DOI 10.37539/2949-1991.2024.23.12.018

Соловьев Анатолий Алексеевич,
к.ф-м.н, профессор, СибАДИ, г. Омск

Камшибаев Жанат Жаскайратович,
старший преподаватель, Торайгыров университет,
г. Павлодар

Поступинских Людмила Анатольевна,
к.п.н., доцент СибАДИ, г. Омск

Юрина Татьяна Александровна,
к.т.н., доцент СибАДИ, г. Омск

О СЕГМЕНТЕ ИНТЕРНЕТА – ДАРКНЕТ
ABOUT THE INTERNET SEGMENT – DARKNET

Аннотация: Новости о сливах и утечках данных, которые всплывают в даркнете, появляются все чаще. Как устроен даркнет, что в нем можно найти и можно ли сохранить анонимность, если есть, что скрывать.

Ключевые слова: скрытая сеть, Tor Browser, I2P, Ноды, утечка баз данных, киберпреступное сообщество, нелегальный доступ, файервол

Даркнет (англ. DarkNet – «скрытая сеть», «темная сеть» или «теневая сеть») – это сегмент интернета, который скрыт из общего доступа. Соединение в нем устанавливается между доверенными пирами (участниками) в зашифрованном виде, с использованием нестандартных портов и протоколов. В даркнете используют собственные DNS, то есть домены, и адресное пространство. Попасть в даркнет можно с помощью специального ПО – например, Tor Browser или I2P.

Tor – это браузер, который шифрует трафик, когда вы находитесь внутри, но на входе и на выходе его все же можно отследить. Tor распределяет ваш трафик по сети, которая состоит из нод (или ретрансляторов) – тысяч серверов, которые создаются и поддерживаются добровольцами, чтобы обеспечить безопасность и анонимность. Каждый раз, когда вы подключаетесь к Tor, он строит самый быстрый и безопасный маршрут, который включает три ноды:

1. Входная нода – используется при подключении. Она видит ваш IP-адрес, но не видит, к чему вы подключаетесь.

2. Средняя нода – та, к которой подключается сам Tor-клиент. Она также не видит ваш IP-адрес или домен, к которому вы подключаетесь, но видит входную ноду и направление трафика.

3. Выходная нода – точка, из которой ваш трафик покидает сеть Tor и перенаправляется на конечный домен. Эта нода знает только то, к чему вы подключаетесь.

Все ноды выбираются случайным образом и периодически меняются.

I2P – это прокси-сервис, который пропускает через себя весь трафик, включая мессенджеры и другие приложения. Он намного медленнее, чем Tor, но обеспечивает и анонимность, и конфиденциальность. Есть также специальные дистрибутивы для операционной системы: их нужно установить на компьютер и перезагрузить его, после чего можно выйти в даркнет. Затем нужно снова перезагрузить компьютер – и все данные о вашей активности исчезают. Сделать что-то, не идентифицировав себя, сейчас практически невозможно. Но есть так называемые уровни анонимности – в зависимости от того, что и от кого вы скрываете.

Tor Browser позволяет достичь высокого уровня анонимности ваших действий в даркнете. Однако провайдер всегда знает, кто вы: у него есть ваши паспортные данные. Он не может отследить конкретные действия внутри дарквеба, не может понять, какой из пользователей внутри многоквартирного дома там находится, но он всегда знает, что мы пользуемся VPN-соединением или Tor Browser.

Для примера математика Д. Богатова обвинили в призывах к терроризму и массовым беспорядкам: его IP-адрес совпал с тем, с которого оставляли экстремистские комментарии на форуме сисадминов. Сам математик объяснял это тем, что поддерживал на своем компьютере выходной узел сети Tor, чтобы его IP-адресом могли пользоваться другие. Все обвинения сняли, но нашли нового обвиняемого из Ставрополя, который признал свою вину. То есть, IP-адрес – это единственная информация, доступная в данном случае ФСБ, МВД и всем желающим. Поэтому внутри самого даркнета можно оставаться анонимным. Однако все зависит от пользователя – что и кому он расскажет. Приставка «дарк» в слове «даркнет» не означает обязательную принадлежность к чему-то незаконному, она говорит лишь о том, что это – сегмент интернета, где все работает немного иначе. И можно перевести ее как «обратную», нежели «темную» сторону».

Помимо теневых форумов с нелегальными активностями даркнет включает в себя большое количество ресурсов, которые не используются для совершения чего-то нелегального: библиотеки без государственной цензуры, аналоги социальных сетей, порталы для общения и многое другое. Надо помнить, что в даркнете пытаются деанонимизировать не конкретных пользователей, а серверы, на которых они общаются. Допустим, мы размещаем сервер в Новой Зеландии, но делаю его доступным только через Tor. Пока никто не знает, где он расположен, все хорошо, но как только это станет известно, к хостеру придут спецслужбы и изымут сервер и все данные на нем. В журнале будет видно, кто посещал сервер, кто его администратор, списки пользователей и сообщений.

Деаниномизируют сервер, как правило, из-за неправильных настроек сайта или браузера: в итоге часть данных передается через открытый интернет, и их можно отследить. Конкретных пользователей ищут намного реже, так как на сервере гораздо больше данных. Такие возможности есть только у спецслужб, которые используют для этого СОРМ (комплекс технических мер для доступа к мобильному и сетевому трафику), и только если пользователи обмениваются трафиком в пределах одной страны.

В даркнете есть множество разных ресурсов, в том числе те, что специализируются на утечках баз данных и продаже информации из них: (сотовые операторы, банки, госслужбы); анонимные почтовые сервисы; порталы для общения и обсуждения любых (в том числе запрещенных) тем; ресурсы для продажи товаров, оборот которых ограничен законодательно или вовсе запрещен; аналоги социальных сетей; онлайн-библиотеки.

Чаще всего в даркнете продают базы данных: данные от взломов аккаунтов – почты, социальных сетей, мессенджеров; расчетные счета и банковские карты, оформленные на подставных лиц; услуги по «пробиву» в базах компаний или госслужб; сервисы по обналичиванию и отмыванию денежных средств; фальшивые документы; анонимные прокси-серверы; услуги различных сотрудников и инсайдеров.

В даркнете представлены различные форумы, которые существуют еще с начала нулевых. В нем огромный пласт киберпреступного сообщества, которое оказывает услуги взлома, нелегального доступа, DDoS-атак и слива баз. Все это можно купить, в том числе, через криптовалюту. Есть специальные посредники, которые гарантируют сделку. У пользователей видны *ник* и данные о количестве проведенных сделок – это главный показатель того, что человеку можно доверять.

В скрытый сегмент *сети* также перебрались лица, осуществляющие офлайн-торговлю незаконными товарами и прочую преступную деятельность, вплоть до заказных убийств. Недавно в Германии закрыли крупнейшую в мире торговую площадку даркнета – DarkMarket. На площадке были зарегистрированы более 500 тыс. человек, которые продавали и покупали запрещенные вещества, фальшивые деньги, украденные кредитные и сим-карты. Всего они совершили более 320 тыс. сделок на сумму €140 млн., более 20 тыс. серверов в Молдавии и Украине конфискованы.

Сейчас базы целиком, как в 2000-х, уже не украсть. Но операторы, которые с ними работают – в полиции, ФМС, банках, сотовых операторах,– оказывают услуги по «пробиву». Здесь работает большая цепочка посредников. Получить банковскую выписку проще всего. Происходит это так: сидит оператор где-нибудь в регионах, проверил кредитную историю двух клиентов, а третья проверка – тот самый «пробив», который он просто фотографирует на телефон. Предотвратить это технически сложно, несмотря на встроенную защиту – системы DLP. Около 60% опрошенных разработчиком российских компаний пострадало от утечек информации и 16% – от промышленного шпионажа. Лишь 12% из них доводили дело до суда. Более чем в 40% случаев виновниками были менеджеры по работе с клиентами, в 22% – бухгалтеры и финансисты, в 20% – менеджеры по снабжению и поставкам. 90% компаний заявили, что их IT-инфраструктура стала намного уязвимее.

В российских госслужбах за последние пару лет ничего кардинально не изменилось: подрядчикам и субподрядчикам точно также отдают недоработанные ТЗ, а информационной безопасности уделяют мало времени. Несмотря на то, что на российском рынке есть такие продвинутые компании, как Group-IB и Positive Technology, пароли от баз данных по-прежнему пишут на стикере и лепят его на компьютер. В итоге главная уязвимость – это физический оператор.

Полностью защититься от утечки невозможно: иначе придется отказаться от мобильного банка, госуслуг и большей части документов. Но можно минимизировать количество данных, которые могут попасть в руки мошенников: не размещайте в сети фото документов, включая электронные билеты и визы; не публикуйте в открытом доступе свою геолокацию или хотя бы делайте это в закрытом профиле; не вводите персональные и платежные данные на подозрительных сайтах; не переходите по ссылкам в письмах и сообщениях, если не уверены в отправителе; используйте разнообразные и сложные пароли в разных аккаунтах. Для этого можно воспользоваться специальным сервисом по подбору паролей. Меняйте пароли не реже, чем раз в три месяца; используйте везде двухфакторную аутентификацию, где это возможно; не указывайте основной номер телефона и e-mail при регистрации на сайтах объявлений или заполнении анкет для получения карт лояльности и кредитов, участия в акциях. Вместо этого пользуйтесь дополнительным или виртуальным номером (такая услуга есть у многих операторов); обращайте внимание на приложения, которые требуют разрешения, не обязательные для их работы (в случае с ОС Android), предупреждения от антивирусного ПО, и сообщения о подозрительной активности или входах в аккаунт с неизвестных устройств.

Проверить, не попал ли ваш e-mail и номер телефона в слитую базу, можно, например, в приложении «Сбербанк Онлайн» в разделах «Безопасность» или «Страхование и защита». Роскомнадзор не может заблокировать сайты в сети Tor еще и потому, что некому выдавать предписания: нет DNS, нет регистратора, нет владельца ресурса. В случае с I2P и подобными сервисами это просто невозможно технически: даже если их заблокировать, тут же появятся новые. Самый радикальный вариант – это аналог китайского файерволла: с его помощью в стране заблокировали многие зарубежные ресурсы. Есть также технология DPI для глубокого анализа и фильтрации пакетов трафика. Ее очень дорого внедрять, но если это сделать,

провайдеры смогут распознавать и блокировать весь подозрительный трафик. Но тогда пользователи просто перейдут в I2P, а потом – еще куда-то, и все потраченные ресурсы будут впустую.

Список литературы:

1. Гарафутдинова Н.Я., Егорова Н.Н., Соловьев А.А. Цифровое мошенничество и методы борьбы с ним // Известия Омского регионального отделения Всероссийского общества охраны природы. Выпуск 16. Омск: ОРО ВООП, 2024. 111 с.

2. Гарафутдинова Н.Я., Поступинских Л.А., Соловьев А.А. О противодействии цифровому мошенничеству // Известия Омского регионального отделения Всероссийского общества охраны природы. Выпуск 16. Омск: ОРО ВООП, 2024. 111 с.

3. Гарафутдинова Н.Я., Селезнева Е.В., Соловьев А.А. Методы кибермошенничества и технологии противодействие им // Известия Омского регионального отделения Всероссийского общества охраны природы. Выпуск 16. Омск: ОРО ВООП, 2024. 111 с.

4. Соловьев А.А., Камшибаев Ж.Ж., Егорова Н.Н., Отс Д.А. Как защититься от телефонных мошенников. / Вектор научной мысли: научный журнал. – №11 (16). СПб., Изд. МИПИ им. Ломоносова, Ноябрь 2024. – С. 132-138.