Фурер О.В., Якупов Д.О. Луковая маршрутизация в браузере «TOR» //
Международный журнал информационных технологий и энергоэффективности.
– 2024. –
Т. 9 № 3(41) с. 16–21

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 004.4

ЛУКОВАЯ МАРШРУТИЗАЦИЯ В БРАУЗЕРЕ «TOR»

Фурер О.В., **[1]Якупов Д.О.**
ФГБОУ ВО "ПОВОЛЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ И ИНФОРМАТИКИ», Самара, Россия (443010, Самарская область, город Самара, ул. Льва Толстого, д.23), e-mail: [1]d.yakupov@psuti.ru

Научная статья рассматривает технологию луковой маршрутизации, применяемую в TOR браузере для анонимизации user-сессии и обхода интернет-цензуры. Благодаря этой системе веб-трафик проходит через несколько маршрутизаторов, которые шифруют и расшифровывают передаваемую информацию на различных этапах, делая невозможным отслеживание источника, IP-адреса назначения и содержания переданных данных. Статья также освещает активные меры по предотвращению использования TOR браузера, включая запрет на его скачивание и распространение, блокировку встроенных в браузер адресов и VPN-сервисов, а также ограничение доступа к определенной доменной зоне. Акцентируется внимание на методах деанонизации пользователей TOR браузера, из которых наиболее эффективным для массового сбора информации является активная система сбора данных или так называемый фингерпринтинг. В завершение делается вывод о возможной уязвимости TOR браузера перед методами деанонимизации, отражающим неспособность пользователей полностью скрыть свои действия в интернете. Луковая маршрутизация является технологией защищенного обмена блоками данных, сохраняющей анонимность пользователя, через компьютерные сети. Сообщения зашифровываются и передаются через несколько сетевых узлов, которые называются луковыми маршрутизаторами. На каждом этапе расшифровывания сетевой узел удаляет слой шифрования полученных данных, чтобы получить трассировочные инструкции и отправить информацию на следующий сетевой узел. Таким образом, промежуточные узлы не знают источник, IP-адрес назначения и содержание переданных данных.

Ключевые слова: Луковая маршрутизация, TOR браузер, анонимизация, цензура в интернете, блокировка TOR, деанонимизация пользователей, фингерпринтинг.

ONION ROUTING IN THE TOR BROWSER

Furer O.V. **[1]Yakupov D.O.**
VOLGA REGION STATE UNIVERSITY OF TELECOMMUNICATIONS AND INFORMATICS, Samara, Russia (443010, Samara, Leo Tolstoy St., 23), e-mail: [1]d.yakupov@psuti.ru

The research paper explores the onion routing technology used in the TOR browser for user session anonymization and circumvention of Internet censorship. This system allows web traffic to pass through several routers that encrypt and decrypt the transmitted information at various stages, rendering it impossible to track the source, destination IP address, and content of the transmitted data. The article also covers active measures to prevent the use of the TOR browser, including a ban on its download and distribution, blocking addresses built into the browser and VPN services, and restricting access to a specific domain zone. Focus is made on methods of de-anonymizing TOR browser users, with the most effective way of mass information collection being an active data collection system or so-called fingerprinting. In conclusion, the paper theorizes on the potential vulnerability of the TOR browser to de-anonymization methods, reflecting users' inability to fully conceal their online activities. Onion routing is a secure data block exchange technology that preserves user anonymity via computer networks. Messages are encrypted and passed through several network nodes, known as 'onion routers'. At each decryption

stage, the network node removes a layer of encryption from the received data to obtain trace instructions and forward the information to the next network node. Hence, intermediate nodes do not know the source, destination IP address, and content of the transmitted data.

Keywords: Onion routing, TOR browser, anonymization, internet censorship, TOR blocking, user de-anonymization, fingerprinting.

Введение

«Tor» или The Onion Router – это веб-браузер, который анонимизирует веб-трафик с помощью луковой маршрутизации, позволяя пользователю легко защитить личность в сети Интернет. Tor-браузер является самым популярным методом обхода цензуры после VPN-сервисов. Он дает возможность каждому пользователю заходить на заблокированные и запрещенные во многих странах сайты за счёт использования распределённой сети серверов. Этот функционал отсутствует у популярных веб-браузеров, таких как Google Chrome, Microsoft Edge и Opera. Такое «преимущество» делает веб-браузер Tor незаконным в некоторых странах. В списках методов и технологий обхода цензуры в интернете значительную роль играет Tor-браузер. Рассмотрим несколько вариантов блокировки Tor-браузера [1].

Принципы работы Tor-браузера

Запрет на скачивание и распространение Tor-браузера. Активная блокировка доступа к сайтам для скачивания программы-установщика и разработка поддельных «сайтов зеркал» для скачивания веб-браузера TOR, и распространения версии веб-браузера без функции анонимизации веб-трафика.

Запрет адресов, вшитых в браузер. Для первого выхода в интернет Tor- браузеру необходимы специальные bridge-relay, которые указаны в настройках браузера, заблокировав их, использование Tor-браузера будет заблокировано (Рисунок 1).

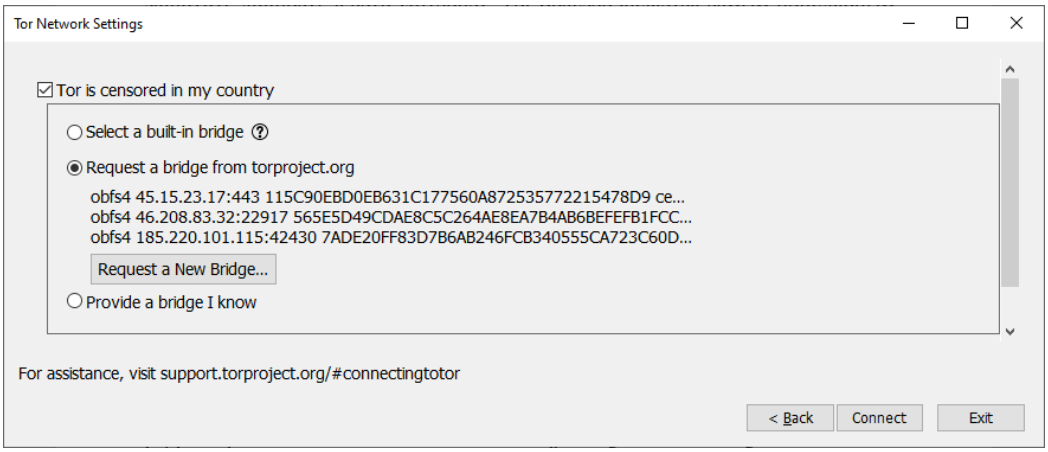

Рисунок 1 – Запрос моста для соединения

Запрет VPN (Virtual Private Network). Существует множество VPN-технологий, позволяющих шифровать трафик и полностью анонизировать прибывание в сети Интернет с отвязкой от регионального расположения. Блокирование назначенных узлов, портов и IP-адресов, выходных серверов устранит возможность VPN-доступа к сети для пользователя.

Блокирование входных узлов. У веб-браузера TOR есть 2 типа узлов: публичные и непубличные, имеющие свой IP-адрес. Большинство пользователей браузера используют публичные узлы для доступа в сеть Интернет. Так как IP-адреса публичных узлов находятся в

общем доступе, можно ограничить большинству пользователей доступ к браузеру, заблокировав IP-адреса узлов.

Блокировка в псевдо-доменной зоне «.onion». Псевдо-домен «.onion» верхнего уровня, схожий по функционалу с доменами «.bitnet» и «.uucp», которые использовались ранее, разработанный для обеспечения доступа к анонимным или псевдо-анонимным адресам сети Tor.

Данный адрес не является полноценными записями DNS, а также их информация не хранится в корневых серверах DNS-северов, но при установке дополнительного программного обеспечения, программы, подобные браузерам, получают доступ к сайтам в доменной зоне .onion, посылая запрос через сеть Tor-серверов. Отправка IP-адреса сайтов в псевдо-доменной зоне .onion в черный список и закрытие доступа является эффективным способом борьбы с луковой маршрутизацией [2].

Блокировка публичных IP-адресов Tor. Существует большое количество сайтов, которые пользуются технологией SSL-сертификатов. Если пользователь неправильно настроил скрытую службу (hidden service) — она будет уязвима для вычисления публичного IP-адреса.

*Атака «DefecTor»***.** Основной целью данной атаки являются DNS-запросы. Данный метод работает паре с корреляционной атакой, выполняя мониторинг маршрута делегирования для FQDN («Fully Qualified Domain Name»), а затем использовать «traceroute» для всех DNS-серверов (Рисунок 2).

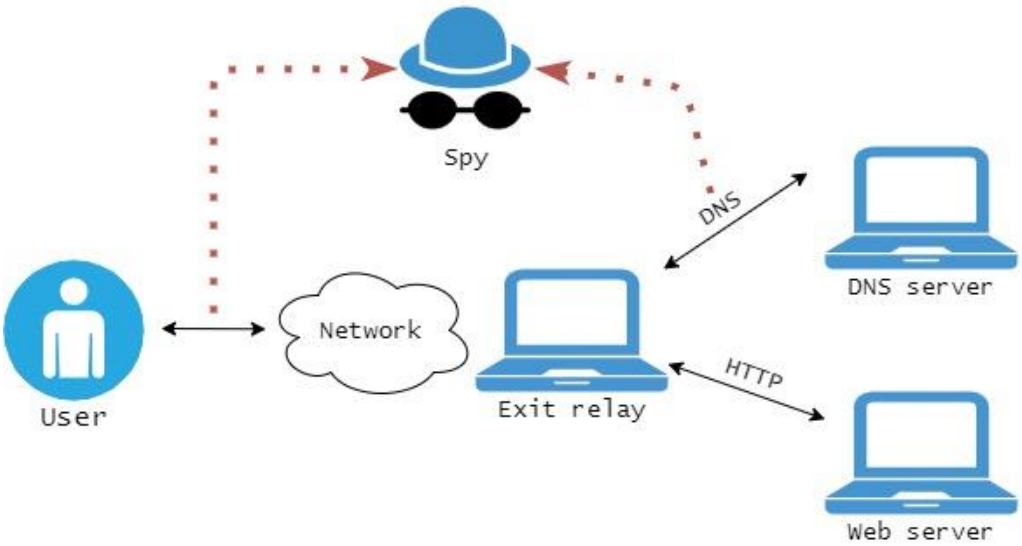

Рисунок 2 – Схема работы «DefecTor».

Атаки на клиентскую часть. У атаки на канал связи между Tor-клиентом и сервером есть возможность анализировать NetFlow-записи на роутерах, которые являются узлами Tor. В NetFlow-записи содержится информация, которая частично деанонимизирует пользователя:

- порт и адрес источника;
- номер протокола, инкапсулируемого в IP;
- значение ToS;
- номер версии протокола;
- номер записи;
- сетевой интерфейс;

- время потока;
- количество блоков данных в потоке;
- IP- адрес default gateway;
- маски подсети.

*Атаки на соединение***.** Атаки на выходные узлы Tor, которые служат последним элементом в расшифровке трафика и являются конечной точкой трафика, которая может стать каналом для утечки информации

Создание сконфигурированной exit-ноды, которая сможет собрать существующие и важные onion-ресурсы.

Для того чтобы создать историю недавно посещенных onion-ресурсов, данный узел перехватывает пакеты HTTP/HTTPS-протоколов пользователя, которые обеспечивают конфиденциальность обмена информации между сайтом и компьютером пользователя. Безопасность данных создается благодаря использованию криптографических протоколов SSL/TLS, имеющих 3 уровня защиты [3]:

1. Шифрование информации для защиты от перехвата.
2. Фиксирование изменения информации.
3. Проверка подлинности информации.

После фильтрации HTTP-пакетов они могут содержать информацию о посещенных ранее сайтах и других действиях пользователя. Однако данная система «сниффинга» не позволяет провести полную деанонимизацию Tor-пользователя, потому что атакующий получает не достаточно данных. Чтобы полностью деанонимизировать Tor-пользователя необходимо подтолкнуть его отдать какие-либо данные, которые смогут деанонизировать его.

*MITM-атака***.** Внедрение в веб-страницы JavaScript-кода и сбор уникальных фингерпринтов посетителей сайта с помощью уязвимостей в XSS и поднятия doorway (Рисунок 3).

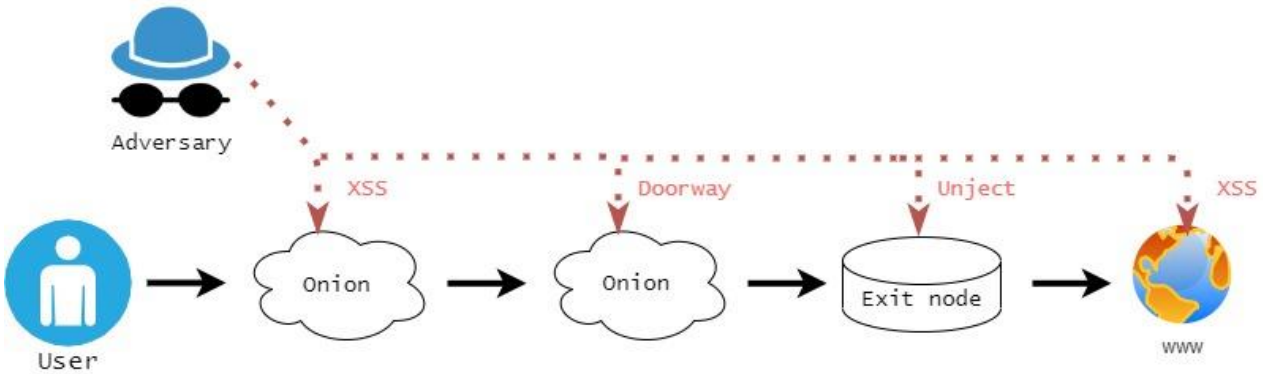

Рисунок 3 – Схема работы MITM-атаки.

Активная система сбора данных. Фингерпринтинг Tor-пользователя или и CBF (Cross-Browser Fingerprinting), то есть кросс-браузерный фингерпринтинг. Данная система считывает характеристики компьютера пользователя, которые проявляют себя независимо от версии браузера при рендеринге и обработке графики. Система замеряет время выполнения графических и системных операций и использует собранную информацию для создания профиля ПК. Информация по которой можно собрать данные о пользователе [4-5]:

Для Tor-браузера:

- разрешение экрана;
- AudioContext;
- список шрифтов.

Для популярных браузеров без «луковой маршрутизации»:

- количество ядер процессора;
- линии, кривые и антиалиасинг;
- Vertex Shader;
- прозрачность в альфа-канале;
- установленные письменности;
- моделирование;
- освещение и построение теней;
- отсечение плоскостей.

Все данные в сочетании позволяют скомпоновать профиль конкретного компьютера. В примере перечислены надежность и энтропия кросс-браузерного метода, которую обеспечивает каждый метод для Tor-браузера (Таблица 1).

Таблица 1 – Сравнительный анализ Single-Browser и Cross-Browser

	Single-Browser	Cross-Browser	
Информация	энтропия	энтропия	надёжность
Разрешение экрана	1.40	0.98	97.57%
AudioContext	1.87	1.02	97.48%
Список шрифтов	10.40	6.58	96.52%

Вывод

Таким образом, рассмотрев наиболее популярные методы деанонизации для луковых сетей, самым эффективным для массового сбора информации о пользователях является активная система сбора данных, которая составляет цифровой отпечаток на основе информации ЭВМ. Полученные результаты показали энтропию 10.40 для списка шрифтов в режиме Single-Browser и 6.58 в режиме Cross-Browser , что является уязвимостью и в совокупности с другой собранной информацией о ЭВМ дает возможность раскрыть личность пользователя. Можно заключить, что с помощью методов деанонизации Tor-браузера пользователи лишаются возможности полностью скрыть свои действия в сети интернет.

Список литературы

1. Как работает Tor и луковая маршрутизация, Dr.Web" [Электронный ресурс]. – Режим доступа: drweb.ru/pravda/issue/number=1237
2. Что такое луковая маршрутизация? База знаний DDoS-Guard [Электронный ресурс]. – Режим доступа: ddos-guard.net/ru/terms/technologies/onion-routing
3. Tor и VPN: что безопаснее и надежнее в 2024 году? [Электронный ресурс]. – Режим доступа: ru.vpnmentor.com/blog/tor-%D0%B8-vpn-%D1

4. Tor Browser, Dark Web, & Function Britannica [Электронный ресурс]. – Режим доступа: britannica.com/technology/Tor-encryption-network
5. Как работает Tor/Хабр–Habr[Электронный ресурс].–Режим доступа: habr.com/ru/articles/357128

References

1. How Tor and onion routing works, Dr.Web" [Electronic resource]. – Access mode: drweb.ru/pravda/issue/number=1237
2. What is onion routing? DDoS-Guard knowledge base [Electronic resource]. – Access mode: ddos-guard.net/ru/terms/technologies/onion-routing
3. Tor and VPN: what is safer and more reliable in 2024? [electronic resource]. – Access mode: ru.vpnmentor.com/blog/tor-%D0%B8-vpn-%D1
4. Tor Browser, Dark Web, & Function Britannica [Electronic resource]. – Access mode: britannica.com/technology/Tor-encryption-network
5. How Tor/Habr–Habr works [Electronic resource]. – Access mode: habr.com/ru/articles/357128