Браузеры-шпионы

В. Болгарчук

В интернете существует немало программ-браузеров, обладающих богатым набором всевозможных функций. Конкуренция между их разработчиками дает свои плоды. Браузеры становятся все более комфортными и удобными в использовании. Но далеко не все пользователи имеют полное преставление о том, какую информацию о вас и вашей системе во время серфинга по сети передает браузер своим создателям. А передают они немало, в том числе — и конфиденциальных данных.

Google Chrome

Без преувеличения, настоящий браузер-шпион. Его создатели интегрировали в эту программу целый комплекс функций, помогающих отслеживать ваше поведение в сети. Во-первых, каждому пользователю браузера по умолчанию присваивается уникальный ID, при этом отслеживаются некоторые аспекты вашего поведения в сети, передаются данные о месте и времени скачивания браузера. Причем отслеживающих инструментов из разряда ID в данном случае существует несколько. Machine ID передает информацию о том, какие на вашем ПК еще установлены программы от Google, и произошло ли их обновление до последних версий. Так называемый Client ID предназначается для предоставления статистических данных об использовании тех или иных функций Chrome. Фактически, на основании всей информации, передаваемой этими клиентами, можно составить довольно полный интернет-портрет пользователя. Ведь именно таким образом идентифицируется каждая конкретная версия браузера.

Шпионскими функциями грешит также специальная программа обновлений Google updater. Кроме того, в компанию попадает информация и об IP-адресах пользователей, что многие юристы уже давно считают нарушением прав конфиденциальности.

Браузер Chrome вообще передает в Google массу данных о пользователе, начиная от поисковых запросов и введенных веб-адресов, и заканчивая сведениями о версии Windows и установленном DirectX. Желание узнать, какие на компьютере пользователя установлены программы от Google, и обновлены ли они до последних версий еще можно понять. Но поводу всего остального хочется задать вполне справедливый вопрос: «Зачем разработчикам браузера информация о том, какая у вас на компьютере установлена операционная система, и тем более DirectX ?"

Представители Google, тем не менее, уверяют, что никакого анализа получаемой информации с целью установления виртуальных портретов пользователей не делают, но верится в это с трудом. И прежде всего потому, что компания наотрез отказывается предоставить доступ к изучению положения дел в данном вопросе сторонним специалистам по вопросам информационной безопасности. На самом деле Google давно владеет поистине огромными массивами информации о пользователях, а кто владеет информацией, тот владеет известно чем. Прежде всего, эти данные представляют маркетинговый интерес, и могут быть успешно использованы в коммерческих целях. Ведь на основе хотя бы той же информации о посещаемых web-страницах можно определить предпочтения пользователя, если рассматривать его в качестве потребителя товара или услуги.

И ни для кого не секрет, что к этим данным же давно проявляют особый интерес страховые компании, банки и другие потенциальные рекламодатели. Пока что шансы заполучить эту информацию у представителей бизнеса практически равны нулю, чего нельзя сказать о спецслужбах. Ведь антитеррористические законы в США уже сейчас

обязывают компании, чья деятельность связана с оказанием интернет-услуг, предоставлять данные, вызвавшие интерес правительства или спецслужб. Непосредственно Google через суды пока успешно сопротивляется попыткам рассекретить свою базу данных. Однако насколько его хватит, неизвестно. И более того — сам факт сосредоточения столь больших массивов информации в руках одной компании, заставляет, как минимум, насторожиться.

Internet Explorer

Один из самых любопытных браузеров. Восьмая версия Internet Explorer (IE), по признанию самих же разработчиков, передает в Microsoft данные о жестком диске и процессоре вашего компьютера. Также собираются и передаются сведения об оперативной памяти и некий специальный зашифрованный код, якобы предназначенный для идентификации компьютера. Уже пробная версия браузера Internet Explorer 8, beta 2 вообще созванивалась с сервером Microsoft на этапе своей установки. Как уверяют в корпорации, таким образом собирается информация о том, какие функции браузера востребованы среди пользователей. Однако зачем в таком случае передается информация о жестких дисках, и тем более «код идентификации компьютера»? На этот вопрос пока ответа нет.

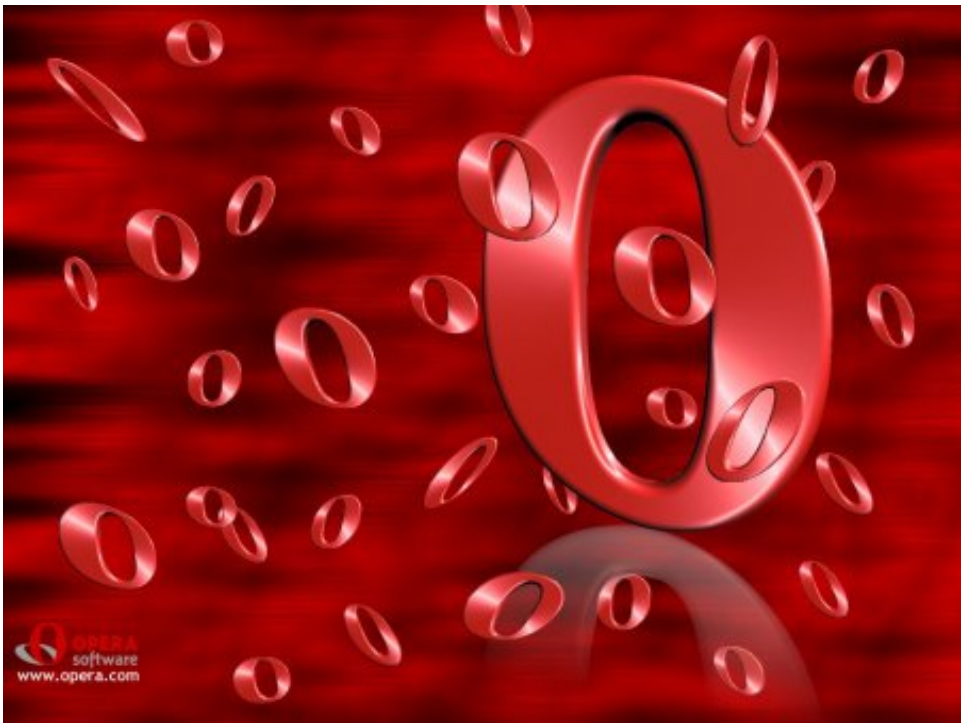
Но и это еще не все. При помощи вроде бы такой удобной функции как «рекомендуемые сайты», создатели Internet Explorer 8 также получают доступ к информации о сайтах и страницах, посещаемых вами в сети. На самом деле функция «рекомендуемые сайты» вроде бы как призвана упростить поиск информации. При загрузке страницы браузер предложит вам список сайтов, схожих с ней по тематике. Действительно удобно, но только дело в том, что реализация этой функции невозможна без передачи информации о списках вводимых адресов непосредственно в корпорацию Microsoft.

Разработчики получают дополнительную информацию о вашем серфинге в сети также и в том случае, если в браузере по умолчанию выбран поисковый сервис Live Search. На этот раз «большой брат» видит не только адреса посещаемых вами сайтов, но и ваши поисковые запросы. И даже выбранные вами результаты поиска. Если Live Search был выбран в качестве средства поиска по умолчанию в старых версиях браузера, при установке самой последней версии Internet Explorer, он просто «подхватывает» эти настройки. В сочетании с активной функцией «рекомендуемые сайты», информация о поисковых запросах передается, даже если вы не используете Live Search в качестве поисковой системы.

Помимо этого, Internet Explorer 8 собирает информацию о пользователе при помощи инструмента SmartScreen, Этот фильтр предназначен для защиты от фишинга, однако посла его активации в Microsoft начинают передаваться данные о том, какие сайты вы посещаете и сколько времени на них проводите. В корпорации не исключают, что таким образом могут передаваться и сведения, вводимые пользователем при заполнении веб-форм, в том числе и пароли. И хотя в Microsoft клятвенно уверяют, что эти данные передаются исключительно в зашифрованном виде, и не несут никакой угрозы утечки конфиденциальной информации, специалисты все же рекомендуют отключить фильтр SmartScreen, а для защиты от фишинга использовать специальные программы.

Opera

Популярный среди пользователей Рунета браузер от норвежской компании Opera software в шпионских замашках стали подозревать недавно. Всему виной применяемая



в последних версиях Opera технология Turbo, позволяющая значительно ускорять процесс загрузки страниц. Суть технологии заключается в том, что при обмене данными между компьютером пользователя и сервером в сети интернет, происходит обработка трафика, в результате которой отсекаются «тяжеловесные» элементы содержимого web-странцы. Также осуществляется сжатие загружаемых изображений, из-за чего страница грузится действительно быстрее.

Однако в этой технологии есть один небольшой нюанс. При включенном режиме Turbo абсопютно весь трафик между сайтами и конкретным пользователем пропускается через сайт Opera software. При этом никакого шифрования данных не происходит, что также вызывает большие сомнения в степени конфиденциальности такого рода серфинга. В Opera software и не скрывают своего интереса к получаемой таким образом информации, якобы собираемой исключительно для изучения статистики использования браузера. А что бы и вовсе развеять всяческие опасения, в компании уверяют, что получаемая информация никак не связана с конкретными пользователями сети. Впрочем, в самой последней версии браузера - Opera 10 режим

Turbo по умолчанию выключен, а саму эту функцию, в отличие от многих аналогичных в Internet Explorer и Chroma, при желании можно просто отключить.

Firefox

Находится на последнем месте в данном обзоре, поскольку, по сравнению с уже упомянутыми программами, в наименьшей степени проявляет шпионское

любопытство. В случае сбоя Firefox попытается передать в Mozilla Foundation специальный Crash Report. В «том отчете будет содержаться информация о странице, во время посещения которой произошел сбой, а также данные об используемой вами версии Windows и конфигурации вашего компьютера. Помимо этого браузер отправит некое «специальное число», предназначенное опять же для идентификации ПК.

Очень похоже на информацию, собираемую браузером Internet Explorer 8, с той лишь разницей, что в случае с Firefox данные будут отправлены только после подтверждения согласия пользователя. Но и здесь не все так просто, поскольку популярный в последнее время «Огнелис» все же пытается шпионить за вашими поисковыми запросами. Эта информация будет передаваться, если воспользоваться поиском от Google, который встроен в браузер. Интересно, что при этом данные о запросах отправляются не в Mozilla, а опять же попадают в распоряжение вездесущего Google. Что бы предотвратить утечку

информации, достаточно просто установить в браузере по умолчанию другой поисковый сервис.

Вместо выводов

Как видно из обзора, обычный серфинг в Интернете на самом деле не так прост, как это может показаться на первый взгляд. При этом информация о вашем компьютере вполне может быть еще более полной. Ведь данные, о которых идет речь в статье - это то, о чем «признались» разработчики, и неизвестно, что передают браузеры на самом деле. В любом случае, посещая сайты, следует быть острожным.

Журнал Компьютерная Практика