Сетевые черви и защита от них

К сетевым червям относятся вредоносные программы, распространяющие свои копии по локальным или глобальным сетям. Для своего распространения сетевые черви используют разнообразные сервисы глобальных и локальных компьютерных сетей: Всемирную паутину, элек тронную почту и т. д.

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

Активизация сетевого червя может вызывать уничтожение программ и данных, а также похищение персональных данных пользователя.

Основным признаком, по которому типы червей различаются между собой, является способ распространения червя — как он передает свою копию на удаленные компьютеры. Однако многие сетевые черви используют более одного способа распространения своих копий по компьютерам ло кальных и глобальных сетей.

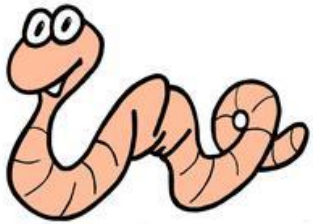
Web черви

Заражение происходит в два этапа. Сначала червь проникает в компьютер-сервер и модифицирует Web-страницы сервера. Затем червь «ждет» посетителей, которые запрашивают информацию с зараженного сервера (например, открывают в браузере зараженную Web-страницу), и таким образом проникает на другие компьютеры сети.

Разновидностью Web-червей являются скрипты — 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 таких червей состоит в том, что в браузере можно запретить получение активных элементов на локальный компьютер.

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

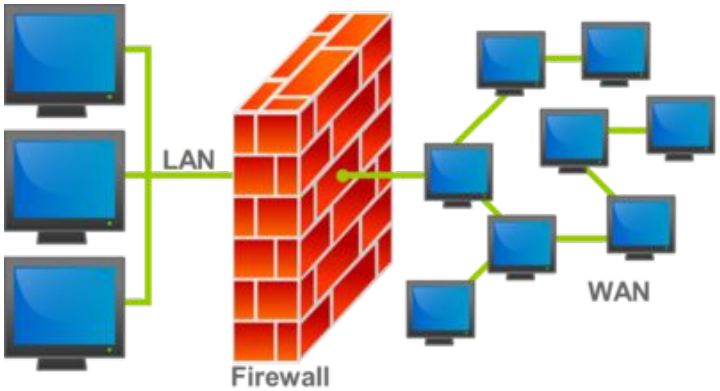


Межсетевой экран

Межсетевой экран — это программное или аппаратное обеспечение, которое проверяет информацию, входящую в компьютер из локальной сети или Интернета, а затем либо отклоняет ее, либо пропускает в компьютер, в зависимости от параметров брандмауэра.

Межсетевой экран обеспечивает проверку всех Web-страниц, поступающих на компьютер пользователя. Каждая Web-страница перехватывается и анализируется межсетевым экраном на присутствие вредоносного кода. Распознавание вредоносных программ происходит на основании баз, используемых в работе межсетевого экрана, и с помощью эвристического алгоритма.

Если Web-страница, к которой обращается пользователь, содержит вредоносный код, доступ к нему блокируется.



Проверка скриптов в браузере

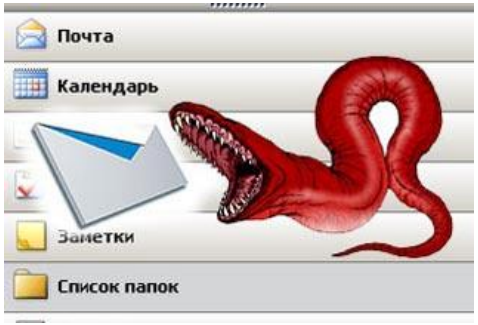
- Каждый запускаемый на Web-странице скрипт перехватывается модулем проверки скриптов и анализируется на присутствие вредоносного кода;
- Если скрипт содержит вредоносный код, модуль проверки скриптов блокирует его, уведомляя пользователя специальным всплывающим сообщением;
- Если в скрипте не обнаружено вредоносного кода, он выполняется.

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. 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



Вопросы

1. 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.

2. Web черви, почтовые черви

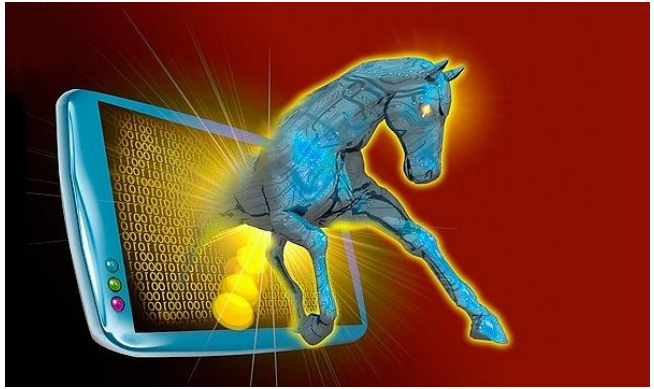
Троянские программы и защита от них

Троянская программа

Троянская программа — вредоносная программа, которая выполняет несанкционированную пользователем передачу управления компьютером удаленному пользователю, а также действия по удалению, модификации, сбору и пересылке информации третьим лицам. Они различаются между собой по тем действиям, которые они производят на зараженном компьютере.

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. При запуске троянец устанавливает себя в системе и затем следит за ней, при этом пользователю не выдается никаких сообщений о действиях троянской программы в системе. В результате «пользователь» этой троянской программы может и не знать о ее присутствии в системе, в то время как его компьютер открыт для удаленного управления.



Троянские программы-шпионы

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.

При запуске троянец устанавливает себя в системе и затем следит за ней, при этом пользователю не выдается никаких сообщений о действиях троянской программы в системе. В результате «пользователь» этой троянской программы может и не знать о ее присутствии в системе, в то время как его компьютер открыт для удаленного управления.

Рекламные программы

Рекламные программы. Рекламные программы встраивают рекламу в основную полезную про грамму и могут выполнять функцию троянских программ. Рекламные программы могут скрытно собирать различную информацию о пользователе компьютера и затем отправлять ее злоумышленнику.

Вопросы

Троянская программа - программа, которая выполняет несанкционированную пользователем передачу управления компьютером удаленному пользователю, а также действия по удалению, модификации, сбору и пересылке информации третьим лицам.

Хакерские утилиты и защита от них

Сетевые атаки

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

DoS-программы реализуют атаку с одного компьютера с ведома пользователя. DoS-программы обычно наносят ущерб удаленным компьютерам и сетям, не нарушая работоспособности зараженного компьютера.

DDoS-программы реализуют распределенные атаки с разных компьютеров, причем без ведома пользователей зараженных компьютеров. Для этого DDoS-программа 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.

Некоторые хакерские утилиты реализуют фатальные сетевые атаки. Такие утилиты используют уязвимости в операционных системах и приложениях и отправляют специально оформленные запросы на атакуемые компьютеры в сети. В результате сетевой запрос специального вида вызывает критическую ошибку в атакуемом приложении, и система прекращает работу.

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.

Утилиты взлома удаленных компьютеров обычно используют уязвимости в операционных системах или приложениях, установленных на атакуемом компьютере. Профилактическая защита от таких хакерских утилит состоит в своевременной загрузке из Интернета обновлений системы безопасности операционной системы и приложений.

Руткиты

Руткит — программа или набор программ для скрытого взятия под контроль взломанной системы. Это утилиты, используемые для сокрытия вредоносной активности. Они маскируют вредоносные программы, чтобы избежать их обнаружения антивирусными программами. Руткиты модифицируют операционную систему на компьютере и заменяют основные ее функции, чтобы скрыть свое со бственное присутствие и действия, которые предпринимает злоумышленник на зараженном компьютере.

Защита от хакерских атак,сетевых червей и троянских программ

Защита компьютерных сетей или отдельных компьютеров от несанкционированного доступа может осуществляться с помощью межсетевого экрана. Межсетевой экран позволяет:

1)блокировать хакерские DoS-атаки, не пропуская на защищаемый компьютер сетевые пакеты с определенных серверов (определенных IP-адресов или доменных имен);

2)не допускать проникновение на защищаемый компьютер сетевых червей (почтовых, Web и др.);

3)препятствовать троянским программам отправлять конфиденциальную информацию о пользователе и компьютере.

Вопросы

1. Сетевые атаки: DoS-программы,DDoS-программы

Утилиты взлома удаленных компьютеров.

Утилиты взлома удаленных компьютеров обычно используют уязвимости в операционных системах или приложениях, установленных на атакуемом компьютере. Профилактическая защита от таких хакерских утилит состоит в своевременной загрузке из Интернета обновлений системы безопасности операционной системы и приложений.

Защита компьютерных сетей или отдельных компьютеров от несанкционированного доступа может осуществляться с помощью межсетевого экрана

2.Руткит -программа или набор программ для скрытого взятия под контроль взломанной системы. Это утилиты, используемые для сокрытия вредоносной активности. Они маскируют вредоносные программы, чтобы избежать их обнаружения антивирусными программами