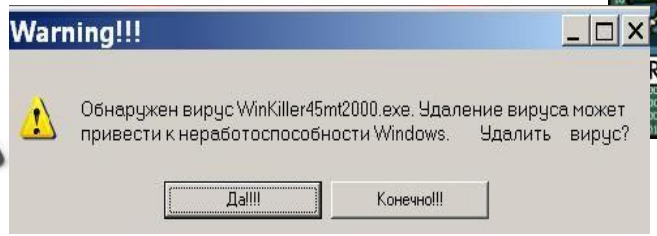
Презентация подготовлена для конкурса «Интернешка»
http://interneshka.org

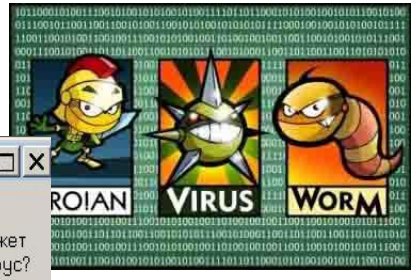
Компьютерные вирусы. Антивирусные программы

Автор: Василенко Александр, 9 класс,
Руководитель: Александрова З.В., учитель физики и информатики
МБОУ СОШ №5 пгт Печенга, Мурманская область

Что же такое компьютерный вирус?

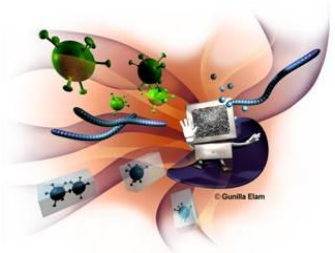
По сути своей это разновидность компьютерных программ. То есть вирус – это обычно небольшая программа, которая предназначена для осуществления каких либо действий.
Вирус может причинить вред хранящейся на компьютере информации просто удалив или подпортив ее. Либо он будет собирать ваши конфиденциальные данные (адреса электронной почты, логины и пароли, платежные данные, например, номера банковских карт и т.д.), а затем переправлять эту информацию своему разработчику. Также вирус может просто открыть доступ к вашему компьютеру для своего хозяина и уж сам разработчик вируса будет решать что делать с вашим компьютером и хранящейся на нем информацией.





Признаки заражения компьютера

- на экран выводятся непредусмотренные сообщения, изображения и звуковые сигналы;
- неожиданно открывается и закрывается лоток CD-ROM-устройства;
- произвольно, без Вашего участия, на вашем компьютере запускаются какие-либо программы;
- на экран выводятся предупреждения о попытке какой-либо из программ вашего компьютера выйти в интернет, хотя Вы никак не инициировали такое ее поведение$вам о сообщениях от вас, которые вы не отправляли;
- в вашем почтовом ящике находится большое количество сообщений без обратного адреса и заголовка.



Косвенные признаки заражения компьютера

- частые зависания и сбои в работе компьютера;
- медленная работа компьютера при запуске программ;
- невозможность загрузки операционной системы;
- исчезновение файлов и каталогов или искажение их содержимого;
- частое обращение к жесткому диску (часто мигает лампочка на системном блоке);
- Microsoft Internet Explorer «зависает» или ведет себя неожиданным образом (например, окно программы невозможно закрыть).



В 90% случаев наличие косвенных симптомов вызвано сбоем в аппаратном или программном обеспечении. Несмотря на то, что подобные симптомы с малой вероятностью свидетельствуют о заражении.

Классы вредоносных программ

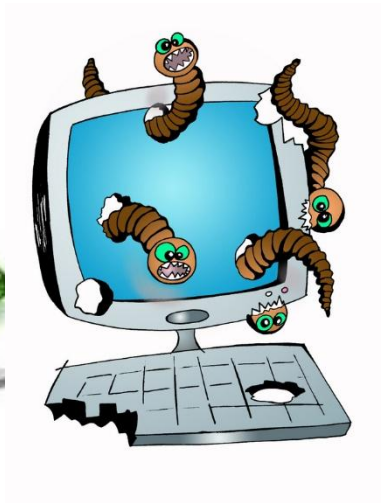
- Вирусы (Viruses)
- Черви (Worms)
- Троянские программы (Trojans)
- Программы-шпионы
- Фишинг (Phishing)
- Программы-рекламы (Adware)
- Потенциально опасные приложения (Riskware)
- Программы-шутки (Jokes)
- Программы-маскировщики (Rootkit)
- Прочие опасные программы
- Спам (Spam)

Классы вредоносных программ

Вирусы (Viruses): программы, которые заражают другие программы – добавляют в них свой код, чтобы получить управление при запуске зараженных файлов. Это простое определение дает возможность выявить основное действие, выполняемое вирусом – заражение. Скорость распространения вирусов несколько ниже, чем у червей.

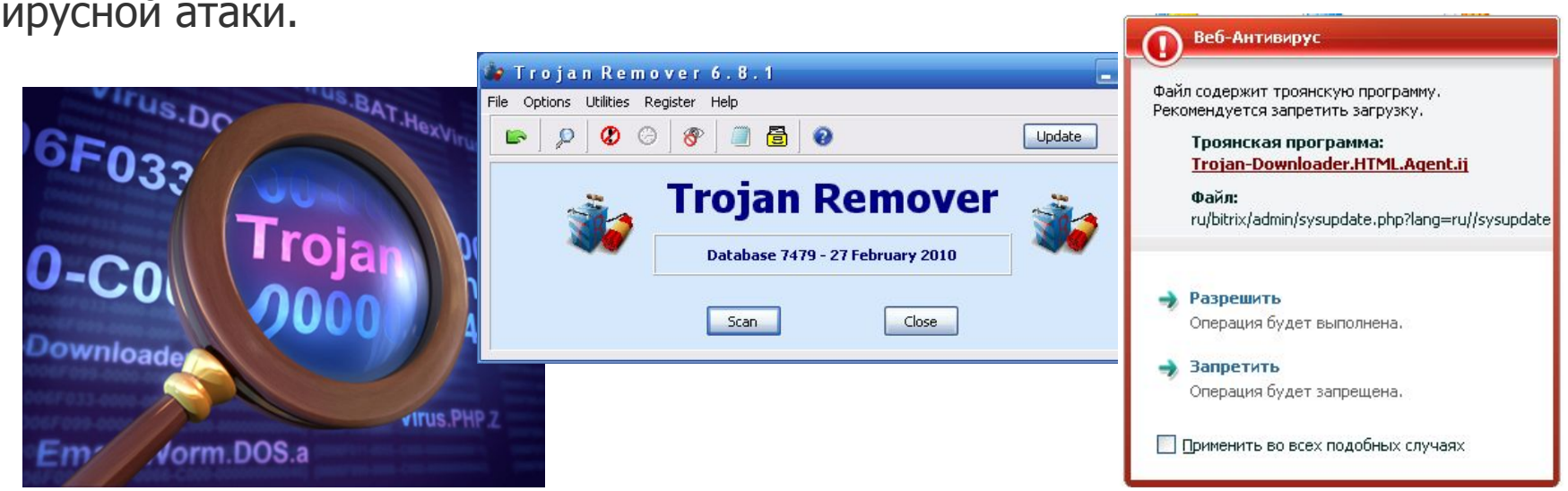
Классы вредоносных программ

Черви (Worms): данная категория вредоносных программ для распространения использует сетевые ресурсы. Название этого класса было дано исходя из способности червей "переползать" с компьютера на компьютер, используя сети, электронную почту и другие информационные каналы. Также благодаря этому черви обладают исключительно высокой скоростью распространения. Черви проникают на компьютер, вычисляют сетевые адреса других компьютеров и рассылают по этим адресам свои копии. Помимо сетевых адресов часто используются данные адресной книги почтовых клиентов. Представители этого класса вредоносных программ иногда создают рабочие файлы на дисках системы, но могут вообще не обращаться к ресурсам компьютера (за исключением оперативной памяти).



Классы вредоносных программ

Троянские программы (Trojans): программы, которые выполняют на поражаемых компьютерах несанкционированные пользователем действия, т.е. в зависимости от каких-либо условий уничтожают информацию на дисках, приводят систему к "зависанию", воруют конфиденциальную информацию и т.д. Данный класс вредоносных программ не является вирусом в традиционном понимании этог термина (т.е. не заражает другие программы или данные); троянские программы н способны самостоятельно проникать на компьютеры и распространяются злоумышленниками под видом "полезного" программного обеспечения. При этом вред, наносимый ими, может во много раз превышать потери от традиционной вирусной атаки.



Классы вредоносных программ

Программы-шпионы: программное обеспечение, позволяющее собирать сведения об отдельно взятом пользователе или организации без их ведома. О наличии программ-шпионов на своем компьютере вы можете и не догадываться. Как правило, целью программ-шпионов является:

- отслеживание действий пользователя на компьютере;
- сбор информации о содержании жесткого диска; сбор информации о качестве связи, способе подключения, скорости модема и т.д.

Однако данные программы не ограничиваются только сбором информации, они представляют реальную угрозу безопасности. Наверняка вы встречались с подобными программами, если при запросе одного адреса веб-сайта открывался совсем другой.

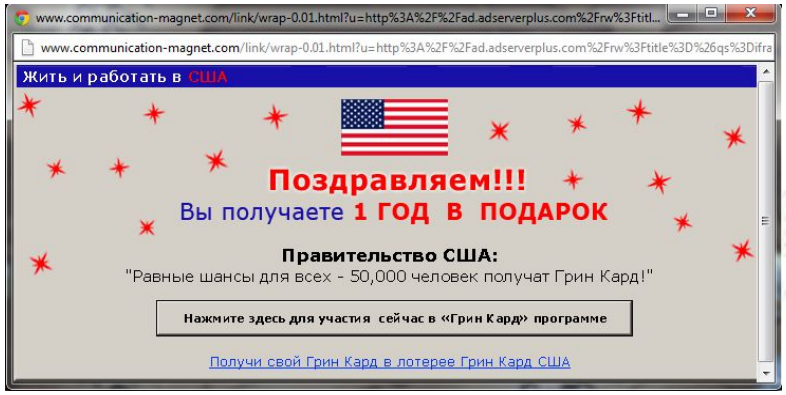
Одной из разновидностей программ-шпионов являются фишинг-рассылки.

Классы вредоносных программ

Фишинг (Phishing) – почтовая рассылка, целью которой является получение от пользователя конфиденциальной информации как правило финансового характера. Такие письма составляются таким образом, чтобы максимально походить на информационные письма от банковских структур, компаний известных брендов. Письма содержат ссылку на заведомо ложный сайт, где пользователю предлагается ввести, например, номер своей кредитной карты и другую конфиденциальную информацию.

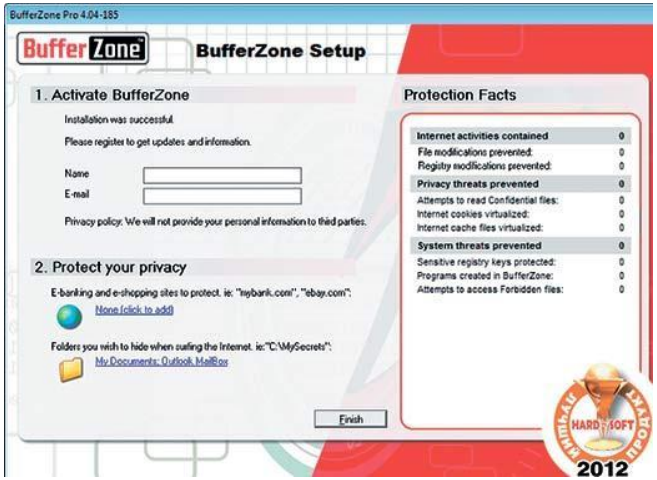
Классы вредоносных программ

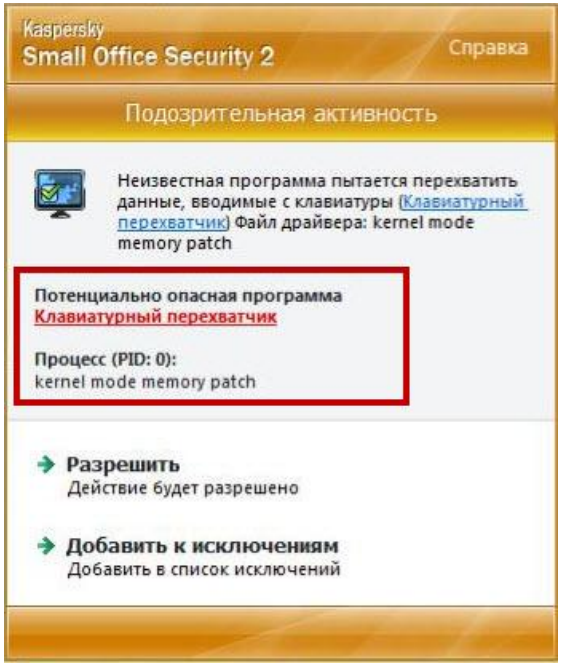
Программы-рекламы (Adware): программный код, без ведома пользователя включенный в программное обеспечение с целью демонстрации рекламных объявлений. Как правило, программы-рекламы встроены в программное обеспечение, распространяющееся бесплатно. Реклама располагается в рабочем интерфейсе. Зачастую данные программы также собирают и переправляют своему разработчику персональную информацию о пользователе.



Классы вредоносных программ

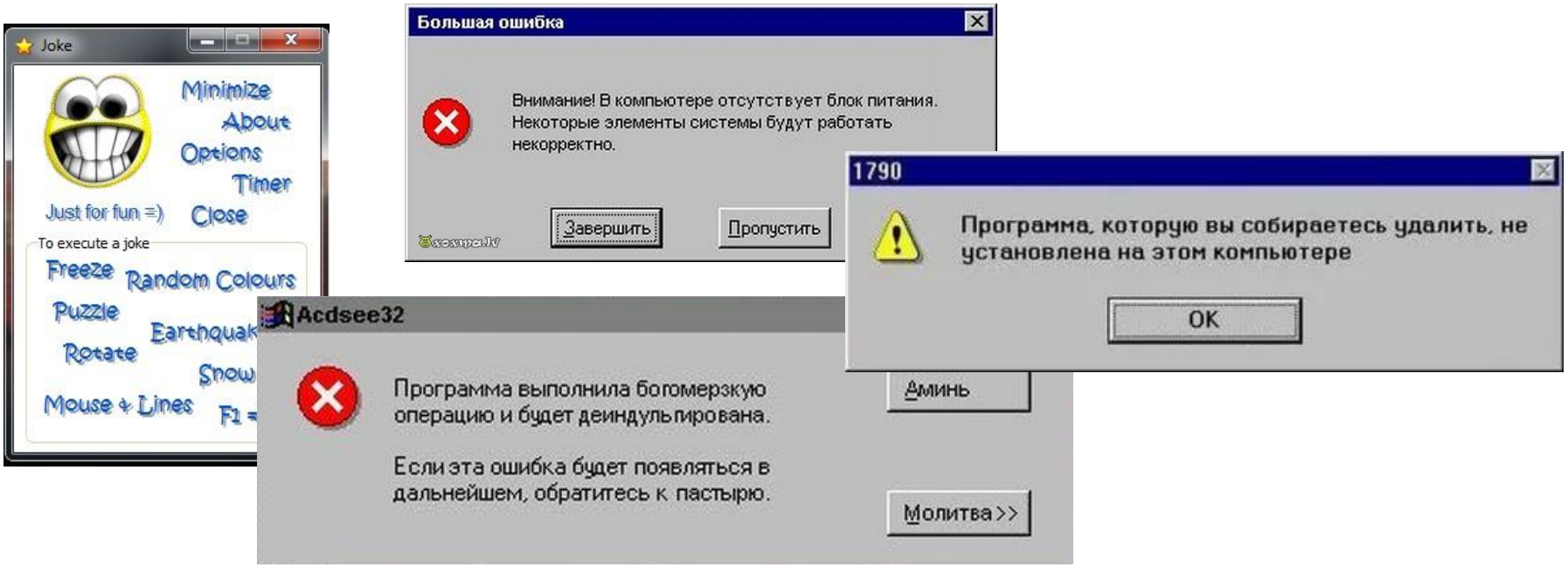
Потенциально опасные приложения (Riskware): программное обеспечение, не являющееся вирусом, но содержащее в себе потенциальную угрозу. При некоторых условиях наличие таких программ на компьютере подвергает ваши данные риску. К таким программам относятся утилиты удаленного администрирования, программы автоматического дозвона на платные ресурсы интернета с использованием Dial Up-соединения и другие.





Классы вредоносных программ

Программы-шутки (Jokes): программное обеспечение, не причиняющее компьютеру какого-либо прямого вреда, но выводящее сообщения о том, что такой вред уже причинен, либо будет причинен при каких-либо условиях. Такие программы часто предупреждают пользователя о несуществующей опасности, например, выводят сообщения о форматировании диска (хотя никакого форматирования на самом деле не происходит), обнаруживают вирусы в незараженных файлах и т.д.

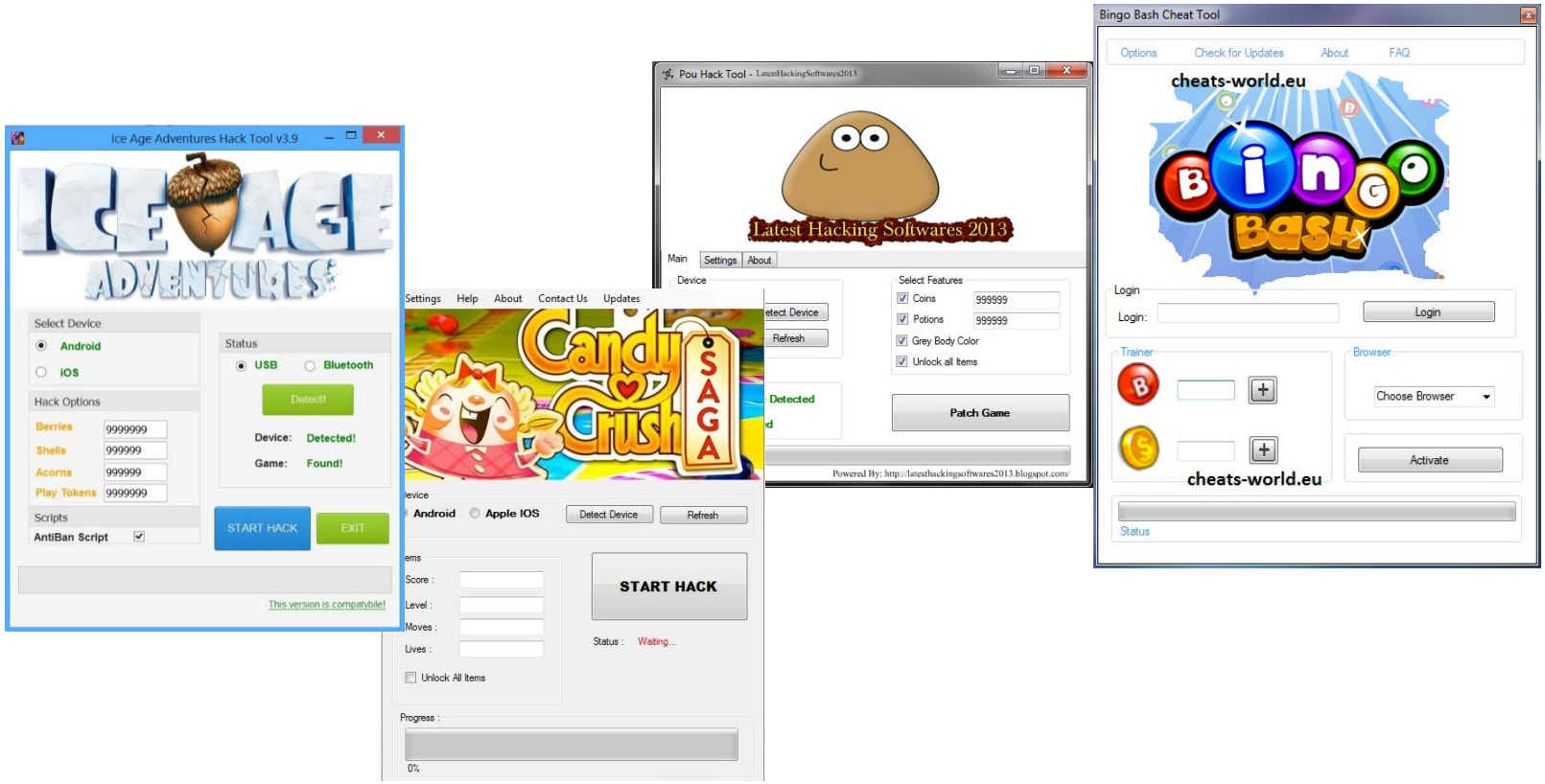


Классы вредоносных программ

Программы-маскировщики (Rootkit): это утилиты, используемые для сокрытия вредоносной активности. Они маскируют вредоносные программы, чтобы избежать их обнаружения антивирусными программами. Rootkit'ы также могут модифицировать операционную систему на компьютере и заменять основные ее функции, чтобы скрыть свое собственное присутствие и действия, которые предпринимает злоумышленник на зараженном компьютере.

Классы вредоносных программ

Прочие опасные программы: разнообразные программы, которые разработаны для создания других вредоносных программ, организации DoS-атак на удаленные сервера, взлома других компьютеров и т. п. К таким программам относятся хакерские утилиты (Hack Tools), конструкторы вирусов и т.д.



Классы вредоносных программ

Спам (Spam): анонимная, массовая почтовая корреспонденция нежелательного характера. Так, спамом являются рассылки политического и агитационного характера, письма, призывающие помочь кому-нибудь.

Отдельную категорию спама составляют письма с предложениями обналичить большую сумму денег или вовлекающие в финансовые пирамиды, а также письма, направленные на кражу паролей и номеров кредитных карт, письма с просьбой переслать знакомым (например, письма счастья) и т. п.

Спам существенно повышает нагрузку на почтовые сервера и повышает риск потери информации, важной для пользователя.

Основные источники проникновения угроз на компьютер

Среди источников проникновения вредоносных программ наиболее опасными являются:

1. **Интернет**
2. **Электронная почта**
3. **Уязвимости в программном обеспечении**
4. **Внешние носители информации**
5. **Пользователи**

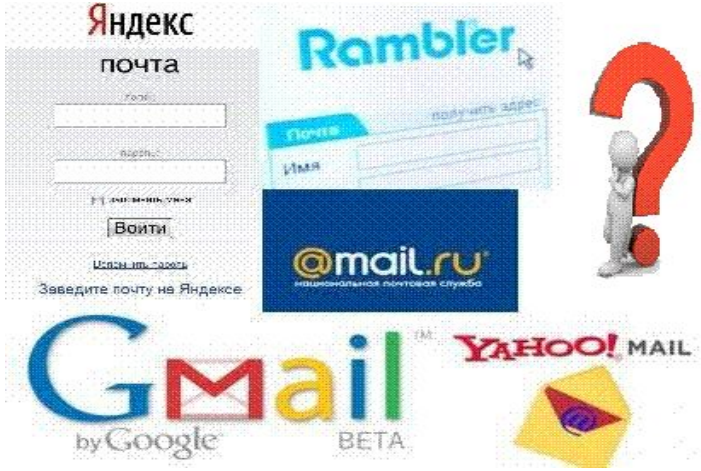
Интернет

Глобальная информационная сеть является основным источником распространения любого рода вредоносных программ. Зловредное ПО может попасть на компьютер при следующих действиях пользователя:

- при посещении сайта, содержащего зловредный код. Примером могут являться drive-by атаки. При drive-by атаках злоумышленники используют наборы эксплойтов, которые могут быть нацелены на уязвимости веб-браузера, его плагины, уязвимости элементов управления ActiveX или бреши в защите стороннего ПО.
- при скачивании с сайтов зловредного ПО, маскирующегося под кейгены, крэки, патчи и т.д.
- при скачивании через peer-to-peer сеть (например, торренты).

Электронная почта

Почтовые сообщения, поступающие в почтовый ящик пользователя и хранящиеся в почтовых базах, могут содержать в себе вирусы. Вредоносные программы могут находиться как во вложении письма, так и в его теле. При открытии письма, при сохранении на диск вложенного в письмо файла вы можете заразить данные на вашем компьютере. Также почтовая корреспонденция может стать источником еще двух угроз: спама и фишинга. Если спам влечет за собой в основном потерю времени, то целью фишинг-писем является ваша конфиденциальная информация (например, номер кредитной карты).



Уязвимости в программном обеспечении

Так называемые «дыры» (эксплойты) в программном обеспечении являются основным источником хакерских атак. Уязвимости позволяют получить хакеру удаленный доступ к вашему компьютеру, а, следовательно, к вашим данным, к доступным вам ресурсам локальной сети, к другим источникам информации.

Рекомендации по составлению надежных паролей

При составлении паролей рекомендуется придерживаться следующих правил:

- Пароль должен содержать не менее шести символов.
- В состав пароля могут входить цифры, латинские буквы, пробелы и специальные символы («.», «,», «?», «!», «<», «>». «”» и др.).
- Рекомендуется составлять пароль из смешанного набора цифровых и буквенных (прописных и строчных) символов.

Не используйте в качестве пароля:

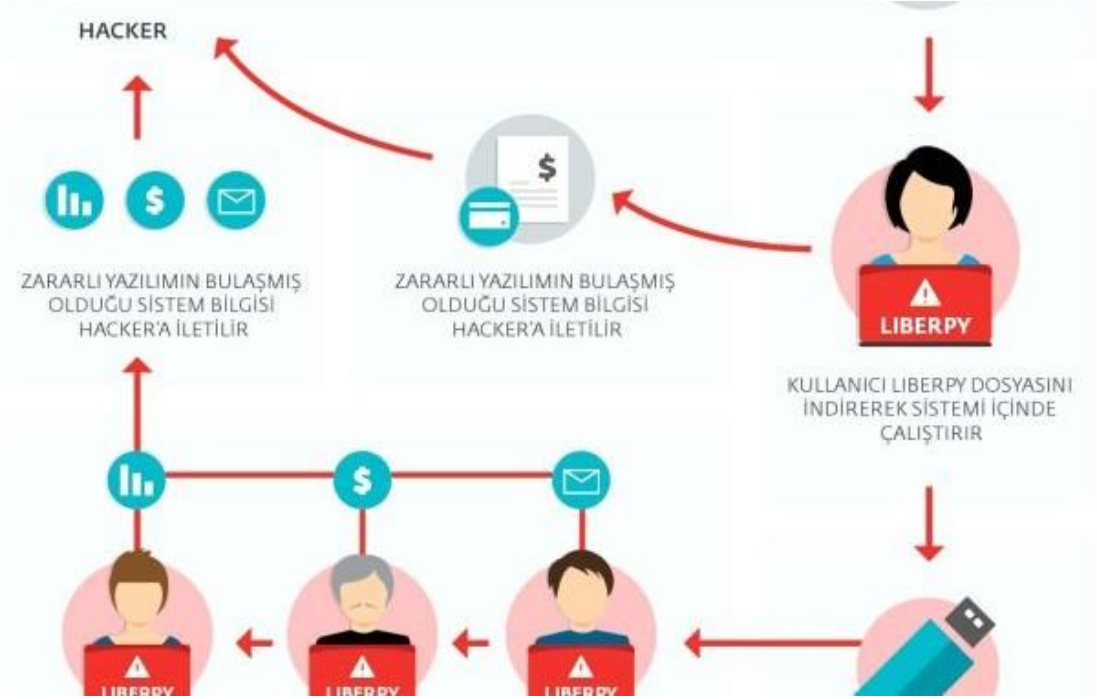
- Общеупотребительные слова и устойчивые словосочетания.
- Наборы символов, представляющие собой комбинации клавиш, расположенных подряд на клавиатуре, такие как: qwerty, 123456789, qazxsw и т. п.
- Персональные данные: имена и фамилии, адреса, номера паспортов, страховых свидетельств и т. п., пароли, созданные для доступа к другим программам (электронная почта, базы данных и пр.).

Внешние носители информации

Для передачи информации по-прежнему широко используются съемные диски, карты расширения памяти (флеш), а также сетевые папки. Запуская какой-либо файл, расположенный на внешнем носителе, вы можете поразить данные на вашем компьютере вирусом и, незаметно для себя, распространить вирус на диски вашего компьютера.

Пользователи

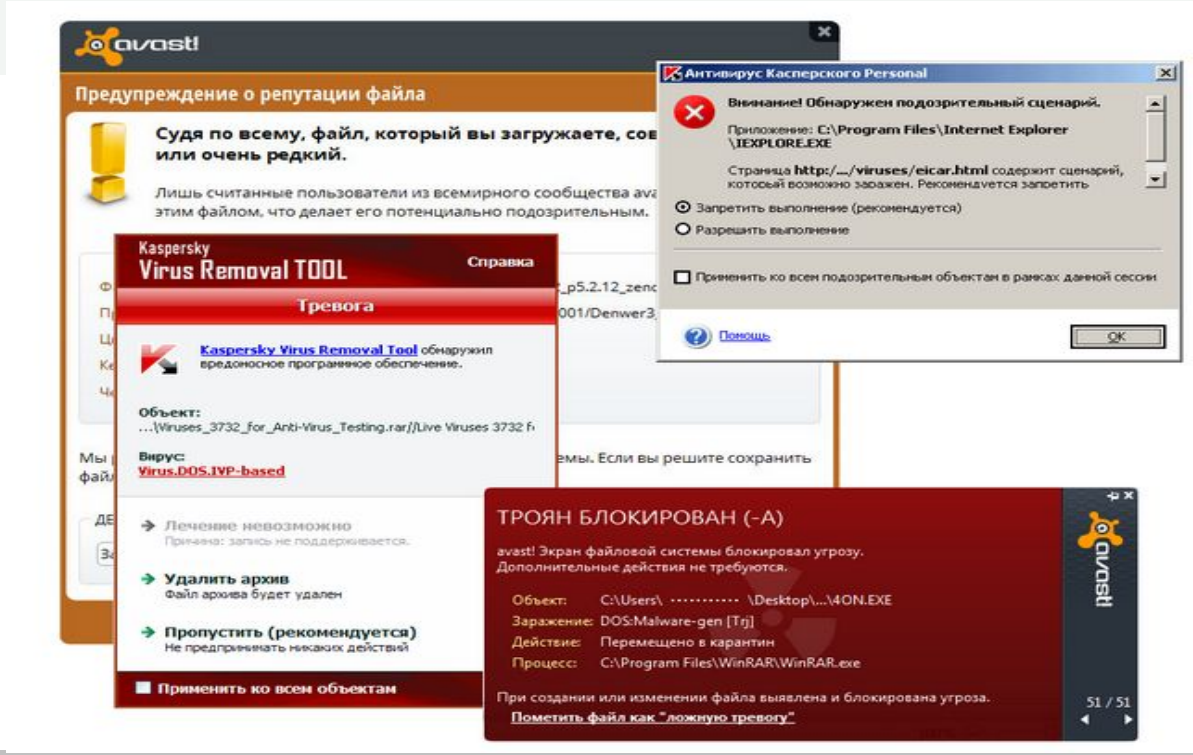
Доверчивые пользователи сами устанавливают безобидные на первый взгляд программы, заражая таким образом свой компьютер. Этот метод называется социальной инженерией – вирусописатели добиваются того, чтобы жертва сама установила зловредное ПО при помощи различных уловок.



Как исключить возможность заражения

Чтобы исключить вероятность заражения компьютера, установите пробную версию одного из продуктов: Internet Security, Kaspersky Total Security. После установки программы обновите антивирусные базы и запустите полную проверку компьютера.

Для проверки компьютера специалисты **Лаборатории Касперского** также рекомендуют использовать бесплатную утилиту Kaspersky Virus Removal Tool 2015.



Спасибо за внимание!

http://support.kaspersky.ru/viruses/common