О безопасности

По материалам сайтов антивирусной системы Касперского и Лиги безопасного интернета

Кто и почему создает вредоносные программы?

- Студенты и школьники, которые хотели попробовать свои силы, но не смогли найти для них более достойного применения.

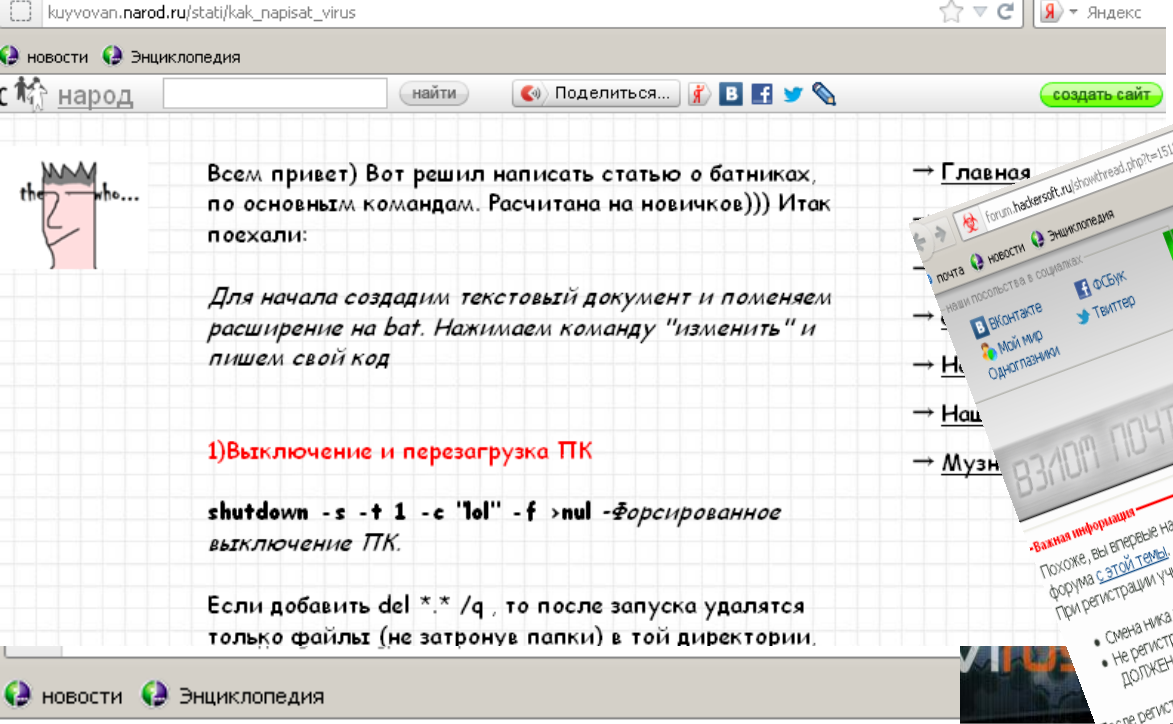
- Такие вирусы писались и пишутся по сей день только для самоутверждения их авторов.

Кто и почему создает вредоносные программы?

- Более продуманные и отлаженные программы создаются профессиональными, талантливыми программистами.
- Такие вирусы нередко используют достаточно оригинальные алгоритмы проникновения в системные области данных, социальный инжиниринг и прочие хитрости

Кто и почему создает вредоносные программы?

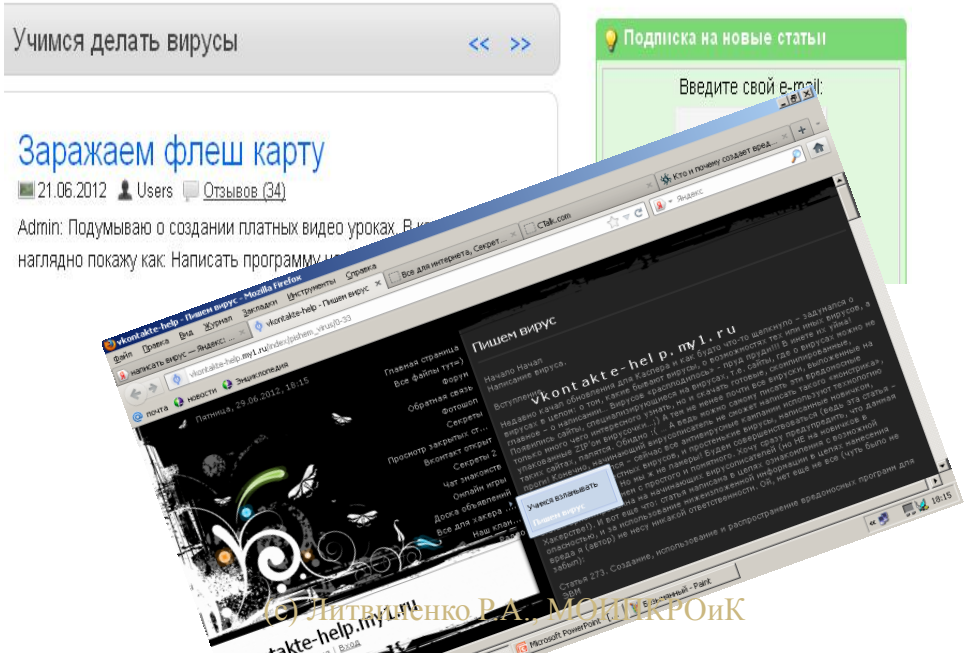
- Программисты – «исследователи» пишут вирусы не ради собственно вирусов, а скорее ради исследования потенциалов «компьютерной фауны.
- Часто авторы подобных вирусов не распространяют свои творения, но могут пропагандировать свои идеи через интернет-ресурсы, посвященные созданию вирусов.



Как написать компьютерный вирус

СОДЕРЖАНИЕ

стр.



Кто и почему создает вредоносные программы?

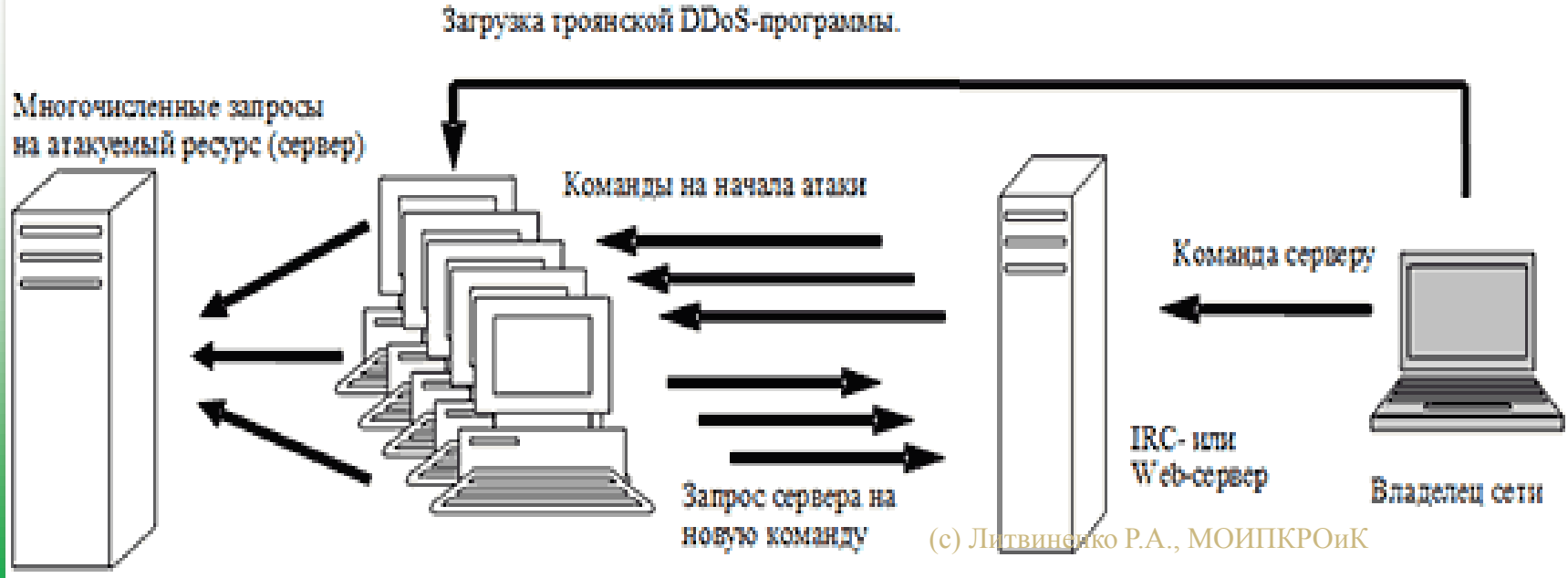
- Компьютерное хулиганство
- Мелкое воровство
- Криминальный бизнес
- Полулегальный бизнес

Мелкое воровство

- В начале 1997 года - первые случаи создания программ, ворующих пароли доступа к системе интернет-провайдеров
- Создаются программы , ворующие регистрационные данные и ключевые файлы различных программных продуктов
- Троянские программы, ворующие персональную информацию из сетевых игр.

Распределённые сетевые атаки

- «Мусорные» запросы на атакуемый ресурс,
- Количество таких запросов многократно превышает возможности ресурса-жертвы.
- Обычные пользователи не в состоянии получить доступ к атакованному ресурсу.



Создание сетей «зомби-машин»

- Создаются программы — «боты», которые централизованно управляются удалённым «хозяином».
- «Хозяин зомби-сети» получает доступ к ресурсам всех заражённых компьютеров и использует их в своих интересах.
- Такие сети «зомби-машин» приобретаются спамерами или сдаются им в аренду

Звонки или рассылка SMS-сообщений

- Регистрируется компания, от лица которой заключается договор с местным телефонным провайдером об оказании платного телефонного сервиса.
- Распространяется программа, осуществляющая несанкционированные пользователем телефонные звонки или отсылку SMS-сообщений с мобильных телефонов.

Воровство интернет-денег

- Программы собирают информацию о кодах доступа к счетам и пересылают ее своему «хозяину».
- Сбор информации осуществляется поиском и расшифровкой файлов, в которых хранятся персональные данные владельца счёта.

Воровство банковской информации

- Показывается окно с изображением, совпадающим с веб-страницей банка
- Запрашивается от пользователя логин и пароль доступа к счету или номер кредитной карты

«Клавиатурные шпионы» ждут подключения пользователя к подлинной банковской веб-странице и затем перехватывают введённые с клавиатуры символы

Кибер-шантаж

- Шифруются пользовательские данные
- Оставляется сообщение о том, что можно купить программу-расшифровщик
- Требовуется перевод некоторой денежной суммы в обмен на пароль

Полулегальный бизнес

Принудительная реклама

Внедрение в систему специальных рекламных компонентов, которые периодически скачивают рекламную информацию с особых серверов и показывают её пользователю.

Полулегальный бизнес

Платные веб-ресурсы

Программы часто устанавливаются в систему без ведома пользователя, например, при посещении веб-сайтов.

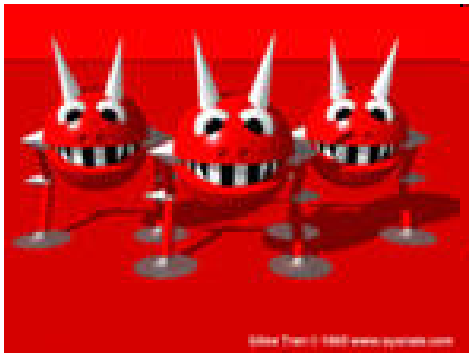
Затем они настойчиво предлагают пользователю посетить тот или иной платный ресурс.

Полулегальный бизнес

Ложные утилиты

- Небольшая программа, которая сообщает о том, что на компьютере обнаружено шпионское программное обеспечение или вирус.
- Предлагается за небольшую сумму приобрести «лекарство», которое, на самом деле, почти ни от чего не лечит.

Способы проникновения вредоносных программ

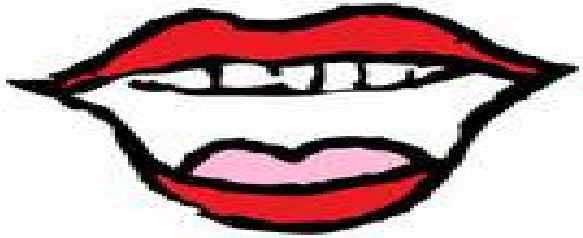


- Социальная инженерия
- Технические приёмы внедрения вредоносного кода в заражаемую систему без ведома пользователя.

Социальная инженерия

Методы социальной инженерии «заставляют» пользователя запустить заражённый файл или открыть ссылку на заражённый веб-сайт.

Задача - заинтересовать пользователя, вынудить его кликнуть по файлу или по ссылке (в письме, смс, в чатах и т.д.)



Социальная инженерия

Например:

- Сообщение содержит какой-либо привлекательный текст, заставляющий ничего не подозревающего пользователя кликнуть на ссылку.

- Используются также возможности файлообменных сетей. Червь или троянская программа выкладывается в сеть под разнообразными «вкусными» названиями.

Социальная инженерия

Фишинг (англ. phishing, от *fishing* — рыбная ловля, выуживание и *password* — пароль) — вид интернет-мошенничества, цель которого — получить идентификационные данные пользователей.

- *создается подложный сайт*
- *обманным путем привлекается пользователь вводит свои конфиденциальные данные – например, регистрационное имя, пароль или PIN-код.*

Фарминг - это процедура скрытного перенаправления жертвы на ложный IP-адрес.

- *заменяют на серверах DNS цифровые адреса легитимных веб-сайтов на адреса поддельных, в результате чего пользователи перенаправляются на сайты мошенников*

Технологические приемы внедрения

- Используются уязвимости, т.е.ошибки в коде или в логике работы различных программ.
- В результате компании-производители уязвимого программного обеспечения оказываются в ситуации цейтнота. Им необходимо максимально быстро исправить ошибку, протестировать результат (обычно называемый «заплаткой», «патчем») и разослать его пользователям

Признаки заражения

- Увеличение исходящего интернет-трафика
- Частые зависания и сбои в работе компьютера
- Попытки неизвестных приложений открыть интернет-соединения
- Случаи несанкционированного доступа к личному банковскому счёту
- Повышенная активность жестких дисков
- Подозрительные файлы

Признаки заражения

- Неожиданные сообщения или изображения
- Получение от вас по электронной почте сообщения, которых вы не посылали.
- Операционная система не загружается при включении компьютера .
- Неадекватное поведение браузера– например, вы не можете закрыть окно обозревателя.

Ущерб от вредоносного ПО

Ущерб от атак вредоносных программ

- От незначительного увеличения размера исходящего трафика до полного отказа работы сети или потери жизненно важной информации.
- Результаты вирусной жизнедеятельности могут оказаться совершенно незаметными для пользователя заражённого компьютера

Ущерб от вредоносного ПО

Отказ работы «железа»

Встречаются троянские программы, периодически открывающие и закрывающие лоток CD/DVD-привода

Возможна поломка привода тех компьютеров, которые не выключаются продолжительное время.

Потеря или кража информации

В случае кражи информации — тем более, в случаях целенаправленной атаки на заведомо определённую жертву — результат может оказаться плачевным для владельца этих данных, особенно если речь идёт об утечке информации, критически важной для пользователя.

Даже если видимого ущерба нет...

- Даже если этот троянец всего лишь «зомби»-сервер, рассылающий спам, он, как минимум, потребляет сетевые и интернет-ресурсы.

- Компьютеры могут стать базой для рассылки спама, атак на другие элементы сети — большинство пользователей просто не задумываются над этим.

Методы и технологии защиты от вредоносных программ

- Использование антивирусной защиты.
- Не доверять всей поступающей на компьютер информации.
- Обращать внимания на информацию от антивирусных компаний
- Устанавливайте обновления, отвечающие за безопасность.
- Никогда не нажимайте кнопку "Согласен" или ОК, чтобы закрыть окно. Щелкните значок с крестиком в верхнем углу окна или нажмите клавиши **Alt + F4**

Методы и технологии защиты от вредоносных программ

- Будьте осторожны со спамом в электронной почте и системах мгновенных сообщений.
- Пользуйтесь учетной записью администратора на своем компьютере только в случае необходимости.
- Сохраняйте резервные копии данных.
- Просматривайте процессы в диспетчере задач

Методы защиты от фишинга и спама

- Убедитесь, что адрес сайта начинается с "https://”.
- Дважды щелкните мышью на значке замка в правом нижнем углу окна браузера и проверьте, совпадает ли адрес, указанный в сертификате безопасности, с текстом в адресной строке браузера.
- Пользуйтесь несколькими адресами электронной почты.
- Не проходите по ссылкам, предлагающим "отписаться от рассылки"

Пароли

- Выбирайте пароли, которые не придется записывать
- Не используйте в качестве пароля реальные слова
- Используйте буквы нижнего и верхнего регистра, а также цифры и другие символы
- Не используйте один и тот же пароль для разных учетных записей.
- Не используйте для защиты своих данных очевидные пароли, которые легко угадать
- Если Вы получили сообщение с подтверждением регистрационной информации и новым паролем, зайдите на соответствующий сайт и смените пароль.

Безопасность детей в Интернете

Доступ к негативной информации

- Контрабанда
- Порно
- Реклама табака и алкоголя
- Изготовление взрывчатых веществ
- Наркотики

Безопасность детей в Интернете

- Риск притеснения со стороны других пользователей, оскорбления и угроз
- Сайты, собирающие информацию о самих детях, семье
- Общение с маньяками, ищущими личной встречи с ребенком

Для безопасности детей в интернете:

- Поговорите с ними о возможных опасностях;
- Пользуйтесь интернетом вместе;
- Поощряйте обсуждение онлайн-опыта;
- Сформулируйте правила работы в интернете;
- С помощью настроек программного обеспечения ограничивайте доступ ребенка к определенному контенту;
- Не забывайте также следовать всем другим правилам защиты от вредоносных программ и хакерских атак.

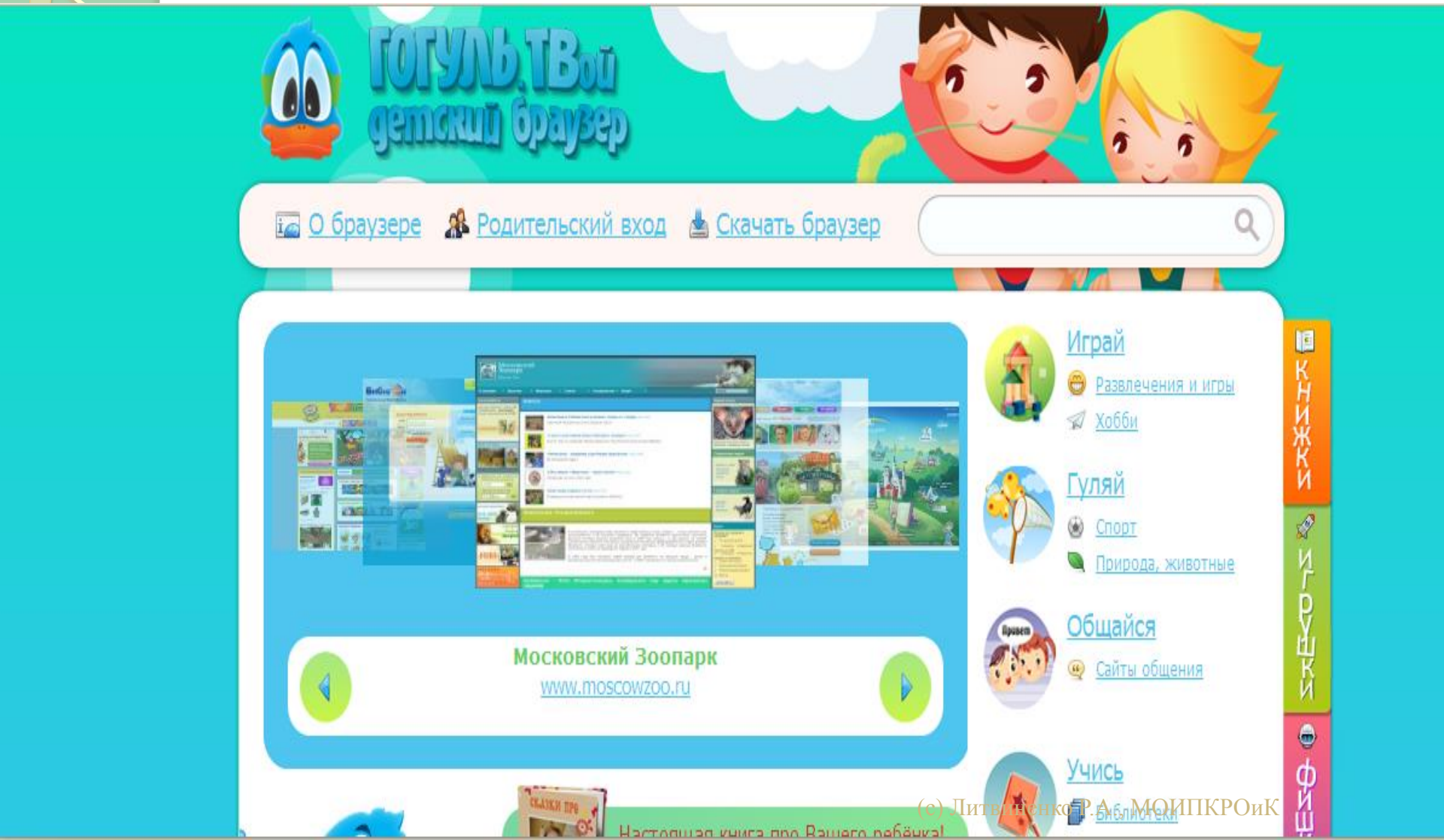
Фильтрация

- анализ информации, проходящей через брандмауэр, и принятие решения о ее доставке пользователю.

- Контент-фильтр работает по статистическому принципу, т.е подсчитывает заранее определённые слова текста и определяет категорию к которой относится содержимое сайта.
- Система позволяет блокировать веб-сайты с содержимым не предназначенным для просмотра.


NetPolice - Персональный клиент фильтрации (для дома и семьи)
NetPolice
Персональный клиент фильтрации
Версия: 1.6 (обновить)
Личный кабинет: my.netpolice.ru
Служба поддержки: info@netpolice.ru
Внимание! Отключение фильтра открывает доступ ко всем сервисам интернета!
Фильтр: Вкл. Откл.
Фильтр
Журнал
Настройки
Мои ресурсы
Профиль не назначен
Порнография:
Вкл. Выкл.
Блокирует доступ к порнографическим сайтам.
Динамическая фильтрация:
Вкл. Выкл.
Анализирует содержимое ресурса по ключевым словам, блокирует ненормативную лексику.
Социальные сети:
Вкл. Выкл.
Блокирует доступ к социальным сетям, сайтам знакомств и чатам.
Онлайн-казино и компьютерные игры:
Вкл. Выкл.
Блокирует доступ к азартным играм в интернет-казино и прочим компьютерным играм.
Услуги обмена сообщениями:
Настроить список услуг...
Вкл. Выкл.
Блокирует доступ к службам обмена сообщениями (ICQ, Google Talk, и т. д.), запрещает передачу почтовых сообщений и сообщений в социальных сетях.
Скачивание файлов:
Настроить список файлов...
Вкл. Выкл.
Блокирует возможность скачивать файлы из интернета.
Файлообменные сети и сайты:
Вкл. Выкл.
Блокирует доступ к сайтам и сетям обмена файлами.
Другие фильтры:
Настроить фильтры...
Вкл. Выкл.
В этом разделе можно настроить фильтры других категорий. Например, фильтр для онлайн-игр.
Часы работы фильтра
12
6
18
0
День
Ночь
Расширенный режим...
Нажатиями левой кнопки мыши на временных отрезках вы можете настраивать часы работы фильтра. Области «День» и «Ночь» также являются кнопками.
Пример
Выключен каждый день с 2:00 до 3:00...
Сохранить и закрыть
Изменить пароль...
(с) Литвиненко Р.А., МОИНКИ ОИК

Детский браузер www.gogul.tv



Методы обнаружения вирусов

- Сканирование файлов для поиска известных вирусов, соответствующих определению в антивирусных базах.
- Обнаружение подозрительного поведения любой из программ, похожего на поведение заражённой программы.

Противодействие антивирусным программам

Упаковка и шифрование кода.

- Значительная часть современных компьютерных червей и троянских программ упакованы или зашифрованы тем или иным способом.
- Антивирусным программам приходится добавлять новые методы распаковки и расшифровки, что снижает качество детектирования

Мутация кода.

- Разбавление троянского кода «мусорными» инструкциями.
- В результате функционал троянской программы сохраняется, но значительно меняется её «внешний вид».

Противодействие антивирусным программам

Скрытие своего присутствия.

Осуществляется перехват и подмена системных функций, благодаря которым зараженный файл не виден ни штатными средствами операционной системы, ни антивирусными программами.

Противодействие антивирусным программам

Остановка работы антивируса .

- Специальные действия против антивирусных программ :
  - поиск их в списке активных приложений
  - попытка остановить их работу
  - порча антивирусных баз данных
  - блоковка получения обновлений и т.п.

Противодействие антивирусным программам

Скрытие своего кода на веб-сайтах

- Веб-страница , на которой присутствуют троянские файлы, модифицируется специальным образом : *если запрос идёт с адреса антивирусной компании, то скачивается какой-нибудь нетроянский файл вместо троянского.*

Атака количеством

- Генерация и распространение в интернете большого количества новых версий троянских программ за короткий промежуток времени.
- В результате на анализ новых образцов антивирусным компаниям требуется время, что даёт злоумышленному коду дополнительный шанс для успешного внедрения в компьютеры.

Качество антивирусной защиты

Регулярность и частота обновлений

Увеличивается как количество новых вредоносных программ, так и частота их появления.

Качество антивирусной защиты

Баланс: производительность или полноценная защита

- Открытие файлов,
- Прочтение из них информации,
- Раскрытие архивов для их проверки и т.п.

Чем тщательнее проверяются файлы, тем больше ресурсов компьютера задействовано.

Совместимость дублирующих антивирусных программ

- Антивирусным программам приходится достаточно глубоко проникать в ядро системы, причем проникать приходится в одни и те же зоны.
- Иногда попытка дублирующего перехвата приводит к краху системы

Самые популярные

- **Антивирус Касперского.**
- **Doctor Web**
- **NOD32**
- **Avast**
- **IKARUS**

Особое мнение

Если компьютер заражен вирусом

- Отключите компьютер от интернета
- Если ОС не загружается, загрузите в безопасном режиме (удерживайте F8, затем выберите Безопасный режим)
- Для загрузки обновлений используйте другой компьютер
- Проведите полную антивирусную проверку компьютера.
- Используйте бесплатные антивирусные утилиты различных лабораторий.

Что делать, если пострадали

- Обратиться в подразделение МВД, осуществляющее борьбу с компьютерными преступлениями
- Сообщить как можно больш… происшеств… подробности

http://www.mvd.ru/projects/attention/