Бесплатные антивирусы: много ЗА и чуть-чуть ПРОТИВ

Владимир Безмалый

Нужно признать, что не только полезное, но и вредоносное ПО — один из наиболее быстроразвивающихся секторов IT-индустрии, и потому большинство пользователей домашних ПК (если не вообще все) так или иначе сталкивались с проблемами, им вызываемыми.

Так, только за третий квартал 2011 г., по данным «Лаборатории Касперского», было отражено 226 116 594 атаки, проводившейся с интернет-ресурсов, размещенных в разных странах мира. Всего в этих инцидентах было зафиксировано 107 413 уникальных модификаций вредоносных и потенциально нежелательных программ (стоит уточнить, что здесь приведена наиболее свежая статистика на время подготовки статьи. — *Прим. ред.*).

Более 75% всех заблокированных веб-угроз — вредоносные URL (адреса веб-страниц с ботами, троянцами-вымогателями и т.п.). Пользователи рискуют попасть туда двумя способами. Во-первых, их тайком перенаправляют с сайтов, в том числе и взломанных легитимных, с внедренными вредоносными скриптами (атака типа drive-by). Во-вторых, зачастую сами они щелкают на опасных ссылках. Злоумышленники распространяют их по электронной почте и в социальных сетях, публикуют на сомнительных или взломанных сайтах, подсовывают в поисковых выдачах, используя методы Blackhat SEO.

Специалисты «Лаборатории Касперского» также составили рейтинг веб-ресурсов, с которых пользователи Kaspersky Security Network (далее — KSN) в третьем квартале 2011 г. чаще всего сами пытались перейти по вредоносным ссылкам.

Среди источников «добровольных» переходов на опасные сайты лидирует социальная сеть Facebook. На компьютерах пользователей KSN в ней ежедневно блокировалось почти 100 тыс.

Top 3 источников перехода по вредоносным ссылкам Q3 2011

Название сайта	Среднее ежедневное количество попыток перехода
Facebook	96 000
Google	30 000
«Яндекс»	24 000

▶ Карта распространения заражений из Сети за третий квартал 2011 г.

попыток перехода по вредоносным ссылкам. Вирусописатели прибегают к множеству приемов социальной инженерии, чтобы ввести пользователей в заблуждение и заставить щелкнуть на ссылке. Больше всего киберпреступники любят использовать горячие темы, заманивая любопытных в ловушки. Традиционно самыми популярными темами-приманками стали утечка пикантных фото голливудских знаменитостей и бесплатная раздача iPhone 5.

На втором и третьем местах расположились поисковые системы Google и «Яндекс». К сожалению, поиск также может быть опасен. Злоумышленники активно применяют технику Blackhat SEO и обманывают поисковые машины. В результате на первые страницы выдачи по популярным запросам попадают ссылки на зараженные сайты. Еще одна причина такого высокого места поисковых систем в данном рейтинге заключается в том, что со страницы поисковой выдачи пользователи могут попадать на популярные веб-сайты, взломанные злоумышленниками. Естественно, о взломе никто и не подозревает до тех пор, пока не появятся очевидные симптомы заражения.

Страны, где пользователи подвергаются наибольшему риску заражения через Интернет

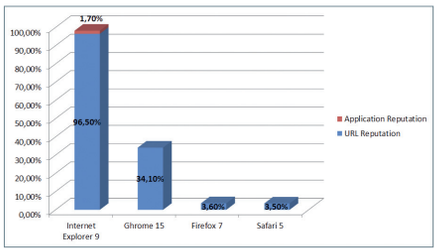
Место	Страна	Уникальные пользователи, %
1	Россия	50,0
2	Оман	47,5
3	Армения	45,4
4	Белоруссия	42,3
5	Азербайджан	41,1
6	Казахстан	40,9
7	Ирак	40,3
8	Таджикистан	39,1
9	Украина	39,1
10	Судан	38,1

Чтобы оценить степень риска заражения через Интернет, которому подвергаются компьютеры в разных странах мира, было подсчитано, насколько часто в течение квартала пользователи в каждой стране сталкивались со срабатыванием веб-антивируса.

То, что Интернет — главный источник зловредов, известно уже лет пятнадцать. И так же давно все понимают, что защиту от вредоносного ПО обеспечивает сочетание различных способов обороны, а именно:

- установка обновлений как для ОС, так и для приложений;
- работа с правами обычного пользователя (или «без административных полномочий в системе»);
- применение интернет-фильтров в браузерах (точнее, в соответствии с терминологией, принятой компанией Microsoft, использование URS — URL Reputation Service и ARS—Application Reputation Service);
- использование антивирусных средств;
- проявление собственной осмотрительности.

Будем считать, что вы следуете всем этим рекомендациям. Однако насколько эффективна защита с помощью интернет-фильтров, встроенных в браузеры? Действительно ли надежно вас могут защитить ваши антивирусные средства? К тому же на просторах бывшего СССР пользователи, как правило, предпочитают бесплатные антивирусы. Способны ли они обеспечить такой же уровень защиты, что и их платные аналоги?



▶ Эффективность интернет-фильтров браузеров

Было проведено тестирование эффективности интернет-фильтров браузеров, опубликованное NSS Lab, результаты которого, представленные в отчете от 6 февраля 2012 г., показаны на рисунке выше.

Обращает на себя внимание резкий отрыв браузера Google Chrome от браузеров Firefox и Safari, что вызывает невольное удивление, ведь по идее все они используют одни и те же базы вредоносных ссылок.

Как оказалось, компания Google разработала собственную функциональность фильтра безопасного просмотра, чтобы блокировать злонамеренные загрузки. Такая возможность недоступна другим браузерам, использующим API Safe Browsing protection (Firefox и Safari). Тем самым, применив односторонний хеш, Google чрезвычайно затруднила для третьей стороны получение доступа к содержанию списка злонамеренной загрузки.

К тому же стоит учесть, что данные тесты проводились на сайтах, расположенных в Северной Америке. Ситуация в русскоязычном сегменте Интернета будет несколько иной.

Также многое зависит от популярности того или иного ресурса. Естественно, в первую очередь будут обрабатываться ссылки, которые ведут на сайты, находящиеся в начале поискового списка.

В данном тестировании для проверки эффективности работы интернет-браузеров в режиме фильтрации были отобраны 100 вредоносных ссылок из русскоязычного сегмента Интернета. После этого на ПК были последовательно установлены последние версии браузеров Internet Explorer, Google Chrome, Safari, Opera и Firefox.

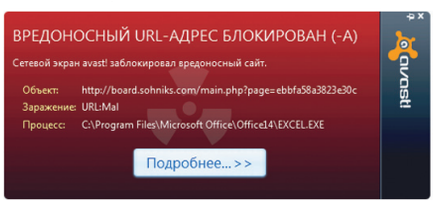
Количество вредоносных ссылок получилось таким: IE — 3%, Google Chrome — 0, Safari — 0, Opera — 1, Firefox — 0%. Неутешительные результаты. В принципе их можно было предсказать заранее.

Почему же они получились такими? Это вполне резонный вопрос, ведь в тесте NSS Labs браузер IE9 достиг 98%. В общем, все вполне очевидно. В процессе тестирования использовались ссылки на малоизвестные сайты, а поскольку в сервисах репутации обрабатываются в первую очередь более распространенные, то обработка наших ссылок была отложена на потом.

Промежуточный вывод из всего изложенного выше таков: при посещении сайтов с низким рейтингом фильтры репутаций практически бессильны. И если вы планируете хотя бы иногда посещать ресурсы второго эшелона, стандартными средствами системы не обойтись, нужен антивирус. Но какой? Подойдет ли бесплатный?

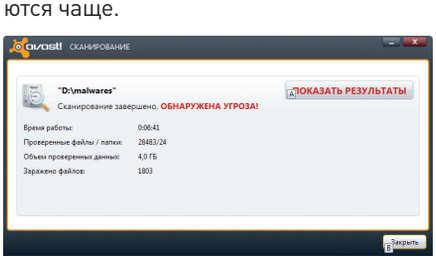
Я решил провести сравнение платных и бесплатных версий популярных у нас Avast!, Avira и AVG на той же базе вредоносных ссылок. Причем не оценивались антивирусы разных марок, а определялась эффективность платной и бесплатной версий одного вендора.

В ходе тестирования с бесплатной версией антивируса Avast Free было обнаружено 22% вредоносных ссылок, а в случае применения Avast! Internet Security — 43%. Далее я испытал обе эти программы на устойчивость к коллекции вредоносного ПО (объемом 4 Гбайт) за январь 2012 г., взятой с сайта http://malwares.pl .



▶ Блокирование вредоносных ссылок с помощью Avast!

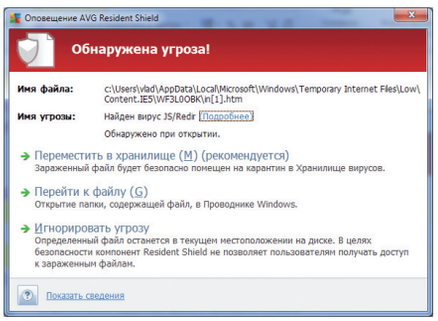
Как показала проверка, Avast! Free обезвредил 81% зловредов, а Avast! Internet Security — 82%. Следовательно, базы сигнатур используются одинаковые, единственное различие в том, что на Avast! Internet Security они обновляются чаще.



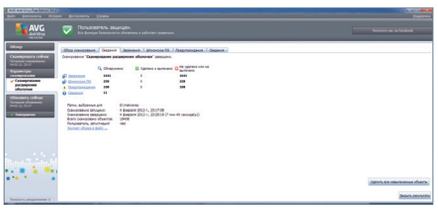
▶ Результаты сканирования

При исследовании с бесплатной версией антивируса AVG Free было обнаружено 10% вредоносных ссылок, а при использовании AVG Internet Security — 15%.

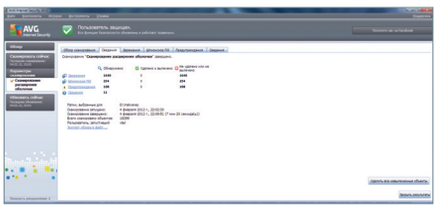
Когда проводился тест на базе вредоносного ПО, то программа AVG Free выявила 89,5%, а платный AVG Internet Security чуть-чуть отстал от него, достигнув 89,3%.



▶ AVG Resident Shield

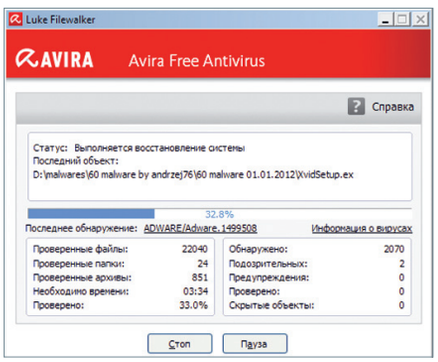


▶ Тестирование AVG Free



▶ Проверка AVG Internet Security

В процессе исследования у бесплатной версии антивируса Avira Free оказалось 9,2 % вредоносных ссылок, а Avira Internet Security распознал 15%. В ходе сканирования результаты получились 93,0% и 93,5% соответственно.



▶ Проверка Avira Free Antivirus

Что бы там ни говорили разработчики, базы сигнатур в платной и бесплатной версиях одинаковы, а значит, при сканировании будут получены схожие результаты в процессе обнаружения вредоносного ПО. Но если речь идет об интернет-угрозах, стоит отметить, что даже связка фильтра интернет-браузера и бесплатного антивируса обеспечит более низкие результаты, чем платный антивирус того же производителя. Поэтому, как ни печально, за собственное спокойствие имеет смысл немного доплатить. ■