Даниил Туровский

Вторжение. Краткая история русских хакеров

Под редакцией Александра Горбачева

Издательство Individuum
Москва, 2019

УДК 004.491
ББК 60.54
Т86

Туровский, Даниил.
Т86 Вторжение. Краткая история русских хакеров / Даниил Туровский. — Москва: Индивидуум, 2019. — 296 с.

ISBN 978-5-6042627-3-3

Летом 2016 года неизвестные выложили в интернет переписку высших чинов Демократической партии США — и российские хакеры, предположительно работающие на Кремль, моментально превратились в один из главных сюжетов мировой политики. Спецкор «Медузы», обладатель премии GQ в номинации «Журналист года» и четырех премий «Редколлегия» Даниил Туровский к тому времени писал об этих людях уже несколько лет: одни из них публиковали архивы почты российских чиновников, другие взламывали госсайты сопредельных стран по просьбе спецслужб, третьи просто зарабатывали миллионы, воруя их по всему миру. «Вторжение» — самая полная история российских хакеров: от советских матшкол и постсоветской нищеты к мировой кибервойне и транснациональным преступным группировкам. Книга описывает новый тип власти — но, как показывает Туровский, люди, которые обладают этой властью, сталкиваются все с теми же моральными дилеммами, выбирая между тюрьмой и сумой, чувством и долгом, добром и злом.

УДК 004.491
ББК 60.54

978-5-6042627-3-3

Оглавление

Часть III

Власть

Часть IV

Война

Предисловие

История русских хакеров — это история подростков всего бывшего СССР. Они росли в семьях советских инженеров, в юности читали киберпанк и научную фантастику, покупали на рынках клоны компьютеров IBM — и вдруг оказывались на хакерских форумах, которые часто заменяли им тоскливую русскую жизнь за окном: грязные улицы, бедность, пустое и пугающее в своей неопределенности будущее.

Пока в США рос экономический пузырь доткомов, хакеры запустили в России свою золотую лихорадку: воровство американских кредиток, взлом счетов банков и интернет-магазинов приносили многим миллионы долларов. Кто-то, боясь бандитов или государства, тщательно прятал их — вкладывая в цветочные магазины или пункты шиномонтажа; другие покупали особняки и дорогие спортивные машины; третьи обзаводились домами за границей и уезжали туда, где краски ярче, чем те, что они привыкли видеть за окном, — на Мальдивы, Кипр, в Израиль.

Биографии этих людей часто похожи на остросюжетные боевики. Когда я разговаривал с ними о прошлом, мне часто казалось, что все их проделки были не только ради денег — они как будто хотели стать героями книг и фильмов вроде тех, которые они так любили в детстве.

В юности я много читал журнал «Хакер», который то и дело советовал, как что-нибудь взломать, — все это напоминало обновленную для нового времени «Поваренную книгу анархиста». Я рос в семье, где у каждого был компьютер, а программирование приветствовалось; вечерами изучал коды сайтов — и пробовал их взламывать. В пятнадцать я раздумывал о том, чтобы

пойти после школы учиться на факультет информационной безопасности — а потом, возможно, работать в ФСБ. К счастью, эти раздумья продлились недолго: вскоре я всерьез увлекся текстами, историями, журналистикой.

Тем не менее полутайное хакерское сообщество, попасть в которое мне так и не удалось, время от времени напоминало о себе. Сначала у знакомых взламывали соцсети и просили денег. Позже уже мои собственные аккаунты из-за работы репортером в России атаковали прогосударственные хакеры.

Эта книга про выбор — и про те пути, которые выбирали люди, которые стали частью хакерской субкультуры. Пока одни оставались романтиками и не думали о деньгах (часть I), другие богатели (часть II); когда пришло время обустраивать отношения с государством, кто-то начал работать на него, а кто-то — против (части III и IV).

Книга основана на текстах, которые я в течение последних лет писал для «Медузы» (meduza.io), одного из немногих независимых российских изданий, но не ограничивается ими. Большую часть материалов я собирал в свободное от работы время, изучая форумы, интернет-архивы, книги, встречаясь с хакерами или — чаще — разговаривая с ними в зашифрованных чатах. Я называю этих людей «русскими хакерами», потому что русскоязычное хакерское сообщество осталось единым: россияне, украинцы, белорусы и выходцы из других стран бывшего СССР росли на одних форумах, создавали совместные группировки и продолжали взламывать свои цели вместе, даже когда их государства вели друг с другом войну.

В чем-то эта книга — путеводитель по миру русскоязычных хакеров с последних лет СССР до нынешних времен; в чем-то — энциклопедия главных лиц; в чем-то — расследование о том, как российские власти построили одни из самых боеспособных кибервойск в мире. В книге много отдельных человеческих историй — по ним можно представить себе, в какой обстановке росли хакеры и что определило их дальнейшую судьбу.

В конце концов, это рассказ о том, как незнакомцы, сидящие за компьютерами, могут ссорить между собой страны, разрушать критическую инфраструктуру (например, отключать электричество в целых регионах) и убивать, не ведя при этом никаких боевых действий и не зная своих жертв.

Пролог

Первый беженец кибервойны

22 августа 2015 года бородатый мужчина в очках зашел с двумя рюкзаками в здание Ленинградского вокзала в Москве. Он прошел к кассам, где купил билет на ближайший «Сапсан» — поезд-экспресс, за 4 часа доезжающий до Санкт-Петербурга.

По прибытии мужчина поспешил к стоящим неподалеку от вокзала маршруткам. Он вырос в Петербурге и знал: микроавтобус до Хельсинки — самый дешевый и незаметный способ попасть из России в Европу. Билет стоит 800 рублей; путь занимает 8 часов, которые путешественник проводит в окружении бедных студентов и спекулянтов, везущих из России в Финляндию сигареты, а обратно — бытовую химию.

Через несколько часов мужчина перешел финскую границу и наконец немного выдохнул. Пока его план удавался: он наверняка сбросил хвост. Он все хорошо продумал: не полетел на самолете, потому что его бы задержали на паспортном контроле; билет на поезд покупал не в интернете, а прямо в кассе на вокзале. Мужчина вспомнил свой предыдущий побег из привычной жизни: десять лет назад он проезжал на троллейбусе мимо вокзала в Петербурге и спонтанно решил переехать в Москву к своей девушке. Вышел на следующей остановке, купил билет на поезд — и уехал на нем навсегда. С девушкой они потом поженились.

В Хельсинки мужчина сел на паром до Стокгольма, а в Швеции обратился к местным правозащитникам, попросив помочь с политическим убежищем. Те отправили его обратно в Финляндию: по европейскому законодательству просить убежище можно только в той стране, через которую человек въехал в Евросоюз.

Вернувшись в Хельсинки, бородатый мужчина нашел помещение с вай-фаем и написал письмо на общую редакционную почту «Медузы», где я работал специальным корреспондентом. Его почтовый адрес по-русски выглядел бы как «Мертваярука1984» — это отсылало одновременно и к антиутопии Джорджа Оруэлла, и к системе «Периметр», комплексу автоматического управления ответным ядерным ударом, созданному в СССР в разгар холодной войны. В Америке «Периметр» называли «Мертвой рукой»: система была придумана так, чтобы запустить ядерные бомбы, даже если все, кто мог это сделать вручную, к тому времени были бы убиты.

В письме мужчина представился Александром Вярей, одним из руководителей *Qrator Labs* — российской компании, занимающейся защитой от DDoS-атак (см. глоссарий). Он рассказал, что российские чиновники и спецслужбы интересуются кибероружием, а он сам был свидетелем того, как оно применялось по распоряжению государства.

«Сейчас, когда в РФ обстановка накаляется, я опасаюсь, что меня могут „припахать“ заниматься организацией атак, так как я уже „в теме“, и я принял решение поставить общественность в известность, — писал Вяря (здесь и далее в цитатах героев сохранены авторские особенности орфографии и пунктуации). — Я считаю, что граждане должны знать, на что тратятся деньги в условиях кризиса. И КТО занимается этими грязными делами. Это не какие-то мелкие жулики. Если раньше все только догадывались, то теперь у вас есть доказательства:) Чтобы меня внезапно не переехала машина, например, мне пришлось покинуть страну. Это решение мне далось очень нелегко, я, считай, потерял хорошую работу, уезжаю от семьи просто в никуда. Плюс сейчас всякие шлюхи вроде *Lifenews* будут меня „мочить“».

Я ответил, что хотел бы подробнее узнать его историю и встретиться лично. Наш разговор сразу же перешел в секретный чат в Telegram — в России 2015 года уже массово начали

пользоваться защищенными чатами, понимая, что российские спецслужбы могут слушать и читать открытые каналы, хотя по закону и должны сначала получить на это разрешение суда.

— Как быстро вы сможете приехать? Собираюсь идти сдаваться и просить защиты, — написал Вяря.

— Послезавтра?

— Оу.

— Долго?

— Нужно остановиться где-то сначала.

— Могу и завтра попробовать.

— Ох, я постараюсь найти какой-нибудь отель, у меня всего 4к на карте осталось.

Вяря остановился в общей комнате одного из городских хостелов. Хельсинки — дорогой город, но ему повезло и он нашел ночлег за 20 евро в сутки. На следующее утро, когда я садился в самолет, я получил от него сообщение: «Непередаваемый экспириенс с хостелом, я впервые. Храпят, говорят во сне, ворочаются всю ночь».

Вскоре мы встретились у торгового центра неподалеку от набережной. Вяря стоял около дверей, нервно оборачиваясь и выглядывая меня среди переходящих через трамвайные пути. Все вещи — два рюкзака — были у него с собой. Мы зашли в ближайшее кафе, заказали кофе, и он начал рассказывать о том, что с ним произошло.

***

Александр Вяря родился в середине 1980-х в ленинградской коммуналке и рос без отца. Когда ему было двенадцать, он увлекся компьютерами — сначала видеоиграми, потом программированием и «железом». Первой его работой была должность системного администратора в компании его двоюродного дяди. Социальные сети тогда только начинали появляться,

но аккаунты в них Вяря не заводил принципиально: не хотел оставлять никаких следов в интернете.

Переехав в Москву, он поработал сетевым инженером в нескольких хостинг-компаниях. В 2012 году он обнаружил на одном из профильных форумов интересную вакансию — и после пары тестовых заданий его взяли в компанию *Qrator*, специализирующуюся на защите от DDoS-атак.

К тому времени она уже лидировала на рынке: среди ее клиентов были и многие независимые СМИ (телеканал «Дождь», «Новая газета», «Ведомости»), и банки («Альфа», «Тинькофф»), и интернет-магазины («Юлмарт», *Lamoda*). По словам Вяри, их услугами даже однажды воспользовался интернет-магазин по продаже кедровых бочек; что удивительно — именно на него была совершена самая серьезная атака за все время его работы в компании. «В России популярно сводить счеты с конкурентами с помощью DDoS-атак, некоторым магазинам один день простоя стоит закрытия», — объяснял он. Такие атаки стоят очень дешево (около 3 тысяч рублей в сутки) и могут при этом вывести незащищенный сайт из строя, что приведет к серьезным убыткам.

Вяря работал в техподдержке и постоянно отвечал на звонки клиентов. Нередко в *Qrator* обращались те, кто недоволен тем, что она защищает в том числе оппозиционные сайты. Весной 2012-го — накануне инаугурации президента Владимира Путина — прогосударственные хакеры-патриоты атаковали сайты «Эха Москвы», «Коммерсанта» и «Дождя» — все они были клиентами *Qrator*. «Зачем же вы защищаете евреев?» — сказал Вяре один из позвонивших в тот день.

Во время выборов мэра Москвы в 2013 году *Qrator* защищал сайт Алексея Навального: оппозиционный политик выдвинул свою кандидатуру и вел успешную кампанию. В какой-то момент Вяря заметил возле офиса компании фургон с тонированными стеклами и антеннами на крыше. В следующие дни он появлялся там почти каждый день. Выходя на обед,

сотрудники *Qrator* пытались заглянуть в фургон и шутили, что тем, кто их прослушивает, надо бы принести пончики.

«Саша — талантливый человек, но очень впечатлительный и с тараканами в голове, — сказал мне его бывший начальник Александр Лямин. — Когда слишком долго работаешь в информационной безопасности, начинаешь меняться, начинаешь во всем видеть угрозу себе».

Так или иначе, к 2015 году Вярю повысили до руководителя службы эксплуатации. Он начал часто ездить за границу: приходилось посещать дата-центры, расположенные в европейских странах, чтобы устанавливать программное обеспечение, способное работать при больших нагрузках — во время атак. В *Qrator* такие серверы с фирменным ПО называют «центрами очистки трафика». Они помогают окружать сайты клиентов виртуальным «забором» с «пограничными пунктами», которые отфильтровывают здоровый трафик от паразитного.

Тогда же компания начала подготовку к открытию первого зарубежного отделения в Праге. Всем сотрудникам делали рабочие визы. Возглавить филиал должен был Вяря.

3 февраля 2015 года генеральному директору *Qrator* Александру Лямину позвонил Вартан Хачатуров, заместитель главы департамента инфраструктурных проектов Минкомсвязи. Хачатуров попросил кого-то из сотрудников компании помочь чиновникам с одним «щекотливым вопросом». Кроме Вяри помогать было некому: все разъехались по конференциям.

Хачатуров связался с Вярей и оставил номер телефона, на который тот отправил сообщение. Ближе к вечеру раздался звонок: звонил некий Василий Бровко. Вяря понятия не имел, кто это. Бровко сказал ему, что через пару дней им вместе необходимо слетать в столицу Болгарии, Софию; все необходимые документы оформит его помощница.

Вяря поискал в интернете информацию о Бровко и схватился за голову. Больше всего ему запомнилось, что тот основал компанию «Апостол», которую Алексей Навальный весной 2013 года

обвинял в том, что она с помощью ботов раскручивала соцсети «Аэрофлота». В последнее время Бровко работал начальником департамента коммуникаций в «Ростехе» — госкорпорации, созданной для производства высокотехнологичной продукции гражданского и военного назначения. Руководил ею Сергей Чемезов, близкий знакомый Владимира Путина.

Вяря предположил, что от него хотят помощи по его профилю — выбрать новую систему защиты от DDoS. Но удивился, что позвали в Болгарию: известные производители соответствующего программного обеспечения находятся в Израиле и Штатах.

5 февраля 2015 года он прилетел в Софию. Отправил сообщение Бровко; тот ответил, что встреча состоится во второй половине дня. Вяря погулял по центру, потом подошел к назначенному месту — помпезному стеклянному зданию *Grand Hotel Sofia*.

Вскоре появился Бровко. В одной руке у него был смартфон российского производства, а в другой айфон; он постоянно что-то на них набирал. Вяря поприветствовал Бровко и сказал, что София — удивительно небольшой город. «Помойка», — бросил Бровко в ответ.

Следом появились двое мужчин. Они оказались сотрудниками местной компании *Packets Technologies* (сайт[1] компании скромно сообщает, что организация специализируется на «разработке передовых сетевых технологий»). Бровко сказал Вяре, что нужно сходить в офис компании: «посмотреть продукт» и высказать свое мнение.

Офис располагался неподалеку. В переговорной один из сотрудников *Packets Technologies* включил презентацию, а заодно рассказал о себе: работал в израильской армии, консультировал по сетевой безопасности крупнейшие интернет-компании, участвовал в *Black Hat* (главная мировая конференция по информационной безопасности, на которую приезжают и представители IT-корпораций, и хакеры).

После этого сотрудник болгарской компании, как утверждает Вяря, заявил: «Сейчас я вам представлю продукт для организации DDoS-атак». Названия у программного обеспечения не было. Сотрудник добавил, что «продукт» умеет организовывать DDoS-атаки на сетевом уровне. Такие атаки «забивают» ресурсы сервера паразитными пакетами, из-за чего система перестает принимать полезные пакеты трафика.

Система представляла собой небольшое устройство — «коробку» с программным обеспечением, установленную на одном из трафикообменников. Для «продукта» была выделена специальная полоса с максимальной мощностью в 10 Гбит/с. Специалисты *Packets Technologies* добавили: система позволяет совершать «коктейльные» — то есть смешанные по типам — атаки, которые труднее всего отражать; кроме того, можно легко увеличить трафик, установив еще одну «коробку». В 2010 году атака силой 10 Гбит/секунду была совершена на серверы *Wikileaks*; мощность крупнейшей DDoS-атаки[2] в истории интернета — голландский хостер *Cyberbunker* против компании *Spamhaus* — достигала 300 Гбит/секунду: как писали в *The New York Times*, она «замедлила интернет».

Закончив с теоретической частью, сотрудник компании запустил VPN-соединение и Tor-браузер, обеспечив себе анонимность (начало такой атаки отследить практически невозможно). Набрал в браузере IP-адрес — открылась страница с крайне простым интерфейсом. Наверху размещалась адресная строка, ниже — около десятка названий подвидов DDoS-атак, рядом с каждой — пустая ячейка, которую можно отметить галочкой. Внизу — кнопка для выбора мощности атаки: от 100 мегабит до 10 гигабит в секунду. «Можно не на всю катушку, если жертве достаточно поменьше», — поясняет Вяря.

Сотрудники компании ввели в строке интерфейса адрес сайта министерства обороны Украины. В соседнем окне открыли страницу сервиса, по которому можно определять работоспособность сайтов. Затем включили программу в полную

силу. Возник график, показывающий мощность атаки — вскоре она достигла 10 Гбит/с. Сервис работоспособности показал, что сайт недоступен. Его попробовали открыть в браузере, но он не загрузился. Через пару минут атаку остановили и сайт снова стал открываться.

Потом они попробовали атаковать сайт украинского министерства обороны на мощности в 100 Мбит/с — он снова перестал работать.

«Давайте проверим на slon.ru», — предложил Бровко, до этого молчавший (я воспроизвожу его реплику со слов Вяри). «Слон» (сейчас называется *Republic*), одно из самых популярных независимых новостных СМИ в России, атаковали на мощности 10 Гбит/с. Сайт перестал открываться и лежал несколько минут. Позже тогдашний главный редактор «Слона» Максим Кашулинский подтвердил мне, что 5 февраля 2015 года они зафиксировали атаку, которая на две минуты обрушила сайт.

«А что, если сайты пользуются защитой? Пробьете?» — спросил Вяря. Ему ответили, что в этом случае придется узнавать реальный адрес сервера (все сервисы защиты пропускают атаку через себя, а реальный адрес сервера маскируют), но у *Packet Technologies* есть соответствующая методика. Вяря уточнил, сколько стоит система; по его словам, Бровко ответил: «Около миллиона долларов».

После встречи Вяря и Бровко отправились в *Grand Hotel Sofia*. Сели в лобби, взяли кофе. Вяря вспоминает, что Бровко больше всего интересовало, как найти реальный адрес сайта и на каких трафикообменниках лучше всего ставить такую систему. Через некоторое время сотрудник «Ростеха» якобы сказал: «Ну что, нам нужен кто-то, кто будет этим управлять». Вяря поперхнулся и сказал: «Нет, извините. Я не хакер. Это против моих принципов, и это противозаконно». Бровко, по словам Вяри, спросил: «Ты знаешь, какая организация тебя сюда пригласила?» Вяря предположил, что он намекает на ФСБ, но вслух сказал, что впредь готов только отвечать на вопросы по технической части. Они добавили друг друга в *Telegram* и разошлись.