Защита от вредоносных программ

Защита информации от вредоносного кода

Шинкаренко Евгений Александрович
МОУ Гимназия № 2 г.Черняховск
Калининградская область

Типы вредоносных программ

Вредоносными программами являются программы, наносящие вред данным и программам, хранящимся на компьютере.

Типы вредоносных программ:

- Вирусы, черви, троянские и хакерские программы.
- Шпионское, рекламное программное обеспечение.
- Потенциально опасное программное обеспечение.

Антивирусные программы.

Современные антивирусные программы обеспечивают комплексную защиту программ и данных на компьютере от всех типов вредоносных программ и методов их проникновения на компьютер.

Популярные антивирусные программы: Антивирус Касперского, Dr.Web, avast и др.

Для защиты от вредоносных программ каждого типа в антивирусной программе предусмотрены отдельные компоненты.

Принцип работы антивирусных программ

Принцип работы антивирусных программ основан на проверке файлов, загрузочных секторов дисков и оперативной памяти и поиске в них известных и новых вредоносных программ.

Для поиска известных вредоносных программ используются сигнатуры угроз. Сигнатура – это некоторая постоянная последовательность программного кода, специфичная для конкретной вредоносной программы.

Эвристический анализ

Для поиска новых вредоносных программ используется алгоритм эвристического сканирования, т.е. анализа последовательности команд в проверяемом объекте. Если «подозрительная» последовательность команд обнаруживается, то антивирусная программа выдает сообщение о возможном заражении объекта.

Антивирусный монитор

Антивирусный монитор запускается автоматически при старте операционной системы и работает в качестве фонового системного процесса, проверяя на вредоносность совершаемые другими программами действия.

Основная задача антивирусного монитора состоит в обеспечении максимальной защиты от вредоносных программ при минимальном замедлении работы компьютера.

Антивирусный сканер

Антивирусный сканер запускается по заранее выбранному расписанию или в произвольный момент времени пользователем.

Антивирусный сканер производит поиск вредоносных программ в оперативной памяти, а также на логических дисках.

Признаки заражения компьютера

- вывод на экран непредусмотренных сообщений или изображений,
- подача непредусмотренных звуковых сигналов,
- неожиданное открытие и закрытие лотка CD/DVD
- произвольный запуск на компьютере каких-либо программ,
- частые зависания и сбои в работе компьютера,
- медленная работа компьютера при запуске программ,
- исчезновение или изменение файлов и папок,
- частые обращения к жесткому диску,
- зависание или неожиданное поведение браузера.

Компьютерные вирусы

Обязательным свойством компьютерного вируса является способность к «размножению» (Самокопированию).

После заражения компьютера вирус может активизироваться и заставить компьютер выполнять какие-либо действия.

Компьютерные вирусы являются вредоносными программами, которые могут «размножаться» и скрытно внедрять свои копии в файлы, загрузочные сектора дисков и документы. Активизация компьютерного вируса может вызывать уничтожение программ и данных.

Загрузочные вирусы

Загрузочные вирусы заражают загрузочный сектор диска.

При заражении дисков загрузочные вирусы «подставляют» свой код вместо программы, получающей управление при загрузке системы, и отдают управление не оригинальному коду загрузчика, а коду вируса.

Файловые вирусы.

Файловые вирусы различными способами внедряются в исполняемые файлы и обычно активизируются при их запуске.

После запуска зараженного файла вирус находится в оперативной памяти компьютера и является активным (т. е. может заражать другие файлы) вплоть до момента выключения компьютера или перезагрузки операционной системы.

Практически все загрузочные и файловые вирусы **резидентны,** т.е. они находятся в оперативной памяти компьютера и в процессе работы могут осуществлять опасные действия.

Макровирусы

Существуют макровирусы для интегрированного офисного приложения Microsoft Office (Word, Excel, PowerPoint и Access). Макровирусы фактически являются макрокомандами (макросами), на встроенном языке программирования Visual Basic for Applications (VBA), которые помещаются в документ.

Макровирусы являются **ограниченно резидентными,** т.е. они находятся в оперативной памяти и заражают документы, пока открыто приложение. Кроме того, макровирусы заражают шаблоны документов, и поэтому активизируются уже при запуске зараженного приложения.

Сетевые черви и защита от них

К сетевым червям (worm) относятся вредоносные программы, распространяющие свои копии по локальным и/или глобальным сетям.

Сетевые черви кроме вредоносных действий могут выполнять шпионскую функцию троянских программ.

Сетевые черви являются вредоносными программами, которые проникают на компьютер, используя сервисы компьютерных сетей. Активизация сетевого червя может вызвать уничтожение программ и данных, а также похищение персональных данных пользователя.

Web- черви

Отдельную категорию составляют черви, использующие для своего распространения Web-серверы.

Заражение происходит в 2 этапа:

- Червь проникает в компьютер-сервер и модифицирует Web – страницы сервера
- Затем червь «ждет» посетителей, которые запрашивают информацию с зараженного сервера (открывают в браузере зараженную Web-страницу), и таким образом проникает на другие компьютеры сети

Разновидность Web-червей являются скрипты – активные элементы (программы) на языках JavaScript или VBScript, которые могут содержаться в файлах Web-страниц.

Профилактическая защита от таких червей состоит в том, что в интернет браузере можно запретить получение активных элементов на локальный компьютер.

Более эффективны Web- антивирусные программы, которые включают межсетевой экран и модуль проверки скриптов на языках JavaScript и VBScript.

Межсетевой экран

Межсетевой экран или **сетевой экран** — комплекс аппаратных или программных средств, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов в соответствии с заданными правилами.

Основной задачей сетевого экрана является защита компьютерных сетей или отдельных узлов от несанкционированного доступа. Также сетевые экраны часто называют фильтрами, так как их основная задача — не пропускать (фильтровать) пакеты, не подходящие под критерии, определённые в конфигурации.

Почтовые черви

Почтовые черви для своего распространения используют электронную почту.

Червь либо отсылает свою копию в виде вложения в электронное письмо, либо отсылает ссылку на свой файл, расположенный на каком-либо сетевом ресурсе.

В первом случае код червя активизируется при открытии (запуске) зараженного вложения, во втором – при открытии ссылки на зараженный файл.

Лавинообразная цепная реакция распространения почтового червя базируется на том, что червь после заражения компьютера начинает рассылать себя по всем адресам электронной почты, которые имеются в адресной книге пользователя.

Профилактическая защита от почтовых червей состоит в том, что не рекомендуется открывать вложенные в почтовые сообщения файла, полученные из сомнительных источников.