Краткий справочник по вредоносным программам

Вредоносные программы

Вредоносные программы – это программы, наносящие вред данным и программам, хранящимся на компьютере.

За создание, использование и распространение вредоносных программ в России и большинстве стран предусмотрена уголовная ответственность

Типы вредоносных программ. Вредоносными программами являются программы, наносящие вред данным и программам, хранящимся на компьютере. Основными типами вредоносных программ являются:

- компьютерные вирусы;
- сетевые черви;
- троянские программы;
- программы показа рекламы (от англ. adware) и программы-шпионы, занимающиеся сбором персональной информации о компьютере и пользователе (от англ. spy-ware);
- хакерские утилиты.

Антивирусные программы.

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

Для поиска известных вирусов используются **сигнатуры**, т. е. некоторые постоянные последовательности двоичного кода, специфичные для этого конкретного вируса. Если антивирусная программа обнаружит такую последовательность в каком-либо файле, то файл считается зараженным вирусом и подлежит лечению.

Для поиска новых вирусов используются **алгоритмы эвристического сканирования**, т. е. анализ последовательности команд в проверяемом объекте. Если «подозрительная» последовательность команд обнаруживается, то антивирусная программа выдает сообщение о возможном заражении объекта.

Большинство антивирусных программ сочетает в себе функции постоянной защиты (**антивирусный монитор**) и функции защиты по требованию пользователя (**антивирусный сканер**).

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

вредоносных программ в оперативной памяти, а также на жестких и сетевых дисках компьютера.

Признаки заражения компьютера.

1. вывод на экран непредусмотренных сообщений или изображений;
2. подача непредусмотренных звуковых сигналов;
3. неожиданное открытие и закрытие лотка CD/DVD дисковода;
4. произвольный запуск на компьютере каких-либо программ;
5. частые «зависания» и сбои в работе компьютера;
6. медленная работа компьютера при запуске программ;
7. исчезновение или изменение файлов и папок;
8. частое обращение к жесткому диску (часто мигает лампочка на системном блоке);
9. «зависание» или неожиданное поведение браузера (например, окно программы невозможно закрыть).

Кроме того, есть некоторые характерные признаки поражения сетевым вирусом через электронную почту;

- друзья или знакомые говорят о полученных от вас сообщениях, которые вы не отправляли;
- в вашем почтовом ящике находится большое количество сообщений без обратного адреса и заголовка.

Действия при наличии признаков заражения компьютера.

1. Сохранить результаты работы на внешнем носителе (дискете, CD- или DVD-диске, флэш-карте и пр.).
2. Отключить компьютер от локальной сети и Интернета, если он к ним был подключен;
3. Если симптом заражения состоит в том, что невозможно загрузиться с жесткого диска компьютера (компьютер выдает ошибку, когда вы его включаете), попробовать загрузиться в режиме защиты от сбоев или с диска аварийной загрузки Windows;
4. Запустить антивирусную программу.

Компьютерные вирусы.

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

Классификация компьютерных вирусов:

- **неопасные**, влияние которых ограничивается уменьшением свободной памяти на диске, графическими, звуковыми и другими внешними эффектами;
- **опасные**, которые могут привести к сбоям и «зависаниям» при работе компьютера;
- **очень опасные**, активизация которых может привести к потере программ и данных (изменению или удалению файлов и каталогов), форматированию

винчестера и т. д.

По способу сохранения и исполнения своего кода вирусы можно разделить на **загрузочные, файловые, макро-вирусы и скрипт-вирусы**.

Загрузочные вирусы. Загрузочные вирусы заражают загрузочный сектор гибкого или жесткого 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.

Профилактическая защита от таких вирусов состоит в отказе от загрузки операционной системы с гибких дисков и установке в BIOS вашего компьютера защиты загрузочного сектора от изменений.

Файловые вирусы. Файловые вирусы различными способами внедряются в исполнимые файлы (командные файлы *.bat, программы *.exe, системные файлы *.com и *.sys, программные библиотеки *.dll и др.) 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.

По способу заражения файловые вирусы разделяют на:

- **перезаписывающие вирусы**, которые записывают свой код вместо кода программы, не изменяя названия исполнимого файла. При запуске программы выполняется код вируса, а не сама программа;
- **вирусы-компаньоны**, которые, как и перезаписывающие вирусы, создают свою копию на месте заражаемой программы, но в отличие от перезаписываемых, не уничтожают оригинальный файл, а переименовывают или перемещают его. При запуске программы вначале выполняется код вируса, а затем управление передается оригинальной программе;
- **паразитические вирусы** — это файловые вирусы, изменяющие содержимое файла, добавляя в него свой код. Код может внедряться в начало, середину или конец программы и выполняется перед, вместе или после программы. При этом зараженная программа сохраняет полную или частичную работоспособность.

Профилактическая защита от файловых вирусов состоит в том, что не рекомендуется запускать на исполнение файлы, полученные из сомнительного источника и предварительно не проверенные антивирусными программами.

Макро-вирусы. Наибольшее распространение получили макро-вирусы для интегрированного офисного приложения Microsoft Office (Word, Excel, PowerPoint и Access). Макро-вирусы фактически являются макрокомандами (макросами) на встроенном языке программирования Visual Basic for Applications (VBA), которые помещаются в документ.

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

Профилактическая защита от макро-вирусов состоит в предотвращении запуска вируса. При открытии документа в приложениях Microsoft Office сообщается о присутствии в них макросов (потенциальных вирусов) и предлагается запретить их загрузку. Выбор запрета на загрузку макросов надежно защитит ваш компьютер от заражения макро-вирусами, однако отключит и полезные макросы, содержащиеся в документе.

Скрипт-вирусы. Особой разновидностью вирусов являются активные элементы (программы) на языках JavaScript или VBScript, которые могут содержаться в файлах Web-страниц. Заражение локального компьютера происходит при их передаче по Всемирной паутине с серверов Интернета в браузер локального компьютера.

Профилактическая защита от скрипт-вирусов состоит в том, что в браузере можно запретить получение активных элементов на локальный компьютер.

Сетевые вирусы

К сетевым червям (от англ. worm) относятся вредоносные программы, распространяющие свои копии по локальным и/или глобальным сетям. Для своего распространения сетевые черви используют разнообразные сервисы глобальных и локальных компьютерных сетей: Всемирную паутину, электронную почту, интерактивное общение, файлообменные сети и т. д.

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

Почтовые черви. Почтовые черви для своего распространения используют электронную почту. Червь отсылает либо свою копию в виде вложения в электронное письмо, либо 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. В обоих случаях эффект одинаков — активизируется код червя. 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 файлы, полученные из сомнительных источников.

Черви, использующие «уязвимости» программного обеспечения. Червь ищет в сети компьютеры, на которых используются операционная система и приложения, содержащие критические уязвимости. Для заражения уязвимых компьютеров червь посылает специально оформленный сетевой пакет или запрос, в результате чего код (или часть кода) червя проникает на компьютер-жертву. Если сетевой пакет содержит только часть кода червя, он затем скачивает основной файл и запускает его на исполнение на зараженном компьютере.

Профилактическая защита от таких червей состоит в том, что рекомендуется своевременно скачивать из Интернета и устанавливать обновления системы безопасности операционной системы и приложений.

Черви, использующие файлообменные сети. Механизм работы подобных червей достаточно прост — для внедрения в файлообменную сеть червю достаточно скопировать себя в папку обмена файлами на одном из компьютеров. Всю остальную работу по распространению червя файлообменная сеть берет на себя — при поиске файлов в сети она сообщит удаленным пользователям о данном файле-черве и предоставит его для скачивания.

Сетевые черви кроме вредоносных действий, которыми обладают и классические компьютерные вирусы, могут выполнять шпионскую функцию троянских программ.

Троянские программы.

Троянская программа, троянец (от англ. trojan) — вредоносная программа, которая выполняет несанкционированную пользователем передачу управления компьютером удаленному пользователю, а также действия по удалению, модификации, сбору и пересылке информации третьим лицам.

Виды троянских программ.

Троянские утилиты удаленного администрирования. Троянские программы этого класса являются утилитами удаленного администрирования компьютеров в сети. Утилиты скрытого управления позволяют принимать или отсылать файлы, запускать и уничтожать их, выводить сообщения, стирать информацию, перезагружать компьютер и т. д.

Троянские программы данного типа являются одним из самых опасных видов вредоносного программного обеспечения, поскольку в них заложена возможность самых разнообразных злоумышленных действий, в том числе они могут быть использованы для обнаружения и передачи конфиденциальной информации.

Троянские программы, ворующие информацию. Такие троянские программы воруют различную информацию с зараженного компьютера. При запуске они ищут файлы, хранящие конфиденциальную информацию о пользователе (банковские реквизиты, пароли доступа к Интернету и др.) и отсылают ее по указанному в коде троянца электронному адресу или адресам.

Троянские программы — инсталляторы вредоносных программ. Троянские программы этого класса скрытно инсталлируют другие вредоносные программ и используются для «подсовывания» на компьютер-жертву вирусов или других троянских программ.

Троянские программы — шпионы. Данные троянцы осуществляют электронный шпионаж за пользователем зараженного компьютера: вводимая с клавиатуры информация, снимки экрана, список активных приложений и действия пользователя с ними сохраняются в каком-либо файле на диске и периодически отправляются злоумышленнику.

Троянские программы этого типа часто используются для кражи информации пользователей различных систем онлайновых платежей и банковских систем.

Рекламные и шпионские программы.

Рекламные программы. Рекламные программы (от англ. **Adware: Ad**vertisement — реклама и Soft**ware** — программное обеспечение) встраивают рекламу в основную полезную программу. Часто рекламные программы входят в состав официально поставляемых условно бесплатных версий программного обеспечения.

Шпионские программы. Шпионские программы (от англ. **Spyware**: **Spy** — шпион и Soft**ware** — программное обеспечение) скрытно собирают различную информацию о пользователе компьютера и затем отправляют ее злоумышленнику.

Куки (от англ. cookies — домашнее печенье) — небольшой текстовый файл, помещаемый Web-сервером на локальный компьютер пользователя.

Cookies применяются для сохранения данных, специфичных для данного пользователя. При вводе регистрационных данных файлы cookies помогают серверу упростить процесс сохранения персональных данных, связанных с текущим пользователем. Если пользователь Интернет-магазина ранее указывал адрес для доставки счетов или товара, вместо повторного ввода этих данных можно указать пароль, позволяющий автоматически заполнить соответствующие поля в форме заказа.

Спам.

Спам (от англ. spam) — это массовая автоматическая рассылка рекламных электронных сообщений, со скрытым или фальсифицированным обратным адресом. Спам распространяется по компьютерным сетям с использованием электронной почты и систем интерактивного общения (типа ICQ), а также по мобильным сетям с использованием службы SMS-сообщений.

Спам приходит потому, что электронный адрес получателя стал известен спамерам (рассылыцикам спама). Чаще всего владелец почтового ящика сам указывает электронный почтовый адрес при регистрации на каком-либо сайте и его обнаруживает специальный робот, «бродящий» по сайтам наподобие индексирующего робота поисковых систем.

Рекламный спам. Некоторые компании, занимающиеся легальным бизнесом, рекламируют свои товары или услуги с помощью спама. Они могут осуществлять его рассылку самостоятельно, но чаще заказывают ее тем компаниям (или лицам), которые на этом специализируются. Привлекательность такой рекламы заключается в ее сравнительно низкой стоимости и большом охвате потенциальных клиентов.

«Нигерийские письма». Иногда спам используется для того, чтобы выманить деньги у получателя письма. Наиболее распространенный способ получил название «нигерийские письма», потому что большое количество таких писем приходило из Нигерии. Такое письмо содержит сообщение о том, что получатель письма может получить большую сумму денег, а отправитель может ему в этом помочь. Затем отправитель письма

просит перевести ему немного денег под предлогом, например, оформления документов или открытия счета. Выманивание этой суммы и является целью мошенников.

Фишинг. Фишинг (от англ. fishing — рыбалка) — еще один способ мошенничества путем обмана пользователей. Он представляет собой попытку выманить у получателя письма данные, которые можно использовать для получения выгоды: номера его кредитных карточек или пароли доступа к системам онлайновых платежей. Такое письмо обычно маскируется под официальное сообщение от администрации банка.

Защита от спама.

Для борьбы со спамом используются антиспамовые фильтры, которые могут быть установлены как на локальных компьютерах пользователей, так и на почтовых серверах провайдеров. Антиспамовые фильтры анализируют содержание письма или пытаются опознать спамера по электронному адресу. Если письмо классифицировано как спам, оно может быть помечено, перемещено в другую папку или даже удалено.

Для затруднения автоматической фильтрации спамовые сообщения часто искажаются, вместо букв используются похожие по начертанию цифры, русские буквы заменяются на латинские, а в случайных местах добавляются пробелы.

Хакерские утилиты.

Сетевые атаки. Сетевые атаки на удаленные серверы реализуются с помощью специальных программ, которые посылают на них специфические запросы. Это приводит к отказу в обслуживании («зависанию» сервера), если ресурсы атакуемого сервера недостаточны для обработки всех поступающих запросов.

DoS-программы (от англ. Denial of Service — отказ в обслуживании) реализуют атаку с одного компьютера с ведома пользователя. DoS-программы обычно наносят ущерб удаленным компьютерам и сетям, не нарушая работоспособность зараженного компьютера.

DDoS-программы (от англ. Distributed DoS — распределенный DoS) реализуют распределенные атаки с разных компьютеров, причем без ведома пользователей зараженных компьютеров. Для этого DDoS-про грамма засылается на компьютеры «жертв-посредников» и после запуска в зависимости от текущей даты или по команде от **хакера** начинает сетевую атаку на указанный сервер в сети.

Утилиты «взлома» удаленных компьютеров. Утилиты «взлома» удаленных компьютеров предназначены для проникновения в удаленные компьютеры с целью дальнейшего управления ими (используя методы троянских программ типа утилит удаленного администрирования) или для внедрения во «взломанную» систему других вредоносных программ.

Руткиты. Руткит (от англ. root kit — «набор для получения прав root») — программа или набор программ для скрытного взятия под контроль «взломанной» системы.

В операционной системе Windows под rootkit принято подразумевать программу, которая внедряется в систему и перехватывает системные функции. Кроме того, как

правило, rootkit может маскировать присутствие в системе любых описанных в его конфигурации процессов, каталогов и файлов на диске, ключей в реестре. Многие rootkit устанавливают в систему свои драйверы и службы (они, естественно, также являются «невидимыми»).

Защита от хакерских атак и сетевых червей. Защита компьютерных сетей или отдельных компьютеров от несанкционированного доступа может осуществляться с помощью межсетевого экрана, или брандмауэра (от англ. firewall). Межсетевой экран может быть реализован как аппаратно, так и программно.

Межсетевой экран позволяет:

- блокировать хакерские DoS-атаки, не пропуская на защищаемый компьютер сетевые пакеты с определенных серверов (определенных IP-адресов или доменных имен);
- не допускать проникновение на защищаемый компьютер сетевых червей (почтовых, Web и др.);
- препятствовать троянским программам отправлять конфиденциальную информацию о пользователе и компьютере.