Tor — Urbanculture

Интернет Проекты
Криптоконспирология

Tor (*бублик*, *тор*, *The Onion Router*) — система серверов, делающая вас анонимом. Система была разработана в СШП для невозбранного веб-серфинга, тайной переписки и прочих кошерных вещей, когда ip адрес должен оставаться неизвестным, а трафик — шифроваться. Радует анонимуса всех стран и народов, огорчает копирастов, борцунов с детской порнографией, вандализмом и спамом. Немного огорчает МОССАД, ФБР, ФСБ, КГБ Белорусии. Но они при случае и сами не прочь воспользоваться. Абсолютной анонимности не дает, но задачу деанонимизации сильно усложняет.

логотип

Принципы работы

Тор представляет собой систему серверов, передающих пакеты информации друг другу по системе туннелей, сформированной случайным образом. Пользователь передает сообщение в зашифрованном виде на входной сервер, тот передает её промежуточному серверу, а тот — выходному. Ответ с сайта идет зашифрованным через те же серверы. IP-адрес пользователя виден только первому серверу в его цепочке. Каждый из серверов способен определить IP-адрес только предыдущего сервера, на чем и строится анонимность. Используется луковое шифрование: источник зашифровывает пакет информации последовательно открытым ключом каждого из серверов цепочки, а при передаче каждый сервер снимает один «слой» шифрования — как в луковице. Это обеспечивает защиту от чтения или подмены информации передающими серверами. Однако если сайт не использует SSL для шифрования информации, то выходной сервер получает её в открытом виде. Это может мешать безопасному использования сети. Официальный софт для серверов Tor не пишет логов о передаваемой информации, поэтому конфискация сервера не поможет выяснить IP-адреса тех, кто им воспользовался. Что не мешает кровавой гэбне запустить свои сервера, пишущие логи, ведь запустить сервер тора может каждый. Если по несчастливой случайности все три сервера цепочки окажутся «крысами», то плакала ваша анонимность. Неправильная настройка системы также дает уязвимость. Для большей анонимности крайне не рекомендуется использовать Java, Flash и остальные плагины браузера. Большинство торрент-клиентов разрушают анонимность, которую создает Tor; для торрентов лучше подойдет I2P. Использование JavaScript не создает дополнительного риска для анонимности, если остальные компоненты браузера настроены как следует. Более подробную информацию можно получить на сайте проекта.

Tor предназначен не только для анонимного посещения сайтов в обычном Интернете, но и для создания своих собственных скрытых сайтов (*hidden service*), доступных пользователям Tor, но недоступных из обычного Интернета (если не считать гейтов вроде onion.to). Скрытый сайт и его посетитель не знают IP-адреса друг друга. Эти сайты открываются через Tor медленнее, чем обычные сайты, зато предоставляют некоторые преимущества:

- владелец сайта остается анонимным (сайт подключается так же, как и клиент, через цепочку серверов),
- не нужно платить за доменное имя и возможность использовать шифрование,
- нет риска, что сайт закроют или отберут (если не потеряешь файл с ключом к сайту),
- не требуется публичный IP-адрес (сайт может обслуживаться домашним компьютером, расположенным за NAT или firewall).

Разумеется, если есть преимущества, то должны быть и недостатки:

- плохое качество связи, далеко не 100%-ный uptime,
- нельзя выбрать доменное имя, которое нравится, так как имя выбирается наугад,
- нет поддоменов,
- дополнительная настройка серверного софта для предотвращения деанонимизации (например, требуется высокая точность часов).

Как тор находит скрытые сайты
При создании скрытого сайта владелец создает пару ключей. Домен сайта является фингерпринтом (хешом публичного ключа). Скрытый сайт наугад выбирает три сервера и через Tor загружает на них свой публичный ключ. Эти три сервера становятся «точками входа» в скрытый сайт. Скрытый сайт собирает вместе информацию о трёх выбранных входных серверах, включающую их публичные ключи. Это описание подписывается закрытым ключом скрытого сайта и вбрасывается в местную распределенную хеш-таблицу (DHT). Ключом в DHT служит доменное имя сайта.

Клиент, желающий подключиться к скрытому сайту, выбирает наугад «соединительный сервер», загадывает случайное число в качестве секрета и через Tor передает его на соединительный сервер. Зная доменное имя, клиент через Tor скачивает из DHT публичный ключ скрытого сайта и список из трёх

входных серверов. Выбранный секрет вместе с адресом соединительного сервера зашифровывается открытым ключом скрытого сайта и через Tor отправляется на один из входных серверов, с которого через Tor попадает на скрытый сайт, который может расшифровать это дело своим закрытым ключом.

Скрытый сайт, зная адрес соединительного сервера и секрет, через Tor отправляет секрет на соединительный сервер. Соединительный сервер сравнивает его с ранее полученным секретом от клиента. Если значения совпадают, то соединительный сервер открывает соединение между клиентом и скрытым сайтом. Связь клиента со скрытым сайтом установлена.

Адрес соединительного сервера известен только клиенту и скрытому сайту. Соединительный сервер нужен, чтобы входные сервера (постоянные для скрытого сайта в течение длительного времени + их адреса известны всем желающим) не отвечали за передачу трафика. В противном случае упростились бы атаки, как технические, так и юридические, на входные сервера с целью прекратить доступ к скрытому сайту.

Общая длина цепочки серверов равна 6, не считая клиента и скрытый сайт. Соединительный сервер находится через два сервера от клиента. В качестве всех серверов, принимающих участие в описанной схеме, могут использоваться все сервера сети Tor, а не только выходные.

[1]

Примеры скрытых сайтов смотри ниже.

На платформе Андроид

> Мы совсем не ручаемся в вашей анонимности, если вы используете Tor на андроиде или айфоне. Основными рекомендациями остаются браузер Tor Browser Bundle и операционная система Tails.

да с луковицей вместо мозга

Вполне себе поднимается. Для этого вам необходима программа Orbot с маркета тут и браузер для просмотра. Если вы обладаете root правами, можете пользоваться своим любимым браузером, если не обладаете, разработчики предложат вам скачать унылый браузер и xmpp клиент. Данный софт работает, но не имеет дополнительных возможностей (нет закладок, истории, нет возможности загрузить файлы) и крайне криво переведен.

Также для этих целей можно использовать мобильный firefox с установленным дополнением для работы с прокси. Ссылка на необходимый плагин имеется в орботе. С этим браузером все гораздо удобнее. Но имеются некоторые особенности, в общем-то для любителей огнелиса.

В последних версиях плагин внезапно перестал работать. Настроить прокси возможно в opera mobile и easy. У некоторых устройств есть возможность прописать прокси в настройках wifi соединения. Каждый выкручивается как может. **!!! Внимание.** Запуская Tor под root-ом, вы несете полную ответственность за сохранность ваших данных, возможность поймать и сразу же запустить sms троян или что-нибудь более мерзкое. Лучше немного пострадать, находясь в безопасности. Тот же онион-форум утверждает, что ничего опасного там не найти, если не искать специально. Но кто знает, можно ли доверять товарищам, использующим JavaScript в тор.

Есть несколько технических особенностей, которые никто не упомянул, но они очень важны. Главное это батарейка. Орбот скушает весь заряд электроэнергии, который имеется, достаточно быстро. Поэтому прежде чем включить, помним, что зарядник должен быть под рукой. Еще одна особенность — количество ресурсов системы, которое он потребит. Чаще всего их не хватит на все остальное. Поэтому смело заходим в раздел «Работающие программы» и глушим все, что нам не надо в настоящий момент. Лучше глушить все, кроме тор, тогда скорость работы будет более-менее сносной. В третьих, если вы делаете это не через вайфай и не с безлимитного тарифа, следите за количеством оставшихся денег на счету. Количество трафика, полученного и переданного, навскидку вы не угадаете. Даже если всегда угадывали.

Факты и мнения

«Пожертвовавший свободой ради безопасности не заслуживает ни свободы, ни безопасности. »

— Бенджамин Франклин

- Прежде чем налаживать тор, еще раз подумайте. Если вам не интересны противозаконные материалы, если нет цели прятаться и делать гадости исподтишка, если вы не хотите что-то купить или продать, что просто так продать нельзя, то не стоит. Честно, там нет ничего прекрасного. Абсолютно свободный человек, не ограниченный страхом, что его ударят банхаммером, а то и пативэн вызовут, может быть реально ужаснен. Многие персонажи хуже животных, потому что животное не испытывает садистского наслаждения. Сделано многое криво и косо, к Артемию там никто не обращается, да и вообще стараются мало. Автору этой статьи не понравилось внутри бублика. Хотя в связи с ситуацией на Украине (блокировкой российских сайтов) Tor стал востребован как никогда.
- Тор можно использовать для анонимизации в обычных интернетах, просматривая их через тор-браузер. Степень анонимности, если вы запретите яву, высокая. Легко преодолевается бан по ip. Но злоупотреблять не стоит, так как забанить по IP все выходные сервера тора — раз плюнуть.
- Тор это ещё одно усилие по пути сохранения свободы слова в Интернете. Люди, считающие, что информация не может быть вредной, а борьба с ср — жалкая попытка лечения симптомов, поддерживают тор и критикуют его только с технической стороны.
- Стоит ли нести тор в массы? Тоже частая тема для обсуждений на местных форумах и бордах. Если резюмировать аргументы сторон: польза от массовости тора состоит в большей анонимности тех, кому анонимность действительно нужна (если бы тор состоял из 3.5 анонимусов, то выяснить, кто из них запостил ср, не составляло бы труда). Ну и польза ещё в мировой справедливости, чтобы у каждого была такая возможность. А критика представлена доводами технического характера (серверный парк тора вряд ли выдержит наплыва пользователей, если не произойдет эквивалентного увеличения числа серверов) и общего характера (рак же).

Примечания

1. ↑ Tor: Hidden Service Protocol

Ссылки

- Проект в человеческом интернете. Узнать подробнее и установить можно отсюда.
- и в твиттере

Ссылки, указанные ниже, вам удастся посмотреть только после установки всего необходимого:

- Внезапно Urbanculture$_{(tor)}$
- E.C.H.O$_{(tor)}$ — социальная сеть, ориентированная на анонимность и безопасность, с удобным интерфейсом и высокой производительностью.

См. также

- Мертвые проекты в сети Tor
- I2P