бунт машин, восстание червей, парад багов в браузерах

крис касперски ака мыщъх, no-email

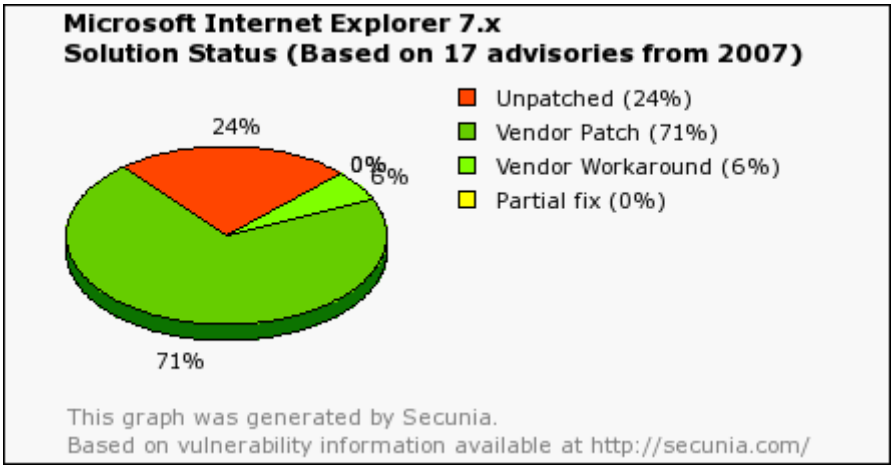
кто верит в магомета, кто в аллаха, кто в иссуса, а кто-то в браузеры без дыр. попытка оспорить постулат веры приводит к священным войнам — декалитрам крови и гигабайтам флейма. провокация? нет, всего лишь статья в которой мы объективно сравниваем различные типы браузеров на предмет безопасности по куче критериев сразу, подтверждая сказанное не только всем весом своего авторитета (мыщъх'и они вообще немного весят), но и обширным фактическим материалом.

введение

Обвальный рост уязвимостей в 5й (и особенно 6й!) версии IE вынудил продвинутых пользователей к переходу на альтернативные браузеры, на которые хакеры уже давно перешли (ну хакеры они всегда в авангарде…). Конкуренты четко просекли ситуацию, сделав ставку на безопасность. "*С FireFox вы повысите свою безопасность и удобство сёрфинга*", "*Opera предоставляет самый быстрый, безопасный и простой в использовании браузер*". Не отстает от них и Microsoft, но при всей агрессивности маркетинга последней, ее рекламе больше никто не верит и ошибки в IE обнаруживаются чуть ли не каждый день, из которых каждая шестая — критическая. Не браузер, а сплошное решето. Работать с ним и шарахаться от каждого шороха, могут либо эктрималы, либо чайники. Остальные уже давно забили и мигрировали в иные миры, откуда уже не возвращаются. Действительно, посидев на Горящем Лисе или Опере недельку-другую, работать под IE никакого желания нет.

Что-то у конкурентов реализовано получше, что-то похуже, но дело ведь не в качестве кода и удобстве использования, а в безопасности! Ругая IE, поклонники альтернативных браузеров совершенно наплевательски относятся к собственной security, не следят за новостями, не скачивают обновлений и вообще ведут себя так, как будто ни дыр, ни хакеров, ни прочих угроз в природе не существует. Между тем, дыры есть везде, в том числе и в текстовых браузерах типа Рыся, просто о них не принято говорить. Почему? Очень просто. Microsoft первая попадает под перекрестный огонь специалистов по безопасности и сетевых обозревателей, а продукция сторонних фирм традиционно остается в стороне, к тому же журнальный бизнес придерживается правила: "бей сильных и не ввязывайся в священные войны!" Писать о дырах в Лисе зачастую просто небезопасно. Тут же закидают гнилыми помидорами и тухлыми яйцами. А вот дыры в IE – это почетно!

Ладно, оставляем лирику и переходим к статистике.



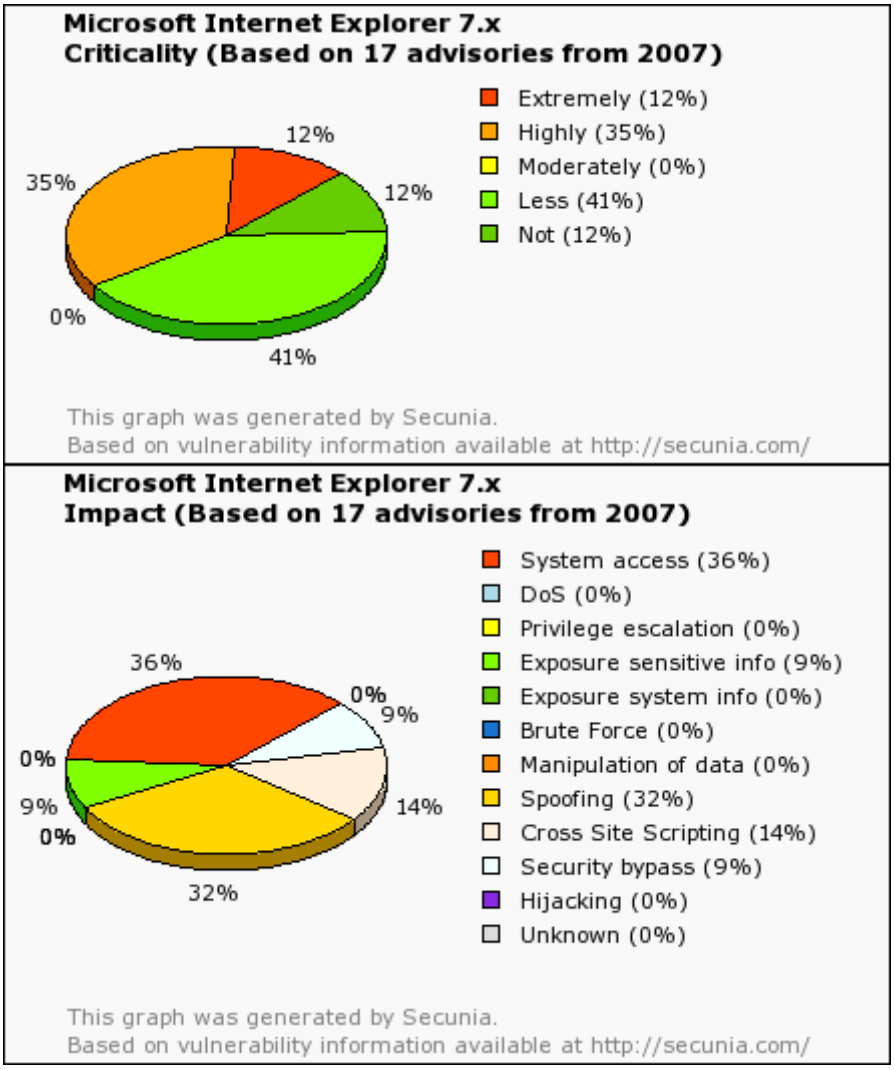


Рисунок 1 статистика по дырам, обнаруженным за 2007 год в IE по данными копании Secunia

Горячий Лис

FireFox собранный на обломках заживо похороненного (а затем эксгумированного и реанимированного) Netscape – просто не может быть надежным браузером по определению. Фирма Netscape была первой, кому пришла в голову мысль внедрить в браузер поддержку Java-скриптов, и дыры в Netscape водились уже тогда, когда Билл Гейтс еще не вкурил в Инетернет и не понял, что Интернет — это тема.

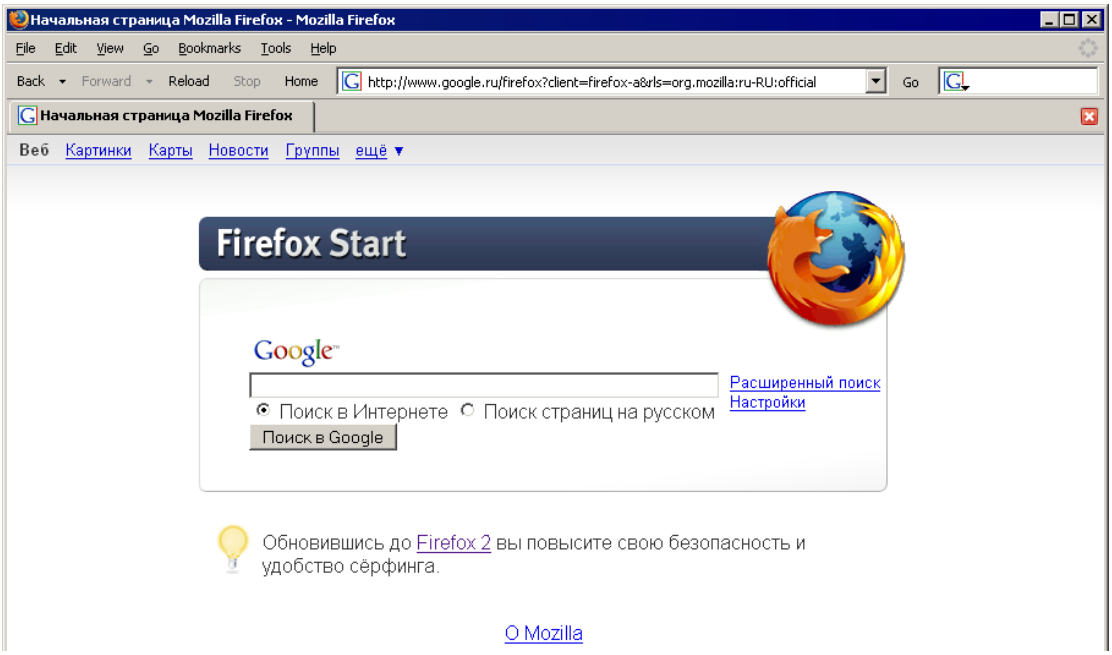


Рисунок 2 внешний вид Горящего Лиса

Войну между Microsoft и Netscape мы оставим на растерзание историкам (им же тоже нужно чем-то питаться), а сами сосредоточимся на достигнутых результатах. Netscape раскрыла исходные тексты своего продукта и начала привлекать к разработке всех желающих, но желающих не было и кворума собрать не удалось. Кому из опытных программистов интересно вкладывать время и силы в мертвый проект, не получая ни прибыли, ни отдачи?! В смысле — ни удовлетворения, ни денег.

Чтобы собрать команду понадобилось несколько лет и мало-помалу новый продукт (окрещенный Горящим Лисом или, по-английски FireFox'ом) стал завоевывать рынок. Первые версии Лиса были ужасны. Часть сайтов вообще не открывалось или отображалась неправильно, оперативная память стремительно утекала, производительность (а точнее полное отсутствие таковой) настойчиво напоминало о себе с первой до последней минуты работы с Горящим Лисом, требуя его периодического перезапуска (чтобы вернуть системе утекшую память).

Рисунок 3 это не след от НЛО, это поклонники Горящего Лиса оттягиваются (наверное хорошей травы обкурились). (РЕДАКТОРУ: картинка есть в хайрезе, так что если что, говори - я перешлю)

А чему удивляться?! Код Лиса написан на смеси приплюстутого си и жабы, а жаба — это уже тормоза. Причем, если IE разбит на множество динамических библиотек, загружаемых в память по мере необходимости (и даже базовые библиотеки грузятся одновременно с отображением пользовательского интерфейса, создавая иллюзию "быстрого старта"), то у Горящего Лиса все свалено в огромный исполняемый файл. Ну разве можно так делать?! Но это еще что… Настройки браузера разбросаны по сотням файлов и эти файлы представлены в текстовом формате и при _каждом_ своем запуске браузер вынужден парсить их заново. Вот, такая, значит, у них оптимизация.

С низкой скоростью работы можно было бы и смириться (зачем торопиться на кладбище?!), если бы не катастрофическая ситуация с безопасностью. Компоненты бразуера, написанные на жабе, освобождают его от ряда врожденных "болезней" языка Си типа переполняющихся буферов, которыми так знаменит IE, но… в Лисе довольно много приплюсного кода и ошибки переполнения (ведущие к удаленному захвату управления компьютером) в нем все-таки имеются, пускай в меньших количествах, чем в IE. Плюс общие ошибки дизайна и кривой (изначально) HTML-движок, добавление новых фич в который ломает всю систему безопасности, образуя многочисленные дыры по всему охраняемому периметру.

А чего еще можно ожидать от "базарного" стиля программирования, когда квалификация разработчиков отличается на несколько порядков и любой пионер (ну не совсем любой, конечно) может вносить изменения в код, не согласуя их с более опытными товарищами, которые, обнаружив подобную самодеятельность, сначала хватаются за валидол, а потом за голову, совершая быстрый отказ взад. Подписавшись на рассылку для разработчиков (или покопавшись в ее архиве) очень быстро устаешь от "кретивной" пионерии, которая сначала что-то делает, а потом думает _что_ они сделали и как с этим жить.

Впрочем, мы вновь углубились в лирику, а обещали статистику. ОК, открываем www.securityfocus.com (можно прямо в Лисе), вбиваем в строку поиска Mozilla FireFox и… получаем 6 страниц уязвимостей по 30 штук в каждой, причем, целый ряд уявзимостей носит множественный характер и на самом деле в Горящем Лисе за всю его историю обнаружено не ~180 дыр, а _намного_ больше. Тот факт, что большинство уязвимостей обнаруживает сами же разработчиками, оперативно затыкая их — ничего не меняет. Другой вопрос, что сообщение о дыре это всего лишь текст, а не исполняемый файл и вовсе не факт, что данная уязвимость действительно представляет реальную угрозу. Атакующему предстоит не только разобраться в технических аспектах (которые обычно не разглашаются), но и решить многие другие проблемы.

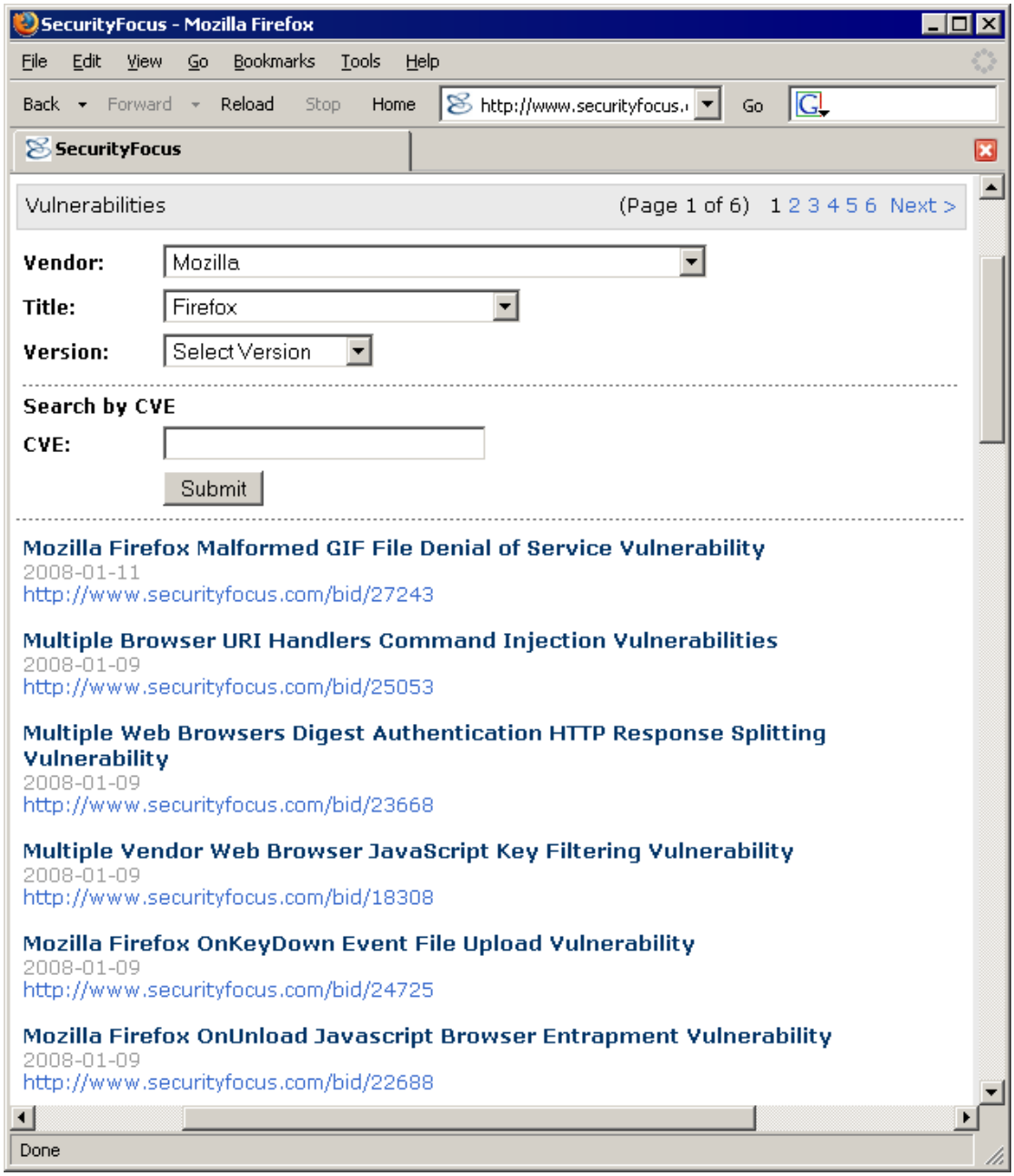


Рисунок 4 дыры, обнаруженные в Горящем Лисе

Короче говоря, не каждая дыра это нора. Угроза исходит главным образом от публичных exploit'ов, которыми может воспользоваться любой желающий. Ему и хакером быть необязательно. Навыков продвинутого пользователя обычно оказывается вполне достаточно. А раз так, идем на www.milw0rm.com, вбиваем в строку поиска FireFox и пожинаем урожай – свыше 20'ти exploit'ов, большинство из которых работает чисто на отказ в обслуживании, но имеется достаточно много дыр, допускающих засылку shell-кода с последующим захватом управления. А вот это уже не хухры-мухры! Это _реальная_ опасность попасть под артобстрел или запустить червя на свой компьютер!

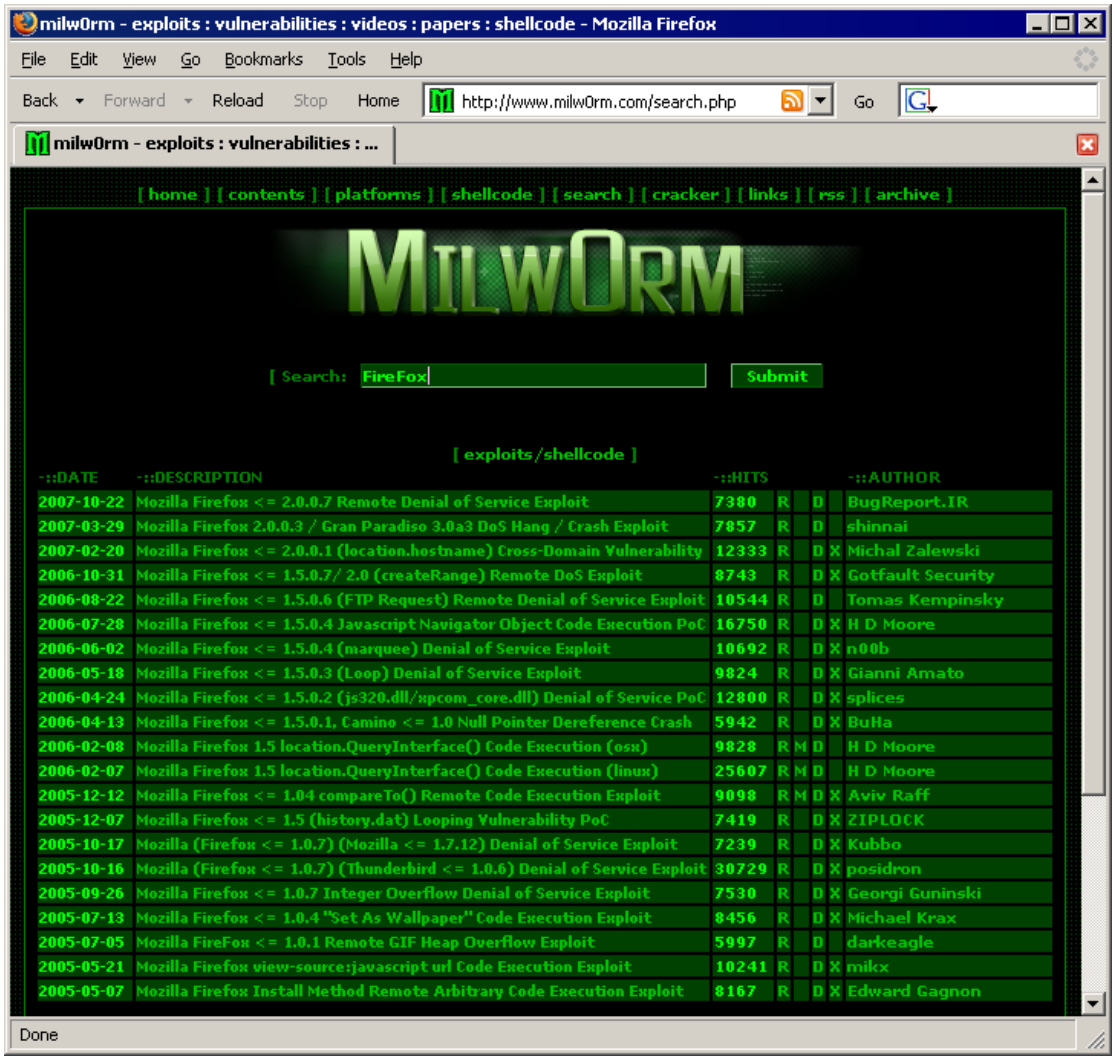


Рисунок 5 exploit'ы для Горящего Лиса

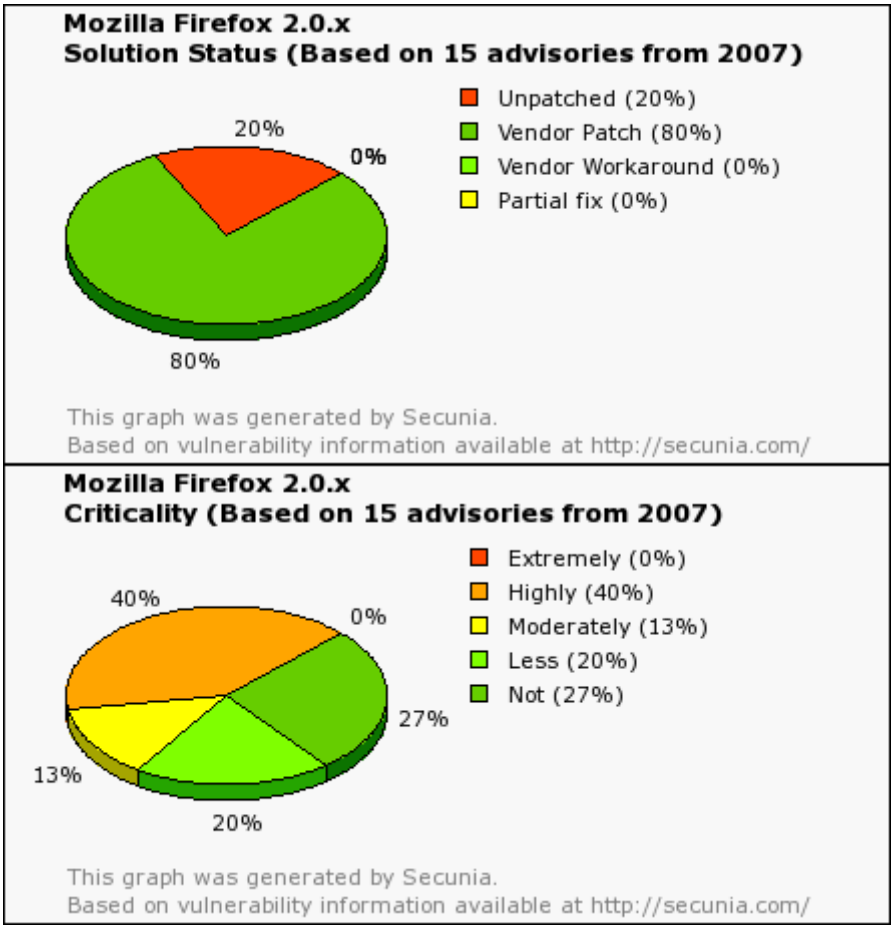
Правда, реальных случаев атак на Горящего Лиса зарегистрированного немного и нет (или практически нет) ни одного червя, который правильно было бы назвать глистом, поскольку червей ловят и едят, а глисты заводятся сами и попробуй потом от них избавится! Самое неприятное, что если пользователи IE в своей массе уже привыкли к его дырам и довольно активно качают обновления (чайников и ламеров мы в расчет не берем), то поклонники Горячего Лиса, уверенные в его непогрешимости, не видят в обновлениях никакой необходимости, тем более, что механизм обновлений должным образом не отлажен. Новые билды выходят нечасто, а качать мегабайты исходных текстов и трахаться с их компиляцией — это извините, каким же мазохистом быт надо?!

Наибольшую опасность представляют уже опубликованные, но еще не залатанные дыры. Для Оперы написан симпатичный винжет, торчащий на Рабочем Столе и отображающий (в реальном времени) количество критических не заткнутых дыр для всех популярных браузеров. "Не заткнутых" имеется ввиду таких дыр, лекарства против которых еще нет и неизвестно, когда оно будет. Первое место по дырам традиционно занимает IE (на момент публикации 7 не заткнутых дыр), за ним с небольшим отрывом идет Лис (5 дыр). Опера находится в самом конце хвоста, пропуская вперед себя UNIX-браузеры, о которым мы говорить все равно не будем. На данный момент дыр в Опере нет (и мыщъх не припомнит когда они там вообще были).

Рисунок 6 виджет для Оперы, отображающей в реальном времени количество _незаткнутых_ дыр в разных браузерах

Тем не менее, IE атакуют порядка на два, а то и на три чаще, чем Горящего Лиса!!! Почему?! Ответ прост как бумеранг: популярность Горящего Лиса существенно ниже, чем IE и написание червей под него просто не окупается. К тому же, Горящего Лиса устанавливают технически продвинутые люди, пользующиеся целым комплексом защитных средств и распознающих присутствие постороннего кода даже без помощи антивируса — достаточно бросить беглый взгляд на Диспетчер Задач или Process Explorer'a Руссиновича.

Растущая популярность Лиса не идет ему на пользу. Код кривой, дырявый, практически ничем не уступающий IE. Стоит только ему существенно потеснить IE, как тысячи хакеров бросятся на поиски дыр (благо исходные тексты доступны) и начнут писать червей одного за другим. Выдержит ли Горячий Лис их натиск?! С таким подходом к разработке навряд ли. Впрочем, не будем строить прогнозов, а предоставим событиям развиваться собственным путем.



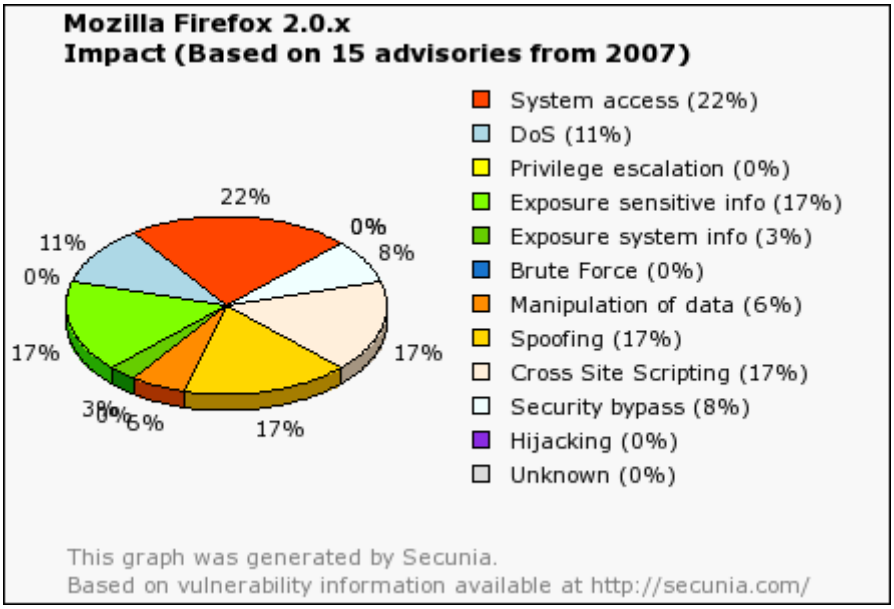


Рисунок 7 статистика по дырам, обнаруженным за 2007 год в Горящем Лисе по данными копании Secunia

Опера

Браузер с закрытыми исходными текстами, но, в отличии от Лиса (основанного на кодах Netscape) и IE (построенного на базе Mosaic), разработанный с чистого листа и спроектированный сплоченной командой весьма неглупых людей. По быстродействию, надежности и удобству пользования Опера рвет конкурентов как тузик грелку, причем, большинство новых фич сначала появляется именно в Опере и только потом у конкурентов.

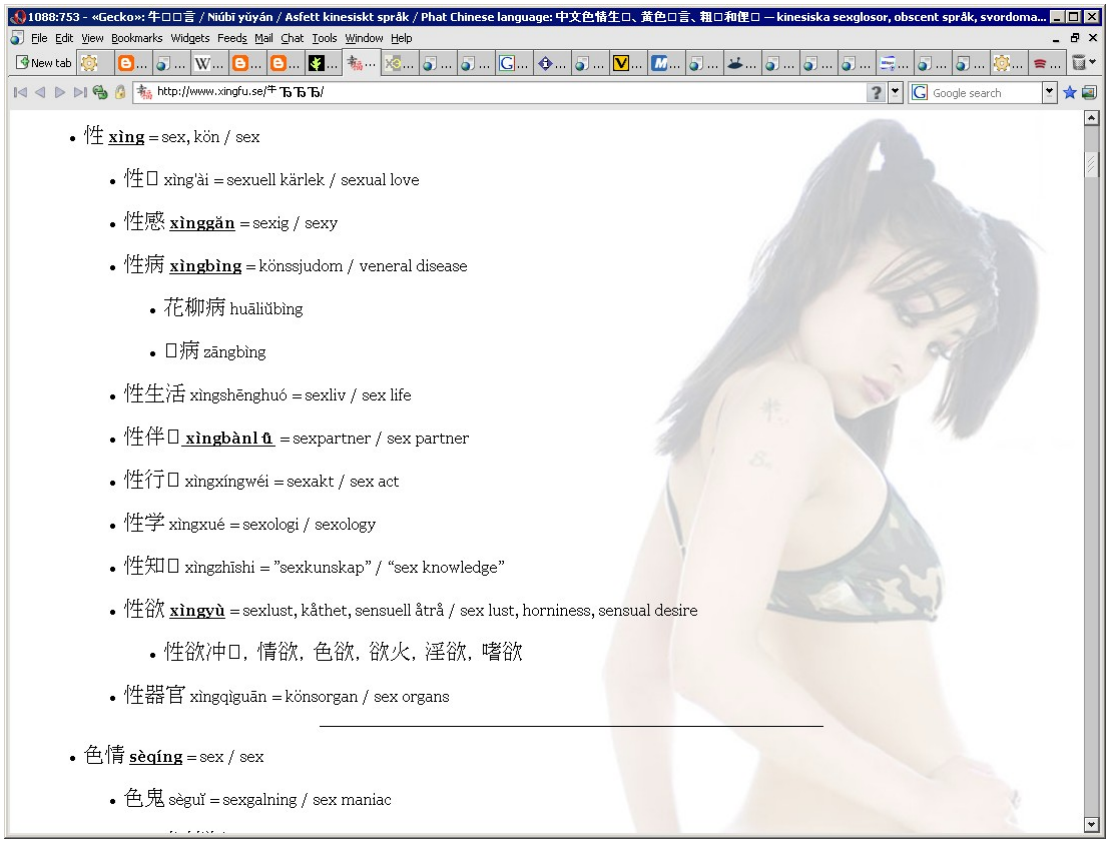


Рисунок 8 так выглядит Опера

Единственный недостаток Оперы (по сравнению с Лисом) — крайне куцая коллекция расширений. Если для Лиса можно найти любое расширение, какое только нужно (или на худой конец, написать его самостоятельно), то в Опере расширения (винжеты) появились лишь недавно, число их невелико, а функциональность жестко ограничена архитектурой и в основном все программисты пишут гаджеты типа трехмерных часов, календарей, органайзеров, индикаторов погоды и прочей фигни. А вот научить YouTube сохранять потоковое видео в формате mpeg4 – слабо?! А ведь для Лиса таких расширений намного больше одного. Лично мыщъх написал пару расширений для www.collarme.com (на котором он проводит кучу свободного и несвободного времени), чтобы с ним было можно работать без помощи мыши — одной лишь клавиатурой. Для Оперы (в силу ограничений, наложенных на винжеты, такую штуку написать уже не получается, или я просто не разобрался как это сделать).

Ошибок в Опере не то, чтобы совсем нет, но явно меньше, чем в Горящем Лисе. Security Focus выдает 4 страницы ошибок (против 6 в Fire Fox), правда, многие ошибки — критические, то есть допускают возможность удаленного выполнения shell-кода, ведущего к захвату системы, а это очень нехорошо.

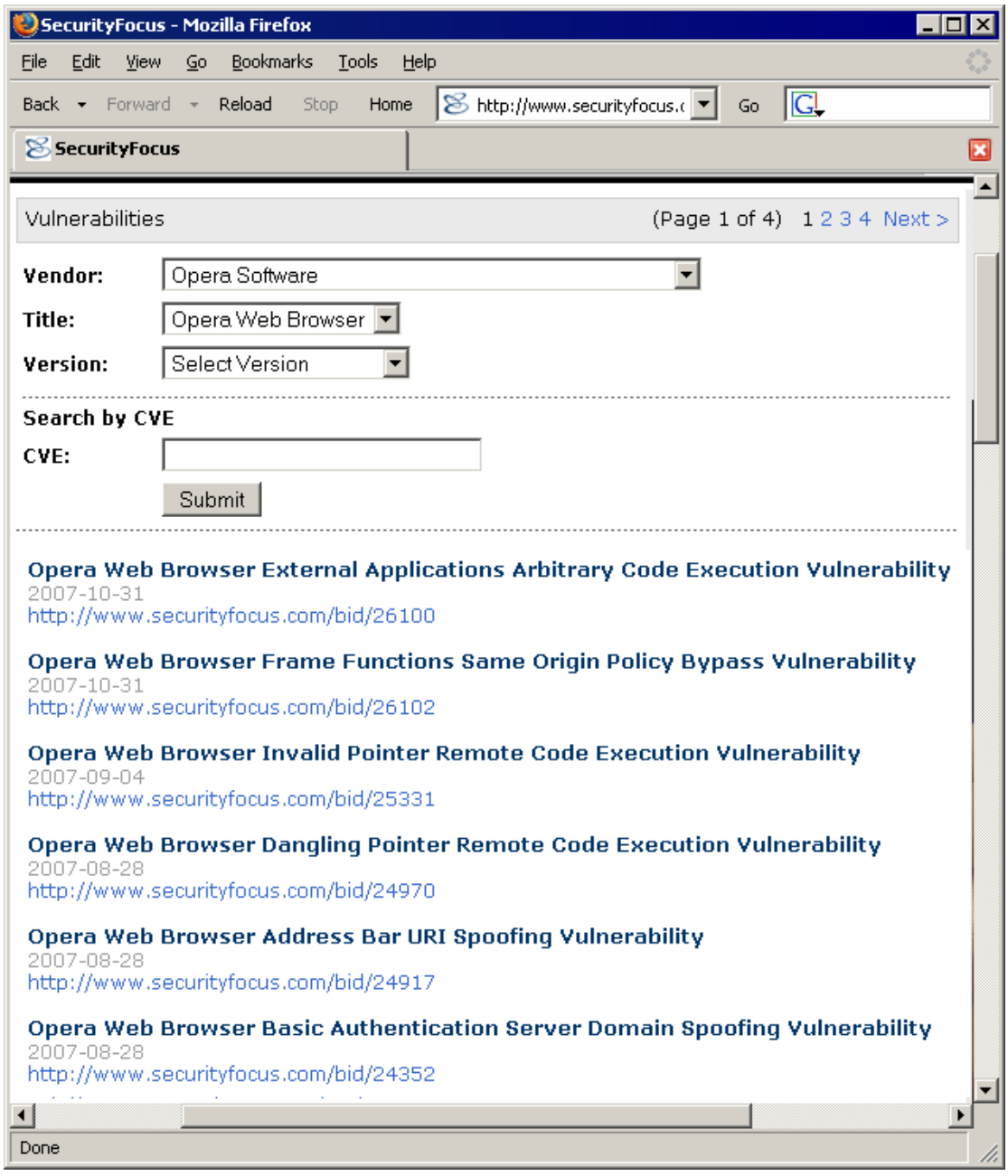


Рисунок 9 дыры в Опере

На www.milw0rm.com валяется около 15 боевых exploit'ов, главным образом работающих на отказ в обслуживании, но есть среди них и парочка таких, что забрасывают shell-код, причем, как и для старых версий Оперы, так и для новых. На сайте компании нет ни одного ресурса, хотя бы косвенно относящегося к безопасности (есть только рекламный логотип, типа Опера самая безопасная). Какие там упоминая о дырах или история исправлений?! Даже у ненавистной всем Microsoft все это есть, не говоря уже о Лисе. В любую минуту зашел, полистал список новых багов, почитал чем они чреваты и, вздохнув, принялся скачивать обновления или всю версию браузера целиком.

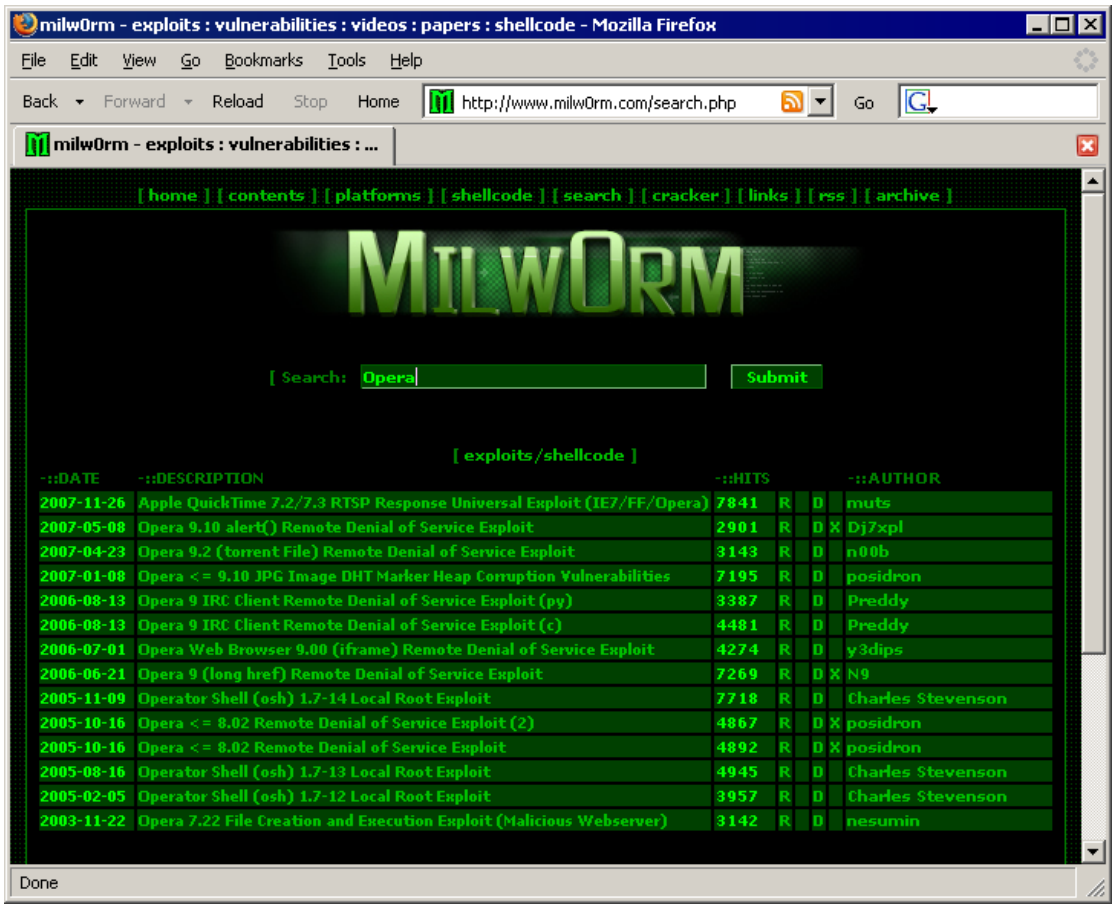


Рисунок 10 exploit'ы для Оперы

Маленький секрет. На ftp-сайте компании можно найти намного больше, чем на WEB'е, в том числе и версии с залатанными дырами, еще не выложенные на WEB. Что за странная политика такая — не зная. От атак Оперу спасает лишь относительно невысокая распространенность последней. Мыщъх'у не известен ни один хакерский сайт, сконструированный специально для "обстрела" Оперы (Лис под удары несколько раз уже попадал, правда, все закончилось благополучно и зараза — благодаря Process Explorer'у Руссиновича была подбита еще на излете).

Закрытость исходных кодов и относительно частый выход новых версий так же существенно повышает "цену" атаки. (закрытость исходных текстов IE чисто формальна, на самом деле их имеют все те, кому они нужны, а поиметь их можно на любом файло-обменнике в архив с сорцами W2K или XP. IE там тоже есть).

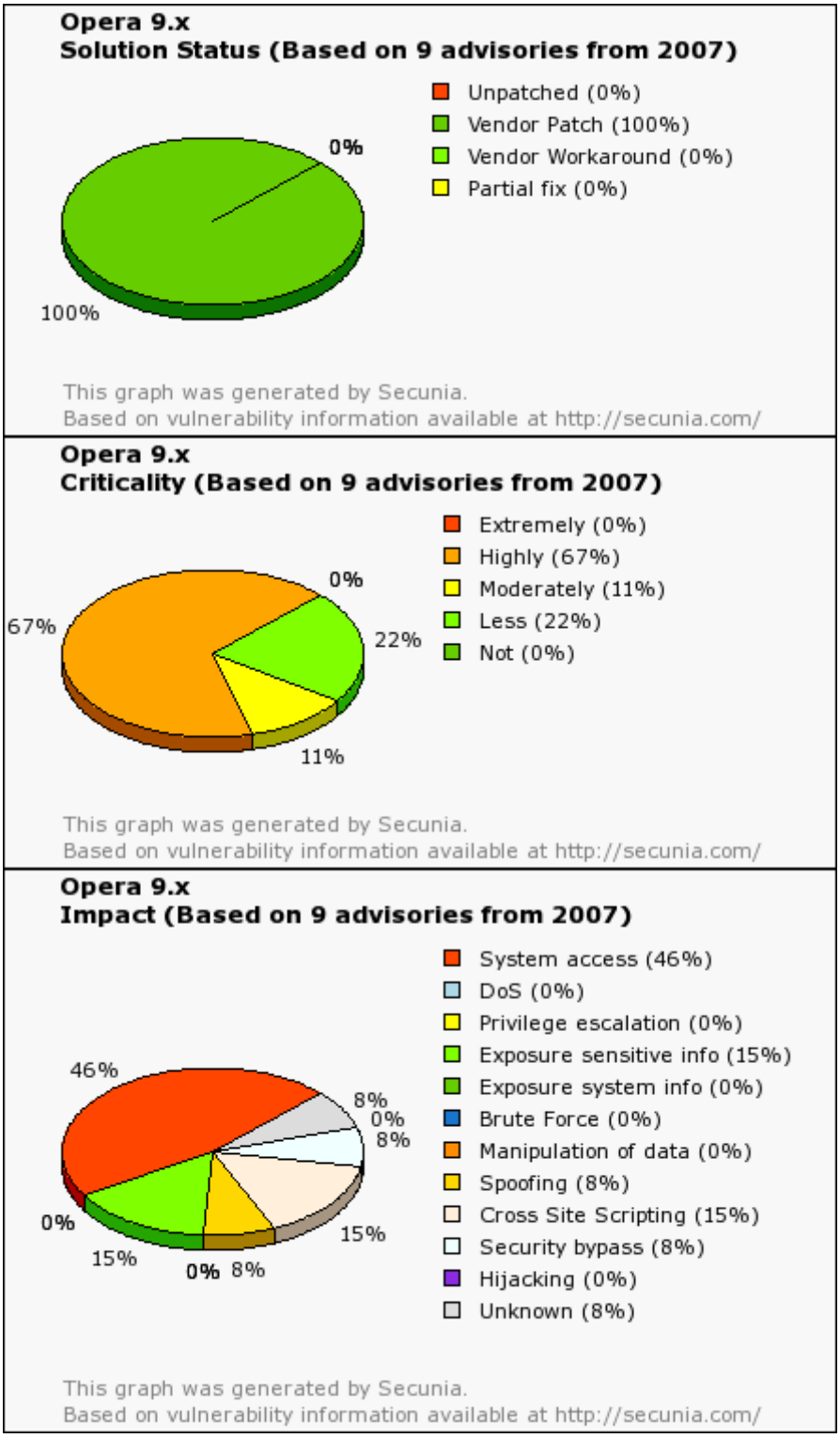


Рисунок 11 статистика по дырам, обнаруженным за 2007 год в Опере по данными копании Secunia

Рысь

Рысем зовут текстовой браузер (он же Lynx), весьма популярный в некоторых кругах и горячо любимый мыщъх'ем. Графику не поддерживает, картинки не грузит, управляется с клавиатуры и серфит с такой скоростью, что только ветер в ушах свисит. Переваривает только базовые теги HTML (да и то не все), скрипы не видит в упор, не говоря уже о всяких там

плавающих фреймах. Казалось бы, ну какие ошибки при такой простоте? Тем более, что новые версии практически не выходят. Да и зачем новые, когда есть неплохо работающие старые?!

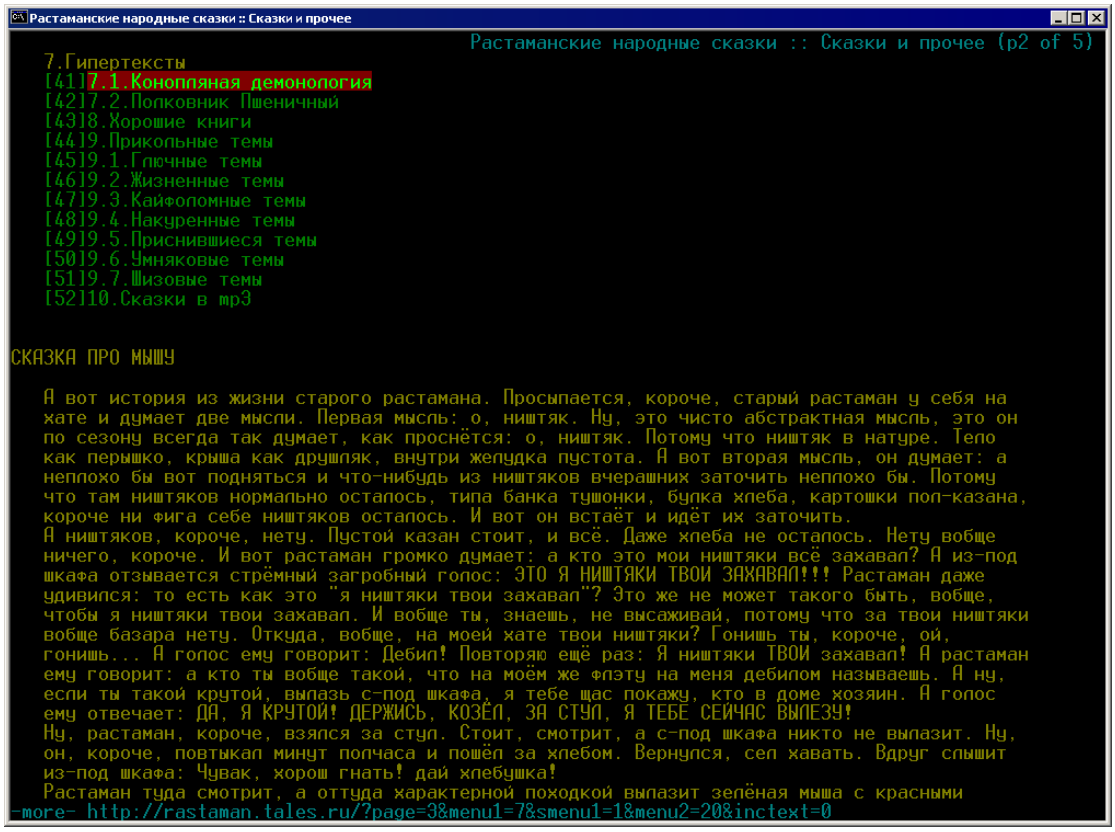


Рисунок 12 текстовой браузер Рысь на охоте

Тем не менее, Security Focus показывает целых 8 ошибок, а на www.milw0rm.com находятся два exploit'a, захватывающие управление компьютером без всяких там отказов в обслуживании, что буквально шокировало мыщъх'а, до этого верящего, что в Рысе ошибок нет и не будет, а оно вон как оказалось… Теперь мыщъх не верит ни браузерам, ни женщинам и прежде чем вновь начать серфить Рысем не внушающие доверия сайты, тщательно изучает его исходных код — вдруг там какой баг, о котором еще никто не знает? То есть, это мыщъх не знает, а тот кому нужно — знает о багах все.

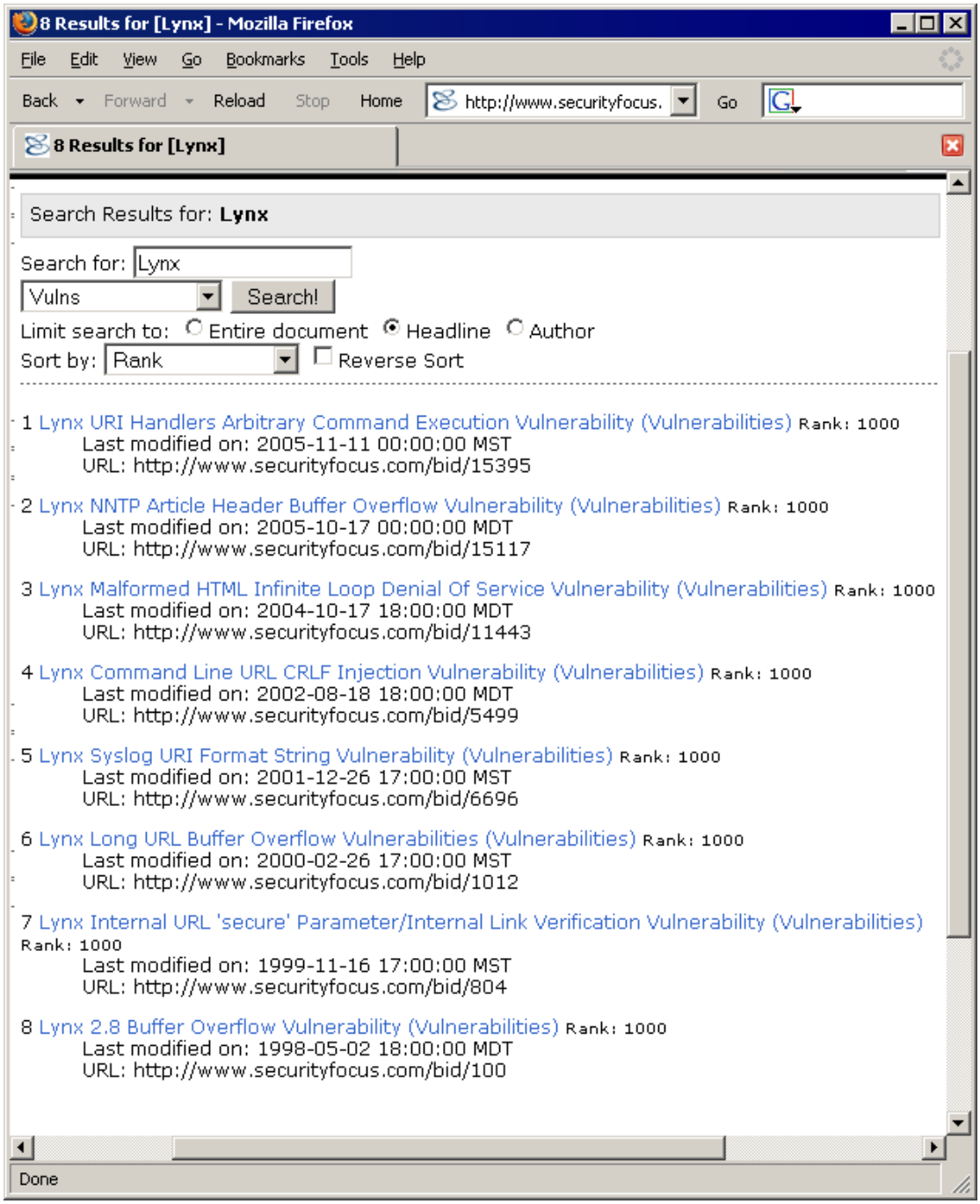


Рисунок 13 дыры, обнаруженные в Рысе за все время его существования

Вот и думай, как не стать параноиком при таком положении дел?! Тем не менее, вероятность попасть под атаку сидя на Рысе — настолько близка к абсолютному нулю, что совершенно несущественна и ею можно на 99% пренебречь, но потенциально небезопасные сайты все-таки лучше просматривать из-под виртуальной машины. Мало ли…

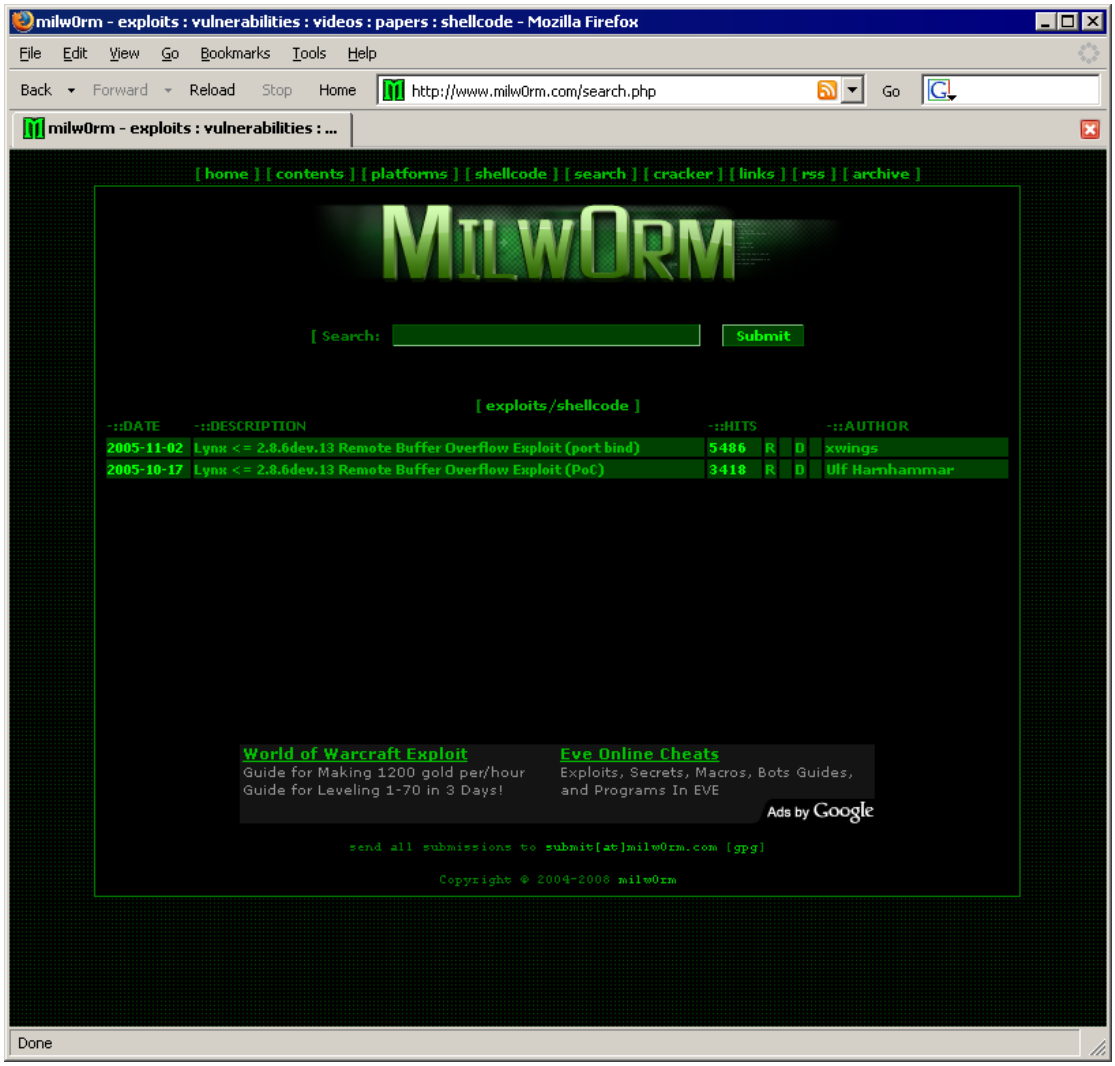


Рисунок 14 exploit'ы для Рыся

>>> врезка плагины

Все браузеры (за исключением, пожалуй, одного лишь Рыся и его текстового собрата Links'a) позволяют устанавливать плагины сторонних производителей: Abobe pdf-reader, Flash player и много еще чего. А в этих плагинах ошибки, между прочим, тоже встречаются. Причем, если плагин портирован сразу под несколько браузеров, уязвимость приобретает масштабный характер.

Так например, в конце 2007 года была обнаружена серьезная дыра в Apple QuickTime Player, допускающая удаленный захват управления и ставящая под угрозу и IE, и Горящего Лиса, и Оперу, Сафари и некоторые другие десктопные и мобильные браузеры, при условии, конечно, что этот плагин на них установлен, а установлен он там достаточно часто.

Ладно, если без встроенного просмотра PDF еще как-то можно и обойтись (хотя, какая разница?! все равно, дыра выскочит при открытии сохраненного документа с локального диска), то без Flash'a живется хреново. То есть, поначалу очень даже хорошо живется — реклама не грузиться и не досаждает, а развлекательные ролики можно посмотреть и под IE. Но вот начинают попадаться сайты, где часть картинок выполнена при помощи Flash-технологий (например, так поступает www.iXBT.com) и… браузер начинает неизбежно обрастать все новыми плагинами.

>>> врезка расширения

В той или иной мере, расширения поддерживают все браузеры (кроме текстовых, конечно) и коллекция этих расширений обычно находится прямо на официальном сервере

компании-разработчика. Вот только… пишут эти расширения все кто попало, а потому таят в себе скрытую угрозу. Наткнувшись на пару расширений для Горящего Лиса, незаметно ворующих пароли с кукисов, мыщъх ради эксперимента создал "троянское расширение" (в кавычках потому, что вся его зловредность сводилось к диалоговому окну грозного вида с надписью "сейчас вам будет нехорошо, а потом еще хуже"), и был просто _ошеломлен_ насколько проста процедура регистрации и каких усилий стоит закачать "троянское" расширение в общий доступ. Никаких. В смысле усилий. Просто берешь и закачиваешь. И прежде, чем разъяренные пользователи успели написать абузу (от английского abuse – жалоба), "троянца" скачало и установило нехилое количество человек. И ведь это был явный "троян", а если бы он действовал тихо, скрытно и незаметно — что тогда?

Сразу же возникает вопрос — какими полномочиями обладают расширения? Ответ: разработчики браузера приложили определенные усилия, чтобы этим самые полномочия не выходили за рамки приличий, ограничиваясь действиями, совершаемыми над текущей страницей браузера. А у Лиса еще и над его настройками (что дает возможность незаметно прописать хакерский proxy для кражи трафика, а потом быстро все вернуть обратно и никто ничего не заметит).

Отформатировать диск или внедрить вируса в исполняемые файлы расширения не могут. Теоретически. Практически же они написаны на Жабе и для ускорения их выполнения браузеры автоматически компилируют их код в память, а ошибок в этих компиляторах столько… Передать управление на заранее подготовленный машинный код после такой компиляции плевое дело, а машинный код может _все_ (ну, пускай и не совсем все, с учетом привилегий браузера и локальных дыр в операционной системе). Имеются и другие просчеты как в механизме взаимодействия расширений с браузером, так и в Жаба-машинах.

Короче говоря, расширения небезопасны, особенно Лисьи. У Оперы в этом смысле дела обстоят намного лучше, но все-таки потенциальная угроза атаки остается вполне реальной и осязаемой. А потому — ни в коем случае не скачивайте расширения, прежде чем их не скачает толпа народу и не убедится в их праведности и верности аллаху. Во всяком случае, антивирусы распознавать нехорошие расширения еще не научились и навряд ли озаботятся этой проблемой в дальнейшем. Хотя… антивирусный бизнес — это индустрия, проворачивающая миллиарды долларов и как только пользователи узнают, что расширения небезопасны и поднимется крик и галдеж, разработчики антивирусов не упустят шанса _продать_ нам свои "пилюли", основанные на эффекте "плацебо", т.е. вере пациента в силу лекарства, но это уже совсем другой разговор.

Однажды начав скачивать расширения, уже просто не можешь удержаться от соблазна упростить свою жизнь, сделав ее приятной в мелочах, и совершенно не понимаешь как же ты раньше ухитрялся обходится без всех этих вещей?!

заключение

Все мы небезгрешны. И браузеры в том числе. Дыры — явление хоть и стихийное, но неизбежное. А против стихии не попрешь. Самое лучше, что можно только сделать это прекратить _верить_ и начать активно действовать. Следить на новостями безопасности, оперативно скачивать и устанавливать обновления/свежие версии/заплатки. Использовать многоуровневые системы защиты: брандмауэры, антивирусы… Ну и, наконец, не щелкать по подозрительным ссылкам. Кстати, существует мнение, что опаснее всего блуждать по порносайтам, но это мнение глубоко ошибочно. На нормальных порносайтах с нормальными доменами (а не отстойниках типа xxxxx.narod.ru) зловредного контента практически не встречается.

И еще, в последнее время Google обзавелся антивирусом, распознающим _некоторые_ типы вредоносного контента и выдающий соответствующее предупреждения под ссылками на страницы, которые пытаются атаковать браузер, так что перед открытием подозрительной ссылки, полученной из ненадежных источников имеет смысл сначала отыскать ее в Google и посмотреть, что он скажет.

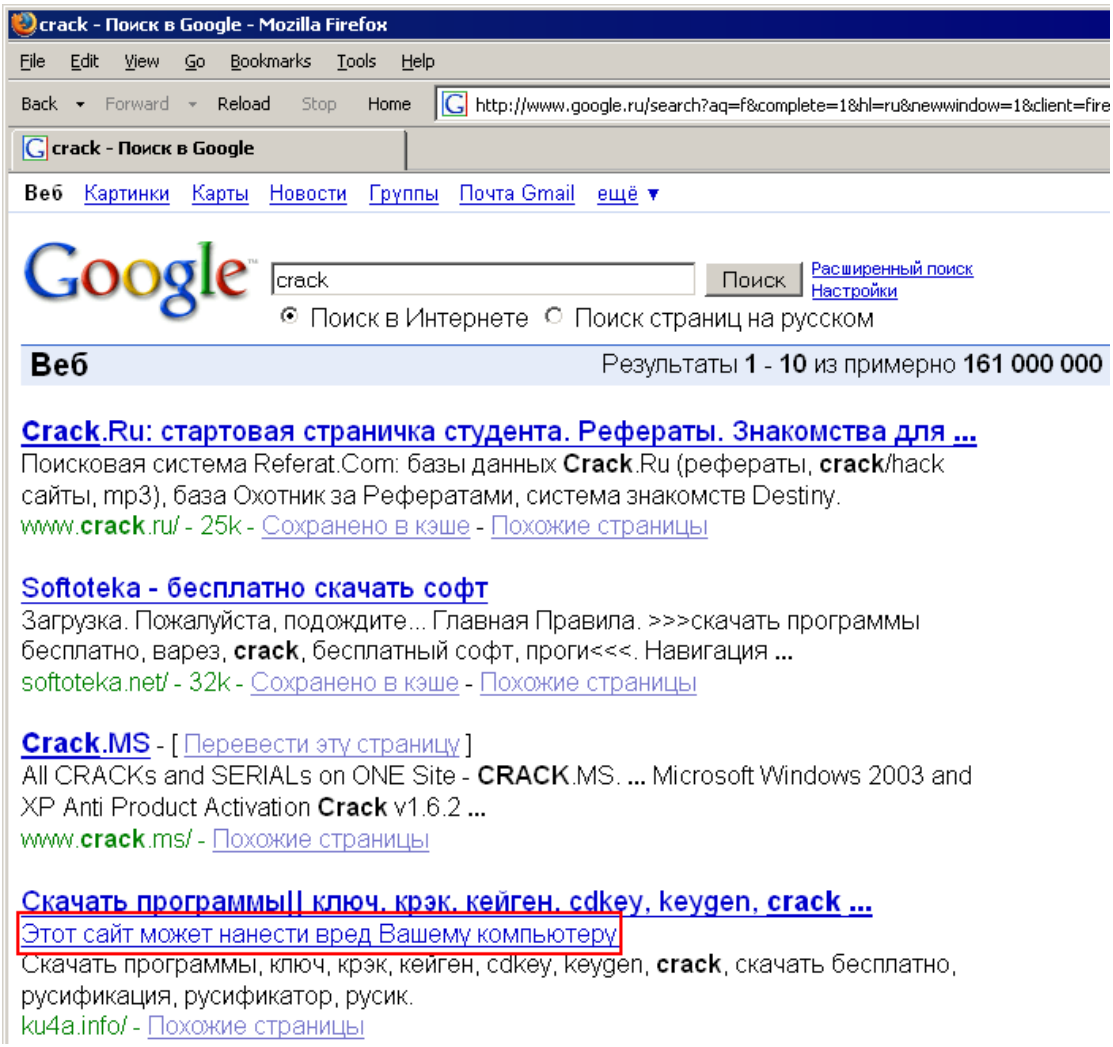


Рисунок 15 Google способен анализировать WEB-страницы и распознавать контент, атакующий браузер