Профилактика проникновения вирусов.

Одним из методов борьбы с вирусами является, как и в медицине, своевременная профилактика. Компьютерная профилактика предполагает соблюдение правил ("компьютерной гигиены"), позволяющих значительно снизить вероятность заражения вирусом и потери каких-либо данных. Профилактика компьютерных вирусов начинается с выявления путей проникновения вируса в компьютер и компьютерные сети.

Рассмотрим основные пути проникновения вирусов в компьютеры пользователей:

1. Глобальные сети – электронная почта.
2. Электронные конференции, файл-серверы ftp.
3. Пиратское программное обеспечение.
4. Локальные сети.
5. Персональные компьютеры "общего пользования".
6. Сервисные службы.

Глобальные сети - электронная почта

Основным источником вирусов на сегодняшний день является глобальная сеть Internet. Наибольшее число заражений вирусом происходит при обмене письмами в форматах Word/Office97. Пользователь зараженного макро-вирусом редактора, сам того не подозревая, рассылает зараженные письма адресатам, которые в свою очередь отправляют новые зараженные письма и т.д.

Локальные сети

Другой путь "быстрого заражения" – локальные сети. Если не принимать необходимых мер защиты, то зараженная рабочая станция при входе в сеть заражает один или несколько служебных файлов на сервере. Далее пользователи при очередном подключении к сети запускают зараженные файлы с сервера, и вирус, таким образом, получает доступ на компьютеры пользователей.

Персональные компьютеры "общего пользования"

Опасность представляют также компьютеры, установленные в учебных заведениях. Если один из студентов принес на своих дискетах вирус и заразил какой-либо учебный компьютер, то очередной вирус будет гулять по всему учебному заведению, включая домашние компьютеры студентов и сотрудников.

Пиратское программное обеспечение

Нелегальные копии программного обеспечения, как это было всегда, являются одной из основных "зон риска". Часто пиратские копии на дискетах и даже на CD-дисках содержат файлы, зараженные самыми разнообразными типами вирусов. Необходимо помнить, что низкая стоимость программы может дорого обойтись при потере данных.

Правила защиты от компьютерных вирусов

1. Внимательно относитесь к программам и документам, которые получаете из глобальных сетей.
2. Перед тем, как запустить файл на выполнение или открыть документ/таблицу, обязательно проверьте его на наличие вирусов.
3. Используйте специализированные антивирусы – для проверки "на лету" (например, SpIDer Guard из пакета Dr. Web и др.) всех файлов, приходящих по электронной почте (и из Интернета в целом).
4. Для уменьшения риска заразить файл на сервере администраторам сетей следует активно использовать стандартные возможности защиты сети, такие как: ограничение прав пользователей; установку атрибутов "только на чтение" или "только на запуск" для всех выполняемых файлов (к сожалению, это не всегда оказывается возможным) и т. д.
5. Регулярно проверяйте сервер обычными антивирусными программами, для удобства и системности используйте планировщики заданий.
6. Целесообразно запустить новое программное обеспечение на тестовом компьютере, не подключенном к общей сети.
7. Используйте лицензионное программное обеспечение, приобретенное у официальных продавцов.
8. Дистрибутивы копий программного обеспечения (в том числе копий операционной системы) необходимо хранить на защищенных от записи дисках.
9. Пользуйтесь только хорошо зарекомендовавшими себя источниками программ и прочих файлов.
10. Постоянно обновляйте вирусные базы используемого антивируса.
11. Старайтесь не запускать непроверенные файлы, в том числе полученные из компьютерной сети. Перед запуском новых программ обязательно проверьте их одним или несколькими антивирусами.
12. Ограничьте (по возможности) круг лиц допущенных к работе на конкретном компьютере.
13. Пользуйтесь утилитами проверки целостности информации. Такие утилиты сохраняют в специальных базах данных информацию о системных областях дисков (или целиком системные области) и информацию о файлах (контрольные суммы, размеры, атрибуты, даты последней модификации файлов и т. д.).
14. Периодически сохраняйте на внешнем носителе файлы, с которыми ведется работа.
15. При работе с Word/Excel включите защиту от макросов, которая сообщает о присутствии макроса в открываемом документе и предоставляет возможность запретить этот макрос. В результате макрос не только не выполняется, но и не виден средствами Word/Excel.

Восстановление зараженных файлов.

При анализе алгоритма вируса необходимо выяснить:

- способ(ы) размножения вируса;
- характер возможных повреждений, которые вирус нанес информации, хранящейся на дисках;
- метод лечения оперативной памяти и зараженных файлов (секторов).

При анализе файлового вируса необходимо выяснить, какие файлы (COM, EXE, SYS) поражаются вирусом, в какое место (места) в файле записывается код вируса - в начало, конец или середину файла, в каком объеме возможно восстановление файла (полностью или частично), в каком месте вирус хранит восстанавливаемую информацию.

При анализе загрузочного вируса основной задачей является выяснение адреса (адресов) сектора, в котором вирус сохраняет первоначальный загрузочный сектор.

Для резидентного вируса требуется также выделить участок кода, создающий резидентную копию вируса. Необходимо также определить, каким образом и где в оперативной памяти вирус выделяет место для своей резидентной копии.

Для анализа макровирусов необходимо получить текст их макросов. Для нешифрованных ("не-стелс") вирусов это достигается при помощи меню Сервис/Макрос. Если же вирус шифрует свои макросы или использует "стелс"-приемы, то необходимо воспользоваться специальными утилитами просмотра макросов. Такие специализированные утилиты есть практически у каждой фирмы-производителя антивирусов, однако, они являются утилитами "внутреннего пользования" и не распространяются за пределы фирм.

В любом случае, если есть возможность, правильнее всего передавать зараженные файлы специалистам антивирусных лабораторий.

Дополнительный материал:

- https://hetmanrecovery.com/ru/recovery_news/recover-virus-infected-files.htm
- https://cyberleninka.ru/article/n/informatsionnaya-bezopasnost-sovremennye-realii-1