Анонимность в интернете

В этой лекции речь пойдёт о связках для выхода в интернет и их особенностях. В практической части будет настройка firefox, который будет использоваться как основной браузер для даркнета, и использование его в связках.

Любую работу в даркнете рекомендую производить только из виртуалок. Причём надо разделять виртуальные машины по назначению и не делать всё с 1 виртуалки. Работа только с одной виртуалке обычно закончится тем, что на ней накопится куча данных, в том числе и важных, а потом в результате работы по неосторожности на неё попадёт вирус и все данные будут либо стёрты, либо похищены. Задача виртуалки - принимать на себя удар в случае атак извне, быть безопасной для основной системы и не давать понизить анонимность при её взломе, а так же хранить данные по работе, для которой она была создана.

Для создания дополнительной виртуальной машины есть несколько опций: установить с нуля как это делалось в практике, либо клонировать уже существующую машину. В VirtualBox есть система снапшотов - снимков состояния машины на определённый момент времени. После создания снапшота все последующие изменения на диске можно откатить до момента снятия снимка. Работает это по принципу создания нового виртуального диска, который хранит изменения с моментом создания копии. Стоит отметить, что виртуальную машину со снапшотами сложнее перенести, потому что там уже нет единого файла состояния. Поэтому если в планах виртуалку переносность куда-то, то лучше не делать linked-clone(привязанные копии) это виртуальной машины или делать только Full Clone - everythink(полные копии всего), которые по сути являются самостоятельными виртуальными системами. Но сами спапшоты - это один из механизмов, который поможет уберечь рабочую виртуалку от попадания вирусов. Перед запуском непроверенного приложения сделайте снапшот(делается просто выбором плавой кнопкой мыши машины в меню virtualbox и выбором пунта **Clone(клонировать)**), а как работать с ним закончите, откатите систему(В virtualbox при выборе машины сверху справа есть 2 кнопки Details(Детали) и **Snapshots(Снимки)**, на вкладке снимки можно перемещаться между состояниями).

Памятка при создании новой машины

Важным элементом защиты является подключения виртуалки только через Gateway. После создания новой машины первое, что надо сделать - зайти в настройки виртуалки в VirtualBox и в Network(Сеть) и установить тип адаптера Internal Network(внутренняя), имя Whonix. Это гарантирует, что весь трафик пойдёт через tor или интернета на машине просто не будет. Опять же напомню, что для доступа в интернет при такой настройке виртуалка с gateway должна быть запущена в фоне.

TOR

Предоставлю вам статью, которой поделились со мной коллеги, статья не моя, но все же она станет неплохим вступлением при знакомстве с тором:

Давайте рассмотрим что такое TOR, рассмотрим его опасность и в тоже время большой плюс безопасности

TOR обрел широкую популярность после проекта Silk Road

TOR - построена на сети компьютеров, через которую информация передаётся схожим с пиринговыми сетями образом, но в зашифрованном виде.

The Onion Router (сокрщ. Tor) — иначе называют "луковый роутер" названный так из-за множества слоёв шифрования, похожих на слои луковицы.

Гуляют байки по интернету что TOP это проект созданный спец службами, чтоб собрать всех преступников в одном месте, и правда, идея неплохая.

Тут же у вас возникает вопрос, а нету ли там какого то бэкдора? Tor имеет открытый исходный код, за все существование его "прощупывали" многие криптографы и специалисты и все проверяющие пришли к выводу что Tor действительно имеет высокий уровень анонимности, каждый из вас так же может просмотреть исходный код, но присутствуют и недостатки, которые мы сегодня рассмотрим.

К сожалению многие думают что Tor это браузер, который просто меняет айпишник, но это далеко не так. Tor - это сеть машин и набор протоколов, а все данные в нём подчиняются правилам внутренней маршрутизации. TOR – это система, создающая свой собственный подуровень интернета, опираясь на те узлы (в большинстве своем обычные пользовательские компьютеры) где она установлена.

- К ресурсу вы выходите через систему других IP.

- Выход осуществляется в обход отечественного провайдера, а значит, ограничения не работают.

- TOR дает возможность шифрования данных. Тем самым затрудняя прослушку и слежку.

Цитата разработчиков Тора:

При подключении через сеть опасно открывать популярные форматы документов .doc и .pdf, потому что они также могут загрузить контент (например, изображения) с внешних источников при открытии их в сторонних программах, не сконфигурированных под Tor. Кроме того, в Tor нельзя пользоваться торрентами: во-первых, они сильно перегружают сеть, во-вторых, из-за особенностей в работе протокола BitTorrent подключения через него осуществляются напрямую, а не через сеть компьютеров волонтёров, анонимизирующих трафик.

Не скажу, что это самый глубокий анализ тора, но несколько ключевых моментов выделю отдельно и раскрою их

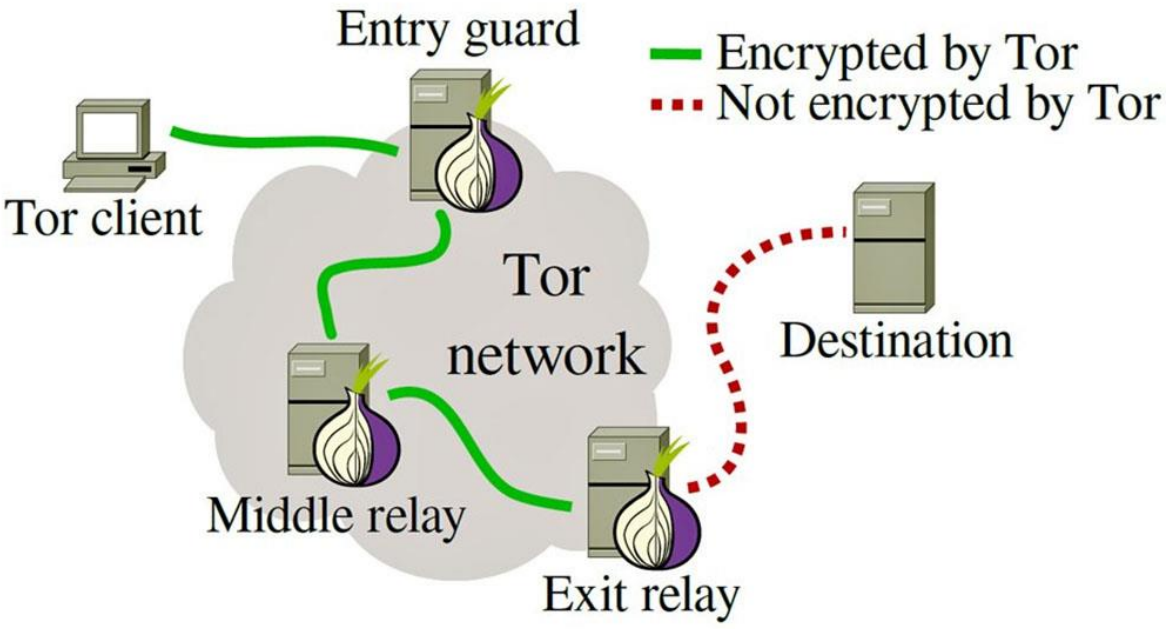
- Tor - не просто браузер для смены IP, а по сути через tor можно передавать абсолютно любой траффик. Например, подключиться к ftp или ssh серверам, заходить на удалённый RDP и т.п. Но некоторые типы запросов там запрещены. Например, ICMP, поэтому команда ping через tor не вернёт никаких результатов.
- Tor подразумевает внутреннюю маршрутизацию перед передачей пакета в сеть. Мощная инфраструктура - одно из основных преимуществ TOR, она позволяет действительно хорошо скрыть связь между источником трафика и выходной нодой. При запросе обычного сайта по умолчанию используется 3 промежуточные ноды(участники пути пакета, для запутывания следов), а при запросе onion ресурса - 6.
- При запросе onion ресурса данные не покидают сеть tor и зашифрованы надёжным образом вплоть до самого сервера. **Но при запросе любого сайта или ресурса вне сети tor, запрос расшифровывается на выходной ноде и теоретически может быть просмотрен или даже изменён**. Эта одна из причин, почему не советуют качать через TOR: нода может подменить exe на вирус.

Выходная нода - один из серверов сети TOR, который является конечным звеном, и с которого запрос отправляется непосредственно в интернет(ответ приходит на него же).

В связи с такой структурой при использовании тор есть следующие опасности

- Трафик гарантированно шифруется полностью только при получении доступа к .onion ресурсу. При загрузке внешнего ресурса(не .onion) шифрование на уровне тора на выходной ноде отсутствует, и, если данные передаются не по зашифрованному протоколу(например, ws, ftp, или http), владелец выходной ноды может прослушать проходящий трафик, вынимать от туда пароли с логинами или вообще подменить страницу или файл, если вы качаете что-то через тор.
- Все ноды в тор принадлежат кому-то, в том числе и у каждой выходной ноды есть свой владелец. Как я сказал выше, на выходной ноде может проскальзывать лишняя информация, которая при должном анализе может указать на вас. Поэтому есть "плохие" ноды, которые создавались с целью слежки или кражи данных. Хорошей нодой вы пользуетесь или нет -- понять невозможно. Список нод общедоступен: https://torstatus.blutmagie.de/ Там есть графа 'Bad Exit', так помечается плохие ноды. Проблема в том, что проверить достоверно невозможно, и надо понимать, что все ноды кроме своей, потенциально плохие.
- Список входных нод известен и даже релейные ноды со временем попадают в него. А это значит, что провайдер может легко составить список людей, регулярно пользующихся тором через сопоставления запрашиваемых IP со списком входных tor нод. А это крайне ему не нравится, можно попасть в список *"ему есть, что скрывать"*. С последующем анализом трафика в пассивном режиме, которое может вылиться в проверку вас. Но до такого дело обычно не доходит если не давать другие поводы проверить соединение. В любом случае VPN спасает от попадания под критерий использования tor'a.

Для того, чтобы более наглядно понять как TOR направляет пакеты, посмотрите на этот график.



Наличие незашифрованного участка в конце неизбежно. Но это не значит, что тор только вредит безопасности и его создали чтобы собрать всех бандитов в одном месте и с выходной ноды трфик стричь. Важным является то, что речь идёт именно о шифровании tor. То есть это дополнительное шифрование, но ничего не мешает трафику быть зашифрованным протоколом общения с сервером. Для веб сайтов это использование протокола https, для веб сокета это wss. Некоторые протоколы его используют в основе, например ssh. Но остаются ресурсы, которые работают по незащищенным протоколам. Это, например, http, ftp, а так же множество приложений обменивается незащищенным трафиком. В итоге, если используется тор, то обязательно надо проверять, что на сайтах, в которых вводится какая-либо важная информация, есть шифрование(протокол https), и никогда нельзя в торе игнорировать ошибки сертификата в браузере, пока не ясна причина, по которой она случилось. Встречаются ноды, которые свой сертификат пихают и с его помощью внедряются в https соединение.

Но помимо конкретных опасностей в tor существует ещё несколько других минусов:

- Все IP адреса Тора в блэк листах. А это значит, что при пользовании google надо будет постоянно разгадывать ребусы, и то в последнее время доступ просто блокируется. Для того, чтобы попасть на большинство сайтов, придётся проходить много проверок.
- Постоянно меняющийся IP не позволяет логиниться на сайтах, где сессия привязывается к IP.
- При попытки входа в онлайн-банк и прочие системы где присутствует антифрод, аккаунт будет моментально заблокирован. Попытка входа через тор равносильна попытке взлома для серьёзных систем защиты.
- Заметное падение скорости соединения.

И есть ещё один нюанс, который редко где упоминается: даже в tor браузере можно снять fingerprint. И в сявзи с тем, что tor browser не используется массово, именно факт его применения зачастую используется как основа для отслеживания пользователя.

fingerprint - уникальный отпечаток браузера. Он генерируется на основе настроек браузера, его версии, конфигурации системы, быстродействия железа и тд.

Снимать отпечаток точно получается не всегда, но чтобы контролировать этот процесс и поддерживать fingerprint когда нам это нужно, возможностей одного tor browser недостаточно.

В придачу есть Java аплеты, Adobe Flash, Adobe Shockwave, QuickTime, VBScript это технологии, с которыми может взаимодействовать браузер, но они не являются его частью. А значит, что и настройки доступа в интернет у них свои, отличные от браузера. И если страница запросила активацию какого-то разрешения, то есть вероятность, что это разрешение выйдет в интернет под реальным IP, а эта угроза безопасности.

На подлесок упомяну, что есть сервисы типа onion.to. Через них без тор браузера можно открыть любой тор сайт, достаточно только в конец добавить .to Но лучше никогда это не использовать, это не анонимно и ваш IP не скрывается, более того создатель сервиса может просматривать весь трафик, так как защиты тора при пользовании такими сервисами нет. И были случаи, когда провайдеры использовали эти сервисы для мошенничества.

Я упомянул все основные особенности и минусы tor, а так же постарался объяснить, почему они есть. Можно конечно всё отключить, чтобы на сервере был доступен только минимум, но работать так будет невозможно. Отказаться от тора мы тоже не можем: он слишком хорошо скрывает реальный IP, но если не забывать о его ограничениях. Об улучшении жизни в торе будет следующая практика. Но для таких дел как посещение onion сайтов или хорошо знакомых форумов тяжёлая артиллерия не нужная, для простого *серого* браузинга вполне подходит tor browser на основной системе.

Для дел покрупнее будет использоваться firefox в виртуалке, который мы настроим на следующем занятии. В основной системе можно его не настраивать потому что работы с неё вестись всё равно не будет.

Поскольку TOR прослушивается, то надо избежать использования http сайтов через него и других незашифрованных протоколов. Это не всегда возможно, и есть метод быть уверенным, **что выходная нода не прослушивается - создать свою**. Из минусов -- IP не меняется, поэтому можно расценить это как продвинутые прокси с хорошим шифрованием. О создании своей ноды и подводных камнях в этом будет ещё отдельно статья.

Использование карт дропов

В практике будет настроен браузер, который достаточно универсальный, но для захода в интернет банки лучше не рисковать и использовать для этих целей RDP деда. **Дедик - dedicated server, выделенный сервер**. Это машина на windows, которая арендуется у хостера и управление которой ведётся удалённо. Есть много сервисов для аренды RDP, можете воспользоватся агрегатором для поиска серверов,(www.poiskvps.ru) выбирайте в качестве оплаты Биткоин.

Для подключения к RDP на виртуалке надо использовать встроенный клиент. Для этого открываем пуск и находим утилиту mstsc.exe, открываем её и вбиваем данные для подключения(даются после оплаты rdp).

На каждую карту используется свой персональный дедик. Их можно использовать не только для захода в банки, но и для работы через них. Если в деле не важен быстрый отклик, то работа через дела может быть удобнее. Для доступа на сайт банка большие мощности не нужны, можно выбрать самую минимальную комплектацию дедика, но объём оперативки важен. Желательно, чтобы её было от 2х ГБ.

Если в конфиге tor установлена своя нода, то её надо убрать на время подключения к дедику. РДП соединение и так шифруется, а использование динамических нод усложняет поиск источника.