Спецслужбы легко вычисляют реальные имена пользователей Tor

ФБР с легкостью провело успешную операцию и задержало студента Гарвардского университета Элдо Кима, который отправил сообщение о бомбе в здании университета. Заметьте, Tor не помог «минеру» и теперь шутнику грозит до 5 лет тюрьмы и штраф в 250 тысяч долларов.

Студент заминировал университет

20-летний студент признался, что написал письмо в надежде избежать итогового экзамена, для верности письмо с угрозой продублировал в адрес отдела безопасности университета и университетской газеты. Хотя здесь он добился успеха: из-за эвакуации все утренние экзамены были отложены, но теперь у парня появились более серьезные проблемы.

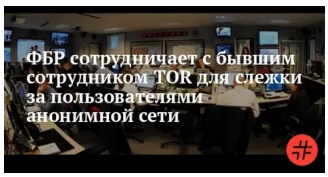
Tor не спасет от вычисления спецслужбами

Ким предпринял меры, чтобы избежать идентификации. Он завел анонимный адрес электронной почты и воспользовался сервисом для анонимизации Tor. Тем не менее, его все равно удалось вычислить. Судя по показаниям агентов ФБР в документах, поданных для суда, спецслужбаполучила список пользователей локальной компьютерной сети в общежитии университета. Они изучили трафик и определили, кто из студентов пользуется сервисом Tor. Как известно, трафик Tor можно определить по характерным признакам. Затем ФБР допросило всех пользователей анонимной сети одного за

другим. Таких оказалось не слишком много, поэтому вычислить преступника оказалось довольно просто.

Общественный Wi-Fi лучше Тора

Можно рассуждать, что студенту не повезло, что он отправлял сообщение со студенческого компьютера. Если бы он сделал это с публичного Wi-Fi, пропустив трафик через какую-нибудь постороннюю машину, то метод ФБР не сработал бы.



Tor от полиции не спасет

Тем не менее, история демонстрирует слабость относительно редких инструментов информационной безопасности, пишет известный криптограф Брюс Шнайер. «Та же самая вещь, которая позволяет скрыть свою причастность, делает тебя главным подозреваемым». ФБР не пришлось взламывать Tor, они просто использовали стандартные полицейские методы для выявления отправителя письма. Другими словами, даже в самой в мощной криптографической защите имеется слабое место – это

сам человек. Если не можешь сломать код, то всегда можно сломать человека.

Провайдеры выявляют пользователей Tor

Аналогичные методы по выявлению пользователей Tor подходят для использования на уровне любого провайдера. Не стоит удивляться, если у спецслужб уже есть список пользователей Tor в каждом городе.

Можно ли отследить человека, если он пользуется Тором?

Проще простого. Во-первых, у спецслужб есть ключи в черному в ходу в операционных системах. Это значит, что пользователь может сидеть за Тором и считать себя в полной безопасности, а в это время по параллельной линии сливается его реальный IP-адрес. Во-вторых, Тор гарантирует безопасность только при строгом соблюдении правил. Вы уверены, что знаете эти правила на 100%? Например, нельзя включать JavaScript. Но некоторые сайты без него не работают. Включил — и твой IP уже известен всем.

Tor не скрывает IP

Очень часто сайт требует включить JavaScript и отказывается работать дальше, пока пользователь не выполнит это требование. Ну так знайте, что если вы включили в Торе исполнение JavaScript, то ваш IP — уже не тайна для постороннего сайта.

Можно ли вычислить пользователя VPN?

Можно. Это сделать сложнее, чем вычислить пользователя TOR. Но дело в том, что настройка VPN — весьма сложный процесс и здесь часто случаются ошибки. Недавно было проведено исследование на эту тему. Оказалось, что примерной 40% существующих сервисов VPN позволяют довольно легко вычислять IP пользователей — из-за грубых ошибок в конфигурации.

Для чего нужен Тор браузер?

Для сокрытия своего IP-адреса при посещении сайтов. Вторая задача браузера Тор — предоставить доступ к тем сайтам, которые были заблокированы на территории России.

Почему Тор не анонимен?

Потому, что бесплатный сыр бывает только в мышеловке. Тор создавался при финансовой поддержке правительства США. Входные ноды TOR видят ваш настоящий IP-адрес, выходные ноды TOR видят весь ваш трафик. Какая уж тут анонимность?

Как скрыть использование TOR

Никак. Ваш реальный IP будет заменен на IP выходной ноды TORa. Этот IP можно проверить по списку узлов сети TOR и установить факт использования.

Как качать файлы через TOR

Можно настроить качалку файлов на работу через прокси, но делать этого не рекомендуется — TOR слишком медленный для скачивания файлов. К тому же, вы забиваете канал и мешаете тем, кому действительно нужна анонимность. Хотите тайно качать файлы — используйте не TOR, а VPN.

Почему Tor небезопасен

В безопасность Tor верят только пионеры, причем именно верят, а не пытаются проанализировать насколько это средство действительно обеспечивает анонимность. А вот эксперты предупреждают о ненадежность Tor уже давно:

** в 2008 году был представлен метод, позволяющий деанонимизировать любого пользователя Tor за 20 минут;*

**в 2013 году появились сообщения о том, что спецслужбы научились помечать Tor-трафик и в некоторых случаях раскрывать личности участников сети;*

**существует способ отслеживать пользователей с помощью рекламной сети Google AdSense;*

** и вообще, бюджет Tor на 40% из "пожертвований" американского правительства.*

Особо следует отметить, что использование Tor без изучения всех нюансов данной системы может обернуться серьезными неприятностями даже для законопослушных пользователей. Например, в декабре 2012 года полиция ворвалась в дом к 20-летнему оператору Tor-узла и предъявила обвинения, предусматривающие от 10 лет тюрьмы. И это при том, что пользователь не совершал противоправных действий, а только предоставил свой компьютер для прохождения анонимного трафика.

Источник

Тэги: не , почему , легко , реальные , имена , ваша , спасает , вычисляют , безопасность , пользователей , спецслужбы , тор