системную программ так, что бы при ее запуске управление сначала передалось ему. Получив доступ к управлению, вирус прежде всего переписывает сам себя в другую рабочую программу и заражает ее. После того как вирус выполнит нужные ему действия, он передает управление той программе, в которой он находится, и она работает как обычно. Тем самым внешне работа зараженной программы выглядит так же, как и незараженной. Наиболее часто вирусом заражаются загрузочный сектор диска и исполняемые файлы, имеющие расширения EXE, COM, SYS, BAT. Реже заражаются текстовые файлы.
- Многие разновидности вирусов устроены так, что при запуске зараженной программы вирус остается в памяти компьютера и время от времени заражает программы и выполняет нежелательные действия на компьютере. Все действия вируса могут выполняться очень быстро и без выдачи каких либо сообщений, по этому пользователю очень трудно, практически невозможно, определить, что в компьютере происходит что-то необычное.
- Сам процесс размножения может быть условно разделен на несколько стадий:
  - Проникновение на компьютер
  - Активация вируса
  - Поиск объектов для заражения
  - Подготовка вирусных копий
  - Внедрение вирусных копий

Особенности реализации каждой стадии порождают атрибуты, набор которых фактически и определяет класс вируса.

Признаки появления вирусов

- При заражении компьютера вирусом важно его обнаружить. Для этого следует знать об основных признаках проявления вирусов. К ним можно отнести следующие:
  1. прекращение работы или неправильная работа ранее успешно функционировавших программ
  2. медленная работа компьютера
  3. невозможность загрузки операционной системы
  4. исчезновение файлов и каталогов или искажение их содержимого
  5. изменение даты и времени модификации файлов
  6. изменение размеров файлов
  7. неожиданное значительное увеличение количества файлов на диске
  8. существенное уменьшение размера свободной оперативной памяти
  9. вывод на экран непредусмотренных сообщений или изображений
  10. подача непредусмотренных звуковых сигналов
  11. частые зависания и сбои в работе компьютера
- Следует отметить, что вышеперечисленные явления необязательно вызываются присутствием вируса, а могут быть следствием других причин.

Действия при заражении вирусом

- При заражении компьютера вирусом (или подозрении на это) важно
- соблюдать четыре правила.

1. Прежде всего не надо торопиться и принимать опрометчивых решений. Как говорится, "семь раз отмерь, один раз отрежь" — непродуманные действия могут привести не только к потере части файлов, которые можно было бы восстановить, но и к повторному заражению компьютера.
2. Одно действие должно быть выполнено немедленно, — надо выключить компьютер, чтобы вирус не продолжал свою работу.
3. Все действия по обнаружению вида заражения и лечению компьютера следует выполнять только после перезагрузки компьютера с защищенной от записи "эталонной" дискеты с операционной системой. При этом следует пользоваться исполняемыми файлами находящимися только на защищенных от записи "эталонных" дискетах. Несоблюдение этого правила может привести к очень тяжелым последствиям,
4. Если Вы не обладаете достаточными опытом и знаниями для лечения компьютера, попросите о помощи более опытных коллег или специалистов.

Основные методы защиты от компьютерных вирусов

Для защиты от вирусов можно использовать:

- Общие средства защиты информации, которые полезны также как страховка от физической порчи дисков, неправильно работающих программ или ошибочных действий пользователей;
- профилактические меры, позволяющие уменьшить вероятность заражения вирусом;
- специализированные программы для защиты от вирусов.

Общие средства защиты информации полезны не только для защиты от вирусов.
Имеются две основные разновидности этих средств:

- копирование информации — создание копий файлов и системных областей дисков;
- разграничение доступа предотвращает несанкционированное использование информации, в частности, защиту от изменений программ и данных вирусами, неправильно работающими программами и ошибочными действиями пользователей.

Несмотря на то, что общие средства защиты информации очень важны для защиты от вирусов, все же их одних недостаточно. Необходимо применять специализированные программы **АНТИВИРУСЫ**. Эти программы можно разделить на несколько видов:

- **Программы - детекторы** позволяют обнаруживать файлы, зараженные одним из нескольких известных вирусов.
- **Программы - доктора**, или фаги, "лечат" зараженные программы или диски, "выкусывая" из зараженных программ тело вируса, т.е. восстанавливая программу в том состоянии, в котором она находилась до заражения вирусом.
- **Программы - ревизоры** сначала запоминают сведения о состоянии программ и системных областей дисков, а затем сравнивают их состояние с исходным. При выявлении несоответствий, об этом сообщается пользователю.
- **Программы - фильтры** располагаются резидентно в оперативной памяти компьютера и перехватывают те обращения к операционной системе, которые используются вирусами для размножения и нанесения вреда, и сообщают о них пользователю. Пользователь может разрешить или запретить выполнение соответствующей операции.
- **Программы - вакцины**, или иммунизаторы, модифицируют программы и диски таким образом, что это не отражается на работе программ, но вирус, от которого производится вакцинация, считает эти программы и диски уже зараженными. Эти программы неэффективны, хотя и могут использоваться для защиты от некоторых типов вирусов, например **autorun – вирусы.**

Необходимо отметить, что, на сегодняшний день, антивирусные программы часто объединяют все эти виды

Как правильно лечить?

- Прежде всего, перезагрузите компьютер, нажав кнопку **Reset**. Такая перезагрузка называется «холодной», в отличие от «теплой», вызываемой комбинацией клавиш **Ctrl-Alt-Del**. Существуют вирусы, которые спокойненько выживают при «теплой» перезагрузке.
- Загрузите компьютер с диска, защищенного от записи и с установленными антивирусными программами. Необходимость хранить антивирусный пакет на отдельной защищенной дискете вызвана не только опасностью заражения антивирусных программ вирусом. Частенько вирус специально ищет на жестком диске программу-антивирус и наносит ей повреждения.
- Старайтесь чаще обновлять ваши антивирусные программы. Причем как отечественные, так и импортные. Отечественные - потому что у нас пишут вирусы все кому не лень и, чтобы быстро разработать антивирусную программу, надо жить здесь. Импортные — потому что все сильнее сливаются «на-ше» и «их» информационные пространства, все больше западных вирусов проникает к нам по глобальным компьютерным сетям.
- При обнаружении зараженного файла желательно скопировать его на дискету и лишь затем лечить антивирусом. Это делается для того, чтобы в случае некорректного лечения файла, что, к сожалению, случается, попытаться полечить файл другим антивирусом.
- Если вам понадобилась программа из ваших старых архивов или резервных копий, не поленитесь проверить ее. Не рискуйте. Лучше преувеличить опасность, чем недооценить ее.

Антивирусы

- **Что такое антивирус?**

  Основные задачи антивируса: препятствование проникновению вирусов в компьютерную систему, обнаружение и устранение вирусов без нанесения повреждений другим объектам, минимизация ущерба от действий вирусов.
- Привожу список самых популярных на сегодняшний день **антивирусов**, в списке только лучшие **антивирусы**:
- Eset NOD32
  Panda
  McAfee
  Symantec
  CAT QuickHeal
  F-Secure
  Fortinet
  Касперский KAV
  Касперский KIS
  Dr.Web
  Avast (бесплатный)
  Avira (бесплатный)

  Можно выбрать и **скачать** любой из выше указанных **антивирусов** для установки на свой компьютер и Вы можете быть в высокой степени уверены в защищённости Вашего компьютера.
- Однако, 100% защиты Вам не даст ни один **антивирус.** Особенно, если Вы используете нелицензионный антивирус и у Вас устаревший **ключ антивируса**.