

безопасный w -серфинг

крик касперски ака мышьх, по-email

сетевые обитатели подвергаются опасности на каждом шагу. темные аллеи хакерских серверов таят в себе скрытую угрозы атаки, жертвой которой становится как электронная наличность, так и содержимое жесткое диска. да и следы своего пребывания в "пикантных" заведениях замести никогда не помешает. чтобы выходить в сеть без страха, совсем не нужно знать дзюдо и быть Шварцем, достаточно просто прочитать эту статью.

введение

Прежде, чем ставить жутко навороченную сигнализацию или врезать выданный из сейфа замок, следует помнить, что информационная безопасность — это не товар, а услуга. Ни один из продуктов (как коммерческих, так и бесплатных), присутствующих на рынке, не в состоянии надежно защитить компьютер, поскольку, на каждую хитрую идею найдется своя хитрая идея (или, как говорят в народе: на каждую хитрую задницу найдется свой болт с резьбой под восемнадцать).

Обеспечивать безопасность компьютера должен профессионал, а не любитель. Этому невозможно выучиться в один день! Выходит... что эта статья бесполезна и если захотят, нас все равно поимеют? Конечно, поимеют да еще так поимеют, что только треск будет стоять! Но ключевое слово здесь: "если захотят". Опытный хакер без труда натянет "продвинутого" пользователя по самые помидоры, даже не прибегая к вазелину. Но весь фокус в том, что пользователей много, а хакеров — мало. Болтов с резьбой под восемнадцать — еще меньше.

Обезопасить себя от массовых червей, воинствующих хулиганов и "людей в погонах" вполне возможно ("там" далеко не Фон Нейманы сидят). Еще проще спрятать любовную переписку от жены или скрыть свое пристрастие к извращенным формамекса от коллег и системного администратора, даже если он вовсе не лох.

Вот для таких целей и была написана эта статья.

факторы угрозы

Количество хакерских атак неуклонно растет и значительная их часть приходится на web-браузеры. Из всех факторов риска в первую очередь можно (и нужно!) выделить следующее три "ипостаси":

- атака на сам браузер с засылкой троянской программы;
- сбор данных о пользователе (с какой страницы пришел, под каким IP);
- сохранение компрометирующих данных о посещенных страницах на жестком диске;

Поясним сказанное на конкретных примерах. Практически все браузеры страдают дефектами разработками (или в просторечии — дырами). Через дыры лезут черви, вирусы и другие вандалы. Независимо от текущей политики безопасности в настройках браузера, при посещении страницы всегда существуют угроза подцепить какую-нибудь заразу, проникающую сквозь антивирусы и брандмауэры. Причем, это относится не только к порнографическим сайтам, но и серверам весьма респектабельных компаний. Известен случай, атаки на "гостевую доску" совсем не хилой фирмы AMD, результатом которой стали тысячи зараженных пользователей. И хотя это не правило, а, скорее, экзотическое исключение, "ездить" на дырявом браузере небезопасно.

К тому же "честные" браузеры негласно передают серверу большой объем информации о пользователе: версию самого браузера (вместе с региональными настройками), языковую кодировку, часовой пояс, URL предыдущей посещаемой страницы, IP-адрес... словом, достаточно для того, чтобы "повеситься". Несмотря на то, что де-юре данная информация не считается конфиденциальной, факт ее разглашения существенно напрягает, когда мышьх выдает себя за девушку Ке-Ке, живущую (по легенде) в Японском городе Фукуока, но использует русскую версию браузера с московской Time-Zone в придачу. Так что легкий флирт очень быстро заканчивается.

Третий фактор — самый серьезный. Компьютер помнит все наши шаги, сохраняя на жестком диске уйму компрометирующей информации, которую не так-то просто удалить.

Каждый гражданин имеет право на тайное посещение сайтов нетрадиционной направленности (или например, сетевых служб доведения), гарантированное Конституцией, но далеко не каждому удается реализовать это право на практике. К тому же, пароли и прочая информация, сохраненная в куках, становится легкой добычей троянских программ, сослуживцев или остальных членов семейства.

Обеспечение собственной безопасности требует целого комплекса защитных мер, которые в грубом приближении делятся на серверные и клиентские. К серверным в первую очередь относится выбор надежного анонимного proxy, о чем мы в "хакере" уже не раз и не два писали, так что не будем повторяться, а лучше сразу займемся клиентской проблемой — то есть браузером.

выбор браузера

Самый популярный сетевой обозреватель всех времен и народов — Internet Explorer ([см. рис. 1](#)) — одновременно с этим самый небезопасный и дырявый. Практически каждую неделю в нем обнаруживается свежая порция новых дыр, а сколько ошибок остается не выявленными — остается только гадать!

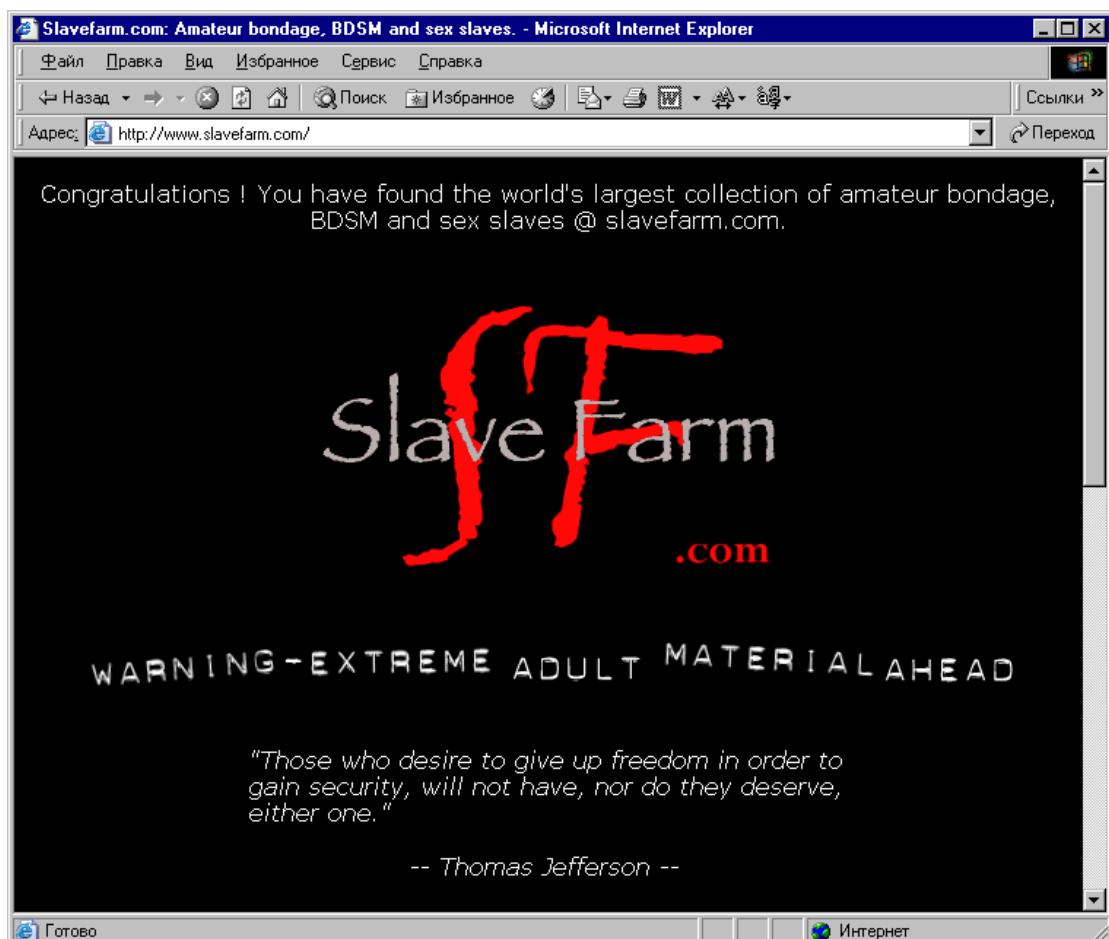


Рисунок 1 внешний вид Internet Explorer'a

Но дыры — это еще туда-сюда. Хуже всего, что IE страдает хроническим недержанием конфиденциальной информации. В первую очередь это относится к кэш'у, истории, activeX компонентам и кукам. По умолчанию, кэш размещается в каталоге: \Documents-n-Settings\user-name\Local Settings\Temporary Internet Files\ и в любой момент может быть удален по команде: сервис → свойства обозревателя → общие → временные файлы интернета → удалить файлы. Но не все так просто! За счет грубых ошибок в системе индексации часть файлов просто не удаляется (в чем легко убедиться, заглянув в указанный каталог после его "очистки"). Кстати говоря, туда же попадают и вложения электронной почты при открытии аттачей в Outlook Express'e и штатными средствами IE они обратно уже не удаляются. Самое интересное, что индексный файл index.dat (находящийся в том же подкаталоге) физически не

очищается и продолжает хранить адреса посещенных сайтов. Да, чисто теоретически, они постепенно затираются в процессе посещения новых страниц, но... не все и не всегда.

Ниже приведен фрагмент индексного файла после его очистки штатными средствами IE. Как видно, владелец компьютера посещал сайты весьма извращенного уклона.

					DOS	3457024
C:\...\Temporary Internet Files\Content.IE5\index.dat						
0000006D10:	68 74 74 70 3A 2F 6C	6F 76 65 2E 6D 61 69 6C	http://love.mail.ru/my/message.p			
0000006D20:	2E 72 75 2F 6D 79 2F 6D	65 73 73 61 67 65 2E 70	htmlle48e2f57.Енδ			
0000006D30:	68 74 6D 6C 65 34 38 65	32 66 35 37 00 F0 AD 0B	ЛенδЛенδЛенδЛенδ			
0000006D40:	0D F0 AD 0B 0D F0 AD 0B	0D F0 AD 0B 0D F0 AD 0B	ЛенδЛенδЛенδЛенδ			
0000006D50:	0D F0 AD 0B 0D F0 AD 0B	0D F0 AD 0B 0D F0 AD 0B	ЛенδЛенδЛенδЛенδ			
0000006D60:	0D F0 AD 0B 0D F0 AD 0B	0D F0 AD 0B 0D F0 AD 0B	ЛенδЛенδЛенδЛенδ			
0000006D70:	0D F0 AD 0B 0D F0 AD 0B	0D F0 AD 0B 0D F0 AD 0B	ЛенδЛенδЛенδЛенδ			
0000006D80:	52 45 44 52 01 00 00 00	D0 92 1D 00 80 AC 7E 3E	REDR0 "T+ Am~>			
0000006D90:	68 74 74 70 3A 2F 77	77 77 2E 63 6F 6C 6C 61	http://www.colla			
0000006DA0:	72 6D 65 2E 63 6F 6D 2F	62 64 73 6D 2F 76 2F 31	rme.com/bdsm/v/1			
0000006DB0:	32 30 35 39 37 2F 64 65	66 61 75 6C 74 2E 68 74	20597/default.ht			
0000006DC0:	6D 30 38 62 63 61 63 32	65 00 AD 0B 0D F0 AD 0B	m08bcac2e.нδЛенδ			
0000006DD0:	0D F0 AD 0B 0D F0 AD 0B	0D F0 AD 0B 0D F0 AD 0B	ЛенδЛенδЛенδЛенδ			
0000006DE0:	0D F0 AD 0B 0D F0 AD 0B	0D F0 AD 0B 0D F0 AD 0B	ЛенδЛенδЛенδЛенδ			
0000006DF0:	0D F0 AD 0B 0D F0 AD 0B	0D F0 AD 0B 0D F0 AD 0B	ЛенδЛенδЛенδЛенδ			
0000006E00:	52 45 44 52 01 00 00 00	60 C7 12 00 80 A4 CF 00	REDR0 "I Ад"			
0000006E10:	68 74 74 70 3A 2F 77	77 77 2E 63 6F 6C 6C 61	http://www.colla			
0000006E20:	72 6D 65 2E 63 6F 6D 2F	62 64 73 6D 2F 76 2F 33	rme.com/bdsm/v/3			
0000006E30:	34 34 38 32 32 2F 64 65	74 61 69 6C 73 2E 68 74	44822/details.ht			
0000006E40:	6D 64 66 62 33 66 35 35	64 00 AD 0B 0D F0 AD 0B	mdfb3f55d.нδЛенδ			
0000006E50:	0D F0 AD 0B 0D F0 AD 0B	0D F0 AD 0B 0D F0 AD 0B	ЛенδЛенδЛенδЛенδ			
0000006E60:	0D F0 AD 0B 0D F0 AD 0B	0D F0 AD 0B 0D F0 AD 0B	ЛенδЛенδЛенδЛенδ			
0000006E70:	0D F0 AD 0B 0D F0 AD 0B	0D F0 AD 0B 0D F0 AD 0B	ЛенδЛенδЛенδЛенδ			
0000006E80:	52 45 44 52 01 00 00 00	C0 55 00 00 80 B5 29 E8	REDR0 "U AH)ш			
0000006E90:	68 74 74 70 3A 2F 77	77 77 2E 6C 69 6E 67 76	http://www.lingvo			
0000006EA0:	6F 2E 72 75 2F 6C 69 6E	67 76 6F 2F 54 72 61 6E	o.ru/lingvo/Tran			
0000006EB0:	73 6C 61 74 65 2E 61 73	70 31 61 31 39 66 32 35	slate.asp1a19f25			
0000006EC0:	34 00 AD 0B 0D F0 AD 0B	0D F0 AD 0B 0D F0 AD 0B	4 нδЛенδЛенδЛенδ			
0000006ED0:	0D F0 AD 0B 0D F0 AD 0B	0D F0 AD 0B 0D F0 AD 0B	ЛенδЛенδЛенδЛенδ			
0000006EE0:	0D F0 AD 0B 0D F0 AD 0B	0D F0 AD 0B 0D F0 AD 0B	ЛенδЛенδЛенδЛенδ			
0000006EF0:	0D F0 AD 0B 0D F0 AD 0B	0D F0 AD 0B 0D F0 AD 0B	ЛенδЛенδЛенδЛенδ			
0000006F00:	52 45 44 52 01 00 00 00	08 59 00 00 00 5C 1E 60	REDR0 "Y \^m			
0000006F10:	68 74 74 70 3A 2F 69	7A 76 72 61 73 68 65 6E	http://izvrashen			
0000006F20:	65 63 2E 72 75 2F 66 6F	72 75 6D 2F 69 6D 61 67	ec.ru/forum/imag			
0000006F30:	65 73 2F 61 76 61 74 61	72 73 2F 31 37 35 32 33	es/avatars/17529			
0000006F40:	30 32 38 35 32 34 32 64	32 65 63 39 39 62 32 34	0285242d2ec99b24			
0000006F50:	35 35 2E 67 69 66 00 0B	0D F0 AD 0B 0D F0 AD 0B	55.gif σЛенδЛенδ			
0000006F60:	0D F0 AD 0B 0D F0 AD 0B	0D F0 AD 0B 0D F0 AD 0B	ЛенδЛенδЛенδЛенδ			
0000006F70:	0D F0 AD 0B 0D F0 AD 0B	0D F0 AD 0B 0D F0 AD 0B	ЛенδЛенδЛенδЛенδ			
0000006F80:	52 45 44 52 01 00 00 00	70 56 00 00 C0 DE AA 13	REDR0 "pV L k!!			
1	2	3	4	5Print	6	7
8Goto	9Video	10	1			

Рисунок 2 содержимое индексного файла кэша IE после "удаления"

Решение состоит в "ручном" удалении всего содержимого папки "Temporary Internet Files", но при этом необходимо выйти из системы и войти под другим пользователем, поскольку в противном случае доступ к части файлов будет заблокирован. Однако, следует помнить, что физического удаления файлов при этом не происходит и утилиты типа GetDataBack могут вернуть их назад, пока они не будет основательно затерты новым содержимым.

История посещения страниц хранится в папке History в том же каталоге, что и Temporary Internet Files. Естественно, лучше (и надежнее всего!) очищать ее вручную. Куки лежат в папке Cookies в подкаталоге на один уровень выше. ActiveX элементы (и создаваемые ими файлы) могут храниться в любом месте диска, где только пожелаю и никакой возможности уследить за ними у нас нет, ведь фактически это обычновенные исполняемые программы!

Кстати, стоит отметить, что при определенных обстоятельствах Windows едет крышей и сохраняет все это хозяйство отнюдь не в Local Settings, а в непосредственно в самом каталоге Windows! Так что приходится быть на чеку! А еще лучше... сменить браузер на более надежный!

Opera

Широко популярный в узких кругах, этот браузер практически не содержит дыр (во всяком случае, документально подтвержденных атак зафиксированного не было) и все данные, поступающие из сети (кэш, куки, история посещений) хранятся в единственном месте — в папке Opera\profile. Там же хранятся skin'ы и другие настройки, поэтому удалять эту папку целиком не рекомендуется. В отличии от IE, она не будет воссоздана автоматически при последующем запуске браузера. А стандартные средства очистки приватного содержимого содержат ряд ошибок, в результате чего качество очистки оставляет желать лучшего.

Тем не менее, блуждая по сети с Оперой, за хакерские атаки можно не волноваться. А содержимое профиля (вместе с самой Оперой) очень легко перенести на FLASH-брелок. Тогда на жестком диске никаких следов нашего пребывания уже не остается.

К тому же, Опера поддерживает развитую и хорошо продуманную систему клавиатурной навигации, обеспечивающую _намного_ более быстрый серфинг, чем IE с его мышами (даже если эти мыши были специально спроектированы под IE). Другое немаловажное достоинство Оперы — ее бесплатность. Новые версии IE уже не являются частью операционной системы как раньше и "раздаются" только легальным пользователям Windows, а в будущем за них планируется взимать дополнительную плату.

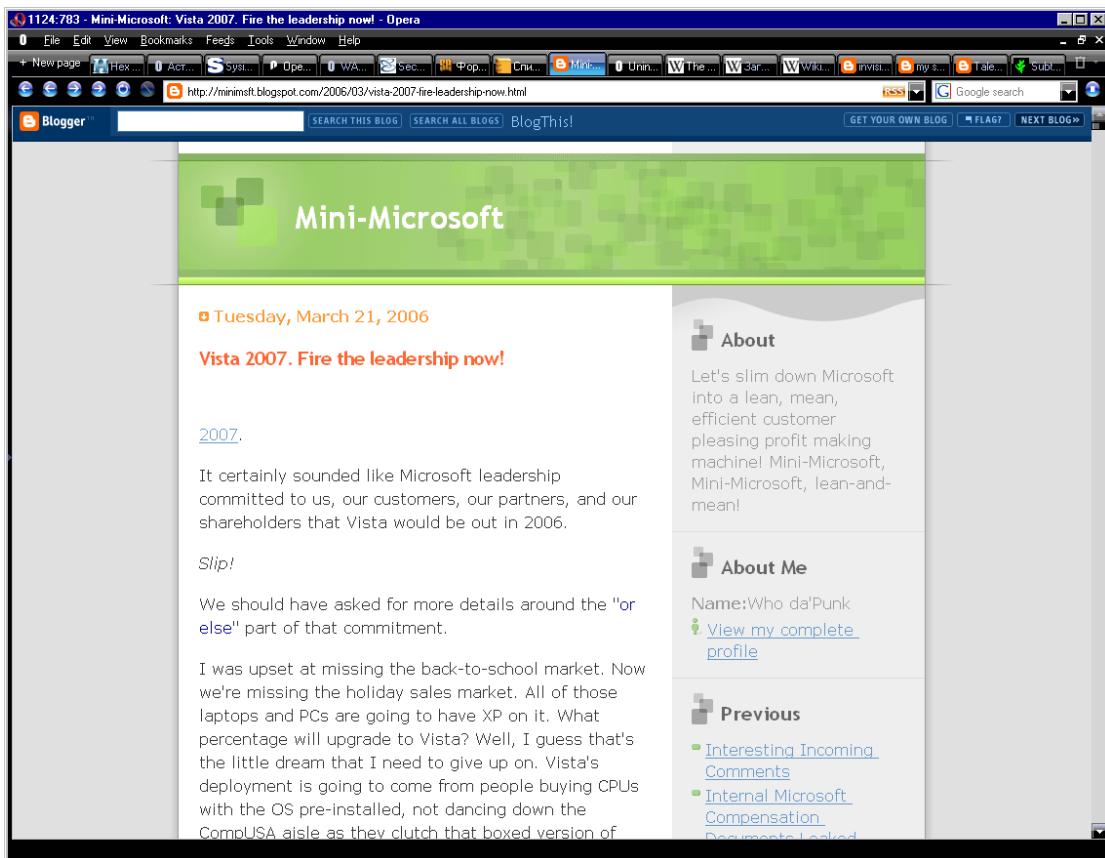


Рисунок 3 внешний вид браузера Opera

FireFox

"Горячий Лис", стихийно возникший на обломках Netscape, довольно популярный, но, увы, дырявый и категорически небезопасный браузер, причем, с каждым днем дыр в нем обнаруживается все больше и больше. И хотя массовых атак на Лисов до сих пор не наблюдалось (в силу того, что подавляющее большинство все-таки сидит под IE, а Лиса ставят себе в основном достаточно продвинутые пользователи, справиться с которыми на порядок сложнее), угроза подцепить троянскую лошадь при посещении w -страницки вполне реальна, а вот стоит ли с ней считаться или понадеяться на авось — каждый должен решать сам.

Свои следы Лис хранит сразу в двух местах: \Documents-n-Settings\user-name\Application Data\Mozilla\Firefox\Profiles\4uszwife.default помимо кучи пользовательских схем,

настроек и расширений дает приют файлам: cookies.txt и history.dat, о назначении которых можно догадаться и без комментариев. Кэш целиком сосредоточен в папке \Documents-n-Settings\user-name\Local Settings\Application Data\Mozilla\Firefox\Profiles\4uszwife.default\Cache и, как и все остальные браузеры, не всегда корректно очищается штатными средствами.

К тому же, для Лисы существует огромное количество расширений, многие из которых запоминают некоторую информацию в своих собственных местах (например, историю поисковых запросов, адреса наиболее часто посещаемых страниц и т. д.).

Так что несмотря на привлекательный антураж и агрессивное продвижение на рынок под флагом открытой программы (но как же она может быть открытой, если логотип и сопутствующее ему окружение является зарегистрированной торговой маркой, вызывавшей раскол в среде разработчиков и в состав дистрибутива Debian уже входит совсем другой Лис, не такой, каким мы его знаем), Лис не является безопасной программой, но этот недостаток с лихвой компенсируется обилием плагинов, расширяющих функциональность Лиса до совершенно недостижимых для IE границ. Пока отдел маркетоидов и дизайнеров покурит хорошей травы и выдумает феничку "реально необходимую каждому пользователю", в Лисе все необходимое реализуется сразу, как только в этом возникает потребность или кого-то озаряет свежая идея.

Тем не менее, использовать Лиса для просмотра "не детского" содержимого мышьх никому бы не рекомендовал.



Рисунок 4 Fire Fox – самый сексуальный браузер

HeatSeek

В отличии от трех предыдущих, HeatSeek — это браузер изначально ориентированный на просмотр adult-контента и потому обладающий рядом несомненных преимуществ. Во-первых, это мощная система шифрования, кодирующая всю информацию, записываемую на жесткий диск, благодаря которой достигается полная приватность и конфиденциальность. Даже если жесткий диск попадет в руки спецслужб без утюга и паяльника, расшифровать его содержимое ни за что не удастся, а нам не придется каждый раз очищать кэш. Шифруется все: содержимое самих страниц, графические изображения, история, куки и даже закладки – ну разве не прелест?! (однако, следует помнить, что **информация, физически проходящая через**

компьютер провайдера, равно как и маршрутизатор локальной сети, передается в незашифрованном виде и если она кэшируется, а обычно она кэшируется, то может быть использована для компромата, чтобы этого не произошло, необходимо использовать https проху сервера или даже более продвинутые защитные механизмы, о которых мы поговорим в другой раз).

Во-вторых, поддержка клавиши "аварийной" маскировки "чем это вы тут занимаетесь?!" вкупе с подавлением всех всплывающих окон и прочей гадости, позволяет наслаждаться порнографическими страницами без риска быть пойманным и схваченным за хвост, даже если за спиной то и дело шастают всякие любопытствующие. Попутно, HeatSeek позволяет просматривать видео-файлы, защищенные DMR (Digital Management Right – Механизм Контроля Авторских Прав), сохраняя их на диске даже тогда, когда они этому всячески сопротивляются и во всех остальных браузерах не сохраняются. В последующих версиях обещана поддержка просмотра DVD с возможностью создания собственной коллекции закладок (естественно, зашифрованных) для мгновенного перехода от одной сцены к другой.

В-третьих, имеется защита от всяких зловредных шпионских программ, стремящихся выведать о пользователе хоть какую-то информацию или подкинуть ему вредоносную троянскую лошадь.

Самое главное, что все это удовольствие не стоит ни копейки и может быть скачено с <http://www.heatseek.com/> совершенно бесплатно, причем без всякого ad-ware или другого замаскированного средства оплаты.

Но то были плюсы. Теперь поговорим о минусах. В отличии от остальных, HeatSeek не является самостоятельным браузером, а основан на движке от IE, активно использующим файл mshtml.dll. Отсюда следуют две новости: плохая и очень плохая: во-первых, мы должны иметь IE, установленный на своем компьютере, а, во-вторых, все атаки, которым подвержен IE, автоматически распространяются и на HeatSeek, что делает его использование совсем небезопасным! Поэтому, обновляться (скачивать заплатки с Microsoft Update) следует как можно чаще.

Впрочем, для Лиса существует специальное расширение, предоставляющее туже самую функциональность, что и HeatSeek: <https://addons.mozilla.org/firefox/1306>, но никаким образом не связанное ни с IE, ни с его дырами. (Впрочем, как уже говорилось, у Лиса и своих дыр достаточно спасает лишь его невысокая распространенность).

Подробнее о HeatSeek'е можно прочитать на страницах Википедии: <http://en.wikipedia.org/wiki/Heatseek>.



Home Buy Support Webmasters Company

**PRIVATE & CONFIDENTIAL
ADULT BROWSER
DOWNLOADER • PLAYER • ORGANIZER**

Download FREE **Buy GOLD**

Why Use Heatseek?

- **Private & Confidential**
Keeps your stuff safe and secure from girlfriend, family, friends. Everything you do within Heatseek stays within Heatseek.
- **Adult Web Browser**
Protects you from popups and viruses. Easy saving of images & movies from your favorite sites.
- **Video & Image Viewer**
Mark your favorite movie scenes, jump to them instantly.
- **Playlists!**
Play your files in just the right order. Just the way you like them.

[Learn More](#)

*Heatseek does not protect against law enforcement seizures. We support the fight against child pornography.

[Privacy Policy](#)

© 2006 Sun River Systems, Inc.

Рисунок 5 главная страница сайта <http://www.heatseek.com/>

тестовые браузеры

Подавляющее большинство пользователей настолько привыкли к графическим браузерам, что даже и представить себе не могут, что помимо них существуют текстовые! И не только существуют, но еще и развиваются! Казалось бы, в наш век, когда 17" мониторы стоят на каждом столе, а сайты без графики можно пересчитать по пальцем одной руки, текстовые браузеры должны были исчезнуть еще в середине девяностых годов прошлого века. Какой прок от страничек, если в них нет картинок?!

Э... ну... мышьх в растерянности теребит усы, не зная что ответить на столь идиотский вопрос. Книжки с картинками он похоронил еще в ясельной группе и с той поры больше интересовался буквами. Основную смысловую нагрузку несет именно текст. Графика (особенно в стиле современно wëб-дизайна) только затрудняет доступ к информации, рассеивает внимание и пожирает львиную долю трафика (причем совершенно зря). Конечно, существуют сайты (например, те же фото-галереи) обязанные своим рождением именно графике, но! во-первых, их не так уже и много, а, во-вторых, текстовые браузеры позволяют сохранять любую картинку на диск для ее последующего просмотра в Irfan Viewer'е или любой другой программе. Неудобно?! Скорее, просто непривычно. Человек, как известно, существует

неприхотливое и ко всему привыкающее (со временем). Ведь вопрос — какие возможности нам предоставляют текстовые браузеры, чтобы мучаться-переучиваться?!

Во-первых, это ошеломляющий уровень безопасности. Будучи очень простыми программами, текстовые браузеры, по своей природе, поддерживают минимум возможностей HTML'a и не содержат фатальных ошибок, позволяя бродить по "грязным" закоулкам, без риска подцепить сетевую заразу.

Во-вторых, скорость восприятия информации (по сравнению с графическими браузерами) повышается порядка на два. На экране виден только текст и больше ничего. Реклама вместе с сопутствующим ей информационным мусором уходит на дно. Изначально рассчитанные на клавиатуру, текстовые браузеры демонстрируют непревзойденную скорость w  -серфинга (как ни крути, на мыши все же меньше кнопок, чем на клавиатуре).

И, в третьих, как показывает практика, при работе в текстовом режиме намного меньше устают глаза и можно безболезненно сидеть за монитором дни и ночи напролет, без всякого ущерба для своего зрения.

Текстовых браузеров существует огромное множество (и время от времени появляются все новые), но хороших из них всего два: классический **lynx** (рысь), выполненный в лучших традициях терминалов 60х и редактора vi и "пижонский" **links** (переводить, я думаю не надо?) с псевдографическими окошками и меню, заставляющих вспомнить свою молодость, проведенную вместе с MS-DOS.

Оба они распространяются в исходных тестах и совершенно бесплатны. Несмотря на то, что основным ареалом их обитания являются UNIX-подобные системы, в сети можно найти множество портов и под Windows.

Главная страница Рыся расположена по адресу: <http://lynx.isc.org>, а если она вдруг окажется недоступна, на этот случай предусмотрено зеркало: <http://lynx.browser.org>. Кроме исходных текстов, документации, свежих fix'ов там же находятся ссылки на Windows-порты.

Кэш страниц, история переходов со страницы на страницу и куки по умолчанию хранятся в том же каталоге, где расположен и сам Рысь (кстати, занимающий чуть больше двух мегабайт). Он не привязан к своему местоположению, ему безразличен реестр, поэтому для достижения максимальной секретности, его рекомендуется перебросить на FLASH-брелок, чтобы не оставлять никаких следов на винте.



Рисунок 6 внешний вид текстового браузера lynx — для быстрого перехода по ссылке достаточно ввести ее номер, расположенный слева или просто подогнать курсор

Браузер links (на самом деле elinks) в последних версиях FreeBSD устанавливается основным текстовым браузером по умолчанию (до этого там был lynx). Он поддерживает JavaScript'ы и многие другие "усовершенствования" HTML'a, игнорируемые Рысем, чем и объясняется рост его популярности (впрочем, мышь этих настроений _не_ разделяет и остается верен своему древнему Рысию, собранному собственными лапами и заточенному под собственный вкус, но это уже личные предпочтения).

Исходные тексты links'a лежат на <http://artax.karlin.mff.cuni.cz/~mikulas/links>, а на <http://links.twibright.com> организован целый посвященный ему портал с кучей полезных советов, документацией, переведенной на различные языки (впрочем, русской среди них до сих пор нет), ну и, конечно, Windows-порты (куда же без них!).

В зависимости от своих настроек, links сохраняет кэш, куки и историю либо в текущей директории (именно текущей, а не своей собственной), либо в домашнем каталоге пользователя в папке .elinks.

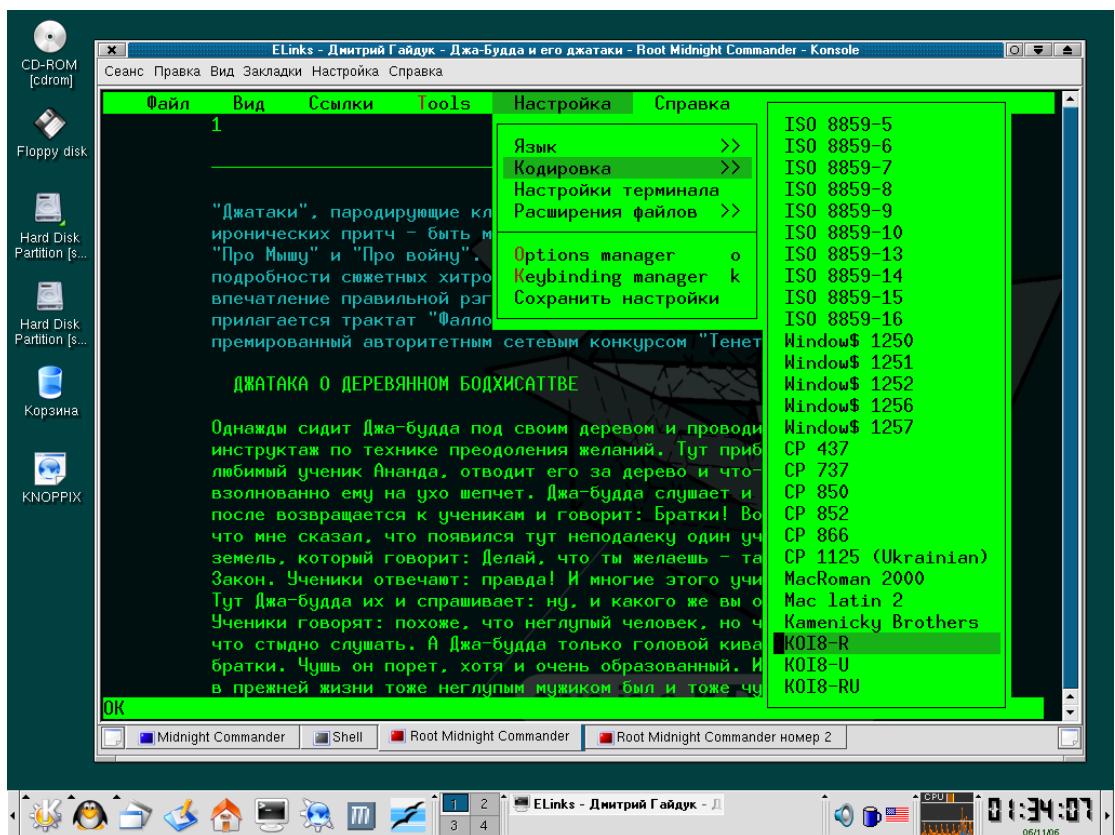


Рисунок 7 "пижонский" links, запущенный под управлением KNOPPIX

с презервативом или без (вместо заключения)

Помимо упомянутых, существуют и другие браузеры, подробнее о которых можно прочитать в специальной статье на Википедии: http://en.wikipedia.org/wiki/List_of_web_browsers (на английском языке).

Разумеется, не все браузеры одинаково безопасны, точнее говоря, большинство из них катастрофически небезопасны (как, например, IE). Текстовые браузеры — наиболее защищенные. Они же — наименее востребованные.

Ирония судьбы? Вовсе нет! Безопасность и свобода антагонистичны по своей природе. То есть, являются борьбой двух противоположностей. Философия — философией, а в реальной жизни приходится выбирать либо комфорт, либо защищенность. Компромиссных браузеров не существует, как не существует компромиссных презервативов. Массовая истерия по поводу мифического СПИДа не имеет под собой никаких оснований. Вероятность заражения не так уж и велика, а медицина сейчас лечит все, в том числе и зараженные компьютеры. Главное — не пренебрегать резервированием и не переоценивать значимость собственной репутации. Скрывать свои естественные наклонности, прятаться от жены и друзей, боясь прослыть

извращенцем... нет, это не для мышьхей. Но... каждый выбирает свой жизненный путь сам. Задача этой статьи вовсе не в том, чтобы кого-то куда-то наставить, а показать какие существуют технические средства и как ими пользоваться, чтобы продолжить свое пребывание в "скорлупе" из которой со временем может быть кто-нибудь да выпустится.

>>> врезка что еще можно предпринять для обеспечения собственной безопасности

Большинство персональных брандмаузеров по умолчанию ведут логи, чтобы в случае атаки было можно разобраться кто нас поимел и куда. Естественно, перед посещением "сакраментальных" местечек сети, протоколирование лучше выключить. А при наличии статического IP нeliшне позвонить провайдеру и попросить исключить себя из области кэширования (по умолчанию, провайдеры кэшируют информацию на своих серверах, экономя на входящем трафике, ведь клиент платит за скэшированные данные по полному прайсу), правда это может несколько замедлить скорость w b-серфинга, но зато уменьшит количество оставляемых следов.