Анонимайзеры

Инкогнито по Интернету

Многие пользователи не догадываются о том, насколько явными могут быть следы их пребывания на любом сайте. Ладно, если бы это были сведения вроде IP-адреса, страны, версии браузера и ОС. Но существуют и скрипты, позволяющие узнать структуру наших жестких дисков, названия файлов, установленное ПО и многое другое.

Если же ваш IP-адрес и e-mail попадут в руки злоумышленников, вы рискуете нарваться на неприятности. Это может быть DoS-атака с помощью специальных программ-нюкеров. Зная ваш адрес электронной почты, «доброжелатели» могут завалить спамом, а то и прислать незваного гостя — троянскую программу, с помощью которой будут хозяйничать на вашем компьютере. Есть и другие, не столь весомые причины, по которым бывает нужно скрыть информацию о себе или представиться кем-нибудь другим. Многие сайты так и норовят оставить следы на жестком диске в виде cookies. А некоторые ресурсы осуществляют фильтрацию посетителей по странам, предоставляя доступ к какой-либо информации, к примеру, исключительно жителям США и Европы. Иногда возникает и такая проблема: хочется войти в чат, а вас заблокировали. А как быть, если ваш системный администратор запретил доступ к каким-то сайтам? В некоторых не очень демократических государствах главный системный администратор — правительство — запрещает своим гражданам посещать определенные ресурсы Сети, не соответствующие или противоречащие господствующей в этом государстве идеологии. Поэтому даже самому добропорядочному пользователю Интернета нужно знать, как сохранить анонимность, скрыть свой IP, а также местонахождение и адрес электронной почты.

Наш молчаливый посредник

Самое главное, что способно выдать с головой, — реальный IP-адрес пользователя. Зная его, можно »

» получить достаточно полные сведения. Если у вас статический IP, информация будет предоставлена непосредственно о вас, если же вы пользуетесь модемным соединением и у вас динамический IP, станет известно о вашем провайдере, получить у которого сведения о вас не составит труда.

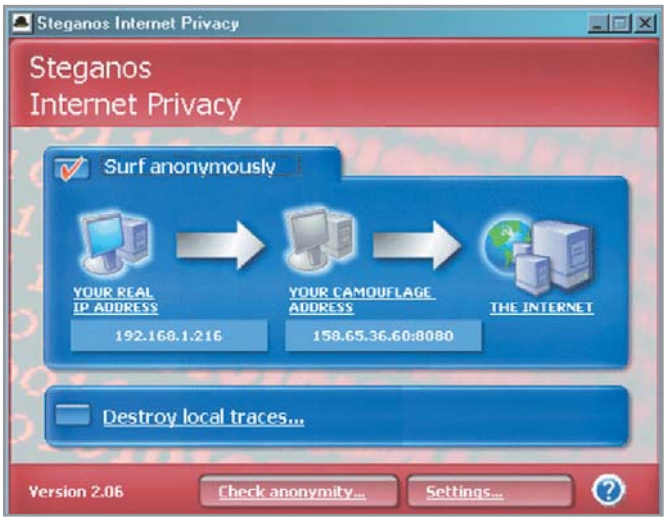
Наиболее простой способ скрыть его — использование анонимных http-прокси-серверов. Английское слово «proxy» означает «посредник, полномочный представитель». Прокси-сервер — это посредник между нами и Интернетом. Через него проходят все наши обращения к сайтам, скачиваются файлы. Мощный прокси способен значительно увеличить скорость соединения за счет кэширования и ретрансляции полученных данных. Файлы Интернета сохраняются локально не на компьютере пользователя, а на диске машины, где установлен прокси, а она, как правило, гораздо мощнее и производительнее. Если пользователь хочет открыть какой-либо документ в Сети, а его незадолго до этого открывал или он сам, или другой пользователь данного прокси, то ему будет выдана локальная копия с диска прокси-сервера. Но тут есть одна немаловажная деталь: если данный документ содержит динамически изменяющийся контент, не исключено, что будет выдана устаревшая версия. Поэтому администратор прокси-сервера должен грамотно установить параметры, определяющие устаревание документа. А главное достоинство прокси — при путешествии по Сети вы везде будете оставлять именно его IP-адрес, а не свой собственный. Владелец какого-либо сайта сможет узнать вашу версию системы и браузера, разрешение и количество цветов экрана, дату и время на нашем компьютере, количество страниц, которое вы просмотрели за текущую сессию, и другую второстепенную информацию. Он не узнает главного — кто вы. Если же злоумышленник решит атаковать этот IP, нападению подвергнется не ваш компьютер, а тот, на котором установлен прокси-сервер, а он защищен гораздо лучше. Дело в том, что прокси появились как раз с той целью, чтобы дать возможность всем объединенным в локальную сеть компьютерам выходить в Интернет, используя только одно подключение и, соответственно, один IP. Большинство прокси принадлежат различным организациям, учебным заведениям и т. п. и чужого пользователя к себе просто не пустят. Но существуют и прокси, открытые для посторонних, администраторы которых по недосмотру или с какими-то специальными целями пускают на них всех «с улицы». Как же найти открытый прокси-сервер? Можно воспользоваться каким-нибудь поисковиком, который выведет на нужные сайты. Как правило, это частные странички, посвященные хакингу или сетевой безопасности, где опубликованы списки адресов анонимных прокси, часть из которых, правда, может не работать.

Можно самостоятельно поискать открытые прокси с помощью специальных программ – например, широко известного и бесплатно распространяемого творения китайских программистов под названием Proxyhunter, сканирующего заданный диапазон IP-адресов, — но это займет слишком много времени. Самый оптимальный вариант — воспользоваться специальной службой Proxychecker, доступной по адресу: www.proxychecker.ru. Она была открыта компанией «СпайЛОГ» в 2001 году и поддерживалась ею до февраля 2002 года, затем обрела самостоятельное существование. Поисковый робот Proxychecker постоянно ищет по всему миру открытые прокси, внося их в свою базу. Уже найденные прокси постоянно проверяются на предмет работоспособности. Достаточно бесплатно зарегистрироваться в этой системе, и вам будет предоставлен огромный список полностью рабочих адресов, где также будет указана страна, которой принадлежит прокси-сервер, и скорость доступа к нему. Подключиться к выбранному прокси-серверу просто. В любом браузере есть функция установки свойств соединения. Нужно найти опцию, отвечающую за соединение через прокси-сервер, и в специальном окне написать имя прокси и его порт, а при необходимости также и параметры для различных сетевых протоколов.

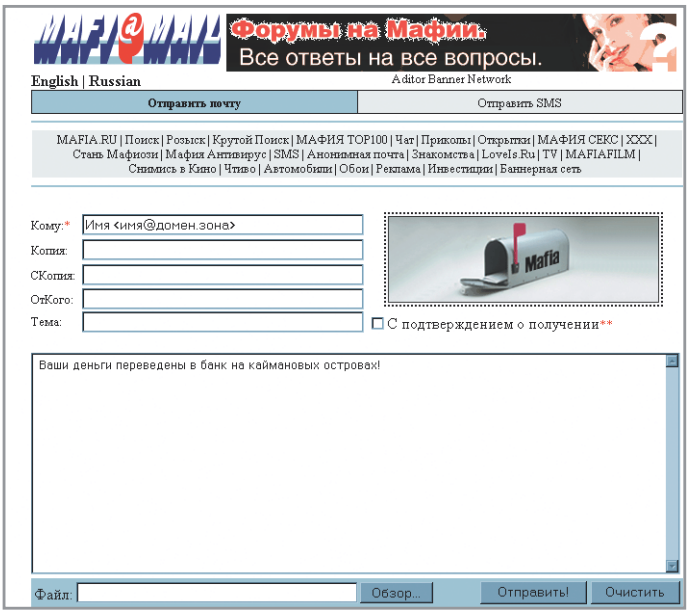
Процесс переключения между анонимными прокси можно автоматизировать. Для этих целей существует утилита Steganos Internet Privacy. С ее помощью можно через определенный промежуток времени (по умолчанию установлено значение 30 с) по принципу рулетки переключаться на новый прокси из прилагаемого списка и, соответственно, получать новый IP-адрес. Список прокси можно и нужно регулярно обновлять с сайта разработчиков. Интерфейс Steganos Internet Privacy очень прост и нагляден, разобраться в нем может даже начинающий пользователь.

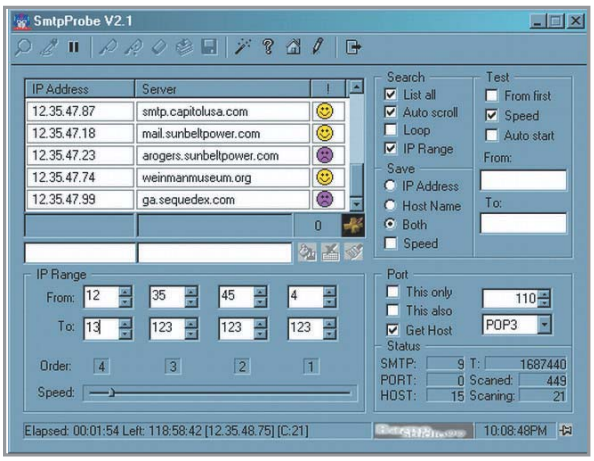
Не все коту масленица

К сожалению, работа с http-прокси имеет свои существенные недостатки. Во-первых, при желании можно все-таки получить сведения о вас у администрации анонимного прокси, а во-вторых, некоторые сайты, например www.yandex.ru, просто не пустят вас к себе. Дело в том, что прокси различаются по степени анонимности. Простой анонимный прокси-сервер в заголовке http-запроса не посылает удаленному хосту переменную HTTP_X_FORWARDED_FOR, что не дает зафиксировать ваш IP-адрес. Однако существу- »



◂ Эта программа позволит вам замаскировать свой реальный IP-адрес, используя анонимные прокси-серверы





▲ SmtpProbe поможет найти открытый анонимный SMTP-сервер

◀ Один из серверов, позволяющих отсылать анонимные письма

» ют и прокси с высокой анонимностью, которые не посылают как переменную HTTP_X_FORWARDED_FOR, так и HTTP_VIA и HTTP_PROXY_CONNECTION, что не позволяет удаленному хосту зафиксировать не только IP, но и то, что вы пользуетесь прокси-сервером. Как же узнать, насколько анонимен тот или иной прокси? На сайте www.proxychecker.ru также предлагается возможность проверки на анонимность любого прокси.

Интернет на страже демократии

В некоторых странах правительство решает, какие сайты могут посещать граждане, и блокирует доступ к запрещенным ресурсам Сети. Как правило, это сайты оппозиционных партий и движений, где критикуется правящий режим данного государства, или страницы низкого морально-нравственного содержания. Вторая категория особенно часто попадает под запрет в мусульманских странах, где действуют законодательные нормы шариата. Специально для того, чтобы граждане этих государств могли свободно пользоваться Интернетом, создан международный проект Peek-a-Booty (www.peek-a-booty.org). Принцип работы проекта следующий. Пользователь запрашивает не разрешенные к посещению сайты не напрямую, а через один или несколько специальных web-узлов, которые являются участниками Peek-a-Booty. При передаче данных используется применяемый в электронной коммерции защищенный протокол SSL Encryption, благодаря чему следящими за трафиком спецслужбами соединение через узел Peek-a-Booty будет воспринято как обычная электронная сделка. Чтобы воспользоваться Peek-a-Booty, необходимо установить и подключить к браузеру специальную программу, затем найти в постоянно обновляемой базе данных проекта один или несколько работоспособных адресов таких web-узлов и подключиться к ним. К сожалению, пока проект находится на стадии бета-тестирования, и доступен только протокол http.

Разновидности анонимайзеров

Тем, у кого нет возможности подключаться к внешним анонимным прокси и изменять настройки браузера (некоторые системные администраторы устанавливают на это запрет для пользователей), можно посоветовать воспользоваться анонимайзером, то есть прокси с высокой степенью анонимности. Анонимайзеры подразделяются на два вида — клиентские приложения и сетевые сервисы, работающие через web-интерфейс. Второй тип более распространен, поэтому рассмотрим его. К сожалению, после событий 11 сентября президент США Джордж Буш выступил с заявлением о необходимости контролировать все и вся в Интернете. Это заявление сильно ударило по анонимайзерам. Часть из них вовсе прекратила существование, как, например, один из лучших, SafeWeb, а некоторые стали платными. Тем не менее анонимайзеры и по сей день остаются одним из наиболее удобных и надежных способов обеспечения анонимного web-серфинга. Внешне анонимайзер представляет собой специальную панель, расположенную в верхней или нижней части рабочего окна браузера и содержащую форму для ввода URL. Многие анонимайзеры включают в эту панель опцию удаления cookies, запрета скриптов, Java-апплетов, ActiveX, баннеров, сокрытия переменной referrer и некоторых других данных. Некоторые анонимайзеры имеют дополнительные функции — SSL Encryption (все набранные адреса и трафик зашифровываются), SmartCookies (все cookies трансформируются в «сессионные» и самоуничтожаются при закрытии браузера) и другие.

Вот наиболее известные из существующих на сегодняшний день анонимайзеров. Собственно Anonymizer (www.anonymizer.com) — один из первых, быстрый и качественный. Когда-то он был бесплатным, затем перешел на частично платную основу, сохранив бесплатный серфинг, сопровождаемый 30-секундной задержкой перед посещением каждого сайта. MegaProxy (www.megaproxy.com) — полностью бесплатный, очень удобный и функциональный, но скорость оставляет желать лучшего. SafeProxy (www.safeproxy.org) — также бесплатный анонимайзер, скорость у него выше, однако все же не как у коммерческих аналогов. BlackCode (www.blackcode.com) — добротный платный анонимайзер с приличной скоро- »

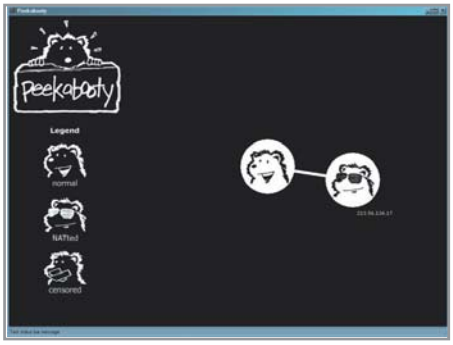
» стью. Guardster (www.guardster.com) — бесплатный и быстрый, но плату взимают другим способом — обилием рекламы, в том числе и во всплывающих окнах. The Cloak (www.the-cloak.com) — бесплатный, с хорошей скоростью.

Пишем анонимку

А как обеспечить себе анонимность при работе с электронной почтой? Отправка анонимного сообщения может быть необходима в том случае, если мы не хотим, чтобы какая-либо информация о нас стала известна адресату. Это могут быть компоненты служебного заголовка письма: IP, x-mailer, from_mail, message_id и др. Существует несколько вариантов того, как можно скрыть свой настоящий e-mail и подставить вместо него любой другой, а также не дать возможности получателю письма узнать наш реальный IP-адрес.

Если мы пользуемся почтой через web-интерфейс, вопрос решается следующим образом: просто настраиваем браузер для работы через анонимный http-прокси или socks-сервер, как было описано выше. Теперь получатель письма не узнает наш реальный IP, но адрес e-mail мы вряд ли скроем. Если нужно скрыть его или подставить вместо него любой другой, можно воспользоваться анонимной web-почтой, которую легко найти, например, по адресу www.mafiamail.ru. Существуют и специальные анонимные почтовые клиенты, или mail-бомберы. Но для работы с ними необходим бесплатный SMTP-сервер, который позволяет отправлять почту без авторизации. Как и в случае с прокси, в Сети имеется великое множество списков таких SMTP. Однако 95% из приведенных в них серверов уже не пустят к себе постороннего пользователя. Лучше попробовать найти открытые SMTP самостоятельно. Для этих целей подойдет программа SmtpProbe. Она сканирует заданный диапазон IP на предмет открытого 25-го порта, который и отвечает за SMTP. Найденные адреса она проверяет на предмет анонимности, имитируя отсылку почты через них. Долго, но зато эффективно. Хотя, скажу по секрету, самый популярный отечественный почтовый сервер www.mail.ru тоже позволяет отправлять через него почту без авторизации. Нужно лишь указать в качестве обратного адреса любой зарегистрированный на сервере, а в качестве SMTP-сервера — smtp.mail.ru. Никакой другой популярный российский почтовый сервер из известных автору такого «безобразия» не позволяет. Правда, IP таким образом не скроешь. Ну а если вам все же необходимо скрыть свой IP и e-mail одновременно?

Здесь нам не обойтись без socks-сервера. Не только браузер, но и обычный почтовый клиент, например Outlook Express или TheBat!, может работать через socks. Для этой цели служит утилита SocksCap. Она позволяет настроить приложение для работы через socks-сервер. Затем запускаем SocksCap и в настройках вводим адрес и порт выбранного сервера. После этого просто перетаскиваем ярлык нашей почтовой программы в окно SocksCap. Теперь программа «соксифицирована». Нажимаем кнопку «Run» на инструментальной панели SocksCap, и наш почтовый клиент запустится и будет работать через socks-сервер. Надо сказать, что не всякую почтовую программу можно «соксифицировать». Ни один из нескольких проверенных mail-бомберов не захотел отсылать почту при посредстве SocksCap, но почтовые клиенты TheBat! и Outlook Express работали исправно. Рассказ о средствах анонимной почты был бы не полон без упоминания отечественной разработки под названием Mega-Mailer. Эта утилита позволяет не только анонимно отсылать почтовые сообщения, соединяясь с SMTP через socks-сервер, но и составлять целые цепочки из socks.



▲ Peek-a-Booty — воспользуйтесь им для анонимного серфинга

Заключение

Мы привели здесь лишь некоторые способы анонимного web-серфинга и отправки анонимной почты. Интернет-технологии развиваются стремительно, так что, возможно, к моменту выхода материала появятся новые «шапки-невидимки». Важно другое: анонимность — вполне законное право любого пользователя Интернета.

■ ■ ■ **Григорий Рудницкий**

Название	ProxyHunter 3.1	SmtpProbe 2.0	SocksCap 2.3	Mega-Mailer 2.1, 3.0, 4.0	Steganos Internet Privacy 2.06
Разработчик	SolarWind Studio	Rain Huang, Ramo Studio	Permeo Technologies, Inc.	Владимир Камаев	Steganos GmbH
Домашняя страница	http://members.ch.tripodasia.com.hk/bfx4sn7ipm	Неизвестна. Программу можно найти по адресу: www.skycn.com/soft/371.html	www.socks.nec.com/reference/sockscap.html	http://giposoft.dax.ru Сайт может быть недоступен. 4-я версия доступна также здесь www.grandspam.net/mm4pro.zip	www.steganos.com
Условия приобретения	Freeware	Freeware	Freeware, Требуется регистрация	2.1 — Бесплатная. Версия 3.0 shareware ($20), 4-я ($30)	7-дневная trial-версия $24.95
Размер дистрибутива	332 Кбайт	170 Кбайт	997 Кбайт	140, 784, 767 Кбайт в зависимости от комплекта	5,3 Мбайт
Операционная система	Windows 98/2000/XP	Windows 98/2000/XP	Windows 98/2000/XP	Windows 98/2000/XP	Windows 98/2000/XP

▲ Описания программ, упомянутых в статье