Автор: Максим Бакулев © Babr24.com Источник: telegra.ph ИНТЕРНЕТ И ИТ, МИР 10195 10.07.2017, 14:08
1736

# Что знает о тебе твой интернет-провайдер

Вообще с провайдерами не все так просто, они по закону должны прослушивать трафик пользователей — не нарушают ли они закон, что они там делают, они конечно не смотрят, но записывают основные данные, люди их без причины не проверяют (то есть это все записывается в автоматическом режиме).

## Рубрика "Вопрос-Ответ":

**Если пользователь открывает определенный сайт, то видно ли это провайдеру?**

Да, в большинстве случаев видно именно доменное имя, редко — просто его IP-адрес. Также записывается время и, когда вы заходили на сайт. Содержимое сайтов также видно.

**А если я захожу на сайт по защищенному протоколу https?**

Тогда провайдер видит только имя сайта или его ИП-адрес и все, содержимое он не видит, так как это защищенное соединение https с шифрованием, поэтому и рекомендуется его использовать.

**Как провайдер может просечь, что я скачал фильм или программу через торрент?**

Дело все в том, что торрент-качалка общается с торрентр-трекером по протоколу HTTP, поэтому провайдер может увидеть все что вы качали (просто при помощи анализа страницы, откуда был скачан .торрент-файл) и когда (начали/закончили). Возможно и подключение по протоколу https, но почему-то даже крупнейший торрент СНГ не поддерживает такой протокол, но вот почему — загадка.

**Провайдер сохраняет все то, что я качаю?**

Нет, это просто физически невозможно, не хватило бы никаких жестких дисков. Обрабатывается трафик на лету, сортируется и ведется статистика, вот как раз она то и складируется годами.

**Может ли провайдер узнать что я скачал .торрент файл?**

Да, может, именно это и они стараются отслеживать — взаимодействие между торрент-клиентом и сервером, анализировать трафик внутри торрент-сети они не могут, ибо это очень и очень накладно.

**А если я использую ВПН, то провайдер ничего не видит?**

Тут как раз штука такая, что при ВПН таки да, провайдер видит кашу — то есть зашифрованные данные и анализировать их, а уж тем более расшифровать он не станет, ибо это почти нереально. Но вот узнать по айпи серверам, что это ВПН специально для шифрования трафика — он может. Это означает, что пользователю есть, что скрывать, делайте выводы сами.


**Если я буду использовать программу openvpn, то через него будет работать все программы в том числе и обновление окна?**

В теории да, и вообще так должно быть. Но на практике все зависит от настроек.

**Может ли провайдер узнать реальный айпи адрес определенного сайта, если я зашел на него через ВПН?**

Вообще-то нет, но тут есть другой момент. Если вдруг ВПН перестанет работать, или если какая-то ошибка, то она просто начнет работать в обычном режиме, то есть без использования ВПН — просто напрямую. Чтобы исправить это, во-первых, нужно настроить сам клиент openvpn, а во-вторых использовать дополнительно фаервол (рекомендую Аутпост фаервол), в котором можно создать глобальные правила движения трафика.

**То есть если ВПН глюканул, провайдер увидит на каком сайте я сижу?**

К сожалению да, при этом автоматически будет все записано.

**Может ли обеспечить анонимность TOP?**

Может, но желательно его немного настроить на использование с IP-адресов кроме все СНГ, а также чтобы адреса менялись чаще, например каждые три минуты. Также для лучшего эффекта советую использовать ретрансляторы (мосты).

**Что провайдер видит, когда я получаю пакеты постоянно с разных айпи адресов?**

У провайдеров есть система обнаружения использования TOP, но я не уверен, работает ли эта система при наличии ретрансляторов. Факт использования TOP также записывается и также говорит провайдеру о том, что этот пользователь может что-то скрывать.

**Видит ли провайдер адрес сайта через TOP или ВПН?**

Нет, только ИП-адрес ВПН или выходной узел сети Tor.

**Видно ли провайдеру полное имя адреса при использовании протокола https-протокола?**

Нет, видно только адрес домена (то есть только site.com), время подключения и переданный объем. Но эти данные не особо полезны для провайдера в плане инфы. Если использовать протокол http, то видно что передается все — и полный адрес и все что вы написали/отправили в сообщение по почте например, но опять же, вот к Gmail, что это не относится — там трафик шифруется.

**То есть если я использую шифрование соединения, то я уже могу быть в списке подозреваемых?**

Нет, не совсем так. С одной стороны — да, но с другой шифрование данных а то и глобальное шифрование всей сети могут использовать не только какие-то хакеры или пользователи — но простые и организации,

которые обеспокоены безопасной передачей данных, что логично и, особенно в банковской сфере.

**Видит ли провайдер факт использования сети i2p?**

Видит, но пока этот вид сети мало знаком провайдерам так, как например Tor, который из-за своей популярности привлекает все больше внимания со стороны спецслужб. Трафик в i2p провайдер видит как шифрованные подключения к разным по IP-адресам, что говорит о том, что клиент работает с P2P сетью.

**Как узнать, нахожусь ли я под СОРМ?**

Расшифровывается эта аббревиатура так — Система технических возможностей для оперативно-розыскных мероприятий. И если вы подключены к интернету в РФ, то вы уже пол умолчанию под надзором. При этом эта система полностью официальная, и трафик обязан проходить через нее, иначе у провайдеров интернета и операторов связи просто аннулируют лицензию.

**Как увидеть весь трафик на компе так, как его видят провайдеры?**

В этом вам поможет утилита для снифинга трафика, лучшая в своем роде это анализатор сетевого трафика.

**Можно ли как-то понять, что за тобой следят?**

На сегодняшний день почти нет, иногда, возможно при активной атаке типа атаки (человек посередине). Если применяется пассивная слежка, то обнаружить ее нереально чисто технически.

**Но что делать тогда, можно ли как-то затруднить слежку?**

Можно разделить интернет, то есть ваше подключение к нему, на две части. Сидите в соцсетях, на сайтах знакомств, смотрите развлекательные сайты, фильмы, все это делайте по обычному подключению. А зашифрованное соединение используйте отдельно и при этом параллельно — например установите для этого виртуальную машину. Таким образом у вас будет более-менее естественная среда так сказать бы, ибо, шифруют трафик многие сайты, и Гугл в своих сервисах, и другие крупные компании. Но с другой стороны, почти все развлекательные сайты трафик НЕ шифруют.

Автор: Максим Бакулев © Babr24.com Источник: telegra.ph ИНТЕРНЕТ И ИТ, МИР 10195 10.07.2017, 14:08
1736
URL: https://babr24.com/?ADE=162071 Bytes: 6472 / 6284 Версия для печати Скачать PDF



Автор текста: **Максим Бакулев**, политический обозреватель.

**НАПИСАТЬ ГЛАВРЕДУ:**

Телеграм: @babr24_link_bot
Эл.почта: newsbabr@gmail.com

**ЗАКАЗАТЬ РАССЛЕДОВАНИЕ:**

эл.почта: bratska.net.net@gmail.com

**КОНТАКТЫ**

Бурятия и Монголия: Станислав Цырь
Телеграм: @bur24_link_bot
эл.почта: bur.babr@gmail.com

Иркутск: Анастасия Суворова
Телеграм: @irk24_link_bot
эл.почта: irkbabr24@gmail.com

Красноярск: Ирина Манская
Телеграм: @kras24_link_bot
эл.почта: krasyar.babr@gmail.com

Новосибирск: Алина Обская
Телеграм: @nsk24_link_bot
эл.почта: nsk.babr@gmail.com

Томск: Николай Ушайкин
Телеграм: @tomsk24_link_bot
эл.почта: tomsk.babr@gmail.com

Прислать свою новость

**ЗАКАЗАТЬ РАЗМЕЩЕНИЕ:**

Рекламная группа "Экватор"
Телеграм: @babrobot_bot
эл.почта: eqquatoria@gmail.com

**СТРАТЕГИЧЕСКОЕ СОТРУДНИЧЕСТВО:**

эл.почта: babrmarket@gmail.com

Подробнее о размещении

Отказ от ответственности

Правила перепечаток

Соглашение о франчайзинге

Что такое Бабр24

Вакансии

Статистика сайта

Архив

Календарь

Зеркала сайта