Презентация подготовлена для конкурса «Интернешка»
http://interneshka.org

Компьютерные вирусы
Антивирусные программ

Автор: Просянок Богдан, 6А класс, МБОУ СОШ №5 пгт Печенга, Мурманская обл.

Виды компьютерных вирусов

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.

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.

Виды компьютерных вирусов

Загрузочные вирусы

Нередко главный загрузочный сектор вашего HDD поражается специальными загрузочными вирусами. Вирусы подобного типа заменяют информацию, которая необходима для беспрепятственного запуска 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.

Виды компьютерных вирусов

Эксплойт

Эксплойт (дословно брешь в безопасности) – это такой скрипт или программа, которые используют специфические дырки и уязвимости ОС или какой-либо программы. Подобным образом в систему проникают программы, с использованием которых могут быть получены права доступа администратора.

Ноах (дословно шутка, ложь, 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.

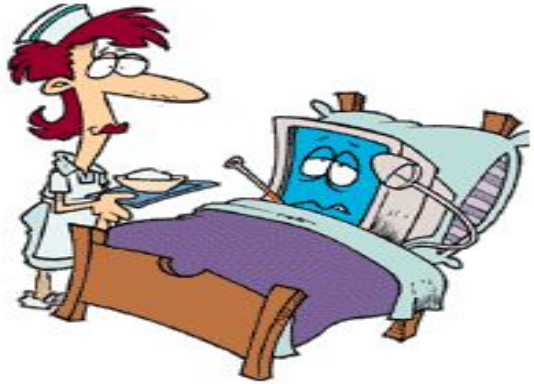
Виды компьютерных вирусов

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. Отличие от обычных вирусов макросов в том, что заражение происходит документов приложения, а не запускаемых файлов приложения.



Виды компьютерных вирусов

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.

Виды компьютерных вирусов

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.

Виды компьютерных вирусов

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**.

Виды 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.

Виды 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.).

Как определить, что на компьютере появились вирусы?

1. компьютер выдает сообщения, не относящиеся к работе ни одной из установленных программ;
2. самопроизвольно открываются окна рекламного или непристойного содержания;
3. компьютер издает непредусмотренные звуковые сигналы;
4. изменяется исходное назначение какого-либо действия на деструктивное (замена домашней страницы в браузере, изменение названий папок и документов);
5. нет доступа к вашими файлам по неизвестным вам причинам;
6. открывается и закрывается, без вашего участия, лоток CD-ROM устройства;
7. выдача брандмауэром (при его наличии на компьютере) сообщений с предупреждением о попытках выхода в Интернет неопознанных программ;
8. наличие в вашем почтовом ящике сообщений без обратного адреса и заголовка;
9. ваши знакомые рассказывают вам об отправленных вами письмах или сообщениях в ICQ, которые вы не отправляли;
10. в работе компьютера возникают частые сбои.

Как могло произойти заражение компьютера?

1. вы открыли письмо от неизвестного вам адресата,
2. вы запустили программу с неизвестного сайта или программу, вложенную вам в письмо,
3. вы открыли фотографию прекрасной девушки/мужчины, которая(ый) якобы хочет с вами познакомиться,
4. вы обнаружили на своей флэшке непонятный новый файл и, не задумываясь, попытались его открыть.

Антивирусная программа

Главную роль в защите компьютера играет не антивирусная программа, а сам пользователь – его рассудительность, внимательность и здравый смысл.

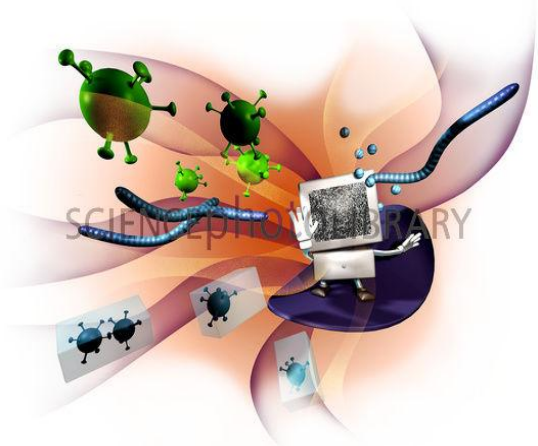
Прежде чем открыть файл или письмо — подумайте, а не пытаются ли вас обмануть? Послание от незнакомого человека со словами типа «Я нашёл интересную игру, посмотри!», безусловно, должно вас насторожить.

Как свести риск заражения вирусами к минимуму?

1. На вашем компьютере должна быть обязательно установлена антивирусная программа известного производителя (например, Dr.Web, Касперский, NOD32, Avira, Avast и т.п.)
2. Антивирусная программа всегда должна быть в актуальном состоянии: обычно программы сами следят за обновлениями своих компонентов, но нелишне время от времени и самому убеждаться в «свежести» антивирусных баз и программных модулей.
3. Ваша операционная система должна автоматически обновляться! Windows без обновлений подвергается большему риску заражения вирусами – поэтому, если система предупреждает вас о том, что автоматическое обновление по какой-либо причине не происходит, необходимо выполнить все рекомендованные действия, а если это не поможет – обратиться к специалисту.

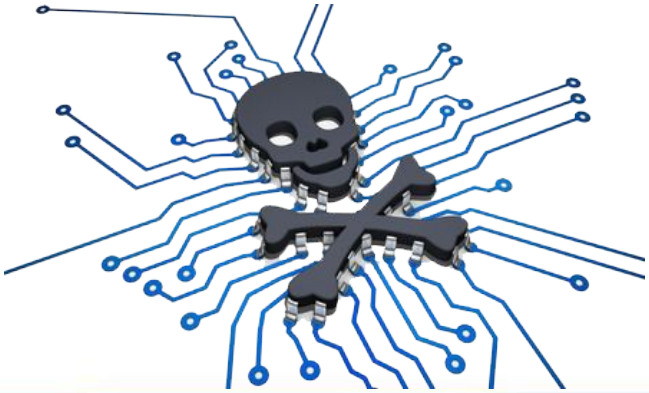
Что делать, если ваш компьютер заражен вирусом?

1. Если на вашем компьютере установлена постоянная антивирусная программа, обязательно обновите ее вирусную базу. После обновления вирусной базы поставьте ваш компьютер на полную проверку и удалите все зараженные объекты, которые антивирус не смог обнаружить ранее. По окончании перезагрузите компьютер.
2. Если на вашем компьютере не установлен постоянный антивирус, вам нужно его установить (рекомендуется использовать программы известных производителей - Dr.Web, Касперский lab., NOD32, AntiVir и т.п.), обязательно обновить его вирусную базу и сделать полную проверку вашего компьютера.



Что делать, если ваш компьютер заражен вирусом?

1. Лучше всего делать проверку в так называемом *«Безопасном режиме»*. Перезагрузите компьютер и перед тем, как у вас появится заставка с загрузкой Windows, нажмите F8, после чего Windows спросит, какой режим загрузки вы предпочитаете, — вам нужно выбрать Безопасный режим (англ. Safe Mode). После того как антивирус проверит весь ваш компьютер, вылечит/удалит зараженные файлы, вы можете перезагрузиться в Нормальный режим (просто сделайте перезагрузку системы еще раз).
2. Для однократной проверки и лечения вашего компьютера от вирусов вы можете загрузить с сайта RiNet (доступ к сайту открыт даже в том случае, если услуга доступа в Интернет заблокирована) антивирусную утилиту CureIt! от компании Dr.Web. При обнаружении вирусов удалите зараженные объекты и перезагрузите компьютер.



Незаконный доступ к вашему компьютеру

Еще одна опасность сети - так называемые хакеры.

С развитием сети Интернет информация становится все более и более доступной. В настоящее время даже технически не образованный человек, посетив один из тысяч хакерских сайтов, может попытаться получить доступ к вашему компьютеру.

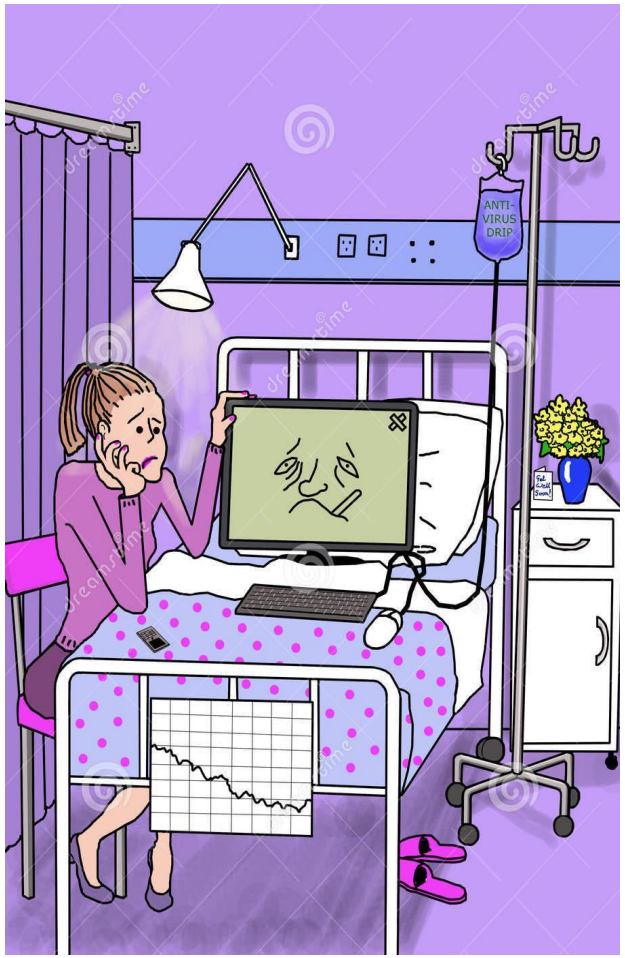
Часто услугами хакеров пользуются фирмы, занимающиеся спамерской деятельностью - незаконной массовой рассылкой рекламы по электронным адресам. Ваш «взломанный» хакером компьютер превращается в сервер, рассылающий спам. Как правило интернет-провайдеры блокируют доступ в сеть абонентам, с чьих компьютеров поступает зловредный трафик.

Некоторые правила по обеспечению вашей сетевой безопасности:

1. Ваша операционная система должна быть в актуальном состоянии, если ваша ОС не поддерживается обновлениями, вы используете ее на свой страх и риск.

2. Если вам не хочется обновлять ОС, пользуйтесь функцией «Только критические обновления и патчи безопасности».

3. Установите себе программу Firewall (он же брандмауэр) стороннего производителя, а не входящий в поставку ОС Windows (кстати, Firewall поможет вам и в борьбе с вирусами).



Спасибо за внимание!