Непростая защита от фишинга

Владимир Безмалый

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

Какие это могут быть атаки? В первую очередь с помощью методов социальной инженерии (фишинг) и атаки вредоносного программного обеспечения. При этом следует учесть, что если раньше можно было посоветовать не ходить на сайты с порнографическим содержимым или хакерским программным обеспечением, то сегодня этого явно недостаточно. Специалисты компании G Data SecurityLabs разделили вредоносные и фишинговые сайты на тематические категории и выделили Top10 самых опасных видов сайтов, где в 2011-м — начале 2012 года подхватить вредоносное программное обеспечение было проще всего (рисунок 1). По статистике компании, во второй половине 2011 года число вредоносных программ увеличилось на 6,8% по сравнению 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 программ даже превзошло ожидания специалистов из лаборатории безопасности G Data SecurityLabs и составило более 2,575 млн новых типов вредоносных программ.

Первое место в Top10 самых опасных сайтов занимают тематические порталы о технологиях и телекоммуникациях (16,2%). В эту категорию входят сайты о компьютерах, технологиях связи, мобильных новинках, о сети Интернет и пр. 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, всевозможные 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 содержимым сайта и возможностью заражения компьютера. Достаточно закономерно, что сайты, связанные с обменом файлов и соединением peer-2-peer (7,1%), также находятся в первой пятерке. Огромный объем вредоносных файлов распространяется вместе с нелегальным контентом среди любителей нарушить закон

Рисунок 1 Распределение атак по тематике сайтов

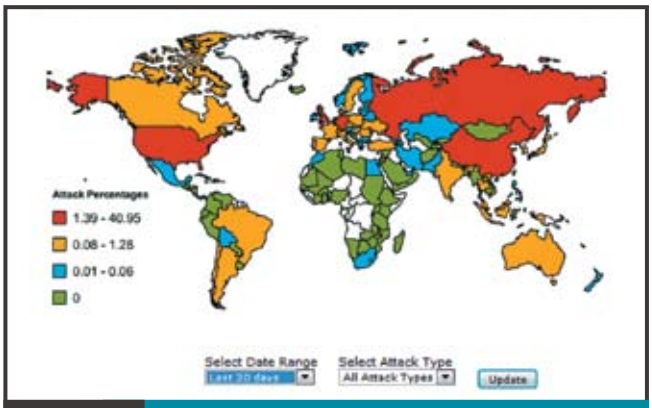

Рисунок 2 Карта интернет-атак за апрель 2012 года

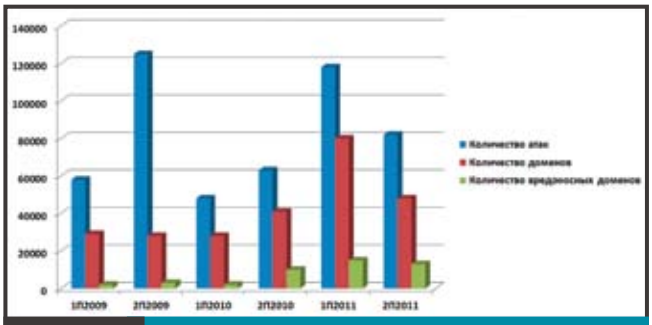

Рисунок 3 Количество атак по версии Anti-Phishing Work Group за 2009–2011 годы

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 и сплетнями о знаменитостях.

Категория с блогами (3,7%), занимающая восьмую позицию, включает любые виды журналов: от фото, аудио и киноблогов до стандартных текстовых блоговых площадок. Так как большая часть контента на подобных сайтах формируется самими пользователями, 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 явной или незаметной форме и причинять вред читателям блогов. И последние два места разделили сайты о путешествиях (3,5%) и игровые порталы (3,3%).

Но, даже учитывая составленный рейтинг, нельзя сказать, 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 на заражение портала. Поэтому безопасность того или иного сайта или сервера напрямую зависит от того, насколько хорошо защищены все его компоненты от всевозможных атак. Например, если существует уязвимое место в системе управления контентом, в плагине или программе, это значит, что каждый веб-сервер, оборудованный этими же компонентами, оказывается в зоне риска независимо от наполнения сайта. А, как известно, обнаружив одну уязвимость, мошенники начинают осуществлять массовые атаки и распространять вредоносные программы, использующие известные слабые места в подобных системах, о чем свидетельствуют атаки Lizamoon или TimThum в 2011 году. Соответственно популярные сайты, привлекающие большое количество пользователей, становятся главной мишенью для злоумышленников.

Как следует из рисунка 2, наибольшее количество атак предпринимается в США, Росси и Китае. Вместе с тем следует учесть, что количество атак год от года растет (рисунок 3).

При этом нужно понимать, что среднее время жизни фишинговых сайтов невелико, а следовательно, их достаточно сложно обнаружить.

Как видно из отчета APWG на рисунке 4, среднее время жизни фишингового сайта составляет сегодня менее 12 часов. Таким образом, на выяснение благонадежности сайта времени совсем немного. В данном случае выигрывает тот производитель антифишингового фильтра, который сможет быстрее и качественнее не только провести проверку, но и доставить информацию пользователям. Логичным в данном случае является применение «облачных» технологий.

Давайте кратко рассмотрим несколько вариантов антифишинговой защиты. Это, прежде всего, антифишинговые фильтры в браузерах и бесплатные антифишинговые модули. Отберем 100 вредоносных ссылок с помощью продукта Kaspersky Internet Security 2012 и проверим их работу. По данным отчета NSS Labs

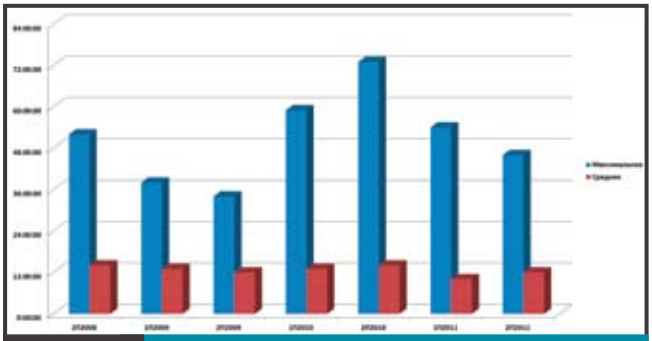

Рисунок 4 Время жизни фишинговых сайтов

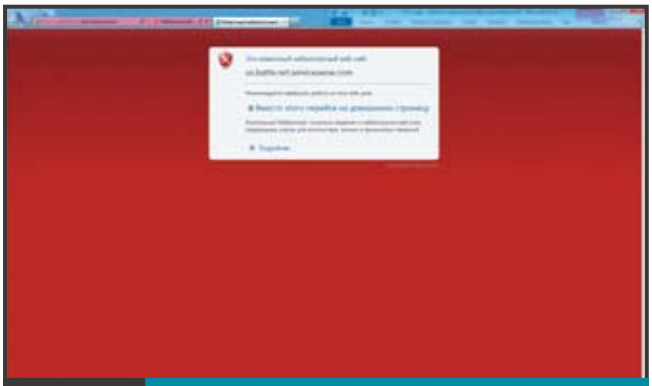

Рисунок 5 Фильтрация в IE9

за третий квартал 2011 года, браузеры блокировали вредоносные ссылки, как показано в таблице 1.

Однако стоит учесть, что данное исследование проводилось на англоязычных сайтах. Если провести его на русскоязычных ресурсах (рисунок 5), результаты будут совсем иными, они показаны в таблице 2.

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

Вторым вариантом защиты является фильтрация с помощью дополнительных внешних антифишинговых фильтров. На сегодня существует большое количество бесплатных внешних фильтров фишинговых ссылок и вредоносного программного обеспечения. Перечислим некоторые из них.

- 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 версии 11 при помощи расширения), Google Chrome и Safari.
  WOT создан на основе сообщества пользователей, 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 тыс. Ссылка на плагин для Internet Explorer http://www.viruslab.ru/download/wot/ie.php. Ссылка на плагин для Firefox http://www.viruslab.ru/download/wot/firefox.php.
- 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. Он эффективно блокирует доступ к известным вредоносным программам и фишинговым веб-сайтам в реальном времени. Его можно использовать вместе с другим установленным защитным программным обеспечением сразу после установки, дополнительные настройки не требуются.

Теперь для Internet Explorer результаты тестов будут выглядеть следующим образом (рисунок 6).

Понятно, что приведенные результаты вызывают вопросы, ведь если в тестах NSS Labs все так замечательно, почему так плохо в России? На мой взгляд, причины полученных данных в том, что:

- предпочтительным рынком для браузеров сегодня является рынок США, на котором и происходят основные события;

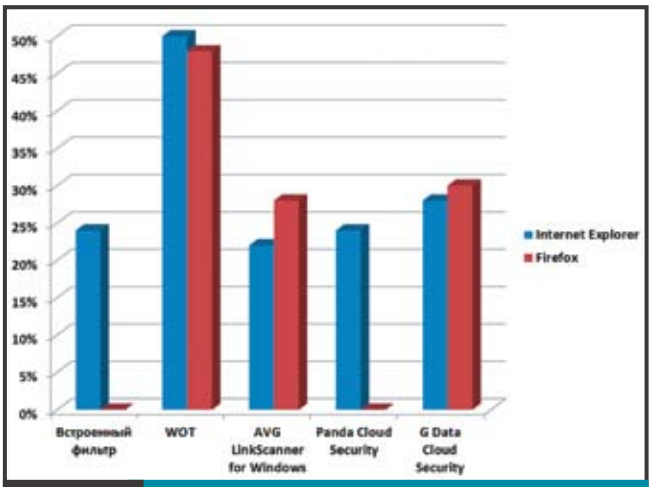

Рисунок 6 Результаты тестов плагинов

Таблица 1 Отчет NSS Labs за III квартал 2011 года

IE9	Chrome 12	Firefox 4	Safari 5	Opera 11
99,2%	13,2%	7,6%	7,6%	6,1%

Таблица 2 Отчет NSS Labs за III квартал 2011 года для русскоязычных сайтов

IE9	Chrome	Firefox
24%	0%	0%

- фишинговые фильтры в браузерах работают на основе данных поисковых машин, в первую очередь Bing и Google (вспомним, что только в Opera используются данные Yandex).

Как следствие, в первую очередь обрабатываются англоязычные страницы и страницы с высоким поисковым рейтингом. А так как среднее время жизни фишинговых ссылок, как указывалось, не превышает 12 часов, то эффективность таких фильтров все же остается низкой. Особенно в русскоязычной части Интернета.

Низкая эффективность бесплатных плагинов (в первую очередь WOT, G Data) обусловлена еще и тем, что решение о том, является ссылка вредоносной или нет, принимается на основании мнения пользователей, а следовательно, ввиду короткой жизни вредоносных ссылок такие модули просто не успевают своевременно их обрабатывать. Хотя покажут среднюю эффективность, если ссылка живет долго.

Наиболее надежными все же являются фильтры фишинговых ссылок в браузерах, особенно при условии использования «облачных» сервисов репутации (стоит добавить, что при этом данные должны собираться не только исходя из мнения пользователей, как это делается у некоторых поставщиков).

Владимир Безмалый (vladb@windowslive.com) — специалист по обеспечению безопасности, имеет звание MVP Consumer Security, Microsoft Security Trusted Advisor