Tor — Lurkmore

«Tor does not magically encrypt all of your Internet activities. Understand what Tor does and does not do for you. »

Tor (иногда: *торъ*, *торт*, *чиполлино*, *лук*, *расовая еврейская сеть Top(a)*, на самом деле: ***T**he **O**nion **R**outer*) — кошегное средство анонимизации в интернетах. В основном используется в комплекте со специальным браузером, для ленивых параноиков выпускается в форме отдельной операционки Tails и комплекта Whonix, о которых дальше.

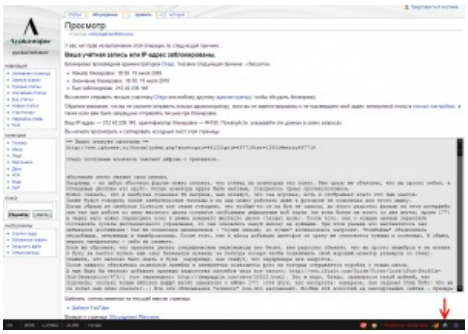
Tor головного мозга для Android

Принципы работы

«Это была слизеринская система доставки сообщений, которая использовалась, когда кто-нибудь хотел связаться с другим человеком так, чтобы никто не узнал, что они разговаривали. Отправитель вручал конверт и десять кнатов тому, у кого была репутация надёжного курьера, тот, в свою очередь передавал конверт и пять кнатов второму курьеру. Второй курьер открывал конверт, обнаруживал внутри второй конверт, на котором было написано имя адресата, и доставлял письмо. Таким образом никто из курьеров не знал одновременно и отправителя, и адресата, поэтому никто не знал, что между ними есть какая-то связь… »

— «Гарри Поттер и методы рационального мышления»

Тор работает по принципу «луковичной маршрутизации». Данные проходят через несколько серверов тора, прежде чем попадут во внешний мир через выходной сервер. Маршрут между серверами тора выбирается случайно для каждого нового соединения и меняется раз в 10 минут, но может быть изменён принудительно, хотите сменить цепочку — обновляйте соединение; данные между серверами шифруются. Однако выходной сервер по определению имеет доступ к нешифрованным пересылаемым данным. Tor децентрализован, а исходники открыты. Так что, если даже США захотят выпилить своё детище, то уже не смогут. Открытый код гарантирует обнаружение троянов и появление форков.



Пример

Анонимность достигается за счёт асимметричного шифрования и пересылки сообщений от отправителя к получателю по цепочке между нодами (серверами-узлами цепочки). У каждой ноды есть сертификат, а это значит что любой человек может создать сообщение, зашифрованное таким образом что его расшифровать сможет только нода для которой оно предназначено. Ноды не выбирают кому пересылать сообщение. Весь маршрут прокладывается до отправки сообщений самим отправителем. Причем ни одна из нод не знает полный маршурт. Асимметричное шифрование позволяет создать безопасные ключи для "классического" симметричного, что необходимо для шифрования инструкций ноде, указывающих кому переслать сообщение дальше по цепочке. Каждая нода знает только от кого она получила сообщение и кому следует его передать далее, поскольку использует лишь один ключ из трёх. В пересылке сообщения всегда участвуют как минимум 3 ноды. Никто из них не знает одновременно и получателя и отправителя. Первая нода знает только отправителя. Последняя -- получателя. Промежуточные ноды знают только соседей.

Стандартные пакеты тора содержат как сервер, так и клиент. Если вы пользуетесь тором и у вас хороший

канал — включите сервер[1]. По умолчанию он *не работает* как выходной и даже как промежуточный сервер. Настроить можно в torrc.

Если паранойя ОСНЕ жжет анус, в конфигурации можно включить ControlPort, указав для него, например, HashedControlPassword, сгенерированный при помощи tor --hash-password password. Подключаться к порту можно с локальной машины при помощи putty (Windows), указав тип соединения Raw или nc (netcat, мультиплатформенный), на прочих же платформах -- при помощи nyx. Здесь открываются широкие возможности.

После аутентификации по команде «authenticate „password“» вы можете:

- запросить новую "личность" (сбросить и обновить все цепочки)

```
signal newnym
```

- посмотреть хелп по статистике

```
getinfo info/names
```

- посмотреть на ваши туннели

```
getinfo circuit-status
```

и увидеть, что на самом деле длина туннеля составляет 4 хопа, где первый — вы, а последний — выход

- если вы релей, посмотреть, кто к вам подключен

```
getinfo orconn-status
```

- получить свежайший список нод прямо с сервера директории

```
getinfo desc/all-recent
```

… и многое другое, читайте control.c в исходниках тор.

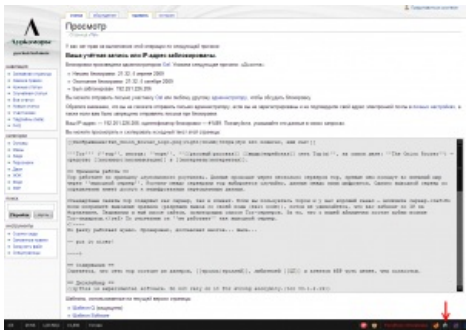
То же самое делает Vidalia, но она толще Putty на целый Qt и устарела. Впрочем, с некоторых пор nyx успешно запускается при помощи WSL, что позволяет меньше нагружать глаза.

С недавних пор у науськанных быдлокодерами политиков стало модно блокировать Tor с помощью DPI (анализа трафика). В ответ Tor родил версию с маскированным трафиком.

Дисклеймер

> «This is experimental software. Do not rely on it for strong anonymity. »
>
> — *tor v0.1.2.19*

> «No anonymity system is perfect these days, and Tor is no exception: you should not rely solely on the current Tor network if you really need strong anonymity. »
>
> — *tor v0.2.0.31*



Пример № 2[2]

Tor сделали, как известно, американские моряки. А у них хер в дюймах, а солярка в галлонах, так что вопрос, насколько стоит сразу радостно бросаться им верить. Да и сами создатели Tor’а предупреждают, что он пока ещё разрабатывается и вы не можете полагаться на него для создания *сильной анонимности* — то бишь, если вы хотите, чтобы ОНИ вас не нашли. Кроме того, недавно была опубликована атака на сеть Tor, позволяющая при определенных усилиях найти источник использующего Tor человека, анализируя трафик сторожевых и выходных серверов, временные задержки и маршрутизацию в сети. Также, спецслужбы, имея доступ к flow магистральных провайдеров и зная время, легко найдут и самого пользователя Tor по специфическим запросам к немногочисленным серверам со списками нод. Поэтому создатели TOPa нас сразу предупреждают, что прятаться от ЦРУ в тор не самая лучшая идея. Однако в прикладных целях он все-таки работает. Кроме того, существует документация с рекомендациями по уменьшению риска

атаки. Там же написано, как перецепить на конец выхода свой анонимно купленный прокси и выбрать страну или узел выхода. Так что для таких б-гоугодных вещей, как преодоление бана по IP, Tor пригоден, еще как!

Пример № 3. Таки да, бывают и такие

Более того. Так как данные шифруются лишь внутри сети, то если выходной сервер решит прослушать, что вы через него передаёте, то он это сделает **без каких-либо сложностей** (не актуально для https, ssh и т.п.). Так, особо рьяным вуайеристом были получены пароли ко множеству посольских почтовых ящиков на серверах правительств ряда стран. Большому Брату вуайеризм пришёлся по вкусу, и вскоре пативэн приехал устроить большую вечеринку.

В этой стране объявили конкурс на взлом Tor'а. Счастливчик получит 3,9 млн рублей и ~~станет изгоем в интернетах~~, может, даже будет работать на гэбню. ИЧСХ, счастливчик нашелся и взялся за работу, но в сентябре 2015 года отказался от выполнения госзаказа. Действительно ли луковица провела шершавым по доблестным губам защитников нашей родины — остается только гадать.

Методы борьбы

Из-за кажущейся неуязвимости, некоторые TOP-тролли совсем потолстели. Это привело к появлению ряда интернет-ресурсов для борцунства с сетью TOP, например, регулярно обновляющихся списков нод и блэклистов.

ЗРК "Top-M1"
Анонимизация уже не потребуется…

В частности, сайт linux.org.ru анально огородился от TOPа после «ночи ахтунгов», когда админы были обижены толстячком, флудившим[3] гомопорнорассказами с нескольких адресов и ников.

Немецкая полиция, как и положено акабам, не заморачивается и в случае чего тупо арестовывает владельца последней ноды в цепочке. Впрочем, от этого она сама может и пострадать, если у вас есть более или менее хороший адвокат.

В Китае с Tor'ом активно борцунствуют «коммунисты», и для работы с ним приходится не реже чем ежедневно искать где-то и вписывать в настройки так называемые «мосты» (хотя там проще прокси найти).

На Апачане Tor вообще не работает, так как все IP там уже давно забанены.

Эта страна без проблем объявила сабж "анонимайзером", позволяющим обходить Роскомнадзорную блокировку сайтов и теперь для доступа к тору потребуется шевелить извилинами почище прежнего.

Эфиопия считается единственной в мире страной, успешно заблокировавшей Tor. В Северной Корее это слово неизвестно.

Драмы

В период между июлем и августом 2013 благодаря действиям доблестных сотрудников ФБР был арестован основатель «Freedom Hosting», 28-летний житель Ирландии Эрик Оуэн Маркес. На его серверах, захваченных местной гэбнёй, были обнаружены сайты с детской порнографией. Прежде он уже не раз получал предупреждения, однако никак на них не реагировал. FBI потребовался год, чтобы обнаружить его местонахождение.

На данный момент, при попытке захода на домены, принадлежащие данному хостингу, вылезает "Down for Maintenance. Sorry, This server is currently offline for maintenance. Please try again in a few hours". Почти все сайты сейчас выключены, а те, что включены, находятся под контролем правительства, так что пока лучше воздержаться от путешествий по иностранным Tor-доменам, ибо Кровавая гэбня не дремлет! Именно из-за закрытия Freedom Hosting сейчас лежат почти все сайты с детской порнографией Тора.

Суть такова. Некоторое, точно не известное, время на скрытых сайтах жил код, который, используя уязвимость браузера, незаметно отправлял на серверы спецслужб IP-адрес, MAC-адрес и имя хоста незадачливого любителя анонимности. Условия для успешной атаки: Firefox не самых свежих версий, Windows и включённый (по умолчанию) JavaScript. Попавшиеся активно срут кирпичами, сушат сухари и уничтожают компьютеры.

Также Гэбня добралась и до Silk Road. 2 октября 2013 года Уильям Росс Ульбрихт (Dread Pirate Roberts) был арестован в Сан-Франциско. Его обвинили в наркоторговле, хакерских атаках и сговоре с целью отмывания денег. Агенты смогли арестовать его благодаря обнаруженной канадским правительством посылке с девятью поддельными документами, отправленной в Сан-Франциско, которые Ульбрихт планировал использовать с целью аренды серверов для Silk Road. Хотя вычислили его не по посылке. Ещё в начале истории сервиса он сам успел наследить на форуме ценителей галлюциногенных грибов.

После такого успеха Гэбня решила не останавливаться на достигнутом и начала охоту на дилеров,

обитавших на Silk Road. И вполне удачно: есть жертвы. Естественно, это только начало. А посему простые пользователи Silk Road начинают срать кирпичами и бегут к адвокатам.

6 ноября сервис открылся вновь.

> 12,500 people have just shown the FBI you cannot kill the idea behind
>
> — *DreadPirateSR*

А 20 ноября началась крупнейшая афера с Bitcoin-ом. Со счетов клиентов, поставщиков и администраторов сайта SheepMarketplace было выведено 96000 BTC! Теперь в результате этой аферы ресурс закрыт, а пользователи отыскивают злоумышленника. Его участь в случае деанонимизации очевидна. График вывода биткоинов можно посмотреть здесь.

В ноябре 2014 в рамках операции ФБР было выпилено более 400 скрытых сервисов — в основном крупнейших торговых площадок — и арестовано несколько человек.

19 декабря 2014 года разработчики Tor'а заявили, что на их детище готовится атака и оно может подавиться мацой. Обошлось.

Не миновали скандалы и Россиюшку. Весной 2017, во время волны антикоррупционных протестов, разыгран спектакль по делу Дмитрия Богатова, открывшего свою экзит-ноду. Преподу математики шьют «организацию массовых беспорядков» и «публичные призывы к терроризму» за два чужих каммента с предложениями прийти на Красную площадь с «горючими материалами». Что характерно, Богатова не выпустили даже после того, как появились новые комментарии от того же автора, пока Богатов был под стражей. Только через год с Богатова были сняты обвинения, однако, возможно, уже после явки с повинной (добровольно или не совсем — история пока умалчивает) другого человека.

Августовский пиздец

В середине августа 2013 года произошёл небывалый взлёт популярности сети Tor. Популярна луковичная сеть стала среди заражённых нодов **русского** ботнета, который ведёт коммуникацию через этот самый Tor. Благодаря анонимности сам сервер, являющийся концентратором ботнета, найти сложно. На сентябрь 4 из 5 клиентов сети — заражённые боты.

И на это можно было бы положить, вот только такой рост нагрузки создал небывалый доселе прецедент, результатом которого стала нагрузка сети, граничащая с лимитом аппаратных мощностей серверов. Другими словами, сеть прогнулась под напором то ли вирусов, то ли Кровавой Гебни. Большинство онион-сайтов не работало. В Tor 0.2.4.17 эта проблема была исправлена.

Tails и Whonix

Готовые комплекты для ленивых и доверчивых анонов, в которых все необходимые меры защиты уже сделаны добрыми разработчиками (доверять им или нет, не спрятан ли там какой-нибудь подарок — выходит за рамки этой статьи и остаётся личным решением каждого юзера. Впрочем, их исходники открыты, а сборки с некоторых пор воспроизводимы).

«Хвосты» — это Live CD: загрузился с любого компа и пошёл троллить, не оставляя никаких следов на винте (без явного желания пользователя — разумеется, подмонтировать винт руками, если надо, никто не запрещает). Некоторое время поддерживала работу с i2p и имитацию внешнего вида самой популярной ОС, но увы.

«Хуникс» — ещё более злая штука: это две виртуалки, одна — шлюз, вторая — рабочий комп, у рабочего компа сетевуха только виртуальная и через неё доступен только шлюз. Даже если запустить на рабочей станции троян под рутом, он не сможет отстучаться в ZOG напрямую, спалив IP — шлюз не пустит. Тейлс в такой ситуации сдаст %username% с потрохами — если вражеская утилита получила возможность править iptables, то пиздец. Также он добавляет дополнительный уровень неразличимости анонов по метаданным: Tor Browser делает на одно лицо только браузеры, Tails — всю операционку, а Whonix — вообще весь комп, и софт, и железо. Даже MAC-адреса одинаковые.

Альтернативное использование

- Tor можно использовать не только для скрытия личности или творения злодейств, а еще и для доступа к портам компьютера с динамическим IP или за NAT. Суть такова: в конфигах Тора включается Hidden Service, указываются порты, после чего компьютер и порты становятся доступны по onion-адресу. Способ бесплатный, более простой и более безопасный, чем настройка VPN, DynDNS, IPv6 и прочей мути, за что уже полюбился установщикам камер наблюдения.
- Используется красноглазиками из Дебиан вместо https. Доступ на onion-сайты зашифрован без SSL.

Also

- В геометрии «тор» — замкнутая поверхность, похожая на бублик.
- Тор — всепогодный тактический зенитный ракетный комплекс.
- Скандинавский бог же.
- По забавному совпадению, с языка Мэндо'а (вымышленный язык вселенной «Star Wars») слово «Тор» переводится как «справедливость».

Что же там есть?

Вполне обоснованно считается, что сеть тора состоит из хакеров, троллей, любителей **ЦП**, наркоманов, барыг и агентов ФБР чуть менее чем полностью. Но на деле она заполонена ботами, неуверенными школьниками и любителями остро поесть.

In 5 Seconds

Представленные ниже ссылки, разумеется, заработают только при подключении к Тору (или по зеркалам, но это не труёвый способ).

Итак, что же внутри нашего бублика? (Осторожно, некоторые из сайтов ниже — кидалово)

- **The Hidden Wiki** (зеркало) — тут даже сказать нечего, это первый сайт, куда должен заглянуть торофаг-неофит. Интернеты этой вашей скрытой вики очень труднодоступны. Причина — в бешеной её популярности среди анонов, что обусловлено очень богатым содержимым: в ней содержатся ссылки практически на все ресурсы интернетов этого вашего тора. Однако следует иметь в виду, что многие ссылки — скам. Важные страницы огорожены от вандалов и спамеров.
- **Hidden Wiki** — клон Хидденвики.
- **The Uncensored Hidden Wiki** — ещё одна вики. Свободна от анальной модерастии.
- **Mixercoin** - биткоин миксер.не требует поддержки JS,самая низкая комиссия
- **Tor Wiki** — и ещё одна.
- **DarkWiki** — русскоязычный аналог Hidden Wiki. Удаляются только ссылки на порноресурсы, в остальном полная свобода действий. К ссылкам можно оставлять комментарии, без какой либо цензуры.
- **BestMixer** — один из наиболее популярных биткойн-миксеров, который позволившей смешивать транзакции в этой и других криптовалютах в интересах анонимности.
- **BitcoinFog**, **Mixmybtc** — миксеры биткоинов.
- **RuOnion блог** — блог о русских торнетах. Обзоры площадок, обсуждение вопросов личной безопасности.
- **RuTOR**, **RASH**, **UNITY Зеркало (v3) UNITY**, **AlphaBay** (зеркало) — торговые площадки-форумы. Оружие, вещества, краденные товары, поддельные документы, хакинг, кардинг, кошельки, пробивание баз, спецустройства и многое другое.
- **Runion** — старейший из существующих на данный момент русскоязычных форумов (работает с 2012 года). Имеется небольшой раздел для торговли, но сам сам проект позиционируется как некоммерческий ресурс. Участниками написано огромное количество статей на самую разную тематику — от информационной безопасности до медицины и права.
- "MEGA DARK MARKET" — Свободная торговая площадка. Официальные моментальные магазины Консорциума с января 2018. Активное зеркало
- **RAMP** — Главный ПАВ форум даркнета. RIP с лета 2017. Выжившие разбежались, рудип до сих пор празднует поминки.
- **HYDRA** — Торговая площадка с веществами.
- **24Bot** — Моментальные магазина. Боты/Сайты.
- **Solaris** — торговая площадка по продаже ПАВ, связана с форумом DarkCon, не требует JS. Временное зеркало
- **Консорциум** — независимое сообщество дилеров с RAMP. В связи с неопределенными событиями, последствиями которых было прекращение работы RAMP, решением Консорциума летом 2017 года был открыт форум CONSORTIUM для координации дальнейших действий, ведения торговой деятельности, сохранения клиентской аудитории, и предотвращения провокационных действий, несущих негативные влияния на рынок. Активное зеркало
- **Darkcon** — форум от Zanzi, позиционируется как приемник RAMP. Временное зеркало
- **Matanga**, **WayAway**, **Anthill**, **Narnia**, **Delos**, **VOID**, **Paradise**, **BlackMart** — русскоязычные форумы/площадки по торговле веществами и **Ukrainian Psy Community** — их украинский коллега.
- **ĒOS** — Яндекс.Маркет российского даркнета. Метапоисковик по торговым площадкам. Временное зеркало
- **Facebook** — популярная социальная сеть. Nuff said.
- **Onelon** — анонимная социальная сеть, позиционируется как самая безопасная и удобная. Чем-то напоминает имиджборд.
- **Fantom** — форум для настоящих параноиков. Регистрация и логин только через PGP-ключи, одноразовые 30-минутные домены для защиты от ДДоС и спама, ЛС шифруются по умолчанию. Имеются интересные статьи по анонимности, хакерству и безопасности.
- **КриптоВики** — секта криптоанархистов. Имеются подробные мануалы по шифрованию и список

полезных ссылок.
- **Общество шифропанков**.
- **Amazon Gift Cards**.
- **Onion Link Directory**, **OnionDir**, **TORDIR** — каталоги сайтов.
- **Web Hosting** — Apache, PHP5, MySQL, SFTP Access, onion Domain, Bitcoin server.
- **Not Evil**, **Candle**, **Torgle**, **TORCH**, **Sinbad Search**, **The Abyss**, **Ahmia** (зеркало в клирнете) — поисковики по луковой сети. Хотя бы один из них точно работает.
- **Oneirun** — русскоязычный поисковик в Торе. Админ вернулся из Нирваны и спиздил у наглосаксов полноценный индексатор. Теперь гордо именует свое поделие Яндексом даркнета.
- **Hydra** — доступное зеркало гидры
- **DuckDuckGo** — поисковик в обычных интернетах, не отслеживающий юзверей жучками и куками.
- **IM-клиент TorChat** — идентификатор скрытого сервиса используется как логин. Поддержки группового общения нет. Название символизирует.
- **Зеркало kiset.org** — анонимный чат со случайным собеседником.
- **Зеркало blockchain.info**, крупнейшего ресурса, где можно наблюдать за кошельками биткоин в режиме реального времени.
- **Зеркало торрент-трекера rutor.info**.
- **Зеркало Encyclopedia Dramatica**. Работает в режиме read-only, так как в условиях анонимности нелегко бороться с вандалами и виртуалами. Google Analytics отключен, но реклама включена. POST-запросы отсекаются. Во имя анонимности посетителей, HTTP-referrer и User-Agent удаляются из запросов и не попадают в логи, блокируются входящие и исходящие печеньки.
- **Флибуста** же. Книжечки.
- **Кавказ-центр** — новости тру-оппозиционеров-террористов.
- **Calyx Institute public Jabber/XMPP server**. Инструкция.
- **Maxima Culpa** — виртуальная исповедальня в Tor и не только. Социальный проект, в котором анонимные гопники и извращуги публично каются в своих грешках.
- **Информационно-вычислительный центр**. Ты под колпаком!
- **Филиал «Пиратской Бухты»**.
- **Местный pastebin**.
- **Обменник для зашифрованных RAR-архивов**.
- **SMS4TOR** — сервис для обмена самоуничтожающимися сообщениями.
- **Kali Linux — Russian Community** — русскоязычное сообщество Kali Linux в Tor.
- **Liberty** — онанимный новостной сайт.
- **CFUD.BIZ** — зеркало интернет-площадки cfud.biz. Хакинг, безопасность, кардинг, обнал и так далее.
- **Debian** — зеркало официального сайта операционной системы для красноглазиков.
- **Deep Web Radio** — радио. По разным потокам можно послушать джаз, кантри, хаус, барокко-музыку и митол.
- **MONITOR** — Альманах Даркнета. Каталог ресурсов сети Tor с независимым рейтингом. Проект разработан при поддержке Консорциума www.TORMONITOR.com
- **Годнотаба** — открытый сервис мониторинга в сети TOR.
- **DarkWiki** — русскоязычная hiddenwiki, каталог onion сайтов без цензуры
- **Кооператив «Черный»** — 1,3,7-триметилксантин. Товар прямиком с колумбийских плантаций! Только цельный продукт, никаких примесей!!! Лучше употреблять в чистом виде. *(спойлер:* Сайт московской кофейни, джаст фор лулз барыжащей закладками с **обычным кофе** за биткоины.*)*
- **ProtonMail**, **Mail2Tor**, **Scryptmail** (зеркало scryptmail.com) — почта для параноиков.
- **Øchan** — зеркало Нульчана.
- **8chan** — зеркало 8ch.net.
- **Lolifox** — зеркало некогда бразильской борды
- **Neboard** — зеркало neboard.me.
- **Вики 404** — зеркало wiki.404.city.
- **Yukon** (зеркало yukon.to), **HireMe** — фриланс-биржи.
- **GoDaddy** — хостинг-сервис и покупка доменов .onion.
- Онион-ответы: **на русском**, **английском**, **испанском** и **португальском**.
- ТorАДицийо же ж.
- **O3Shop** — магазин ветерана торговли веществами.
- **AlcoTown.ru** — доставка алкоголя в ночное время.
- **OTZOVIK** — Отзовик, форум для отзывов, рекомендаций, предостережений, жалоб русскоязычного населения дипвеба.
- **DarknetStats** — аналитика русского даркнета. Временное зеркало
- **VK-Photo.onion** — Частные фотографии девушек со всего СНГ.
- **Narnia — Smells like Freedom** — первая в даркнете соцсеть анонимусов. Да, соцсеть, да, для анонимусов.
- **BitTorrent трекер RuTracker.org** — Рутрекер теперь и в даркнете!
- **ЦРУ**, при том таки да. Для желающих продать родимые секреты, и не повстречаться с товарищем майором.

- **Fresh Onions** — Каталог onion сайтов в сети tor. Регулярно обновляется, а также проверяет доступность имеющихся в каталоге сайтов. На данный момент содержит ссылки почти на все известные ресурсы в скрытой сети.

Ссылки

- Блог о TOR.
- Агентство национальной безопасности США шпионит за пользователями Tor.
- Torproject.org.
- Предупреждение, или Как можно запалиться и с Тором.
- Атаки на Tor.
- Основатель Freedom Hosting арестован в Ирландии и ждет экстрадиции в США.
- Подключение к Tor для чайников.
- Onion routing в английской педивикии.
- Как вычислить IP в сети Tor за 20 минут.
- Поставь себе Tor и получи PROFIT!
- Генерация читаемых имён .onion-сайтов (наподобие Silk Road'a).
- Скрытая доска на Нульчане.
- Как пользоваться IRC через Tor.
- Tor2web.org.
- Web Of Dark — блог о Tor'е и технологиях анонимности. Новости, статьи, руководства и статистика.

См. также

- I2P
- Proxy

Примечания

1. ↑ Но потом не удивляйтесь, что вас забанят по IP на Форчанчике, Педивикии и ещё массе сайтов, мониторящих список Tor-серверов, просто потому, что ваш IP присутствует в публикуемых списках нодов, а вовсе не за то, что с вашей айпишечки постят хуйню всякие боты. Это называется «превентивные меры защиты». Примерно как у РКН.
2. ↑ Эти два выходных сервера забанены. Анон к этому не имеет отношения.
3. ↑ [1], [2], [3], [4], [5], [6], [7], [8], [9], [10]/

Интернет

Интернеты 127.0.0.1 ADSL Bitcoin CMS DDoS Frequently asked questions GPON I2P Internet White Knight IPv6 IRC MediaGet Miranda NO CARRIER QIP Ru@razlogoff.org SEO Skype Tor TOS Via WAP Ёбаное ВТ Админ Акадо Американские интернеты Анонимус Аська Бан Бесплатный хостинг картинок Блог Блогосфера Бот Ботнет Браузерка Бугагашечки Бурление говн Вап-чаты Веб 1.0 Веб 2.0 Вики Виртуал Вордфильтр Голосование ногами Гостевуха Диалап Дом.ру Домашняя страница Дорвей Единый реестр запрещённых сайтов Жаббер Заповеди интернета Заработок в интернете Идентификация пользователей в интернете Известные интернет-флешмобы Имиджборд Инвайт Интернет-магазин Интернет-сервисы Искра Кик Кириллические домены Кликбейт Коммент Комьюнити Лесенка Лог Локалка Макхост Мем Микроблог Мобильный интернет Модератор Некропост Ник Оптимизатор Ответы Офлайн Оффтопик Письма счастья Подкаст Поисковая бомба Покровитель интернетов Пост Правила интернетов Предыдущий оратор Премодерация Пруфлинк Рерайтинг Ростелеком Сабж Сетевые онанисты Симпафка Синдром вахтёра Ситилайн Скайнет Скриншот Смайл Социальная сеть

Software

12309 1C 3DS MAX 8-bit Ache666 Alt+F4 Android BonziBuddy BrainFuck BSOD C++ Chaos Constructions Cookies Copyright Ctrl+Alt+Del Denuvo DOS DRM Embrace, extend and extinguish FL Studio Flash FreeBSD GIMP GNU Emacs Google Google Earth I2P Internet Explorer Java Lolifox LovinGOD Low Orbit Ion Cannon Me MediaGet MenuetOS Microsoft Miranda Movie Maker MS Paint Open source Opera PowerPoint PunkBuster QIP Quit ReactOS Rm -rf SAP SecuROM Sheep.exe Skype

StarForce Steam Tor Windows Windows 7 Windows Phone 7 Windows Phone 8 Windows Vista Wine Winlogon.exe Wishmaster Word ^H ^W Автоответчик Антивирус Ассемблер Баг Билл Гейтс и Стив Джобс Блокнот Бот Ботнет Браузер Варез Винлок Вирусная сцена Генерал Фейлор Глюк Гуй Даунгрейд Демосцена Джоэл Спольски Донат Защита от дурака Звонилка Интернеты Кевин Митник Китайские пингвины Костыль Красноглазики Леннарт Поттеринг Линуксоид Линус Торвальдс Лог Ман Машинный перевод Мегапиксель

Just Another Fucking Acronym

14/88 1C 265 A.C.A.B. ADSL AFAIK AFK AISB AJAX Aka All your base are belong to us AMV ASAP ASL ASMR ASUS EEE BAT BBS BDSM BOFH BRB BSOD BTW CMS Command & Conquer Copyright Counter-Strike CYA DC DDoS Delicious flat chest Direct Connect DIY DJ Doki Doki Literature Club! DOS DRM EFG Etc Five Nights at Freddy's Frequently asked questions FTL FTN FTW FUBAR GIF GIMP GNAA GPON Grammar nazi Grand Theft Auto GTFO Happy Tree Friends HBO How It Should Have Ended I see what you did there I2P IANAL IDDQD IIRC IMHO In before Internet Explorer IRC IRL ITT JB (ЛОР) JFGI Kerbal Space Program KFC KISS Let's get ready to rumble! LFS Livejournal.com LMAO LMD LOL Low Orbit Ion Cannon M4 MacOS Microsoft MILF MMORPG MSX MTV N.B. NASCAR NEDM NES NoNaMe Not Your Personal Army NRB NSFW O RLY? OK OMG OS/2 P. S. P2P Panty and Stocking with Garterbelt

w:Tor en.w:Tor (anonymity network)