Товарищ майор обойдет VPN

Почему бесплатные анонимайзеры не помогут вам спрятаться и какие способы лучше

Компания Metric Labs, изучив самые популярные VPN, доступные для бесплатного скачивания в магазинах Google и Apple, с удивлением обнаружила, что 60% программ во главе списка либо созданы китайскими программистами, либо принадлежат китайским компаниям.

Допускаю, что рядовому западному потребителю, воспитанному в духе интернационализма, до китайской наследственности мало дела, зато для профессионала в сфере цифровой безопасности худшей рекомендации не придумаешь.

В январе 2017 года Поднебесная партия и ее правительство запустили суровую «чистку» услуг, покушающихся на «национальный цифровой суверенитет».

Основной удар пришелся на частные лица и компании, предоставляющие несознательным гражданам сервис VPN. После поголовной обязательной регистрации — читай: внедрении в программный код «бэкдоров», открывающих государству свободный доступ к приватным данным пользователей, — горстку несогласных показательно наказали и вывели из игры.

Предприниматель By Сяньян, окормлявший своим VPN 8 тысяч иностранных граждан и 5 тысяч юридических лиц с 2013 года, получил 74 тысячи долларов штрафа и пять лет отсидки на нарах.

Можно подумать, что китайская кампания борьбы с VPN направлена на отваживание населения от посещения запрещенных сайтов (коих в Китае три четверти мирового интернета).

Мне, однако, кажется, что борьба с несознательными гражданами в стране генетической сознательности — дело десятое. Гораздо важнее для партии и правительства, одержимого страхом перед технологическим отставанием от Запада, получить контроль за информационными потоками этого самого Запада.

Контролируя якобы частные VPN, китайское государство превращается во второй Google, с тем только преимуществом, что поисковой системой пользуются все подряд, а VPN устанавливают, как правило, лишь те, кому есть что скрывать.

Тайно перлюстрируя трафик западных пользователей, купившихся на бесплатный статус популярных VPN приложений в Google Play Store и Apple iTunes Store, китайские власти могут как самостоятельно использовать полученные данные, так и продавать их конкурентам в случае, если пользователи китайских VPN-услуг работают в западных корпорациях и случайно выбалтывают ценную информацию.

Петр САРУХАНОВ — «Новая»

Возникает вопрос: а что нам, гражданам Российской Федерации, до того, что частный трафик попадет в руки китайских властей? Тем более что не только китайские VPN несут в себе потенциальную угрозу утечки данных, но и, к примеру, американские, в юрисдикции которых после 9/11 создано множество законодательных лазеек, открывающих доступ к формально приватной информации (куда мы ходили, что смотрели и т.п.).

Нам же нет дела до китайцев и американцев, главное, чтобы наши цифровые похождения не попали в руки родному Роскомнадзору. Не так ли?

Боюсь, что не так. Однако нет нужды тратить время на доказательство банальной апофегемы, что бесплатный сыр случается только в мышеловках. Продуктивнее разобраться с вопросом по существу: «Нужен ли нам VPN в принципе?»

Подавляющее большинство пользователей Рунета убеждено, что VPN обеспечит им три важных «прикрытия».

Во-первых, позволит посещать сайты из черного списка Роскомнадзора. Не то чтобы это было больно надо, но негоже, когда чужой дядя за тебя решает, что можно смотреть и читать, а что нельзя.

Во-вторых, VPN обещает скрыть сетевую активность. Не то чтобы это было больно надо сейчас, но впрок — пригодится. Мало ли, что там случится дальше, на чем нас повяжут, какой очередной «ВКонтакте» подведет под суму (или того хуже).

В-третьих, VPN сулит нам главную нирвану советского (и постсоветского) человека — анонимность. В тревожных обществах чем ты неприметнее, тем дольше продержишься.

Парадокс, однако, в том, что для всех перечисленных задач VPN либо не совсем нужен, либо бесполезен. Для посещения запретных сайтов VPN избыточен, потому что хватает простенького прокси-сервера, либо вообще без лишней мороки — браузера Opera или TOR.

Сокрытие сетевой активности — штука, безусловно, полезная, однако она никоим образом не обеспечивает анонимности, потому что при желании нашу анонимность очень просто раскрыть совершенно с другого бока.

Вас никто не будет мучить паяльником, если вы где-то там интимно и неприметно анонимизируете в Сети. Государству по шарабану безымянные и никому не интересные статистические единицы. Государству лишь важно, чтобы вы не баламутили мозги окружающим и не поднимали лишней волны («не будили низменные страсти», как сказал бы поэт).

Стоит, однако, вам где-то публично «неправильно» высказаться, собрать аудиторию и — главное! — вызвать опасный общественный резонанс, как государство вами заинтересуется и быстро «преодолеет» вашу анонимность, как я уже сказал, с другого бока: не через ваш IP-адрес, скрытый VPN, а через ваши социальные связи.

> «Ни один профессиональный «крамольщик» не пользуется для отправки сообщений мессенджером Telegram»

В криптографии есть правило: нельзя использовать самые надежные алгоритмы шифрования, а затем сохранить свои 100-значные пароли в каком-нибудь файле Word с простенькой защитой, преодолеваемой простым перебором за 15 минут.

Защита системы всегда равна защите самого слабого звена этой системы. Даже если вы скроете свой IP-адрес с помощью лучшего в мире VPN (не китайского), вас непременно «вычислят» по совокупности ваших социальных связей на той площадке, где вы допустили «крамолу».

Вежливые дяди составят список восторженных читателей вашего поста, у кого-нибудь обнаружится реальный IP-адрес, а оттуда до адреса проживания в реаллайфе — рукой подать.

Вашего поклонника навестят часа в четыре утра. Потом второго, третьего. С четвертым вы, оказывается, сидели за одной партой в школе. Так что не удивляйтесь, что через пару-тройку дней вас примут под белые рученьки вместе со всеми вашими идеологическими потрохами и годовой подпиской на надежный платный VPN.

Что касается любви наших граждан к анонимности, то для трезвомыслия не хватает лишь толики дополнительного знания: белая ворона, как бы она ни шифровалась в листве сумеречного парка, всегда заметна на фоне стаи своих черных собратьев.

Иными словами, если подавляющее большинство обывателей вокруг вас не пользуется шифрованием, а вы один такой продвинутый, вас вычислят еще до того, как вы успеете написать слово «Долой...».

В свое время на этом погорела модная система шифрования электронных писем Pretty Good Privacy Филиппа Циммермана. Все электронные письма, закодированные PGP, содержали ключ в открытой текстовой форме, который начинался со строки «—BEGIN PGP SIGNATURE—».

По этому признаку из потока почтовых сообщений быстро извлекаются зашифрованные письма, и при желании третья заинтересованная сторона может обстоятельно и без суеты изучить всю последующую сетевую (и не только сетевую) активность горе-шифровальщиков.

Из сказанного вытекает, что обязательным условием по-настоящему скрытого от посторонних глаз обмена информацией должна быть стеганография.

Эффективность защиты определяется не столько надежностью алгоритмов шифрования, сколько отсутствием следов самой защиты как таковой. Скажем, сообщение, зашифрованное PGP, должно посылаться не простым текстом, а встраиваться в какое-нибудь изображение.

Со стороны JPEG-файл выглядит как обыкновенная картинка, и никому в голову не придет, что получатель вашего письма с помощью специальной программы сначала извлечет зашифрованное сообщение из мнимой графики, а затем его расшифрует. И это лишь вершина айсберга под названием стеганография.

Полагаю, читатель теперь ясно осознает пропасть, отделяющую пользователя «ВКонтакте» с его трогательными репостами, от профессионального конспиратора, выполняющего оперативное задание. Если уж сольсберийские шпилеведы умудряются так грубо прокалываться, что же требовать от попов, исполняющих под запись «Мурку»?

Какие можно сделать практические выводы из всего сказанного?

Во-первых, для задач большинства рядовых пользователей Рунета VPN — избыточное решение. Так что не важно, какие VPN используются — китайские бесплатные или некитайские платные.

Во-вторых, нужно понимать, что инструменты борьбы, задействованные репрессивными режимами вроде китайского и еще пары-тройки всем знакомых политобразований, защищают власть только от дураков. Потому что только дураки репостят провокационные картинки и мемы (почти без исключения троллями-провокаторами и создаваемые), зная, что по существующим законам (как бы мы к этим законам ни относились) их действия являются уголовно наказуемыми.

В-третьих, можно не сомневаться в том, что ни один профессиональный «крамольщик» не пользуется для отправки мгновенных сообщений мессенджером Telegram, не заводит дурацких аккаунтов в «ВКонтакте», не постит селфи на фоне секретных гаубиц в Instagram, не оставляет цифровых следов в кэше браузера, не принимает куки-файлы, да и просто никогда не выходит в интернет через штатную операционную систему своего ноутбука.

Как говорят американцы: «Can you spell TAILS to me» («Произнеси-ка мне по буквам слово TAILS»).

Ну да если вы знаете, что такое TAILS, вам вообще не следовало читать эту статью!

Сергей ГОЛУБИЦКИЙ —
специально для «Новой»