УДК 004.056 **Информационные технологии**

Камбулов Данил Александрович, *студент I курса, магистрант,*
Федеральное государственное бюджетное образовательное учреждение высшего образования "Донской государственный технический университет" (г. Ростов-на-Дону)

ОБЕСПЕЧЕНИЕ АНОНИМНОСТИ В СЕТИ ИНТЕРНЕТ С ИСПОЛЬЗОВАНИЕМ ТЕХНОЛОГИИ «ЛУКОВИЧНОЙ» МАРШРУТИЗАЦИИ БРАУЗЕР TOR

Аннотация: Настоящая работа посвящена анализу технологий «луковичной» маршрутизации браузер Tor. Рассмотрены различные атаки на анонимную сеть с целью деанонимизации пользователя. Изучены принципы взаимодействия узлов в «луковичной» маршрутизации браузер Tor.

Ключевые слова: информационная безопасность, Tor, узел, маршрутизация, обеспечение анонимности, мост, DoS-атака, анализ трафика.

Annotation: This paper is devoted to the analysis of "bulbous" routing technologies in Tor. Various attacks on the anonymous network for the purpose of deanonymization of the user are considered. The principles of node interaction in the "onion" routing of the Tor browser are studied.

Keyword: information security, Tor, node, routing, anonymity, bridge, DoS attack, traffic analysis.

Ни для кого не секрет, что с появлением интернета в современном мире и повседневной жизни резко возрос уровень преступности (так называемые «кибер-преступления»). Для профилактики, предотвращения и даже раскрытия преступлений правоохранительным органам приходится использовать современные технологии, отслеживая при помощи сети-Интернет

противоправную деятельность злоумышленников, что зачастую бывает крайне сложно. Приходится очень постараться, чтобы установить и разоблачить нарушителей, которые умело скрывают и маскируют свои противоправные действия от посторонних глаз. В это трудно поверить, но остаться в сети-Интернет незамеченным очень легко и многие из общеизвестных способов при работе во «всемирной паутине» делают нас анонимными. Вместе с тем, ряд из них уже хорошо известен правоохранительным органам и сразу же выявляется, другие же просто устарели и стали малоэффективными. Однако технический прогресс не стоит на месте, создаются новые усовершенствованные способы по анонимизации трафика из сети-Интернет, которые доступны обычному пользователю.

Об одном из таких методов пойдет речь в данной статье. Проведем анализ всех плюсов-минусов, и насколько хорошо он скрывает нашу личную информацию и деятельность в сети.

TOR (от аббревиатуры The Onion Router «луковичная система роутеров») [1] - свободное программное обеспечение, позволяющее устанавливать анонимное сетевое соединение (далее – Tor, ПО).

Система Tor была разработана в одном из военных ведомств США, однако для каких именно целей – история умалчивает. В двухтысячном году по неизвестным причинам исходный код был рассекречен и ПО попало в статус свободно распространяемого. Сейчас его может использовать любой, кому необходимо скрыть свою деятельность в сети-Интернет.

На данный момент система Tor насчитывает в себе больше 7 тыс. находящихся по всему миру узлов, которыми управляют пользователи данной программы. При совершении анонимного исходящего соединения происходит обращение Tor-браузера к серверу каталогов HSDir и загружает список доступных ретрансляторов (компьютеры, работающие в качестве прокси-серверов), из которых создается цепочка серверов (рис. 1), что в свою очередь предоставляет возможность выхода в сеть.

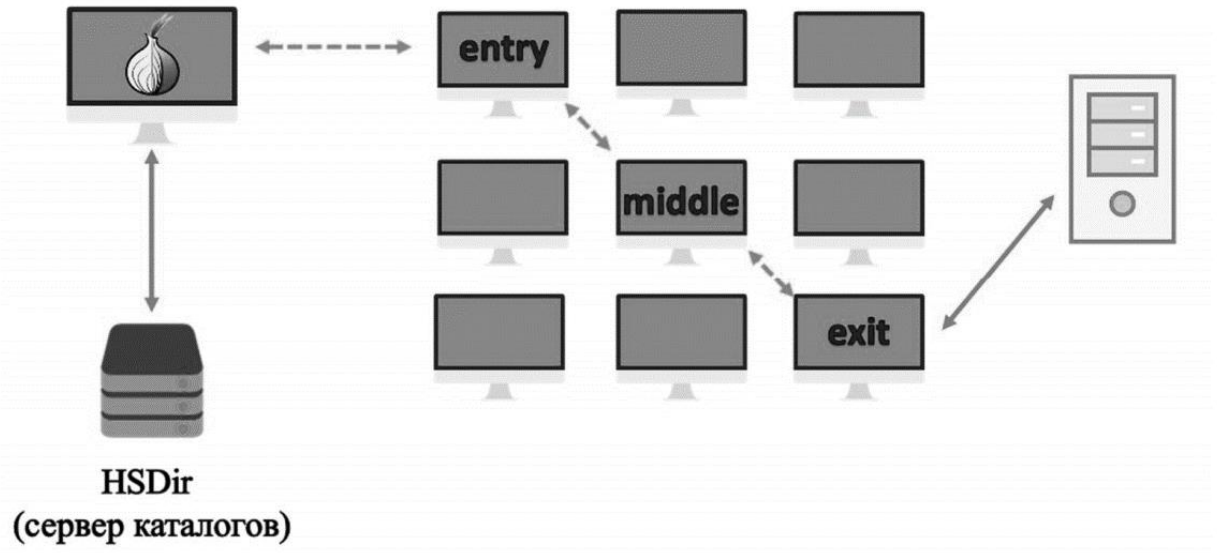

Рисунок 1 – Построение цепочки Tor – браузера

Существует три типа узлов:

— Входной или как еще называется «сторожевой» - точка доступа в сеть. Входной узел выбирается из высокоскоростных стабильных ретрансляторов, которые работают долгое время.

— Промежуточный узел – происходит передача трафика от входного к выходному. В результате данной операции узлу не предоставляется информация о предыдущих и последующих.

— Выходной узел – это точка выхода из сети, которая отправляет трафик до запрашиваемого клиентом ресурса. Выходные узлы выполняют особую роль, так как передают трафик в конечный пункт. На операторах выходных узлов лежит особая ответственность, поскольку они отправляют трафик в пункт назначения и все действия, совершаемые через Tor, будут связываться с выходным узлом, тем самым ставя под угрозу личную информацию пользователя.

На каждом участке пути происходит шифрование маршрутизации, но содержимое пакетов не шифруется. Из-за многоуровнего шифрования информацию может расшифровать только выходной узел.

Рассмотрим способ соединение клиента через Tor-браузер.

На начальном этапе идет отправка пакетов первому узлу, в нем находится закодированный адрес промежуточного узла. Первый узел, зная ключ для расшифровки пакета и адрес следующего узла, переправляет туда пакет. Промежуточный узел, получив пакет, имеет ключ для адреса выходного узла.

И так продолжается до тех пор, пока пакет данных не дойдет до пункта назначения.

Именно из-за такой технологии произошло название «The Onion Router-луковичная система роутеров», так как данный процесс напоминает последовательное снятие слоев с лука, чтобы добраться до сердцевины, то есть, до начальных данных, которые отправлял пользователь.

В случае перехвата пакета информации на одном из участков сети, возможно узнать данные только о двух ближайших промежуточных серверах. Из-за частичного удаления информации маршрутизации не удастся узнать адреса конечных пунктов.

Выходные узлы знают исходные данные, потому что они отправляют их в конечный пункт и могут извлекать из трафика личную информацию, которая передается открытым текстом по HTTP (Hyper Text Transfer Protocol — «протокол передачи гипертекста») и FTP (File Transfer Protocol — протокол передачи файлов) [2].

Из-за сложного шифрования ретрансляторам не удастся узнать полный путь данных от отправителя до получателя. Так как трафик пользователя скрыт и узлы не несут ответственность за содержимое передаваемых данных, узнать какие сайты вы посещали не представляется возможным.

Узлы и мосты:

После запуска Tor - браузера ему надо получить списки всех узлов. Этот список не засекречен и его открытость важна. Вместе с тем существует проблема: так как с помощью Tor-браузера пользователи скрывают свою активность в сети-Интернет, встал вопрос о его блокировке правительством.

Существует два способа блокировки:

1) Запрещать доступ пользователям, выходящим из Tor: этот способ, позволяет предотвратить посещение определенного сервиса. Для этого необходимо загрузить список выходных узлов и постепенно блокировать исходящий трафик из них. Разработчики браузера не могут препятствовать данной процедуре.

2) Запрещать доступ пользователям, входящим в Tor: данный способ блокирует всех входящих пользователей и не дает им посещать ни какие сайты. После этого браузер станет бесполезным, потому что прекращается обход цензуры.

Если бы существовали только узлы, то это было бы возможным, так как можно было бы скачать список входных узлов и заблокировать весь трафик. Но разработчикам удалось найти решение – мосты.

Мост - это выкладываемые в сеть Internet узлы, которые обеспечивают взаимосвязь двух или нескольких локальных сетей[3]. Логичным был бы вопрос: «если мосты скрыты, то где их брать?». Однако существует список мостов BridgeDB от разработчиков.

Клиенты получают некоторую часть от списка мостов, для того чтобы связаться с оставшейся частью в сети. Это необходимо для предотвращения блокировки сети. Узнать весь список мостов не получится, так как он строго засекречен. Некоторые мосты возможно узнать, если запустить в сеть промежуточный узел, который будет отслеживать входящие запросы. Так как к узлу обращаются входные узлы и мосты, то можно отследить те узлы, которых нет в открытом списке.

Как работает сеть Tor на низком уровне?

В Tor-клиенте содержится определенное количество информации о 10 поддерживаемых доверенными лицами мощных узлах. Они отслеживают состояние всей сети и называются «Directory Authorities (DA, управляющие списками)». Эти узлы выбирают, когда и каким узлам работать.

Почему именно 10? Дело в том, что 9 DA работают со списками узлов, а один DA – со списком мостов.

Как DA поддерживают стабильность Tor?

Работоспособность узлов зависит от частоты обновления документа, который имеет название «консенсус». Управляющие списки поддерживают его при помощи голосования. Происходит это в несколько этапов:

— каждый DA создаёт список известных узлов;

— после подсчитывает все остальные данные – флаги узла, веса трафика и т.п.;

— отправляет данные как «голосование за статус» всем остальным;

— получает голоса всех остальных;

— комбинирует и подписывает все параметры всех голосов;

— отправляет подписанные данные остальным;

— большинство DA должны согласовать данные и подтвердить наличие консенсуса;

— консенсус публикуется каждым DA.

Для того, чтобы любой пользователь имел доступ к скачиванию последней версии, публикация документа осуществляется по HTTP.

В Tor не все узлы выполняют поставленную задачу. Поэтому была создана система «Exitmap» для отлова некачественных выходных узлов. Для каждого выходного узла запускается модуль. Он производит скачивание файлов, и все результаты заносятся в отдельный файл. Данный модуль использует библиотеки «Stem» (предназначенные для работы с Tor), которые позволяют строить схемы для выходного узла. В 2013 году, используя этот модуль, разработчики нашли 65 из 1000 испорченных узлов, которые подменяли трафик, что могло привести к отслеживанию информации. «Exitmap» по сей день работает и поддерживается разработчиками.

На сегодняшний день выделяют несколько видов атак анонимизации на Tor – браузер.

1. Атаки на пользователя. Наиболее эффективными атаками в этом направлении являются Torben-атака и RAPTOR-атака. Суть Torben – атаки заключается в том, что что злоумышленник может контролировать

зашифрованное соединение между пользователем и входным узлом, а также внедрять на отображаемы страницы пользователя специальные маркеры. Как правило маркеры вставляются на сайт в виде рекламных баннеров. Маркер генерирует характерный шаблон, который можно обнаружить между пользователем и входным узлом (рис. 2). Тем самым данный механизм позволяет деанонимизировать пользователей web – сайтов, на которых был размещен маркер.

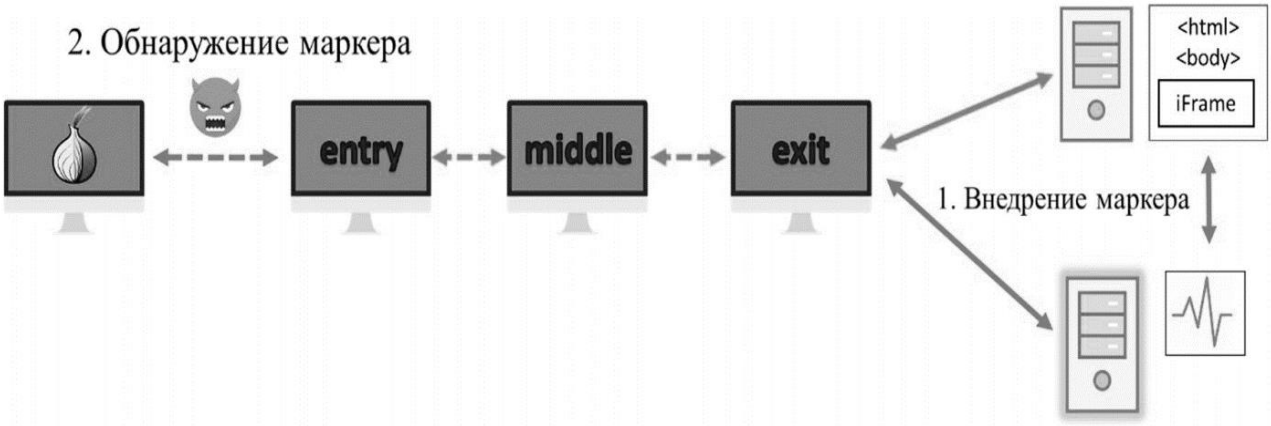

Рисунок 2 – Реализация Torben-атаки

Маркер состоит из 20-ти байтового значения SHA-1 отслеживаемых URL - адресов web - страниц. Отсюда следует, что существует совпадение между URL – адресами и их маркерами. Для их обнаружения существует многоклассовая машина SVM (support vector machine - метод опорных векторов) с вероятностными выводами последовательностей отдельных маркеров веб-страниц. Система использует вероятностное сравнение для выбора наиболее подходящего маркера.

Данная система позволяет обнаруживать маркеры с точностью более 91%, с наименьшим показателем ложных срабатываний.

Согласно вышеописанному процессу построения луковичной маршрутизации, входной узел является единственным узлом, который взаимодействует напрямую с пользователем. Для того, чтобы подменить входной узел на зараженный, используют различные методы блокирования соединения, с целью перенаправления пользователя на необходимый узел.

Данный процесс можно реализовать с помощью провайдера или сетевых администраторов.

Raptor атака (с англ. Routing attacks on privacy in Tor) - – атака на Tor, где в качестве атакующей стороны выступает автономная система. RAPTOR атака использует динамические аспекты протокола BGP.

Атака состоит из трех частей:

— асимметричный анализ трафика. В нем анализируются поля TCP-заголовков для выявления номера TCP-последовательности и номер TCP-подтверждения доставки. Вычисляется корреляция между этими полями;

— анализ натуральных перебоев. Путь между клиентом и входной нодой постоянно меняется, а это повышает вероятность попадания в коррумпированную автономную систему;

— BGP-сниффинг – коррумпированная автономная система производит атаку «человек посередине» между клиентом и входным узлом. Это позволит автономной системе выполнять ассиметричный анализ трафика.

2) Атаки на сервер. Данные атаки реализуются с помощью специальных сервисов. Атака Cell counting (атака с пометкой ячеек). Для реализации данной атаки злоумышленник должен иметь контроль над входным и выходным узлом сети Tor (рис. 3). При ее реализации входной узел дублирует сообщение, с последующим сохранением IP – адреса пользователя и время дублирования. На выходном узле злоумышлений производит сканирование сети, с целью засечь дубликат сообщения, а затем вычислить IP – адрес и порт подключения. После таких манипуляций злоумышленник может вычислить пользователя и какие URL – страницы он посещал.

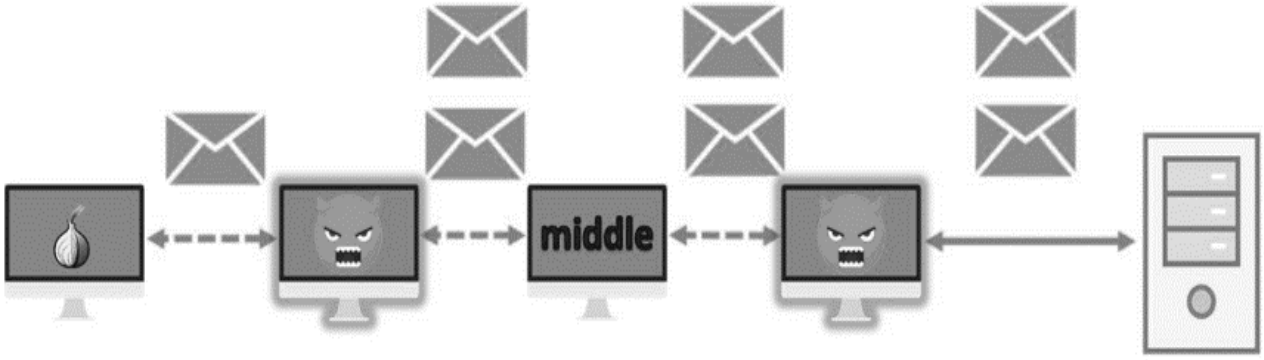

Рисунок 3 – Реализация Cell counting attack

Следующий вид атаки на сервер – это Off-path MitM attack. Данная атака позволят злоумышленник позволяет получить доступ к метаданным скрытой службы. Объектом атаки выступает HSDir сервис. HSDir – каталог скрытой службы (Hidden Service directory). Эти каталоги содержат информацию, позволяющую получать доступ к onion-доменам (псевдодомены верхнего уровня, созданные для обеспечения доступа к анонимным или псевдоанонимным адресам сети Tor [6]), не нарушая анонимности пользователя.

Для реализации данной атаки злоумышленнику необходимо скомпрометировать закрытый ключ скрытого сервиса, а также создать ложного клиента для имитации подключения к серверу. Реализации атаки представлена на рисунке 4.

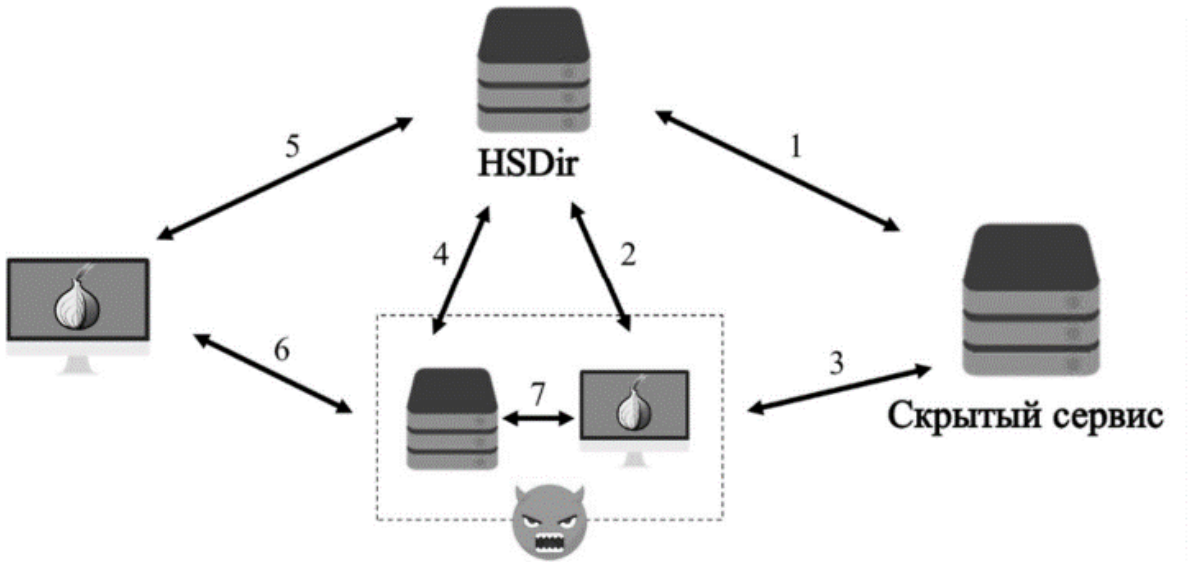

Рисунок 4 – Реализация Off-path MitM attack

Основные этапы:

1. На начальном этапе скрытый сервис обращается к каталогу и подгружает дескрипторы.
2. Злоумышленник получает информацию из необходимого каталога HSDir.
3. Злоумышленник имитирует работу клиента, тем самым устанавливает соединение со скрытым сервисом.
4. Имитируя работу скрытого сервиса, злоумышленник использует скомпрометированный закрытый ключ и загружает новые дескрипторы в HSDir.
5. Клиент, захотев подключиться к скрытому сервису, загружает дескрипторы с HSDir.
6. Клиент подключается к «скрытому сервису» (злоумышленнику).
7. Злоумышленник передает трафик клиента скрытой службе.
8. Злоумышленник находится между сервисом и выходной нодой, где трафик передается.

3) Атака на сервер(узел). CellFlood DoS attack. В сети Tor существуют различные виды сообщений для обмена информацией между узлами. Именно обработка некоторых из них на узлах сети легла в основу этого вида атаки [5]. Атака использует запросы создания цепи (CREATE), которые быстро генерируются атакующим, однако они будут требовать большое количество вычислительных ресурсов от узла для ее обработки. Поэтому из-за криптографических операции обработка CREATE-сообщения занимает в 4 раза больше времени, чем его генерация.

Узел, получающий CREATE-сообщения быстрее, чем его процессор может обработать, отвечает на них, посылая DESTROY-сообщения в ответ. Следовательно, узел, находящийся под атакой, будет отклонять запросы от легитимных узлов (рис. 5).

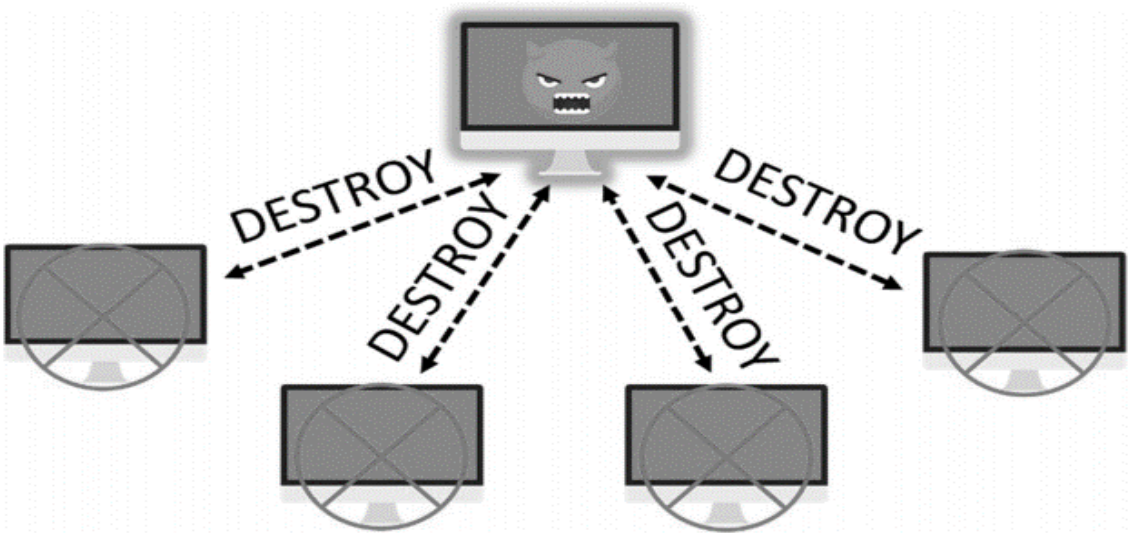

Рисунок 5 – CellFlood DoS attack

Если атакующий заинтересован в том, чтобы исключить узел или набор узлов из сети Tor, ему выгоднее использовать данный вид атаки, нежели чем обычную и более требовательную по ресурсам классическую DDoS-атаку.

В течение нескольких лет этой уязвимостью активно пользуются злоумышленники. Сначала о подобного рода типе атак сообщали легитимные сайты даркнета (анонимная сеть не связанных между собой виртуальных туннелей, предоставляющая передачу данных в зашифрованном виде [2]), но в последнее время уязвимость используется преимущественно для атак на подпольные торговые площадки. В марте 2019 г. администрация одного из крупнейших черных рынков даркнета Dream Market объявила о его закрытии после серии мощных DDoS - атак. Через месяц после закрытия Dream Market DDoS-атакам подверглись другие крупные торговые площадки, в том числе Empire Market и Nightmare Market. Постоянные DDoS - атаки вынуждают операторов onion сайтов переходить с Tor на I2P. Действительно DDoS в обоих

случаях. В заключении хотим рассказать о достоинствах и недостатках Tor браузера.

Подводя итоги хотелось бы рассмотреть достоинства и недостатки Tor – браузера. Среди достоинств самым главным и важным является анонимизация трафика путем сокрытия вашего IP-адреса. Следует также выделить возможность открыть любой закрытый сайт, не зависимо от интернета - провайдера. Кроме того, Tor – бесплатный и прост в эксплуатации, поэтому любой пользователь может его установить.

На ряду с достоинствами есть и ряд недостатков, к которым относятся следующие:

1. Интернет-провайдер узнает, что вы используете TOR, так как список входных узлов находится в открытом доступе.

2. Сайт должен быть доступен в интернете. То есть анонимен только клиент, но не сервер.

3. Не спасает от атаки через плагины и XSS.

4. Многие Интернет-сервисы будут открываться медленнее или не открываться вообще, так как другой IP-адрес может быть заблокированным или находиться в черном списке.

5. Относительно медленный для работы в интернете.

На сегодняшний день, Tor и любые другие анонимайзеры не дают гарантии того, что пользователя не смогут идентифицировать. Помимо идентификации по IP-адресам существует множество других способов деанонимизации. Рассмотренные процессы требуют больших вычислительных мощностей. Поэтому проведение вышеперечисленных типов атак возможно только государственными организациями или частными компаниями, обладающими соответствующим вычислительным потенциалом.

Библиографический список:

1. Tor // https://ru.wikipedia.org – свободная энциклопедия [Электронный ресурс]. - https://ru.wikipedia.org/wiki/Tor – (дата обращения: 09.10.2020).

2. Авдошин С. М. Технология анонимных сетей / С. М. Авдошин, А. В. Лазаренко // Информационные технологии. – 2016. – Т. 22, № 4. – С. 284–291.

3. Что такое HTTP, FTP, POP3, SMTP и telnet? // www.shkolazhizni.ru – познавательный журнал. [Электронный ресурс]. - https://shkolazhizni.ru/computers/articles/7670/ – (дата обращения: 09.10.2020).

4. Локальные мосты - предшественники коммутаторов // http://citforum.ru – электронная библиотека [Электронный ресурс]. - http://citforum.ru/nets/lsok/glava_3 – (дата обращения: 09.10.2020).

5. Arp D. Torben: A practical side-channel attack for deanonymizing Tor communication / D. Arp, F. Yamaguchi, K. Rieck // Proc. 10th ACM Symp. Inf. Comput. Commun. Security (ASIA CCS). – 2015. – P. 597–602.

6. Hornet. – Режим доступа: https://hornet.com/, свободный. – Заглавие с экрана. – Яз. англ. – (дата обращения: 09.10.2020).