ТАК ЛИ ОПАСЕН DARKNET?

После серии терактов в Европе таинственный Даркнет стал восприниматься как неконтролируемое место торговли наркотиками, фальшивыми документами и оружием. Действительно ли это так?

Наркотики, оружие, фальшивые документы и удостоверения личности, украденные данные от сетевых аккаунтов и кредитных карт, наемные убийцы — на теневых интернет-площадках можно найти все, с чем человек с хорошей репутацией не хотел бы связываться в течение всей своей жизни. Чтобы обменяться товаром или заказать услугу, достаточно счета с биткоинами и пары кликов. В общем и целом, все было относительно спокойно. Но когда 22 июля 18-летний Давид С. совершил убийство девяти человек в Мюнхене, после чего покончил с собой, представители мира цифровых технологий предположили, что школьник мог приобрести орудие преступления через Даркнет — и «темный Интернет» неожиданно предстал в роли супермаркета со свободным доступом, в котором можно купить все, включая оружие и боеприпасы.

Но не все так просто, как может показаться на первый взгляд. Обнаруженные следователями сообщения стрелка, оставленные на форумах, показывают, что потенциальный покупатель, по-видимому, до тех пор, пока ему не было предложено нужное оружие, вынужден был делать все новые запросы на протяжении месяцев. Ассортимент предлагаемого товара был весьма ограничен, а вот желающих похвастаться нелегальным оружием, скрывающихся под вымышленными сетевыми никами, оказалось гораздо больше. По поводу массового убийства в Мюнхене представитель немецкого общества хакеров Chaos Computer Club (CCC) сообщил немецкому информационному агентству DPA, что торговля наркотиками и оружием в Даркнете происходит в гораздо меньших объемах, чем за пределами Сети.

80 дел, 240 тысяч преступлений

Данные Федерального ведомства уголовной полиции Германии (BKA) подкрепляют это впечатление. Как сообщил в конце июля глава BKA Хольгер Мюнх, в настоящее время по подозрению в торговле оружием и взрывчатыми веществами в Даркнете BKA ведет около 80 дел. По сравнению с более чем 240 000 уголовных преступлений, связанных с использованием Интернета как средства совершения преступления, дела по которым, по сообщениям BKA, были возбуждены в 2015 году, эта цифра ничтожно мала. Такой резкий диссонанс может, с одной стороны, говорить о том, что «темная паутина» представляет для следователей гораздо меньшую проблему, чем обычные мошенничества на eBay. Но с другой стороны, такие показатели можно объяснить тем, что общая статистика охватывает нарушения всякого рода, а данные по Даркнету — только тяжкие преступления, например, ту же незаконную торговлю оружием и взрывчатыми веществами.

Небольшое число заведенных дел удивляет еще сильнее, если учесть тот факт, что даже неспециалисты могут попасть в этот сегмент с первой попытки. Чтобы воспользоваться технологией Tor (см. подрубрику сверху), наиболее популярной анонимной сети, достаточно установить пакет Tor Browser Bundle. Кроме Tor, существуют проекты I2P, Freenet, а также недавно представленный Riffle. Для создания зашифрованных соединений и сохранения анонимности пользователей и серверов эти сети используют обычную инфраструктуру Интернета. Даркнет вступает в права после того, как все соединения и серверы становятся невидимы для Google, Bing и других поисковиков.

Как работает сеть Tor

Браузер Tor — это модифицированная версия Firefox, которая перенаправляет весь трафик по Сети, используя прокси-серверы — узлы, которые выбираются случайным образом. Прежде чем отправить пакет в Сеть на входном узле (entry node), браузер последовательно шифрует пакет тремя ключами для каждого узла. Чтобы снизить вероятность прослушивания, ПО меняет узлы каждые десять минут. Входной узел отправляет данные на узел-ретранслятор, отвечающий за пересылку трафика (relay node), который узнает, куда отправить пакет дальше, когда расшифровывает предназначенный для него слой шифра. Конечный, выходной узел (exit node) окончательно расшифровывает пакет и передает данные на целевой сервер. Таким образом, на каждом этапе перенаправления пакета соответствующий узел «удаляет» слой шифра аналогично тому, как чистят луковицу (англ. onion; Tor, собственно, — The Onion Router — «луковая маршрутизация»). В результате ретрансляторы-посредники знают, от каких входных узлов они получили пакет, но не знают истинного отправителя. Выходные узлы знают, на какой адрес отправлять пакеты в итоге и от каких ретрансляторов они их получили, но не знают IP-адресов других участников сети. Другими словами, ни один узел не располагает всеми сведениями о передаче пакетов, которые оказались бы полезными для слежки. Теоретически использовать прокси-серверы Tor может любой желающий.

Светлая сторона темной сети

Изначально система Tor была создана исследователями, которые в первые годы ее существования, с 2001 по 2004 годы, сотрудничали с различными ведомствами министерства обороны США. Конечно, они вовсе не собирались разворачивать инфраструктуру, которую можно было бы безопасно использовать для незаконной деятельности. Точнее, цель проекта состояла в разработке способа анонимного обмена данными в Интернете. Тотчас же вслед за государственными служащими системой не преминули воспользоваться преступники. Так, Tor для кого-то был инструментом, а для кого-то оказался удобным оружием.

Еще одна группа интернет-пользователей не может обойтись без Tor: состоит она из диссидентов и жителей тех стран, →

Такой пистолет модели Glock 17 мюнхенский стрелок приобрел в Даркнете

ФОТО: компании-производители; Wikipedia/Nukes4Tots, CC BY-SA 3.0; Wikipedia/By Laura Poitras/Praxis Films, CC BY-SA 3.0

+++ ДАРКНЕТ В ЦИФРАХ +++ ДАРКНЕТ В ЦИФРАХ +++ ДАРКНЕТ В ЦИФРАХ +++ ДАРКНЕТ В ЦИФРАХ +++ ДАРКНЕТ В ЦИФРАХ

Количество пользователей, использующих *браузер Tor* по всему миру:
около 1,6 млн

Количество пользователей, использующих браузер Tor *в России:*
около 250 тысяч

Количество анонимных скрытых служб *(hidden services)* в сети Tor:
около 55 тысяч

+ ДАРКНЕТ В ЦИФРАХ +++ ДАРКНЕТ В ЦИФРАХ +++ ДАРКНЕТ В ЦИФРАХ +++ ДАРКНЕТ В ЦИФРАХ +++ ДАРКНЕТ В ЦИФРАХ +++

Количество ***ретрансляторов*** в анонимной сети Tor
около семи тысяч

Общая ***пропускная способность*** на всех ретрансляторах сети Tor
около 180 Гбит/с

Объемы трафика анонимных скрытых служб Tor
900 Мбит/с

правительства которых не страдают избытком демократии. Медийные организации тоже прибегают к услугам анонимных сетей, чтобы обеспечить безопасность разоблачителям, предоставляющим им информацию. Эдвард Сноуден, например, для передачи журналистам The Guardian и The Washington Post сведений о проекте АНБ PRISM, касающемся тотальной слежки американских спецслужб за гражданами по всему миру, использовал дистрибутив Linux под названием TAILS, в котором Tor применяется по умолчанию. В сети Tor, конечно же, есть серверы для обмена сообщениями и серверы форумов, блоги диссидентов-правозащитников, а также литературный журнал (The Torist) и даже полноценный доступ к Facebook. Использование данной социальной сети в Tor — учитывая обязательный ввод имени пользователя, это покажется нелепым, — совершенно анонимно: дело в том, что серверы Facebook работают в «темной паутине».

Эдвард Сноуден, один из самых известных пользователей Даркнета

Русскоязычное подполье

Не только небольшие с технической точки зрения усилия объясняют легкодоступность Даркнета. Существуют различные русскоязычные форумы и торговые площадки, скрытые от публичного доступа, то есть начинающим уголовникам вроде мюнхенского стрелка необязательно объясняться по-английски. Ассортимент товаров на них сам по себе такой же, как на крупных зарубежных торговых площадках, хотя количество экземпляров ограничено.

Более того, поставщики адаптируют индивидуальный товар и услуги под российскую действительность. Так, нередко предлагается купить данные для входа, украденные у жителей РФ, а для доставки товаров, купленных через похищенные данные, задействуются упаковочные станции компании DHL, пользующиеся большой популярностью — вся нужная для этого информация тоже циркулирует на форумах.

Правоохранители в неведении?

Внезапно появившееся внимание СМИ к анонимным сетям создает впечатление, что BKA и другие органы заинтересовались Даркнетом только после бойни в Мюнхене. Но это не так. Еще за месяцы до стрельбы представитель прокуратуры округа Ферден Маркус Хойслер заявил: «Расследования на немецких подпольных форумах — работа не рутинная, но, тем не менее, она является регулярной частью нашей деятельности. За некоторыми немецкими форумами мы следим и в настоящий момент». Среди прочего Хойслер вел следствие по делу владельцев интернет-площадки по торговле наркотиками Chemical Love, которую полиции удалось закрыть — доступ к ней осуществлялся все из той же «темной паутины». А после массового убийства в Мюнхене BKA по-

«Даркнет представляет собой одно из основных направлений деятельности BKA»

Хольгер Мюнх,
глава Федерального ведомства уголовной полиции Германии

спешило заявить на самом высоком бюрократическом языке, что борьба с киберпреступностью «именно в области «темного Интернета» представляет собой «одно из основных направлений деятельности BKA».

То, что уголовное преследование в противостоянии подпольной деятельности в Даркнете в действительности далеко не беспомощно, подтверждает дело, получившее название Oxywhite. 29-летний наркоторговец из Санкт-Августина вел активную деятельность на различных немецкоязычных подпольных форумах, и среди прочего на самой крупной в свое время площадке — **crimenetwork.biz**, насчитывающей тогда восемь тысяч активных участников. В начале декабря 2015 года, когда между поставщиком оружия DW Performance-Guns в Баден-Вюртемберге и участником форума под ником Oxywhite обнаружилась связь, оперативная группа и подразделение спецназа федеральной полиции Германии GSG9 провели обыск в квартире последнего. Торговая площадка подозревалась в доставке оружия

+ ДАРКНЕТ В ЦИФРАХ +++ ДАРКНЕТ В ЦИФРАХ +++ ДАРКНЕТ В ЦИФРАХ +++ ДАРКНЕТ В ЦИФРАХ +++ ДАРКНЕТ В ЦИФРАХ +++

Цена за ***украденный*** аккаунт службы такси Uber, предлагаемый в Даркнете
$1

Недельная зарплата ***администратора*** площадки Silk Road
от 1000 до 2000 долларов США

Страна, которая предпринимает ***попытки ввести цензуру*** на сеть Tor больше всех остальных
Казахстан

Стоимость ***биткоинов*** (на момент изъятия), которые ФБР конфисковало по делу о Silk Road
$33,6 млн

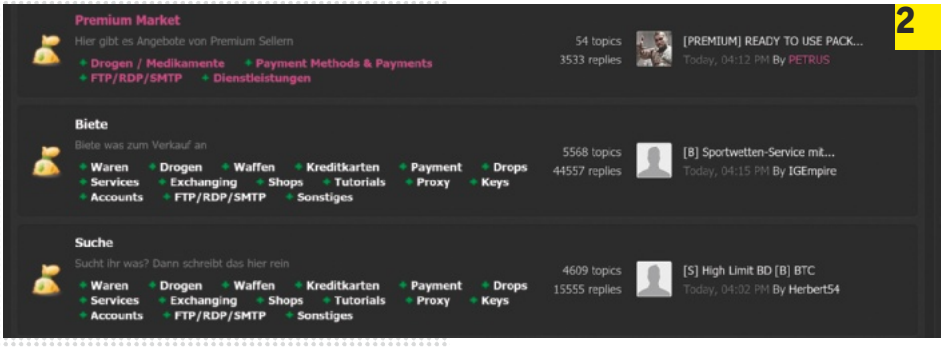
Общий оборот, который был достигнут на площадке Silk Road
$1,2 млрд

Стоимость биткоинов, изъятых у Dread Pirate Roberts, владельца Silk Road
$3,6 млн

1

Темные дела

Crimenetwork 1 — преемник ныне закрытого crimenet.biz 2. DW Performance-Guns 3 нахально расхваливал свой опасный товар вплоть до самого мая



2

3

парижским террористам и поэтому находилась под наблюдением. На одном из форумов, доступ к которым был возможен только из Tor, Oxywhite заказал на DW Performance-Guns полуавтоматическое оружие. «DW», к слову, означает «dark web», что объясняет, каким образом поставщик находит покупателей. В конечном итоге связи с террористами, устроившими теракты в Париже, не обнаружилось. Однако в результате слежки, установленной на упаковочной станции, на которую Oxywhite заказал доставку своего оружия, оперативники узнали его имя. А то, что в ходе обыска дома Oxywhite обнаружилось более двух с половиной килограммов амфетамина, который полиция конфисковала, оказалось случайным совпадением, поскольку, не имея на руках ордера на производство обыска и изъятие оружия, полиция не смогла бы попасть в квартиру.

25 тысяч таблеток экстази

Большой резонанс в мае этого года вызвала новость о прекращении деятельности онлайн-магазина Chemical Shop и подпольного форума **crimenetwork.biz** (CNW) — двух наиболее крупных немецкоязычных мест встречи. В общей сложности следователи задержали пять пользователей Chemical и изъяли 54 кг амфетамина, 4 кг героина, 1,3 кг кокаина, а также около 25 тысяч таблеток экстази. Против собственно Crimenetwork действия полиции, судя по всему, направлены не были. Это или сопутствующий ущерб, или администратор Crimenetwork под ником sync попросту скрылся после того, как его деловой партнер z100, администратор Chemical Love, столкнулся с неприятностями на работе. Видимо, оба администратора тесно сотрудничали и использовали одну и ту же серверную инфраструктуру. Sync отчислял по 10 000 евро (712 000 рублей) каждый месяц за использование техники, на которой базировался Chemical Love. Так или иначе, биткоин-кошелек, который полагался sync как посреднику, был обнулен, и $33 500 (2,1 млн рублей) были отправлены на биткоин-миксер — сервис, который в довольно прозрачной биткоин-сети полностью скрывает происхождение монет.

И если учитывать такие суммы, количество настоящих операций по продаже оружия и объемы изъятых наркотиков, то «темная паутина» перестает производить впечатление крупной перевалочной площадки — она скорее кажется небольшой барахолкой за углом. Опасность для общества в ней разглядеть трудно. Тем более власти — назло всем техническим проблемам — кажется, в некоторой степени являются хозяином положения. А поскольку у Даркнета есть светлая сторона, остается надеяться, что политики воздержатся от радикальных мер.

++ ДАРКНЕТ В ЦИФРАХ +++ ДАРКНЕТ В ЦИФРАХ +++ДАРКНЕТ В ЦИФРАХ +++ДАРКНЕТ В ЦИФРАХ +++ ДАРКНЕТ В ЦИФРАХ ++

Срок, который получил бывший владелец немецкого онлайн-магазина Shiny Flakes, занимающегося наркоторговлей
7 лет

Объем проданных на Shiny Flakes за период с декабря 2013 г. по февраль 2015 г. ***наркотиков***
914 кг

Количество предложений по категории ***«Наркотики»*** на площадке Alpha Bay
118 672