Виды компьютерных вирусов и антивирусов

Подготовил:
Дурнев Алексей
7,,А”

Содержание

Рекламные программы

Под рекламными и информационными программами понимаются такие программы, которые, помимо своей основной функции, также демонстрируют рекламные баннеры и всевозможные всплывающие окна с рекламой. Такие сообщения с рекламой порой бывает достаточно нелегко скрыть или отключить. Такие рекламные программы основываются при работе на поведение пользователей компьютера и являются достаточно проблемными по соображениям безопасности системы.



Бэкдоры (Backdoor)

Утилиты скрытого администрирования позволяют, обходя системы защиты, поставить компьютер установившего пользователя под свой контроль. Программа, которая работает в невидимом режиме, дает хакеру неограниченные права для управления системой. С помощью таких backdoor-программ можно получить доступ к персональным и личным данным пользователя. Нередко такие программы используются в целях заражения системы компьютерными вирусами и для скрытой установки вредоносных программ без ведома пользователя.



Загрузочные вирусы

Нередко главный загрузочный сектор вашего HDD поражается специальными загрузочными вирусами. Вирусы подобного типа заменяют информацию, которая необходима для беспрепятственного запуска системы. Одно из последствий действия таковой вредоносной программы это невозможность загрузки операционной системы…

Bot-сеть

Bot-сеть это полноценная сеть в Интернет, которая подлежит администрированию злоумышленником и состоящая из многих инфицированных компьютеров, которые взаимодействуют между собой. Контроль над такой сетью достигается с использованием вирусов или троянов, которые проникают в систему. При работе, вредоносные программы никак себя не проявляют, ожидая команды со стороны злоумышленника. Подобные сети применяются для рассылки СПАМ сообщений или для организации DDoS атак на нужные сервера. Что интересно, пользователи зараженных компьютеров могут совершенно не догадываться о происходящем в сети.



мистификация, шутка, обман)

Уже на протяжении нескольких лет многие пользователи сети Интернет получают электронные сообщения о вирусах, которые распространяются якобы посредством e-mail. Подобные предупреждения массово рассылаются со слезной просьбой отправить их всем контактам из вашего личного листа.

Ловушки

Honeypot (горшочек меда) – это сетевая служба, которая имеет задачу наблюдать за всей сетью и фиксировать атаки, при возникновении очага. Простой пользователь совершенно не догадывается о существовании такой службы. Если же хакер исследует и мониторит сеть на наличие брешей, то он может воспользоваться услугами, которые предлагает такая ловушка. При этом будет сделана запись в log-файлы, а также сработает автоматическая сигнализация.



Макровирусы

Макровирусы - это очень маленькие программы, которые написаны на макроязыке приложений. Такие программки распространяются только среди тех документов, которые созданы именно для этого приложения. Для активации таких вредоносных программ необходим запуск приложения, а также выполнение инфицированного файла-макроса. Отличие от обычных вирусов макросов в том, что заражение происходит документов приложения, а не запускаемых файлов приложения.

Фарминг

Фарминг - это скрытая манипуляция host-файлом браузера для того, чтобы направить пользователя на фальшивый сайт. Мошенники содержат у себя сервера больших объемов, на таких серверах хранятся большая база фальшивых интернет-страниц. При манипуляции host-файлом при помощи трояна или вируса вполне возможно манипулирование зараженной системой. В результате этого зараженная система будет загружать только фальшивые сайты, даже в том случае, если Вы правильно введете адрес в строке браузера.



Фишинг

Phishing дословно переводится как "выуживание" личной информации пользователя при нахождении в сети интернет. Злоумышленник при своих действиях отправляет потенциальной жертве электронное письмо, где указано, что необходимо выслать личную информацию для подтверждения. Нередко это имя и фамилия пользователя, необходимые пароли, PIN коды для доступа к счетам пользователя онлайн. С использованием таких похищенных данных, хакер вполне может выдать себя за другое лицо и осуществить любые действия от его имени.



Полиморфные вирусы

Полиморфные вирусы – это вирусы, использующие маскировку и перевоплощения в работе. В процессе они могут изменять свой программный код самостоятельно, а поэтому их очень сложно обнаружить, потому что сигнатура изменяется с течением времени.

Программные вирусы

Компьютерный вирус - это обычная программа, которая обладает самостоятельно прикрепляться к другим работающим программам, таким образом, поражая их работу. Вирусы самостоятельно распространяют свои копии, это значительно отличает их от троянских программ. Также отличие вируса от червя в том, что для работы вирусу нужна программа, к которой он может приписать свой код.



Руткит

Руткит – это определенный набор программных средств, который скрыто устанавливается в систему пользователя, обеспечивая при этом сокрытие личного логина киберпреступника и различных процессов, при этом делая копии данных.

Скрипт-вирусы и черви

Такие виды компьютерных вирусов достаточно просты для написания и распространяются в основном посредством электронной почты. Скриптовые вирусы используют скриптовые языки для работы чтобы добавлять себя к новым созданным скриптам или распространяться через функции операционной сети. Нередко заражение происходит по e-mail или в результате обмена файлами между пользователями. Червь это программа, которая размножается самостоятельно, но которая инфицирует при этом другие программы. Черви при размножении не могут стать частью других программ, что отличает их от обычных **видов компьютерных вирусов**.

Шпионское ПО

Шпионы могут переслать личные данные пользователя без его ведома третьим лицам. Шпионские программы при этом анализируют поведение пользователя в сети Интернет, а также, основываясь на собранных данных, демонстрируют пользователю рекламу или pop-up (всплывающие окна), которые непременно заинтересуют пользователя.



Троянские программы

Троянские программы это программы, которые должны выполнять определенные полезные функции, но после запуска таких программ выполняются действия другого характера (разрушительные). Трояны не могут размножаться самостоятельно, и это основное их отличие их от компьютерных вирусов.

Зомби

Зомби - это инфицированный компьютер, который инфицирован вредоносными программами. Такой компьютер позволяет хакерам удаленно администрировать систему и с помощью этого совершать различные нужные действия (DoS атаку, рассылка спама и т.п.).

Антивирус

Программа, созданная для защиты от вирусов.Если вирус будет скачен на компьютер, то антивирус его распознает и удалит.Так же можно сканировать компьютер и удалить файлы, предоставляющие угрозу.