DNSCrypt: ПРЯЧЕМ DNS-ТРАФИК

Защита DNS-соединений для параноиков

Используя VPN, ты думаешь, что за тобой никто не подсматривает и передаваемые данные защищены? Ты ошибаешься. Сейчас попробую объяснить почему.

Денис Колисниченко
dhsilabs@gmail.com

ВКРАТЦЕ О DNSCRYPT

При использовании HTTPS или SSL твой HTTP-трафик зашифрован, то есть защищен. Когда ты используешь VPN, шифруется уже весь твой трафик (конечно, все зависит от настроек VPN, но, как правило, так оно и есть). Но иногда, даже когда используется VPN, твои DNS-запросы не зашифрованы, они передаются как есть, что открывает огромное пространство для «творчества», включая MITM-атаки, перенаправление трафика и многое другое.

Тут на помощь приходит опенсорсная утилита DNSCrypt, разработанная хорошо известными тебе создателями OpenDNS, — программа, позволяющая шифровать DNS-запросы. После ее установки на компьютер твои соединения также будут защищены и ты сможешь более безопасно бороздить просторы интернета. Конечно, DNSCrypt — это не панацея от всех проблем, а только одно из средств обеспечения безопасности. Для шифрования всего трафика все еще нужно использовать VPN-соединение, но в паре с DNSCrypt будет безопаснее. Если тебя такое краткое объяснение устроило, можешь сразу переходить к разделу, где я буду описывать установку и использование программы.

ДЛЯ НАСТОЯЩИХ ПАРАНОИКОВ

Попробуем разобраться глубже. Этот раздел предназначен для настоящих параноиков. Если ты ценишь свое время, тогда можешь сразу перейти к установке программы.

Итак, как говорится, лучше один раз увидеть, чем сто раз услышать. Посмотри на рисунок 1. Допустим, клиент (ноутбук на рисунке) пытается обратиться к dkws.org.ua. Первым делом он должен разрешить символьное имя узла в IP-адрес. Если же конфигурация сети такова, что используется DNS-сервер провайдера (незашифрованное соединение, красная линия на рисунке), то разрешение символьного имени в IP-адрес происходит по незашифрованному соединению.

Да, какие данные ты будешь передавать на dkws.org.ua, никто не узнает. Но есть несколько очень неприятных моментов. Во-первых, провайдер, просмотрев логи DNS, сможет узнать, какие сайты ты посещал. Тебе это нужно? Во-вторых, вероятна возможность атак DNS-спуфинг и DNS-снупинг. Подробно описывать их не буду, об этом уже написано множество статей. В двух словах ситуация может быть следующей: некто между тобой и провайдером может перехватить DNS-запрос (а так как запросы не шифруются, то перехватить запрос и прочитать его содержимое не составит никакого труда) и отправить тебе «поддельный» ответ. В результате вместо того, чтобы посетить dkws.org.ua, ты перейдешь на сайт злоумышленника, как две капли воды похожий на тот, который тебе нужен, введешь свой пароль от форума, ну а дальше развитие событий, думаю, ясно.

Описанная ситуация называется DNS leaking («утечка DNS»). DNS leaking происходит, когда твоя система даже после соединения с VPN-сервером или Tor продолжает запрашивать DNS-серверы провайдера для разрешения доменных имен. Каждый раз, когда ты посещаешь новый сайт, соединяешься с новым сервером или запускаешь какое-то сетевое приложение, твоя система обращается к DNS провайдера, чтобы разрешить имя в IP. В итоге твой провайдер или любой желающий, находящийся на «последней миле», то есть между тобой и провайдером, может получить все имена узлов, к которым ты обращаешься. Приведенный выше вариант с подменой IP-адреса совсем жестокий, но в любом случае есть возможность отслеживать посещенные тобой узлы и использовать эту информацию в собственных целях.

Если ты «боишься» своего провайдера или просто не хочешь, чтобы он видел, какие сайты ты посещаешь, можешь (разумеется, кроме использования VPN и других средств защиты) дополнительно настроить свой компьютер на использование DNS-серверов проекта OpenDNS (www.opendns.com). На данный момент это следующие серверы:

- 208.67.222.222;
- 208.67.220.220.

При этом тебе не нужно никакое другое дополнительное программное обеспечение. Просто настрой свою систему на использование этих DNS-серверов.

Но все равно остается проблема перехвата DNS-соединений. Да, ты уже обращаешься не к DNS провайдера, а к OpenDNS, но все еще можно перехватить пакеты и посмотреть, что в них. То есть при желании можно узнать, к каким узлам ты обращался.

Вот мы и подошли к DNSCrypt. Эта программулина позволяет зашифровать твое DNS-соединение. Теперь твой провайдер (и все, кто между тобой и им) точно не узнает, какие сайты ты посещаешь! Еще раз повторюсь. Эта программа не замена Tor или VPN. По-прежнему остальные передаваемые тобой данные передаются без шифрования, если ты не используешь ни VPN, ни Tor. Программа шифрует только DNS-трафик.

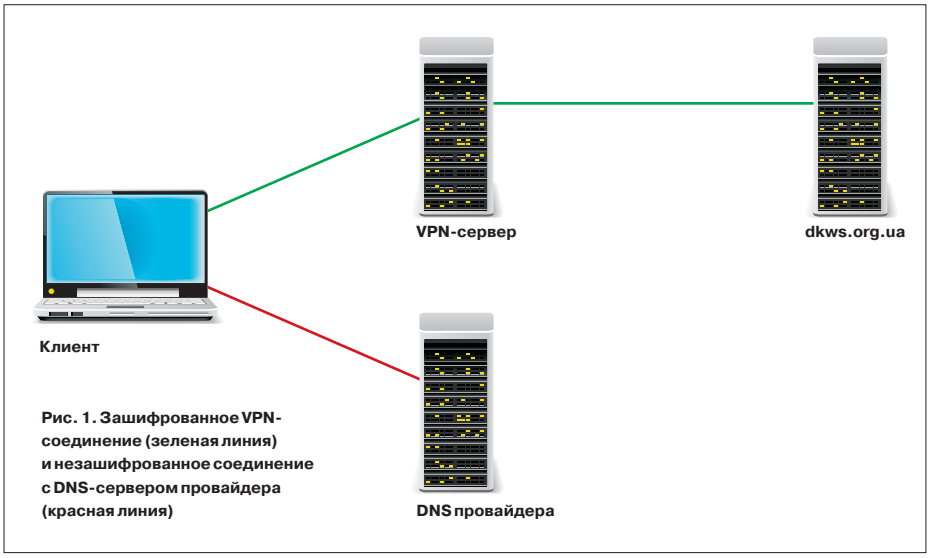

Рис. 1. Зашифрованное VPN-соединение (зеленая линия) и незашифрованное соединение с DNS-сервером провайдера (красная линия)

DNS LEAK

Сайт https://www.dnsleaktest.com позволяет определить «утечку» DNS и объясняет, как от нее избавиться. Просто зайди на этот сайт. Нажав кнопку Check for DNS leaks now, ты получишь список DNS-серверов, через которые могут проходить твои запросы. Следовательно, ты увидишь, кто именно может узнать, какие сайты ты посещаешь (рис. 2).

Как показано на рис. 2, владельцы 12 DNS-серверов имеют возможность записывать все посещенные мною сайты. Но поскольку я работаю через Tor, то меня этот вопрос мало беспокоит.

На страничке bit.ly/1ctmgaJ описано, как исправить эту уязвимость (то есть что сделать, чтобы после подключения к VPN твоя система использовала DNS-серверы VPN-провайдера, а не твоего интернет-провайдера). Повторять все это не вижу смысла, поскольку любой справится с пошаговой последовательностью действий.

УСТАНОВКА И ИСПОЛЬЗОВАНИЕ DNSCRYPT

Самый простой способ защитить свое DNS-соединение — это использовать DNSCrypt. Можно, конечно, следовать рекомендациям от www.dnsleaktest.com, а можно пойти по пути наименьшего сопротивления и просто установить DNSCrypt.

Первым делом качаем сам DNSCrypt (https://github.com/opendns/dnscrypt-win-client). Я сразу привел ссылку на GitHub, откуда можно скачать программу. Если хочешь получить о ней дополнительную информацию, тогда тебе сюда: bit.ly/vjGXjB. Чтобы скачать программу с GitHub, нажми кнопку Download ZIP. Будет загружен архив с исходниками DNSCrypt. Уже откомпилированная версия находится в каталоге DNSCrypt архива. Распакуй файлы. В принципе тебе нужен только один файл — dnscrypt-proxy.exe. Он находится в том самом каталоге. Все остальное (исходники) можно удалить.

Но это еще не все. Если ты уже погуглил, то, значит, видел скриншоты DNSCrypt. Запустив dnscrypt-proxy.exe, ты понял, что что-то не то. Программа запустилась в окне командной строки. Все правильно, ты скачал сам прокси, а теперь еще нужно скачать к нему оболочку. На GitHub есть еще один проект — необходимая нам оболочка (bit.ly/ADxggQ).

Аналогичным образом скачай ZIP-архив, распакуй его куда-нибудь. В каталоге binaries/Release/ будет программа dnscrypt-winclient.exe. Скопируй этот файл в каталог, в котором находится файл dnscrypt-proxy.exe.

Осталось только запустить dnscrypt-proxy.exe. В появившемся окне выбери сетевые адаптеры, которые нужно защитить, и нажми кнопку Start. Если все нормально, тогда возле кнопки Stop (в нее превратится кнопка Start) появится надпись DNSCrypt is running (рис. 3). Кстати, обрати внимание, что интерфейс для OS X выглядит несколько иначе (клиент для OS X можно взять здесь: bit.ly/rCNp01).

В КАЧЕСТВЕ ЗАКЛЮЧЕНИЯ

Статья получилась не очень большая, поскольку сама программа очень проста в использовании. Но она была бы неполной, если бы я не упомянул и о VPN. Если ты прочитал эту статью, тебя она заинтересовала, но ты еще не пользуешься услугами VPN-провайдера для шифрования своих данных, то самое время это сделать. Один из VPN-провайдеров — SecurityKISS (www.securitykiss.com) предоставит тебе безопасный туннель для передачи твоих данных, а DNSCrypt обеспечит защиту DNS-соединений. Конечно, SecurityKISS платный (бесплатный тарифный план можно использовать разве что для ознакомления), но ведь за безопасность нужно платить? Можно использовать, конечно, и Tor (о котором уже писалось в одном из предыдущих выпусков), но Tor работает относительно медленно, и это, как ни крути, не VPN — весь трафик «торифицировать» не получится. В любом случае (какой бы вариант ты ни выбрал) теперь твои DNS-соединения защищены. Осталось только определиться со средством шифрования трафика (если ты это еще не сделал).

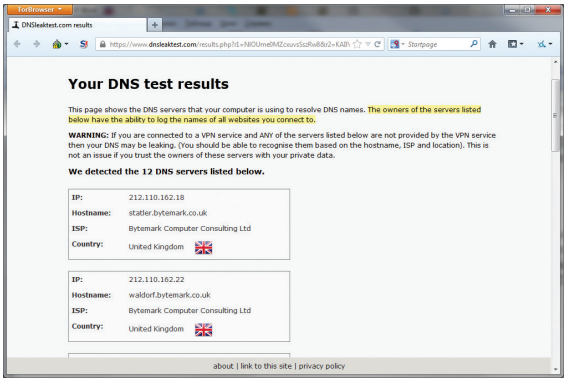

Рис. 2. Список DNS-серверов

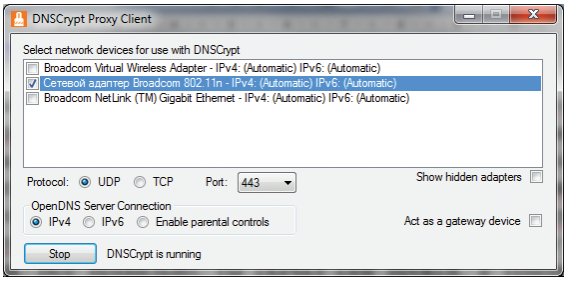

Рис. 3. DNSCrypt запущен

WWW

DNS snooping: bit.ly/18xQA4v

DNS spoofing: en.wikipedia.org/wiki/DNS_spoofing