УДК 502.3:504.5-03
МРНТИ 87.17.09

АНОНИМИЗАЦИЯ И ДЕАНОНИМИЗАЦИЯ. «КИБЕРТЕНЬ» В ИНТЕРНЕТЕ

А.И. МАСАЛОВИЧ[1], С.Т. АМАНЖОЛОВА[1], Е.Л. ШЕВЧЕНКО[2], С.А. САМБУРСКАЯ[2]

[1]ООО «Лавина Пульс», Москва, Российская Федерация
[2]Международный университет информационных технологий

Аннотация: *В 1990-х годах, когда началось активное развитие Всемирной сети-Интернет, популярность анонимайзеров не достигала такого пика, как это происходит сегодня. Причиной резкого роста востребованности средств обеспечения анонимности являются многочисленные скандалы, связанные с нарушением секретности персональных данных пользователя: изменение политики конфиденциальности Telegram, согласно которой компания теперь может раскрывать иностранным правительственным спецслужбам персональные данные пользователей, подозреваемых в терроризме; участие Facebook в сборе данных 50 миллионов американцев компанией Cambridge Analytica; тотальная слежка американских спецслужб за информационными коммуникациями между гражданами многих государств по всему миру, при помощи существующих информационных сетей связи, раскрытая Эдвардом Сноуденом. Эти и многие другие громкие скандалы о нарушении конфиденциальности пользователей Всемирной сети привели к тому, что начали создаваться различные способы анонимизации в Интернете. На сегодняшний день наиболее популярными представителями анонимайзеров считаются Tor, VPN и прокси-серверы. Существует распространенное мнение, что эти методы способны обеспечить полную анонимность пользователя сети. Но так ли это? Возможна ли вообще полная анонимность в Интернете? Чтобы ответить на эти актуальные на сегодняшний день вопросы, нужно четко понимать, что из себя представляют анонимизация и деанонимизация, а также деление их на виды. В случае анонимизации, мы рассмотрим виды анонимайзеров, алгоритмы их работы, а также плюсы и минусы каждого из них. При рассмотрении деанонимизаии, мы изучим разделение ее на две категории, затем заострим внимание на самых распространенных методах совершения кибератак.*

Ключевые слова: *анонимность, анонимизация, деанонимизация, анонимайзеры, Интернет, прокси-сервер, VPN, Tor*

ANONIMIZATION AND DEANONIMIZATION. “CYBERTH” ON THE INTERNET

Abstract: *In the 1990s, when the active development of the World Wide Web began, the popularity of anonymizers did not reach such a peak as it is today. The reason for the sharp increase in the demand for anonymity tools is the numerous scandals related to the violation of the privacy of personal user data: changing the privacy policy of Telegram messenger, according to which the company can now disclose the personal data of users suspected of terrorism to foreign government intelligence agencies; Facebook's participation in Cambridge Analytica's data collection for 50 million Americans; total surveillance of US intelligence services for information communications between citizens of many countries around the world, using existing information networks, disclosed by Edward Snowden. These and many other high-profile scandals about the violation of the privacy of users of the World Wide Web have led to the fact that they began to create various ways to anonymize the Internet. Today, Tor, VPN and proxy servers are considered the most popular representatives. There is a widespread belief that these methods are capable of ensuring the complete anonymity of the network user. But is it? Is it possible at all complete anonymity on the Internet? To answer these questions that are relevant today, you need to clearly understand what anonymization and de-anonymization are, as well as their division into species. In the case of anonymization, we consider the types of anonymizers, the algorithms of their work, as well as the pros and cons of each of them. When considering deanonimization, we will study its division into two categories, then we will focus on the most common methods of committing cyber-attacks.*

Keywords: *anonymity, anonymization, de-anonymization, anonymizers, Internet, proxy server, VPN, Tor*

АНОНИМИЗАЦИЯ ЖӘНЕ ДЕАНОНИМИЗАЦИЯ . ИНТЕРНЕТКЕ КӨМЕК КӨРІНІСІ

Аңдатпа: *Анонимизация жағдайында біз анонимизаторлардың түрлерін, олардың жұмыс алгоритмдерін, сондай-ақ олардың әрқайсысының артықшылығы мен кемшіліктерін қарастырамыз. Деканонизацияны қараған кезде, біз оның бөлінуін екі санатқа бөлеміз, содан кейін кибершабуылдың ең кең таралған әдістеріне назар аударамыз. 1990-шы жылдарда, Бүкіләлемдік желінің белсенді дамуы басталған кезде, анонимизаторлардың танымалдылығы бүгінгідей осындай шыңға жете алмады. Анонимдік құралдарға сұраныстың күрт артуының себебі – жеке пайдаланушының деректерінің құпиялылығын бұзумен байланысты көптеген дау-дамайлар: Telegram құпиялылық саясатын өзгертеді, оған сәйкес компания қазіргі уақытта терроризмге күдіктенген қолданушылардың жеке деректерін шетелдік үкіметтік жедел уәкілетті органдарға жария ете алады; 50 миллион американдықтар үшін Cambridge Analytica компаниясының деректер жинауына Facebook қатысуы; Эдвард Сноуден жарияланған қолданыстағы ақпараттық желілерді пайдалана отырып, бүкіл әлемдегі көптеген елдердің азаматтары арасындағы ақпараттық коммуникациялар үшін АҚШ-тың барлау қызметтерінің жалпы қадағалауы. Осы және көптеген басқа да жоғары дәрежелі дау-шарлар Дүниежүзілік Ғаламтор желісін пайдаланушылардың жеке өміріне қол сұғушылықты бұзу туралы ғаламтор желісін анонимді түрде әртүрлі жолдармен жасай бастады. Бүгінгі таңда Tor, VPN және прокси серверлер ең танымал өкілдер болып саналады. Бұл әдістер желі қолданушысының толық анонимділігін қамтамасыз етуге қабілетті екендігі туралы кеңінен таралған пікір бар. Бірақ бұл ғаламторда толық жасырын болуы мүмкін бе? Бүгінгі сұраққа жауап беру үшін сіз анонимизация мен деанонимизацияның қандай екенін, сондай-ақ олардың түрлерге бөлінуін терең түсінуіңіз керек.*

Түйінді сөздер: *анонимдік, анонимизация, анонимизаторлар, интернет, прокси-сервер, VPN, Tor*

Список сокращений

API - application programming interface
CGI - computer-generated imagery
HTTP - Hyper Text Transfer Protocol
HTTPS - Hyper Text Transfer Protocol Secure
I2P - invisible internet project
IP - Internet Protocol
L2TP - Layer 2 Tunneling Protocol
MAC - Media Access Control
OSI - open systems interconnection
PPTP - Point-to-Point Tunneling Protocol
SOCKS - SOCKet Secure
TOR - The Onion Router
VPN - VirtualPrivateNetwork
ПО - программное обеспечение

Введение. Любая деятельность в Интернете фиксируется, так или иначе. Поиск информации, отправка электронных писем, посещение сайтов, онлайн-покупки и активность в социальных сетях - все это оставляет определенные цифровые следы или, как их еще называют, – «кибертень». Данный след дает возможность уникализироватьпользователя. Это является угрозой персональным данным, так как открытая деятельность в Интернете может быть опасной не только для правонарушителей, которые рискуют быть обнаруженными, но и для обычных пользователей, из-за возможности стать жертвой хакерской атаки. Также не стоит забывать о крупных скандалах, связанных с PRISM – программой слежения за пользователями, принятой на вооружение Агентством национальной безопасности США, обнародованной Эдвардом Сноуденом. Возникает серьезный вопрос, стоит ли чувствовать себя в безопасности всякий раз, когда вы заходите во Всемирную сеть? Ведь на сотрудничество со спецслужбами пошли многие крупные компании: Microsoft (Hotmail), Google (GoogleMail), Yahoo, Facebook, YouTube, Skype, Apple. Однако, есть определенные инструменты, посредством которых можно сильно усложнить процесс сбора информации о Вас из Интернета, делая его нерентабельным для хакеров и прочих «собирателей» конфиденциальных сведений.

Анонимизация. *Понятие анонимизации.* Анонимизацией в Интернете считаются различные способы остаться незамеченными во Всемирной сети. Понятие такой анонимности возникло в конце 1980-х годов. Сначала для ее достижения использовались весьма поверхностные методы, такие как псевдонимы. Позже, в 90-х годах XX века, с развитием Всемирной паутины, наступил новый этап технологического прогресса. Тогда же начали появляться и различные методы анонимизации. На сегодняшний день мы можем разделить анонимность в Интернете на два направления:

- «Социальная анонимность» – это то, что человек сам осознанно или неосознанно рассказывает о себе в Сети.
- «Техническая анонимность» – обеспечение анонимности с использованием технических средств и приложений.

Цели анонимизации. Перед тем, как предпринимать какие-либо попытки анонимизировать свою деятельность в сети, следует четко определить, зачем нужна скрытностьи от кого следует защищать конфиденциальные данные. Причины скрывать свою деятельность в Интернете очень разнообразны. Они могут быть связаны не только с целью защититься от возможных противоправных действий со стороны третьих лиц, но и с совершением их самим лицом, стремящимся к анонимности.И так, зачем же нужнаанонимизация в Интернете? Все, что передается в незашифрованном виде, может быть перехвачено и изменено. А провайдер может с легкостью идентифицировать запрос с точностью до мак-адреса и клиентского договора. Если вы пользуетесь Gmail для чтения рабочей или личной почты или используете браузер Chrome, то корпорации Google будет доступна информация об активностипользователя. Российские сервисы поступают аналогично.Поэтому и возникает необходимость в анонимизации.

Способы анонимизации. Для обеспечения анонимности в Интернете применяются различные сети, работающие поверх глобальной сети. Для того, чтобы достигнуть более высокого уровня анонимности, используются анонимайзеры. Они представляют из себя технические средства для сокрытия информации об Интернет-пользователе и его действиях в Сети. На сегодняшний день существует множество анонимайзеров, которые помогут сохранить конфиденциальность в Интернете. Самыми популярными и часто используемыми являютсяследующие:

- Прокси-сервер
- VPN
- Браузер Tor
- I2P

Рассмотрим подробнее каждый из них.

*Прокси-серверы.*Обычно, под прокси-сервером подразумевают сервер, выступающий посредником между клиентом и адресатом. В плане обеспечения анонимности прокси-серверы делятся на несколько видов:

- HTTP-прокси-серверы пропускают через себя только HTTP-траффик, по умолчанию добавляя в передаваемые данные информацию о применении прокси;
- SOCKS-прокси-серверы, в отличие от HTTP-прокси-серверов, передают всю информацию, ничего не добавляя от себя. Протокол SOCKS находится на сеансовом уровне модели OSI, этим достигается независимость от высокоуровневых протоколов, что и позволяет SOCKS пропускать через себя весь траффик, а не только HTTP;
- CGI-прокси представляет собой web-сервер с формой, где клиент вводит адрес нужного сайта. После чего открывается страница запрошенного ресурса, но в адресной строке браузера виден адрес CGI-прокси. CGI-прокси, как и любой web-сервер может использовать https для защиты канала связи между собой и клиентом.

Схема работы прокси-сервера довольно простая:

Самым главным плюсом использования прокси-серверов является их доступность. В Интернете можно найти достаточно много бесплатных прокси. Основными минусами являются необходимо постоянно фильтровать трафик для HTTP-серверов, необходимость настраивать каждое новое приложение или устанавливать специальное программное обеспечение.

*VPN.*Говоря про приватность и анонимность в Сети, нельзя обойти стороной использование для этих целей VPN. VirtualPrivateNetwork (VPN) или «виртуаль-

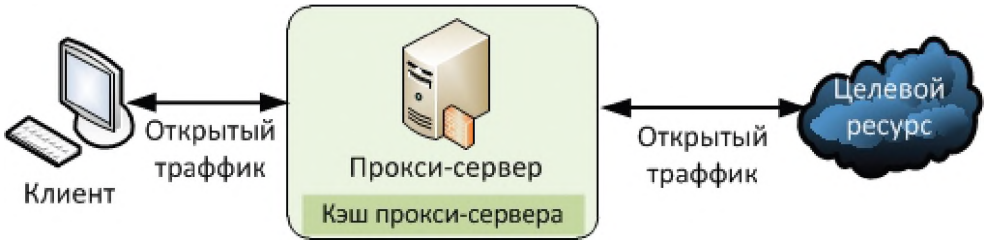


Рис. 1 – работа прокси-сервера

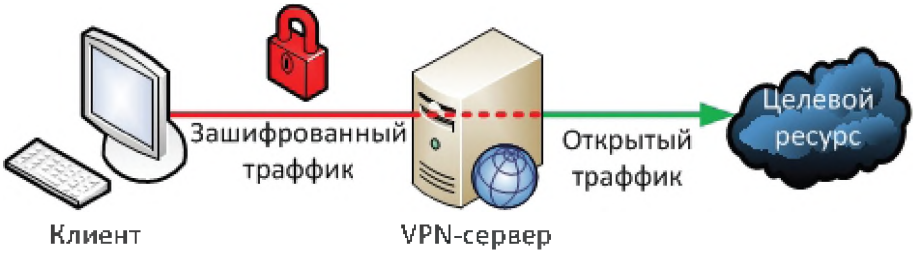


Рис. 2 – схема работы VPN

ная частная сеть» - это технология, посредством которой создают одно или более соединений поверх другой сети. При этом соединение между абонентом и VPN-сервером шифруется, благодаря чему создается максимально анонимный доступ в Интернет. И он будет таковым не только для веб-ресурсов, но и для провайдеров.

Наиболее распространенными являются следующие VPN-протоколы:

- OpenVPN - открытый, безопасный протокол, помогающий сохранить анонимность в сети, но требующий установки отдельного программного обеспечения(ПО);
- SSTP –по безопасности сопоставим с OpenVPN, но нет нужды устанавливать дополнительное ПО. Однако, есть ограничения в платформах;
- L2TP + IPSec. Данная связка обеспечивает повышенную анонимность данных, поскольку в ней два уровня защиты. Туннельный протокол L2TP позволяет оставаться анонимом при передаче трафика, а IPSec его шифрует;
- PPTP - безопасность в сравнении с остальными не на столь высоком уровне, но его легко установить и настроить.

Главные преимущества VPN в том, что он обеспечивает максимальную безопасность трафика и при этом не требует долгой и сложной настройки. Из минусов можно отметить низкую скорость соединения и дополнительную нагрузку на устройство.

*Браузер Tor.*TheOnionRouter (Tor) или луковичные маршрутизаторы - это браузер с открытым программным обеспечением, использующий послойную систему маршрутизаторов, с помощью которой между пользователем и веб-ресурсами устанавливаетсязашифрованное соединение. Как правило, эта система состоит из трех узлов, каждому из которых неизвестны адреса клиента и ресурса одновременно. Кроме того, Tor шифрует сообщения отдельно для каждого узла, а открытый трафик виден только выходному роутеру.

Среди плюсов Браузера Tor можно отметить высокую степень анонимности и простоту использования. Минусами являются низкая скорость, наличие управляющих серверов и отсутствие шифрования на выходном трафике.

*I2P.*Помимо «луковой маршрутизации», существует еще и «чесночная». I2P (invisibleinternetproject) — это анонимная сеть, работающая поверх Интернета. В ней есть свои сайты, форумы и другие сервисы, также нигде не используются ip-адреса. Работа I2P реализуется на «входящих» и «выхо-

дящих» туннелях, поэтому запросы и ответы идут через разные узлы. Каждые десять минут эти туннели перестраиваются. «Чесночная маршрутизация» подразумевает, что сообщение («чеснок») может содержать в себе множество «зубчиков» — полностью сформированных сообщений с информацией по их доставке. В один «чеснок» в момент его формирования может закладываться много «зубчиков», часть из них может быть нашими, а часть транзитными. Является ли тот или иной «зубчик» в «чесноке» нашим сообщением, или это чужое транзитное сообщение, которое проходит через нас, знает только тот, кто создал «чеснок». Основная задача I2P — анонимный хостинг сервисов, а не предоставление анонимного доступа в глобальную сеть, то есть размещение в сети веб-сайтов.

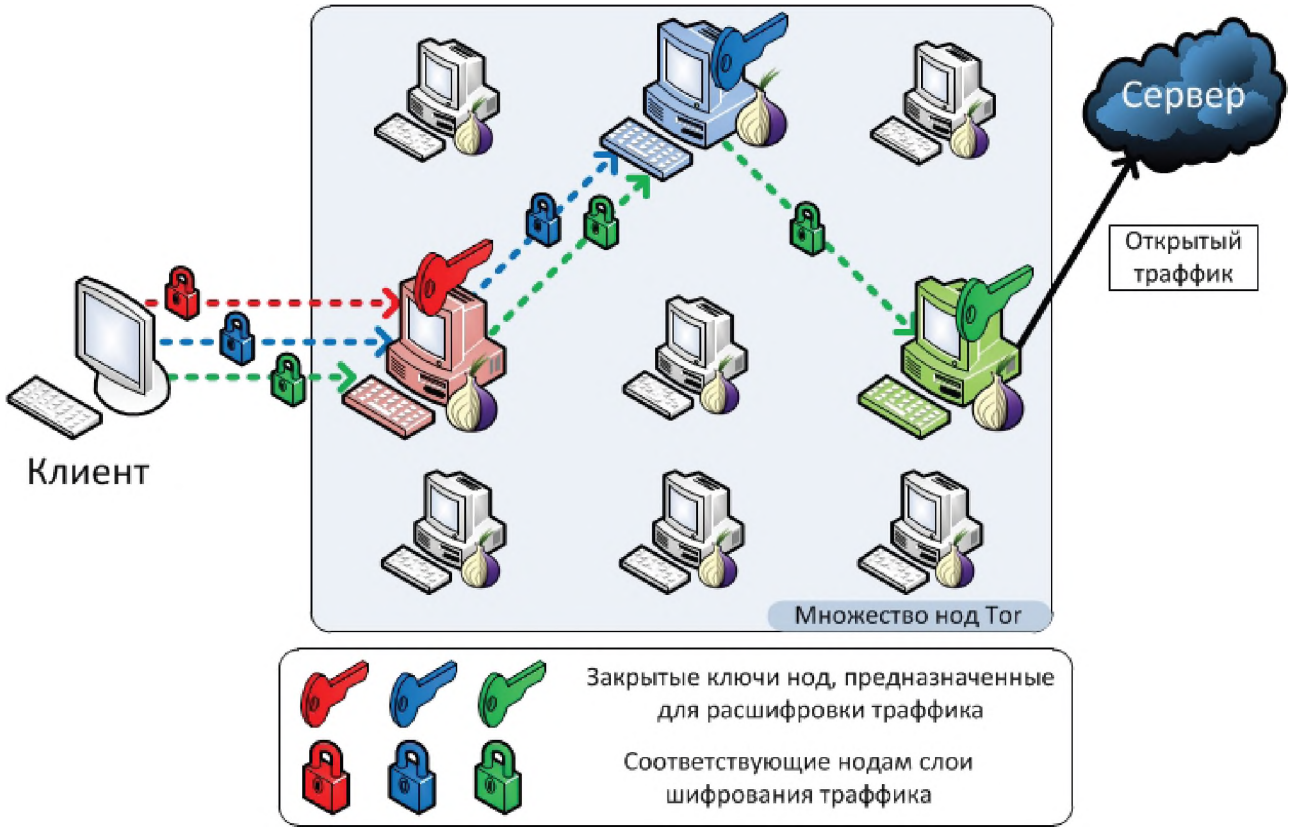


Рис. 3 – Схема работы Браузера Tor

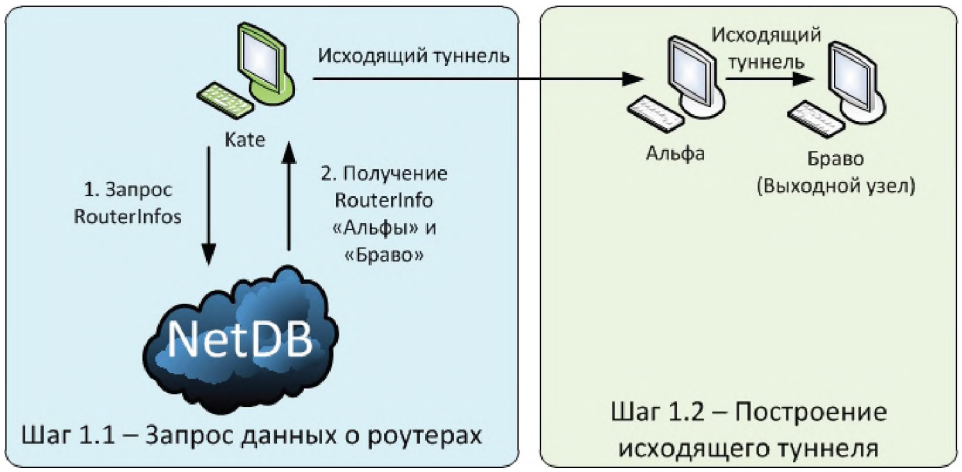


Рис. 4 – Схема работы I2P (шаг 1)

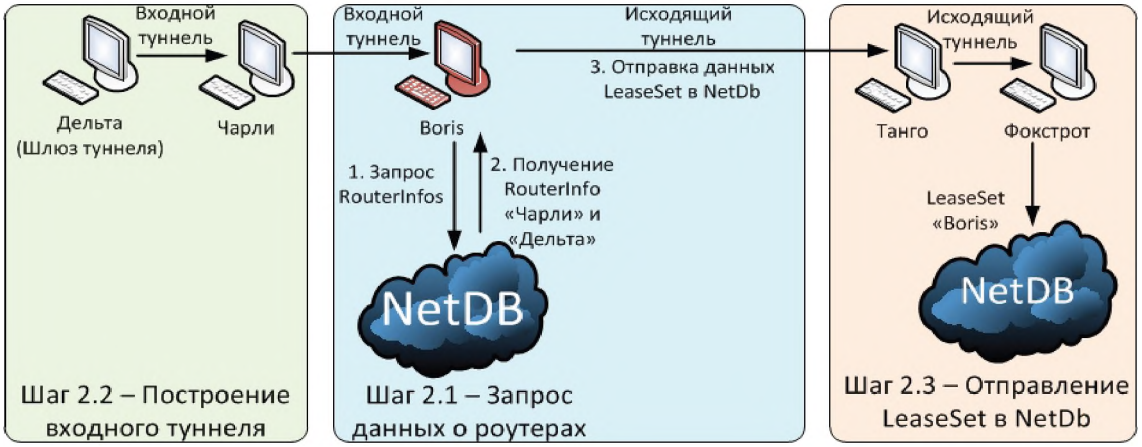


Рис. 5 – Схема работы I2P (шаг 2)

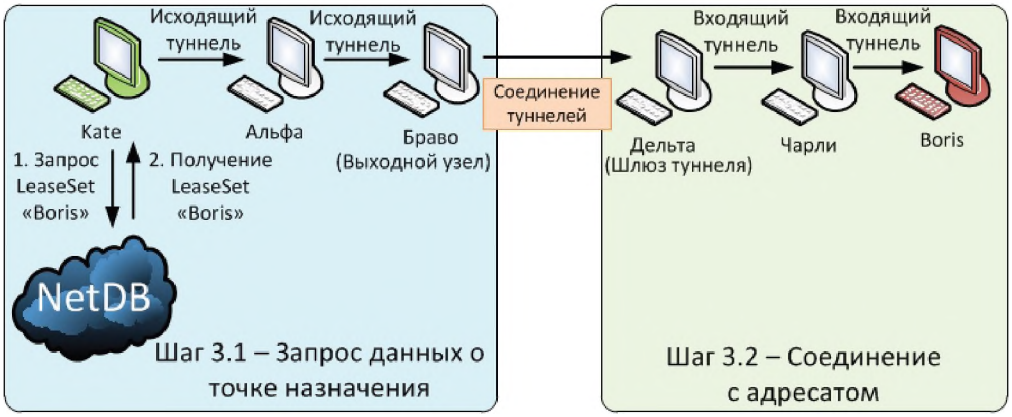


Рис. 6 – Схема работы I2P (шаг 3)

Плюсами I2P являются высокая степень анонимности, устойчивость сети, сквозное шифрование между клиентом и адресатом. В качестве минусов можно выделить низкую скорость и «свой Интернет».

*Деанонимизация. Понятие деанонимизации.*Несмотря на то, что многие считают, что VPN, Tor или прокси-серверы позволяют оставаться полностью анонимным в сети, в реальности существует около 10 различных способов вычисления реального IP-адреса пользователя, минуя эти средства защиты. Правоохранительные органы, спецслужбы и хакеры уже успешно применяют их в своей практике. Следствием таковых действий является деанонимизация – процесс установления личности пользователя в сети, либо подлинного места выхода в сеть.

Ключевым моментом вуспешнойдеанонимизации является уникализация - поиск и сбор уникальных идентификаторов браузера для формирования уникального отпечатка, по которому всегда можно будет узнавать данный браузер, независимо от IP-адреса. Все пользователи сети оставляют некие цифровые следы, которые включают в себя время нахождения в сети, cookies, информация о разрешении монитора, установленных в системе шрифтов, часового пояса, плагины, установленные в браузере. Именно по этим данным проводится уникализация браузеров пользователей, которая может быть использована для отслеживания и деанонимизации.

*Виды деанонимизации.*На основе методологии установления личности, можно выделить два вида деанонимизации: пассивную и активную. Оба вида активно применяются в реальности, поэтому стоит рассмотреть их подробнее.

Первый вид, пассивнаядеанонимизация, представляет собой установление личности

по IP-адресу imac-адресу. Здесь мы не наносим прямого вреда пользователю, так как выявление личности происходит без атак на него.

В случае активной деанонимизация, установление личности проходит посредством атаки на пользователя путем использования вредоносного ПО, эксплуатирования уязвимостей или социальной инженерии. Также иногда используется и комплекс различных атак.

Выбор вида деанонимизации зависит от ситуации, возможностей и умения атакующего и от самого анонима, так как причины для сокрытия личности бывают разными и усилия, затрачиваемые на анонимизацию, напрямую зависят от них. Поэтому стоит различать среднего пользователя, личность которого можно узнать с помощью провайдера, и реального киберпреступника, на деанонимизацию которого придется потратить больше времени и применить различные методы.

*Методы деанонимизации.*Чтобы подробнее рассмотреть методы деанонимизации, стоит их сначала разделить на два вида, описанных ранее.

К числу методов пассивнойдеанонимизации можно отнести:

- деанонимизация через сторонние сайты;
- деанонимизация с помощью сопоставления соединений;
- деанонимизация через cookies;
- деанонимизация с помощью уникального отпечатка;
- cross-device tracking;
- тайминг-атака.

Активнуюдеанонимизацию можно произвести с помощью таких методов, как:

- деанонимизация с использованием файлов-приманок;
- деанонимизация путем эксплуатации уязвимостей;
- добровольнаядеанонимизация путем использования социальной инженерии;

Далее мы рассмотрим каждый метод, начиная с методов пассивнойдеанонимизации.

*Деанонимизация через сторонние сайты.*К сожалению, довольно часто вероятность деанонимизации зависит именно от самого анонима, а точнее от его ошибки. А ошибки в этой области стоят довольно дорого, и деанонимизация через сторонние сайты является тому доказательством.

Допустим, что имеется только IP-адрес персонального VPN анонима, так как у него нет доверия к VPN сервисам, по отпечатку браузера его не отследить, потому что он использует разные браузеры для личных и рабочих целей. На первый взгляд, тупиковая ситуация. Но если аноним зайдет с рабочего VPN на страницу в социальных сетях, это позволит нам установить его личность. IP-адрес его VPN подвергается проверке наиспользование его для посещения социальных сетей и иных популярных сервисов, и если такая ошибка была допущена, ничего не стоит деанонимизировать его, так как обычно представители социальных сетей идут на контакт с правоохранительными органами.

*Деанонимизация с помощью сопоставления соединений.*Сопоставление соединений – это один из самых распространенных методов деанонимизации пользователей VPN и proxy, применяемых спецслужбами и правоохранительными органами.

Допустим, у нас снова есть только IP-адрес VPN анонима и дата выхода в Интернет с таким адресом. В случае, если мы находимся на месте правоохранительных органов, у нас есть система оперативно-розыскных мероприятий, которая сканирует трафик всех пользователей, также есть контакт с провайдерами, у которых по закону есть данные об активности пользователей. Хоть и записанный VPN-трафик зашифрован, мы можем узнать кто из жителей в интересующий промежуток времени устанавливал зашифрованное соединение с нужным VPN-сервером, например, в Австралии. Да, таких пользователей может оказаться несколько, но обычно не больше десяти. В дальнейшем для определения необходимого нам человека используются стандартные практики расследования.

*Деанонимизация через cookies.*Cookies - небольшой фрагмент данных, отправленный веб-сервером и хранимый на компьютере пользователя, обычно используется для аутентификации пользователя, хранения персональных предпочтений и настроек пользователя, отслеживания состояния сеанса доступа пользователя и ведения статистики о пользователях. Сейчас cookies это довольно обычная вещь на просторах Интернета и используется на многих сайтах.

Правоохранительныморганам нужно просто иметь контакт с администраторами подходящих сайтов, например, хакерских форумов в открытом Интернете. Далее можно настроить проверку cookies у всех неавторизованных пользователей, запись информацию об имеющихся у них на форуме аккаунтах и их текущие IP-адреса. В случае, если кто-то не воспользуется VPN вне своего аккаунта, его подлинный IP-адрес будет установлен, за чем последует деанонимизация.

*Деанонимизация с помощью уникального отпечатка.*При установке соединения с сайтом, он получает сведения о вашем браузере: например, язык браузера, разрешение, системное время (последнее часто используется для проверки наличия VPN или Proxy в случае несовпадения примерной локации и часового пояса), которые используются для улучшения качества работы с сайтом.

Далее уникализация пользователей сайтов происходит благодаря уникальным отпечаткам браузера, таким как Canvasfingerprint, WebGLfingerprint и др.

Canvas - это HTML5 API, который используется для графики и анимации на веб-странице с помощью JavaScript.

WebGL - это JavaScript API для рендеринга интерактивной 3D-графики в любом совместимом веб-браузере без использования плагинов.

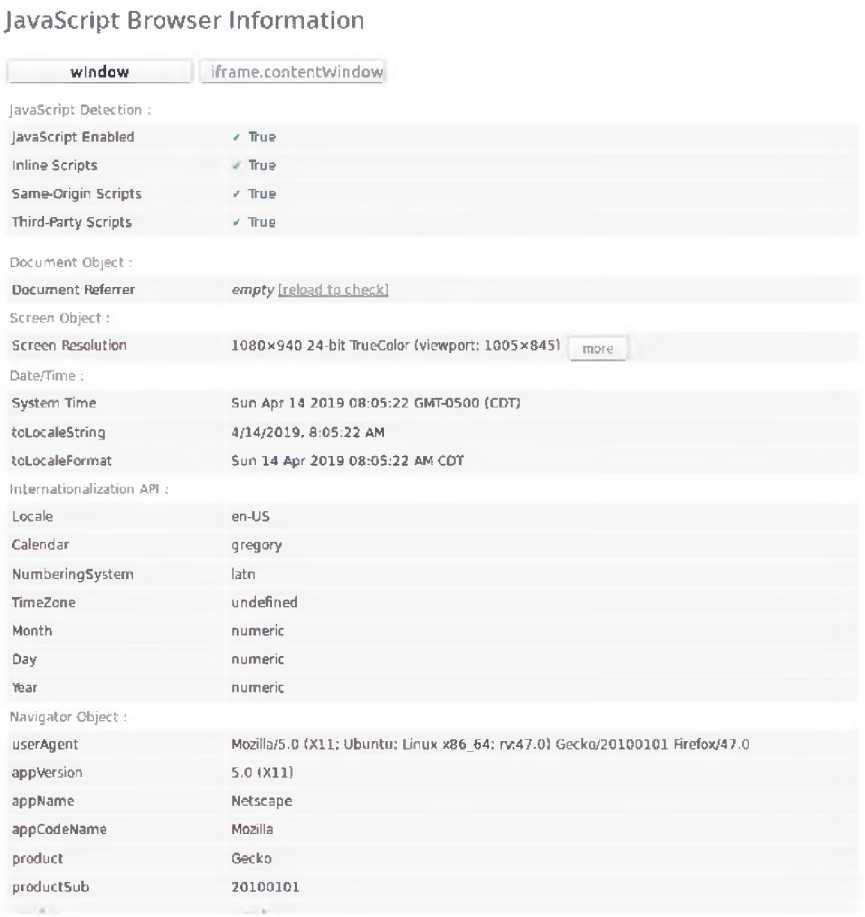
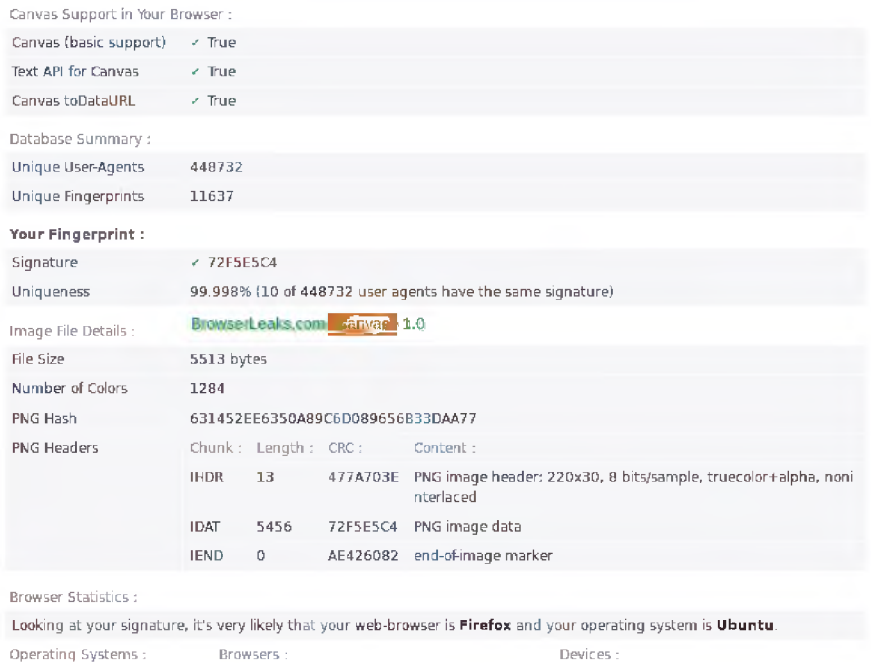


Рис. 7 – Информация о браузере с сайта https://browserleaks.com/javascript


Canvas Support in Your Browser :

Canvas (basic support)	✓ True
Text API for Canvas	✓ True
Canvas toDataURL	✓ True

Database Summary :

Unique User-Agents	448732
Unique Fingerprints	11637

Your Fingerprint :

Signature	✓ 72F5E5C4
Uniqueness	99.998% (10 of 448732 user agents have the same signature)

Image File Details : BrowserLeaks.com canvas 1.0

File Size	5513 bytes
Number of Colors	1284
PNG Hash	631452EE6350A89C6D089656B33DAA77

PNG Headers

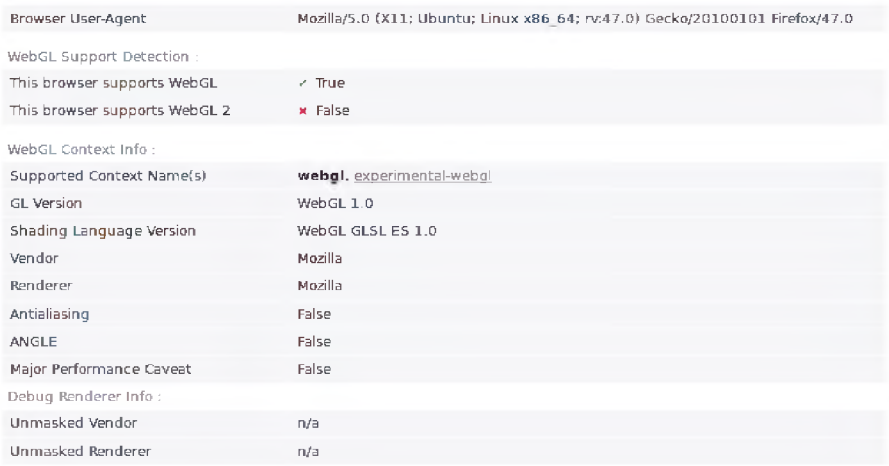
Chunk :	Length :	CRC :	Content :
IHDR	13	477A703E	PNG image header: 220x30, 8 bits/sample, truecolor+alpha, noninterlaced
IDAT	5456	72F5E5C4	PNG image data
IEND	0	AE426082	end-of-image marker

Browser Statistics :

Looking at your signature, it's very likely that your web-browser is **Firefox** and your operating system is **Ubuntu**.

Operating Systems : Browsers : Devices :

Рис. 8 – Отпечаток Canvas с сайта https://browserleaks.com/canvas


Browser User-Agent	Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:47.0) Gecko/20100101 Firefox/47.0

WebGL Support Detection :

This browser supports WebGL	✓ True
This browser supports WebGL 2	✖ False

WebGL Context Info :

Supported Context Name(s)	**webgl.** experimental-webgl
GL Version	WebGL 1.0
Shading Language Version	WebGL GLSL ES 1.0
Vendor	Mozilla
Renderer	Mozilla
Antialiasing	False
ANGLE	False
Major Performance Caveat	False

Debug Renderer Info :

Unmasked Vendor	n/a
Unmasked Renderer	n/a

Рис. 9 – Отпечаток WebGL с сайта https://browserleaks.com/webgl

Теперь, в случае, если злоумышленник будет использовать один браузер для работы и личных целей, можно будет обратиться к представителям социальных сетей, которые могут проверить наличие пользователей с такими же отпечатками, что приведет к деанонимизации.

Этот метод работает с пользователями VPN и Proxy, но не с пользователями TOR-браузера, так как его еще не удавалось уникализировать.

Cross-devicetracking. Cross-devicetracking – тип атак, представляющих возможность отслеживать пользователя с помощью несколько устройств, которая эффективно применяется при деанонимизациикиберпреступников, использующих для сокрытия подлинного IP-адреса Tor, VPN и proxy.

Этот вид деанонимизации мы отнесли к пассивной, так как машине пользователя не наносится вреда.

Для проведения этой атаки используется абсолютно безвредный сайт. При загрузке сайта активизируется звуковой маячок, который улавливают окружающие устройства. Даже если компьютер анонима хорошо защищен, нет полной уверенности, что другие окружающие его устройства имеют такой же уровень защиты, поэтому эта атака имеет довольно высокую вероятность успеха. Данные о получении сигнала будут незамедлительно переданы устройством на сервера какого-либо приложения, с которым сотрудничают правоохранительные органы или спецслужбы, вместе с координатами и IP-адресом.

Тайминг- атака. Такой метод идеально подходит для отслеживания пользователя кого-либо сервиса, с которым не удается сотрудничать.

Для осуществления такого метода необходима программа, которая фиксирует время входа и выхода, например, в мессенджер. Затем с помощью системы оперативно-розыскных мероприятий можно определить, кто имел доступ к сети TOR именно в это время. С каждой проверкой последующей временной точки, круг подозреваемых сужается. Дальше уже для определения необходимого нам человека используются стандартные практики расследования.

Теперь мы рассмотрим методы активной деанонимизации.

Деанонимизация с использованием файлов-приманок. Очень распространенный и эффективный метод активнойдеанонимизации, который может обойти даже Tor. Заключается в создании документа, который будет устанавливать соединением с сервером и отправлять IP-адрес. Он не будет рассмотрен как вредоносный файл, так как соединение с сервером – это не вредоносный функционал. Даже если файл будет открыт на виртуальной машине, в качестве песочницы, атака будет успешной, так как виртуальная машина по умолчанию не блокирует соединения, а анонимность Tor браузера распространяется только на сайты, открываемые в нем.

Единственная сложность может возникнуть в том, что для соединения с сервером необходимо открытие файла-приманки на компьютере жертвы, простое скачивание не приведет к результату. Но для этого можно воспользоваться социальной инженерией, с помощью которой можно убедить анонима в необходимости открытия файла.

Деанонимизация путем эксплуатации уязвимостей. Данный метод предполагает обнаружение уязвимости в одном из средств обеспечения анонимности.

Например, уязвимость CVE-2017-1663 заключается в том, что версии Tor браузера до 8.0 были подвержены уязвимости раскрытия информации, которая позволяла обойти функ-

Действие	Дата	Время
Вошел	22.04.2018	11:07
Вышел	22.04.2018	12:30
Вошел	22.04.2018	14:47
Вышел	22.04.2018	16:54
Вошел	22.04.2018	20:15
Вышел	22.04.2018	23:27
Вошел	23.04.2018	11:22
Вышел	23.04.2018	15:17

Рис. 10 – Таблица входов и выходов

```
Advisory ID:            SGMA18-002
Title:                  Tor Browser Deanonymization With SMB
Product:                Tor Browser < 8.0, Firefox < 62 / < 60.2.0esr
Vendor:                 torproject.org, mozilla.org
Type:                   Information Disclosure
Risk level:             4 / 5
Credits:                filippo.cavallarin@wearesegment.com
CVE:                    CVE-2017-16639
Vendor notification:    2017-11-02
Vendor fix:             2018-09-05
Public disclosure:      2018-09-12


Details

Tor Browser version < 8.0 and Firefox version < 62 / < 60.2.0esr are affected by an information
disclosure vulnerability that allows remote attackers to bypass the intended anonymity feature and
discover a client IP address. The vulnerability affects Windows users only and needs user interaction to
be exploited.
It's a different vulnerability than CVE-2017-16541 (even if it's similar in the concept and it comes
from the same author).

The vulnerability exists because the browser(s) fails to block UNC paths to be loaded in the address bar
leading to a connection to an arbitrary SMB server.
The Universal Naming Convention (UNC) is the naming system used in Microsoft Windows for accessing
shared network folders and printers. By accessing a UNC path it's possible to automatically mount a
network share and access its resources. For example "dir \\evil-attacker.com\share\file" will connect to
evil-attacker.com using SMB protocol and get access to shared file.
When a UNC path is typed or pasted into the address bar the operating system will immediately try to
connect to the specified server bypassing the configured proxy and revealing the true identity of the
user. Note that the connection is triggered as soon as the UNC path is pasted into the address bar
(without the need to hit the return key).
```

Рис. 11 – Описание уязвимости CVE-2017-1663

цию предполагаемой анонимности и обнаружить IP-адрес клиента. Уязвимость затрагивала пользователей Windows. Уязвимость была устранена в сентябре 2018 года, но есть вероятность появления новых уязвимостей, которые могут проэксплуатировать не только хакеры, но и спецслужбы.

Добровольная деанонимизация путем использования социальной инженерии. Для использования такого метода хакерами или спецслужбами обычно создается подделка какого-либо популярного сайта. Здесь также важно использовать сайт, на который с большей вероятностью зайдет аноним. Далее на сайте устанавливается проверка наличия средств анонимности, например, проверка провайдера или сравнение примерного расположения по IP-адресу с системным временем. В случае использования VPN или Proxy, сайт выдает ошибку,наподобие «Доступ запрещен. Этот веб-сайт не поддерживает соединение через прокси». В случае, если аноним отключит анонимайзер, произойдет его деанонимизация

Заключение

Несмотря на популярность и большое разнообразие существующих ныне анонимайзеров, обеспечить полную анонимность в сети не просто сложно, а невозможно. Любого пользователя можно деанонимизировать, успешность атаки будет зависеть от времени и возможностей атакующего. Подводя итоги статьи, можно выделить следующие пункты, необходимые для успешного обеспечения анонимности:

- использовать связку средств обеспечения анонимности, наиболее популярной является $User \rightarrow VPN \rightarrow Virtual \rightarrow Tor \rightarrow Proxy \rightarrow \rightarrow Internet$;
- контролировать деятельность в Интернете, во избежание ошибок, ведущих к деанонимизации.

Даже в случае соблюдения этих инструкций, обеспечить, а главное сохранить полную анонимность в Интернете не представляется возможным.

Ссылки

1. https://clck.ru/Fc9SL
2. https://book.cyberyozh.com/ru/
3. https://packetstormsecurity.com/files/149351/Tor-Browser-SMB-Deanonymization-Information-Disclosure.html
4. https://habr.com/ru/post/237335/#Anonim
5. https://habr.com/ru/post/190396/
6. https://vkoshelek.com/anonimnost-v-internete-10-sposobov/
7. https://xakep.ru/2014/09/24/anonimuos-tips/