Ты туда не ходи, ты сюда ходи…

Большинство злоумышленников в Интернете при атаке в той или иной мере используют приемы социальной инженерии. Как защититься?

Безмалый В.Ф.

MVP Consumer Security

Microsoft Security Trusted Advisor

Сегодня сложно представить себе работу с компьютером без Интернет. Дома или на работе, так или иначе мы общаемся через Интернет, читаем новости, совершаем покупки. Однако стоит понимать, что Интернет это не только среда для обмена данными, но и место где каждый из нас в той или иной мере может подвергнуться атакам со стороны злоумышленников.

Какие это могут быть атаки? В первую очередь атаки социальной инженерии (фишинг) и атаки вредоносного программного обеспечения. При этом следует учесть, что если ранее можно было советовать не ходить на сайты связанные с порнографией или различного рода «кряками» к программному обеспечению, то сегодня этого явно не достаточно.

Специалисты G Data SecurityLabs разделили вредоносные и фишинговые сайты на тематические категории и выделили Top10 самых опасных видов сайтов, где в 2011-начале 2012 года подхватить вредоносное ПО было проще всего.

Для начала рассмотрим статистику.

Во второй половине 2011 года число вредоносных семей увеличилось в 6,8 % в сравнении с этим же периодом в предыдущем году, что в общей сложности составило 1 300 146 новых типов зловредов. Иными словами, каждый день мошенниками создается в среднем около 7 229 вредоносных ссылок. Более того в 2011 году число вредоносных семей даже превзошло ожидания специалистов из лаборатории безопасности G Data SecurityLabs и составило более 2,575 млн. новых типов зловредов.

Рисунок 1 Распределение атак по тематике сайтов

Первое место в Top10 самых опасных сайтов занимают тематические порталы о технологиях и телекоммуникациях (16,2 %). В эту категорию входят веб-сайты о компьютерах, технологиях связи, мобильных новинках, о сети Интернет и прочее. Самое интересное, что посетители подобных порталов – зачастую люди грамотные в области информационной безопасности, но именно они принимают основной удар от интернет-атак. Во вторую группу входят сайты под общим названием бизнес (11,3 %): бизнес-издания, порталы бизнес-новостей, всевозможных курсы лекций, сервисы для повышения эффективности бизнеса. И только третью позицию с долей чуть больше 10 % занимают сайты с порнографическим контентом, которые всегда имели дурную репутацию из-за содержания вредоносного кода. Как бы то ни было исследование, проведенное G Data в прошлом году, показывает отсутствие какой-либо связи между порнографическим содержанием и возможностью заражения ПК. Достаточно закономерно, что сайты, связанные с обменом файлов и peer-2-peer (7,1 %) соединением, также находятся в первой пятерке рейтинга. Огромный объем вредоносных файлов распространяется вместе с нелегальным контентом среди любителей преступить закон об авторском праве. С этой группой напрямую связана и следующая категория опасных сайтов, которая расположилась на шестом месте, – развлечения (5,2 %). К ней относятся развлекательные порталы с музыкой, фильмами, видео с концертов, сайты с новостями из мира шоу-бизнеса, сплетнями о знаменитостях.

Категория с блогами (3,7 %), занимающая восьмую позицию включает любые виды блогов, от фото, аудио и кино-блогов, до стандартных текстовых блоговых площадок. Так как большая часть контента на подобных сайтах формируется самим пользователем, то нерадивым авторам блога будет несложно ввести своих читателей в заблуждение и заманить на опасные ссылки. Зачастую блоговые платформы не могут похвастаться хорошим техническим оснащением, которое поможет противостоять опасностям. Это позволяет злоумышленникам внедрять вредоносный контент в заметной или незаметной форме и причинять вред читателям того или иного блога, заинтересованным в его тематике. И последние два места разделили сайты о путешествиях (3,5 %) и игровые порталы (3,3 %).

Но, даже учитывая составленный рейтинг, нельзя говорить о том, что тема сайта является главным фактором для кибермошенников в вопросе размещения опасных ловушек. Еще больше их интересует количество наивных пользователей, которые посетят сайт, и минимальные затраты для заражения портала. Поэтому безопасность того или иного веб-сайта или сервера напрямую зависит от того, насколько хорошо защищены все его компоненты от всевозможных атак. Например, если существует уязвимость в системе управления контентом, в плагине или программе, это значит, что каждый веб-сервер, оборудованный этим же компонентами, оказывается в зоне риска независимо от наполнения сайта. А, как известно, обнаружив одну уязвимость, мошенники начинают осуществлять массовые атаки и распространять вредоносные эксплоиты в подобных системах, о чем свидетельствуют атаки Lizamoon или TimThum в 2011 году. Соответственно популярные стандартные сайты, привлекающие большое количество пользователей, становятся главной мишенью для злоумышленников.

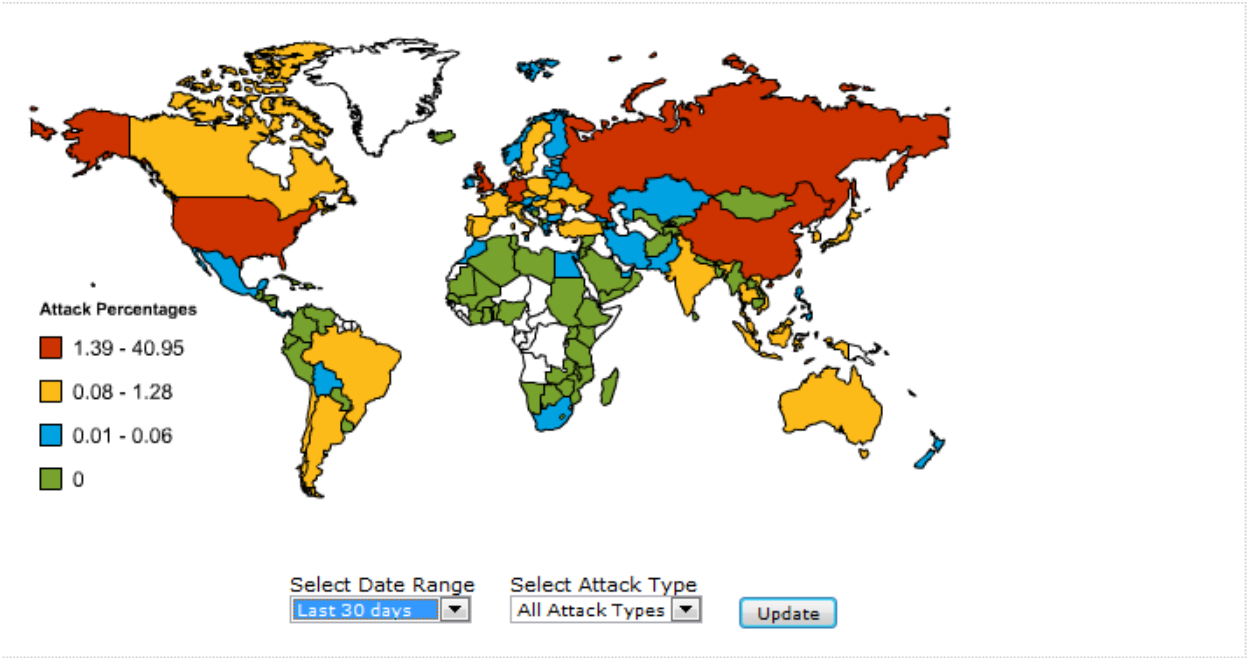


Рисунок 2 Карта интернет-атак за апрель 2012 года

Как следует из рисунка 2, наибольшее количество атак осуществляется в США, Росси и Китае.

Вместе с тем следует учесть, что количество атак растет год от года (рисунок 3)

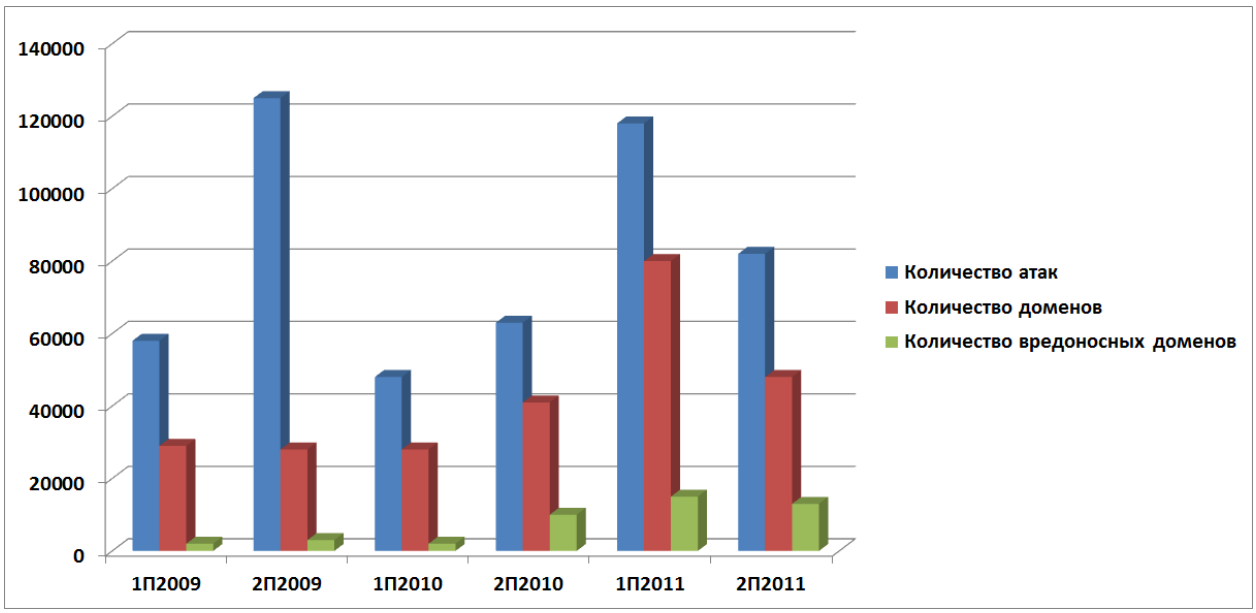


Рисунок 3 Количество атак по версии Anti-Phishing Work Group за 2009-2011 годы

Вместе с тем, следует учесть, что среднее время жизни фишинговых сайтов невелико, а, следовательно, их достаточно сложно обнаружить.

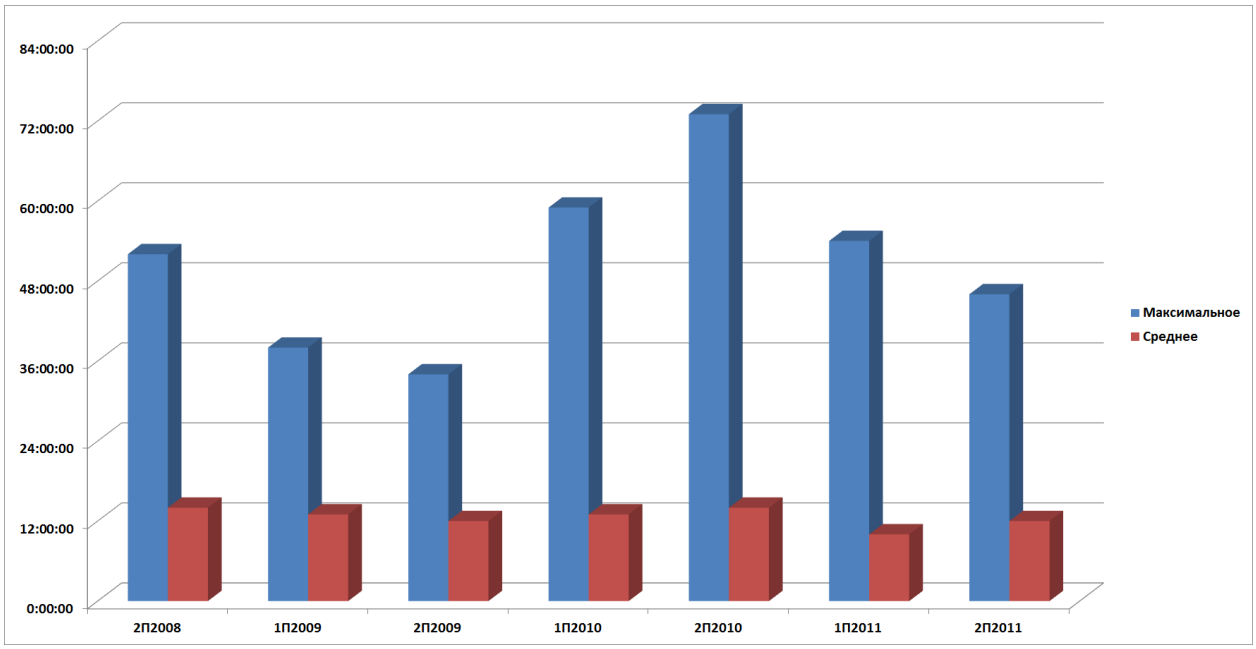


Рисунок 4 Время жизни фишинговых сайтов

Как видно из отчета APWG – среднее время жизни фишингового сайта составляет сегодня менее 12 часов. Соответственно, исходя из этого можно сказать, что время на определение того, является ли сайт фишинговым или нет – резко уменьшается. В данном случае выигрывает тот производитель антифишингового фильтра, кто сможет быстрее и качественнее не только провести проверку, но и доставить эти данные пользователям. Естественным в данном случае является использование облачных технологий.

В данной статье мы рассмотрим несколько вариантов антифишинговой защиты. Это как антифишинговые фильтры в браузерах, так и бесплатные антифишинговые плагины.

Для теста были отобраны 100 вредоносных ссылок с помощью продукта Kaspersky Internet Security 2012.

Согласно отчета NSS Labs за 3-й квартал 2011 года браузеры блокировали вредоносные ссылки следующим образом

IE9	Chrome 12	Firefox 4	Safari 5	Opera 11
99.2%	13.2%	7.6%	7.6%	6.1%

Однако стоит учесть, что данное исследование проводилось на англоязычных сайтах. Если провести его на русскоязычных – результаты будут совсем иными.

IE9	Chrome	Firefox
24%	0%	0%

Как видите, по результатам можно сказать, что фильтрация только с помощью фильтров браузеров – явно недостаточна.

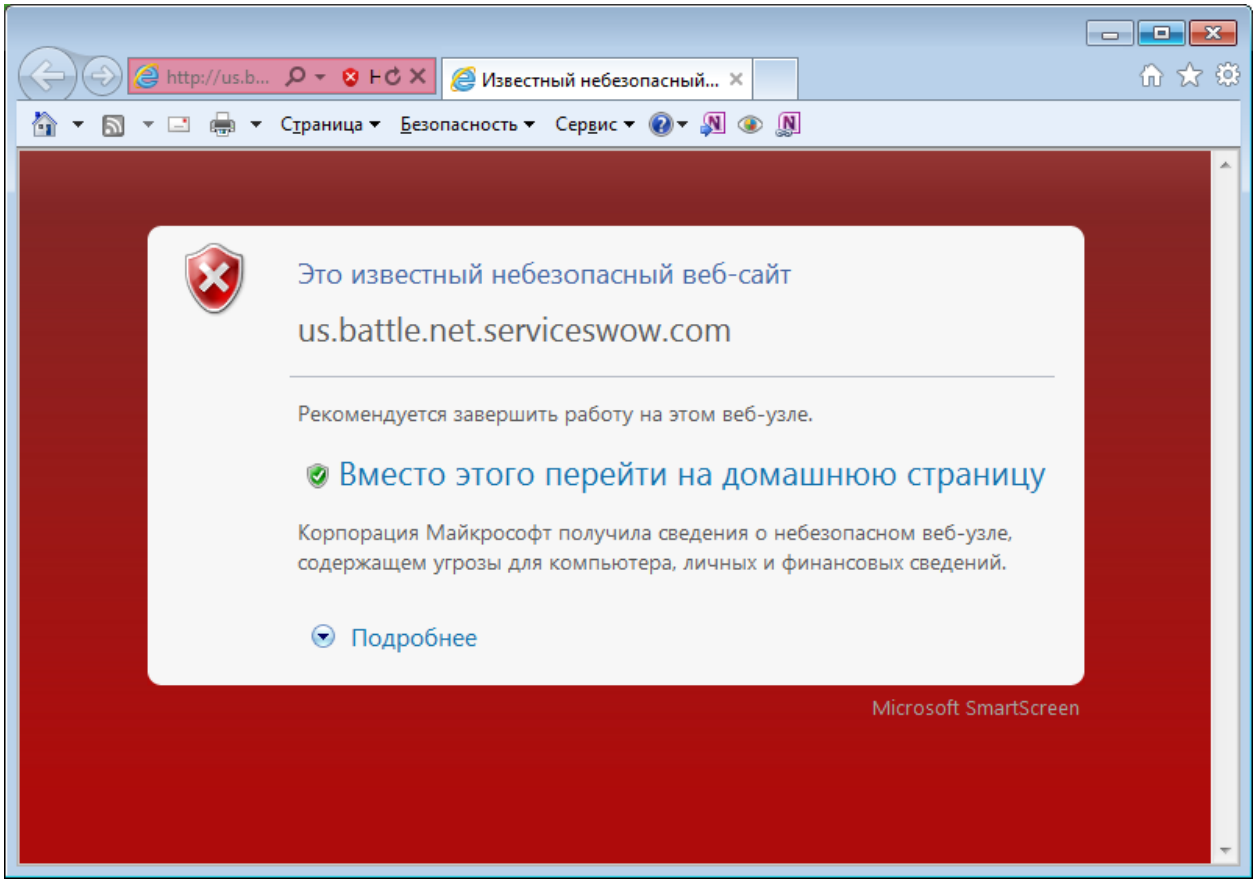


Рисунок 5 Фильтрация в IE9

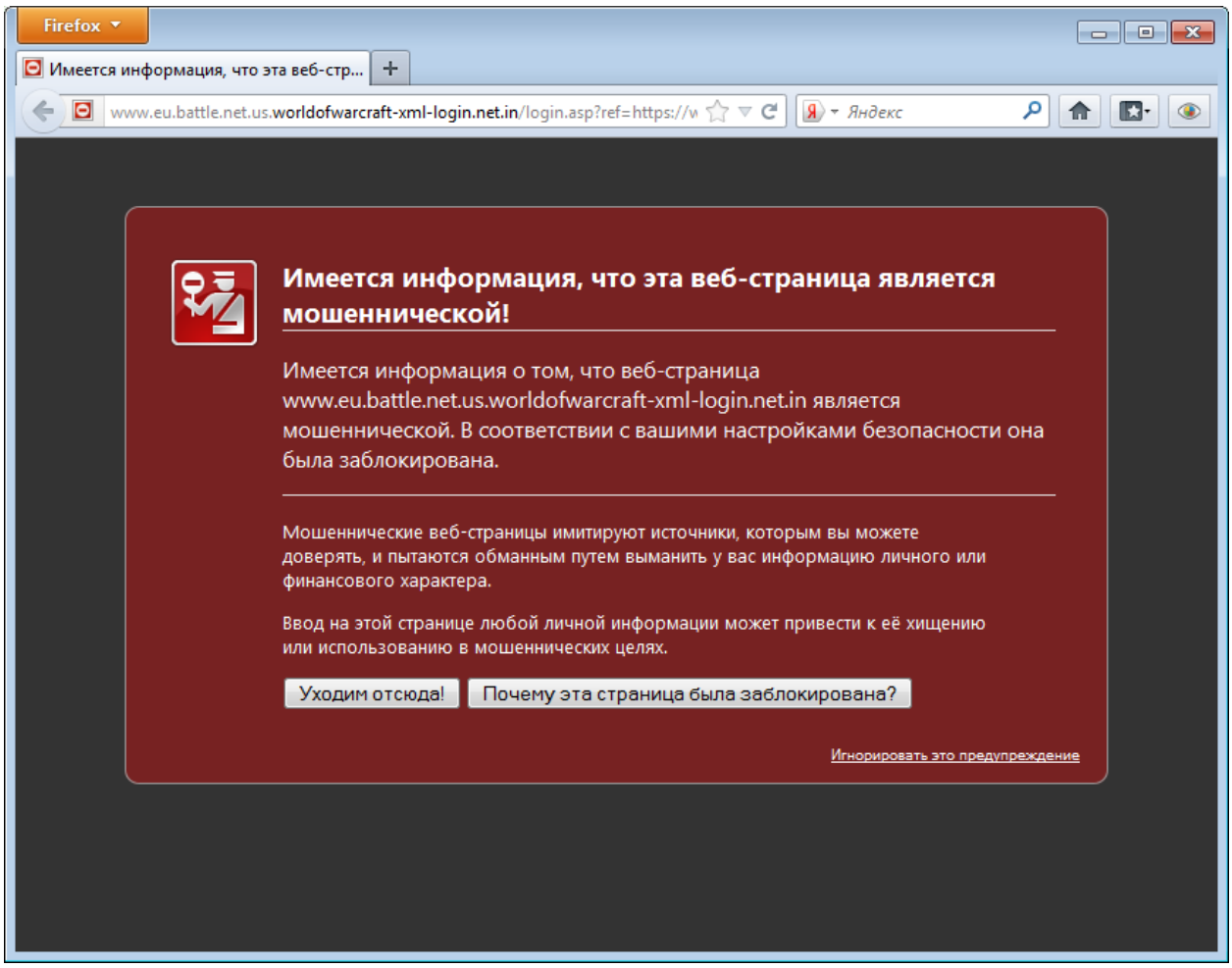


Рисунок 6 Результат фильтрации в Firefox

Вторым вариантом фильтрации является фильтрация с помощью дополнительных внешних антифишинговых фильтров.

На сегодня существует большое количество бесплатных внешних фильтров фишинговых ссылок и вредоносного ПО. Рассмотрим некоторые из них.

WOT

WOT (Web of Trust) — это бесплатная надстройка к браузеру, которая предупреждает Интернет-пользователя во время поиска информации или совершения покупок о потенциально небезопасных веб-страницах. WOT совместим с такими браузерами как Internet Explorer, Mozilla Firefox, Opera (в 11 версии при помощи расширения), Google Chrome и Safari.

WOT создан на основе сообщества, и уровень доверия к тому или иному сайту зависит от оценок, выставленных его предыдущими посетителями. Рейтинги постоянно обновляются миллионами пользователей WOT-сообщества, а также многочисленными проверенными ресурсами (например, списки фишинговых сайтов). Количество русскоязычных активных пользователей WOT составляет 103 тысячи.

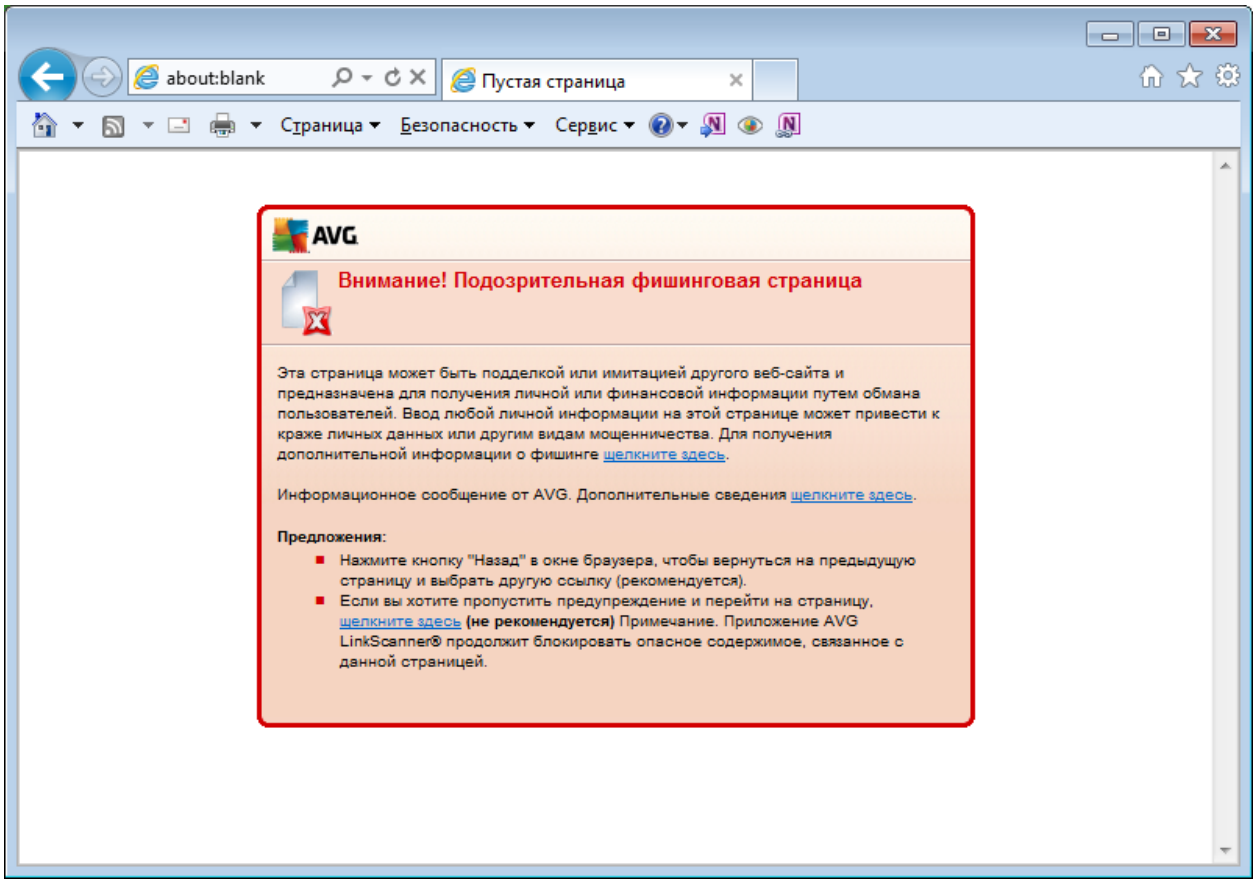
http://www.viruslab.ru/download/wot/ie.php - ссылка на плагин для Internet Explorer

http://www.viruslab.ru/download/wot/firefox.php - ссылка на плагин для Firefox

AVG LinkScanner for Windows

Бесплатный плагин для Internet Explorer и Firefox.

Загрузить его можно по адресу http://www.avg.com/ww-en/linkscanner



Panda Cloud Security

Бесплатный облачный антивирус http://www.cloudantivirus.com/en/#!free-antivirus-download

G Data Cloud Security

Бесплатный антивирус http://www.free-cloudsecurity.com/ru/

G Data CloudSecurity - это новый бесплатный плагин для самых распространенных браузеров Internet Explorer и Mozilla Firefox

Плагин эффективно блокирует доступ известных вредоносных программ и фишинговых веб-сайтов в реальном времени. Его можно использовать вместе с другим установленным защитным ПО сразу после установки, дополнительные настройки не требуются. Простой путь к большей безопасности в Интернете от G Data, первоклассного производителя защитного программного обеспечения.

- Совместим со всеми другими программами безопасности
- Препятствует доступу вредоносных программ и фишинговых веб-сайтов
- Устанавливается один раз, не требует обновлений
- Не влияет на работу компьютера

- Идеальное дополнение к бесплатным антивирусным программам

Для Internet Explorer результаты тестов будут выглядеть следующим образом

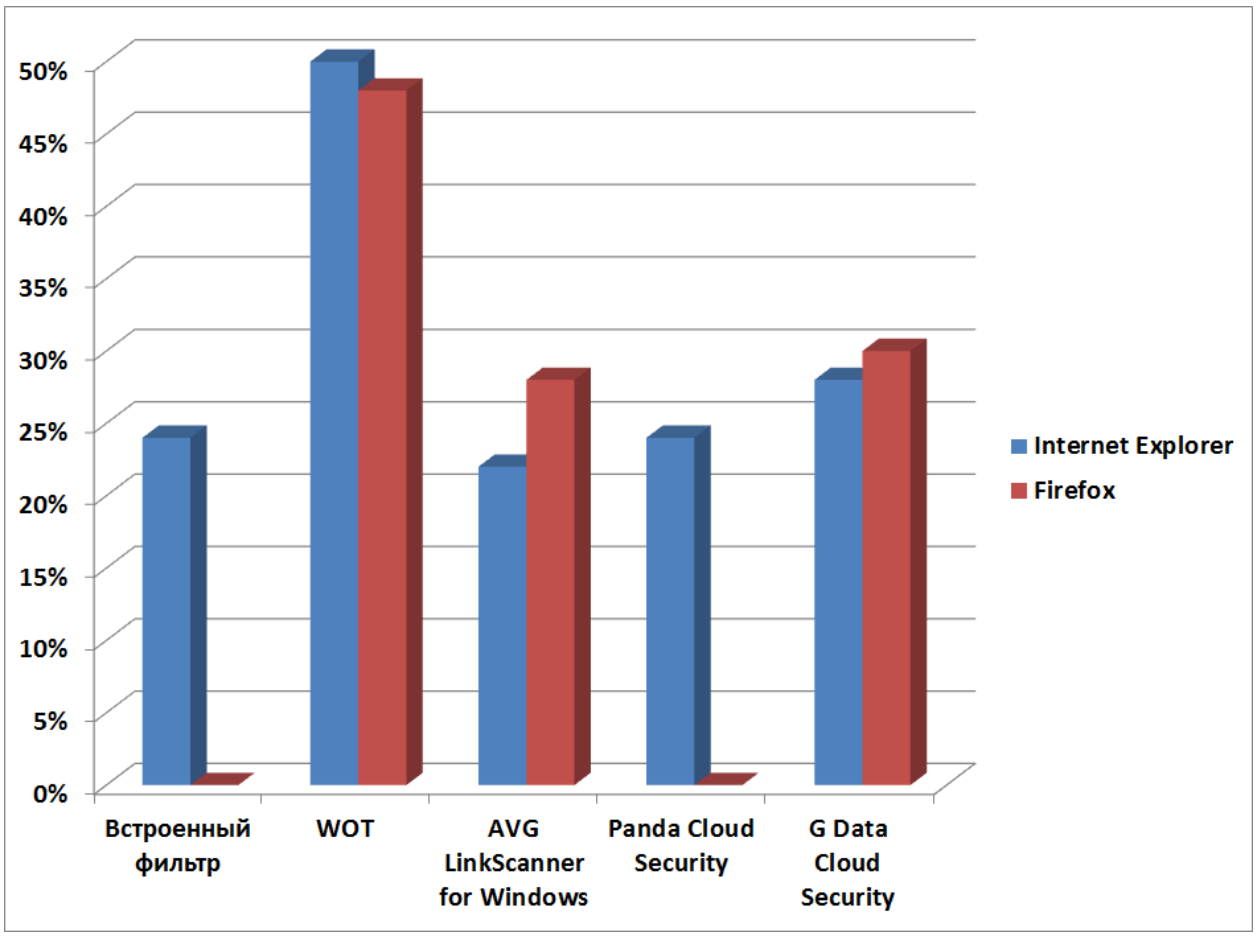


Рисунок 7 Результаты тестов плагинов

Вывод, который можно сделать на основе проведенного исследования.

Если вы хотите использовать исключительно бесплатные плагины, то стоит обратить внимание на WOT, однако максимальную безопасность от атак подобного рода все же можно обеспечить с помощью Kaspersky Internet Security 2012. Как было отмечено выше, коллекция вредоносных ссылок была собрана именно с помощью данного продукта, т.е. он обеспечил 100% защиту.