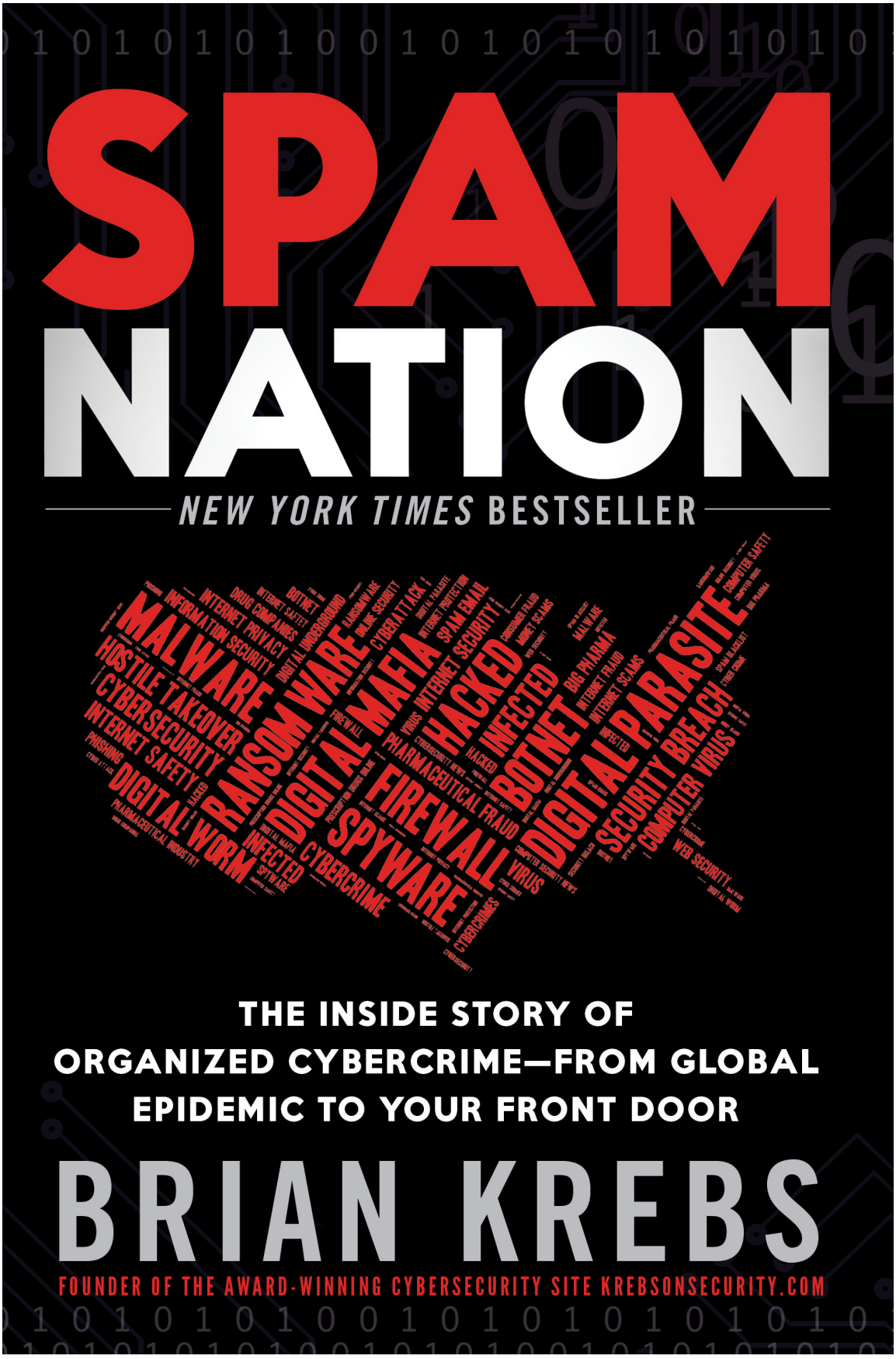
Спамерская нация. Внутренняя история организованной киберпреступности

Русский перевод расследования Брайана Кребса об организованной киберпреступности, спам-партнёрках, ботнетах, платёжных системах и борьбе с преступной инфраструктурой.

Больше крутых материалов в моём телеграм-канале @grogrigs

Вводные материалы



SPAM NATION

Бестселлер New York Times

Внутренняя история организованной киберпреступности: от глобальной эпидемии до вашего порога

Брайан Кребс

Основатель отмеченного наградами сайта о кибербезопасности KrebsOnSecurity.com.

Красная типографическая карта Соединённых Штатов составлена из многократно повторяющихся терминов: вредоносные программы, враждебный захват, кибербезопасность, безопасность в Интернете, цифровой мир, информационная безопасность, конфиденциальность в Интернете, вымогательство, цифровое подполье, фармацевтические компании, ботнет, межсетевой экран, кибератака, спам-письмо, интернет-безопасность, взлом, заражение, большая фарма, интернет-мошенничество, интернет-аферисты, контрафакт, фармацевтическое мошенничество, вирус, цифровой паразит, нарушение безопасности, компьютерный вирус, веб-безопасность, шпионские программы, киберпреступность и фишинг.

Титульный лист

SPAM NATION

Внутренняя история организованной киберпреступности: от глобальной эпидемии до вашего порога

Брайан Кребс

Sourcebooks

Выходные данные

Дизайн обложки: The Book Designers.

Издано Sourcebooks, Inc.

P.O. Box 4410, Naperville, Illinois 60567-4410
(630) 961-3900
Факс: (630) 961-2168
sourcebooks.com

Каталожные данные Библиотеки Конгресса

Кребс, Брайан.

Spam Nation: внутренняя история организованной киберпреступности: от глобальной эпидемии до вашего порога / Брайан Кребс.

страниц, см

1. Компьютерные преступления - Соединённые Штаты. 2. Мошенничество в Интернете - Соединённые Штаты. 3. Спам (электронная почта). 4. Фишинг. 5. Организованная преступность - Соединённые Штаты. I. Заглавие.

HV6773.2.K74 2014
364.16’80973-dc23
2014023007

Напечатано и переплетено в Соединённых Штатах Америки.

VP 10 9 8 7 6 5 4 3 2 1

Посвящение

Моему BizMgr.

Кто есть кто в кибермире

ПАВЕЛ ВРУБЛЕВСКИЙ, также известный как RedEye, - сооснователь ChronoPay, процессинговой компании для высокорисковых карточных платежей и поставщика платёжных услуг, тесно связанного с индустрией мошеннических антивирусов. Сооснователь партнёрской программы интернет-аптек Rx-Promotion.

ЮРИЙ КАБАЕНКОВ, также известный как Hellman, - совладелец Rx-Promotion вместе с Павлом Врублевским.

ИГОРЬ ГУСЕВ, также известный как Desp, - сооснователь ChronoPay и совладелец партнёрских программ аптечного спама SpamIt и GlavMed.

ДМИТРИЙ СТУПИН - совладелец, наряду с Игорем Гусевым, партнёрских аптечных программ SpamIt и GlavMed.

ИГОРЬ ВИШНЕВСКИЙ - спамер, помогавший разрабатывать спамерский ботнет Cutwail, а некогда также деловой партнёр крупного спамера Дмитрия Нечволода по прозвищу Gugle.

ДМИТРИЙ НЕЧВОЛОД, также известный как Gugle, - один из наиболее успешных спамеров SpamIt и Rx-Promotion. Gugle сдавал свой спамерский ботнет Cutwail в аренду многим другим распространителям нежелательной почты.

ГЕННАДИЙ ЛОГИНОВ - белорус и руководитель военизированной организованной преступной группировки, известной как The Village. Партнёр Александра Рубацкого, участвовавший в похищении с целью получения выкупа Евгения Петровского по прозвищу Pet, конкурирующего предпринимателя.

АЛЕКСАНДР РУБАЦКИЙ - белорусский хакер, тесно связанный с индустрией детской порнографии, который позднее основал Russian Business Network (RBN) в Санкт-Петербурге, Россия.

ЕВГЕНИЙ ПЕТРОВСКИЙ, также известный как Pet, - белорусский владелец компаний Sunbill и BillCards, сетей обработки платежей по кредитным картам, которые были глубоко вовлечены в обработку платежей для сайтов с детской порнографией.

НИКОЛАЙ МАККОЛО, также известный как Kolya, - молодой предприниматель, стоявший за McColo Corp., которая до своего краха в 2008 году была одним из самых популярных поставщиков веб-хостинга в преступном киберподполье.

ЛЕОНИД КУВАЕВ - осуждённый спамер, управлявший партнёрской программой аптечного спама RxPartners. В настоящее время Куваев отбывает в России десятилетний тюремный срок за растление детей и детскую порнографию.

ИГОРЬ И ДМИТРИЙ АРТИМОВИЧИ, также известные как Engel, - братья, которые, предположительно, управляли спамерским ботнетом Festi и были близкими союзниками Врублевского. В 2013 году братьев признали виновными в использовании Festi для атаки на сайт Assist, конкурента ChronoPay, хотя они это отрицают.

COSMA - спамер, работавший и на GlavMed-SpamIt, и на Rx-Promotion, а также главный автор огромного ботнета Rustock.

SEVERA - спамер, работавший и на GlavMed-SpamIt, и на Rx-Promotion, и предполагаемый автор ботнетов Waledac и Storm.

Предисловие

После выхода первого издания *Spam Nation* в твёрдом переплёте я выступал на многочисленных мероприятиях и встречах с читателями, посвящённых проблемам киберпреступности и кибербезопасности. Мне часто задают вопрос: «Почему вы решили включить слово spam в название своей книги? Нежелательная почта никому не нравится, так зачем кому-то вообще открывать такую книгу?» Кроме того, читатели, похоже, недоумевают, почему на обложке изображены Соединённые Штаты, если столь многие киберпреступники, о которых я пишу, находятся в России и бывших советских республиках.

Я выбрал это название по нескольким причинам. Во-первых, нравится нам это или нет, но спам служит основным средством совершения большинства киберпреступлений. Большинство людей связывает спам с нежелательной почтой, которой, как им кажется, можно не придавать значения. Однако это понятие охватывает и вредоносные письма, в том числе послания со зловредными программами, замаскированными под вызывающие доверие вложения, а также фишинговые атаки, предназначенные для кражи ваших банковских реквизитов и другой учётной информации.

Во-вторых, я хотел показать, что - по крайней мере традиционно - американцы были и причиной существования, и главной мишенью большей части спама и киберпреступности. Спама не было бы, если бы его рассылка не приносила прибыли, а невероятные миллионы американских потребителей откликаются на спам и совершают покупки по таким сообщениям, тем самым поддерживая цикл мошенничества и злоупотреблений, от которого страдаем все мы.

Наконец, как подробно рассказано в главе 2, первые пионеры киберпреступности, создавшие большую часть спамерской индустрии, смогли это сделать потому, что годами беспрепятственно действовали с площадок американских хостинг-провайдеров. Те, казалось, либо совершенно не сознавали, какой репутацией обладают выбранные ими деловые партнёры, либо намеренно закрывали на это глаза. Но в последнее время игнорировать действия этих спамеров и хакеров стало невозможно ни для кого из нас, потому что теперь они бьют по самому больному месту - по нашим кошелькам.

Стефани Боуэн, мой любезный и настойчивый редактор в Sourcebooks, добивалась, чтобы в первом издании *Spam Nation* в твёрдом переплёте обсуждалась эпидемия взломов с кражей данных кредитных карт, которая за последний год охватила магазины по всему миру, но прежде всего здесь, в Соединённых Штатах. В то время мне казалось, что эта тема не вполне вписывается в ход повествования, однако Стефани всё равно ухитрилась вставить в главу 1 упоминание о взломе Target Corporation в декабре 2013 года.

Поразмыслив ещё, я теперь понимаю, что она была права: эти кражи карточных данных могут многое рассказать о состоянии современной организованной киберпреступности, которой в значительной степени посвящена эта книга. Стоит отметить, что взлом Target начался со спам-письма, отправленного поставщику услуг отопления, вентиляции и кондиционирования воздуха, который работал с Target и имел удалённый доступ к отдельным участкам её сети. В спам-сообщении находилась вредоносная программа, замаскированная под документ, связанный с деятельностью компании. Проникнув в компьютеры подрядчика, злоумышленники смогли воспользоваться этим доступом, чтобы взломать сеть Target. Остальное уже история.

По словам источников, с которыми беседовал автор, вредоносную программу отправила подрядчику сеть взломанных компьютеров, известная как ботнет Cutwail, - та самая машина для рассылки преступного спама, которую построили два персонажа, подробно описанных в этой книге. Как я писал в последней главе *Spam Nation*, в наши дни киберпреступники, управляющие огромными спамерскими механизмами, тратят всё больше ресурсов на выпуск вредоносного спама, нацеленного на учётные данные потребителей, и всё меньше - на коммерческую рекламу

сомнительных товаров вроде поддельных лекарств.

Мне удалось первым рассказать о взломе Target, потому что воры, похитившие у торговой сети сорок миллионов номеров кредитных и дебетовых карт, затем выставили их на продажу на открытых сетевых базарах. Я установил, что источником украденных карт была Target, обнаружив их и воспользовавшись теми же пробелами в знаниях финансовой отрасли, которые преступники используют для кражи данных, но я делал это, чтобы помочь компаниям разобраться в причинах этих кибератак.

Что это за пробелы? Ещё до того, как был обнаружен взлом Target, я потратил много времени на установление связей с источниками в небольших банках, которые, казалось бы, должны стремиться вкладываться в кибербезопасность ради защиты собственных средств и активов своих клиентов. Многих читателей это, возможно, удивит, но специалистам по борьбе с мошенничеством во многих таких учреждениях на самом деле обычно не хватает денег или ресурсов, а происходящее на подпольных рынках киберпреступности они видят далеко не во всей полноте. Вместе с тем эти банки - а их существуют тысячи - весьма охотно делятся информацией, если считают, что взамен получат более качественные сведения о тенденциях мошенничества, способных обойтись им в крупную сумму, например заблаговременное предупреждение о серьёзном взломе торговой сети.

Крупные банки с Уолл-стрит платят компаниям, занимающимся киберразведкой, за поиск и передачу сведений о том, как брендами этих банков злоупотребляют на скрытых сетевых форумах и рынках. Поэтому большие банки располагают гораздо более целостной картиной мошеннических схем. Этому помогает и сам их размер - огромное количество счетов, которыми они управляют, - и то, что эти колоссальные учреждения участвуют во множестве направлений финансовой деятельности. Когда происходит крупное мошенничество вроде взлома Target, они обычно замечают всплески обмана сразу в нескольких направлениях бизнеса. Поэтому у них больше возможностей распознать мошенничество сразу после его начала, если только оно достаточно масштабно.

Поразительно, что Visa, MasterCard и другие платёжные системы сообщают банкам о конкретных выпущенных ими клиентских картах, которые, по заключению этих систем, были скомпрометированы при взломе торговой компании, но не говорят банкам, какой именно продавец был взломан. Крупные банки обычно способны сами выяснить, какого продавца взломали, - опять же, если инцидент достаточно велик. Небольшие же банки мечутся, пытаясь установить виновного, чтобы впредь блокировать операции у скомпрометированного продавца и ограничить свои финансовые потери от мошенничества с этими картами.

Примечательно, что организованные киберпреступники пользуются именно этим разрывом в финансовой системе: чем дольше банки топчутся на месте, пытаясь выяснить, кого взломали, тем дольше преступники, взломавшие продавца, могут сбывать украденные карты и получать прибыль. Тем временем платёжные системы продолжают взимать комиссии с банков и продавцов за операции независимо от того, законны они или нет. Поэтому, если вы хотите узнать, кого только что взломали, лучшие сведения найдутся в подпольных магазинах, а не у компаний по информационной безопасности или платёжных ассоциаций.

Мне, во всяком случае, стало ясно, что вся система кредитных карт в Соединённых Штатах сейчас устроена так, что любой участник операции может надёжно переложить вину за происшествие, спор или мошенничество на другого участника. Главная причина, по которой Соединённые Штаты до сих пор полностью не перешли на более безопасный стандарт работы с кредитными картами, такой как карты с чипом и ПИН-кодом, во многом заключается в многолетних взаимных обвинениях банков и розничной торговли. Банки говорили: «Если бы продавцы только начали устанавливать терминалы для карт с чипом и ПИН-кодом, мы бы начали выпускать такие карты». Продавцы отвечали: «Зачем нам тратиться на модернизацию всех платёжных терминалов для работы с

чипом и ПИН-кодом, когда почти ни один банк не выпускает такие карты?» Так продолжалось годами, а киберпреступники тем временем атаковали одну крупную торговую сеть за другой и со смехом шли к банкомату.

Те же преступные машины, которые выбрасывают в сеть потоки спама, обычно применяются и для грубых атак типа «отказ в обслуживании», лишающих людей, компании и организации доступа к Интернету. За последние месяцы атаки типа «отказ в обслуживании» достигли эпического размаха. Мой сайт KrebsOnSecurity.com уже почти год подвергается практически непрерывным атакам. Те же злоумышленники, которые атаковали мой сайт, использовали свою преступную машину, чтобы 25 декабря 2014 года отключить от игровых сетей Sony и Microsoft миллионы пользователей.

При этом хочу подчеркнуть: причина вовсе *не* в том, что заблудшие юнцы, управляющие этими атаками, являются сколько-нибудь искушёнными хакерами. Напротив, большинство из них, вероятно, не сумело бы взломать даже бумажный пакет. Но печальная правда состоит в том, что сегодня стало поразительно легко проводить массированные атаки, способные надолго лишить доступа к сети компании из списка Fortune 500.

Большинство этих атак запускается через преступные сетевые сервисы, работающие по принципу «наведи и щёлкни», причём многие из них принимают даже PayPal. Некоторые такие сервисы получают мощность для атак от захваченных взломанных компьютеров, но большая их часть, по-видимому, пользуется тем, что сейчас к Интернету подключено более тридцати миллионов неправильно настроенных или безнадёжно устаревших систем. В основном это старые DSL-маршрутизаторы, которыми пользуются такие же люди, как вы и я, и которые нам зачастую предоставляют операторы кабельной связи и интернет-провайдеры. Эти устройства можно удалённо и без малейшего труда обратить в орудие сокрушительных атак. Часть таких систем находится здесь, в Соединённых Штатах, но подавляющее большинство размещено в сетях интернет-провайдеров развивающихся стран по всему миру.

Мне хотелось бы увидеть более глобальные и систематические усилия, направленные на резкое сокращение числа этих устаревших, в основном неремонтопригодных и незащищённых систем. Подобно тому как мы финансируем борьбу с полиомиелитом, малярией и другими предотвратимыми заболеваниями, которые ежегодно убивают миллионы людей, у нас нет сколько-нибудь убедительного оправдания отказу профинансировать целенаправленную замену таких систем ради безопасности наших данных, компаний и личностей, не говоря уже об экономии миллиардов долларов в долгосрочной перспективе. Разумеется, это обойдётся дорого, но, возможно, для Интернета стоило бы создать своего рода виртуальное «товарищество домовладельцев», в которое Соединённые Штаты и их состоятельные союзники ежегодно вносили бы средства на решение некоторых проблем киберпреступности и небольшую уборку в нашем общем квартале. Даже умеренно успешная программа искоренения не сократит число уязвимых для злоупотреблений систем с тридцати миллионов до нуля за одну ночь, но приблизиться к нулю вполне возможно, и этим стоит заняться.

К слову, в конце 2014 года Sony подверглась кибератаке другого рода. Её подразделение Sony Pictures Entertainment стало жертвой масштабного взлома, при котором злоумышленники похитили гигантские объёмы данных о сотрудниках и конфиденциальной информации Sony, после чего пригрозили обнародовать эти сведения, если руководство компании не выплатит выкуп. Sony отказалась, и хакеры выложили данные в Интернет на всеобщее обозрение. Кроме того, они запустили во внутренние сети компании вредоносную программу, предназначенную для уничтожения значительной части её внутренних компьютерных систем.

Правительство США публично заявило, что считает ответственными за вредоносную атаку на Sony северокорейских хакеров, однако многие представители сообщества специалистов по безопасности по-прежнему не убеждены в этой версии событий. Тем не менее эта атака стала идеальным завершением года, отмеченного всё более разрушительными нападениями, целью

которых были кража данных и вымогательство как у корпораций, так и у других компаний.

Эта стремительно растущая киберугроза, известная как ransomware, шифрует все файлы, фотографии, видеозаписи и документы на вашем компьютере до тех пор, пока вы не заплатите произвольно назначенную сумму, чтобы получить их обратно. Возможно, неудивительно, что ransomware чаще всего распространяется через вредоносный спам, но заражение происходит и тогда, когда пользователи Интернета не прививают своим компьютерам последние обновления безопасности программного обеспечения.

Сегодняшний Интернет - поистине преобразующий мир инструмент общения и обучения, который ежедневно невероятно обогащает жизнь миллиардов людей. И всё же никогда прежде за всю историю Интернета эта среда не была настолько наполнена ловушками и негодяями, стремящимися обобрать неосторожных. Возможно, вы не понимаете ценности своего компьютера, подключения к Интернету, почтового ящика или цифровых файлов, но я гарантирую: злоумышленники её понимают и научились весьма искусно извлекать из этих цифровых активов всю их стоимость.

Каждому из нас, кто пользуется сетью, отведена важная роль в том, чтобы сделать Интернет более безопасным и полезным местом. Но не заблуждайтесь: те, кто предпочитает в блаженном неведении уклоняться от своей роли в решении проблемы, почти неизбежно сами становятся частью проблемы. Вот почему так важно прочитать эту книгу: она поможет вам понять собственную роль во всём происходящем, узнать, как этому воспрепятствовать, и защитить себя.

Советы о том, как защитить себя и своих близких от новейших сетевых атак и мошеннических схем, вы также найдёте в последней главе этой книги. Берегите себя.

Брайан Кребс

Глава 1. Паразит

Тёмно-синий BMW 760 подъехал к пешеходному переходу у светофора в центре Москвы. Рядом остановился чёрный Porsche Cayenne. Было два часа дня, воскресенье, 2 сентября 2007 года, и на обычно переполненных улицах возле прославленной Сухаревской площади почти не было машин: лишь туристы и местные жители прогуливались по широким тротуарам с обеих сторон бульвара. Дневное солнце, весь день согревавшее улицы, уже клонилось к горизонту, и близлежащие исторические здания отбрасывали всё более длинные тени.

Водитель BMW, печально известный местный мошенник под хакерским псевдонимом Jaks, в тот день только что стал отцом. Он и его пассажир отметили это событие изрядным количеством водки. Время и место идеально подходили для того, чтобы разрешить давнее соперничество с водителем Porsche и выяснить, чья машина быстрее. Оба водителя взревели двигателями, без слов договариваясь наперегонки преодолеть короткий прямой отрезок до большой городской площади впереди.

Когда загорелся зелёный, визг шин по асфальту эхом прокатился на сотни метров по главной площади. Прохожие обернулись посмотреть, как мощные машины рванули с перекрёстка, не уступая друг другу и разгоняясь до безумной скорости.

Промчавшись середину дистанции на скорости свыше 200 километров в час, Jaks внезапно потерял управление, задел Porsche и врезался в огромный металлический фонарный столб. Соревнование закончилось мгновенно, и победителя не было. BMW разорвало надвое, а неподалёку остался дымящийся искорёженный Porsche. Водители обеих машин выбрались из обломков и, хромая и ползя, покинули место аварии. Но пассажир BMW, подававший большие надежды двадцатитрёхлетний интернет-предприниматель Николай Макколо, погиб на месте: его почти обезглавленное тело оказалось зажато под роскошным автомобилем.

Коля, как Макколо называли друзья, был небольшой знаменитостью в преступном киберподполье и самым молодым сотрудником семейной компании интернет-хостинга, носившей его фамилию, McColo Corp. В то время правоохранительные органы разных стран лишь начинали осознавать финансовые и организационные угрозы со стороны организованной киберпреступности, а McColo Corp. уже заслужила репутацию её эпицентра: места, где киберпреступники могли надёжно обосноваться, почти не опасаясь, что иностранные следователи обнаружат их сетевые вложения и схемы или поставят их под угрозу.

К моменту гибели Коли хостинг-провайдер его семьи служил главной базой для крупнейших в мире предприятий, которые рассылали нежелательную почту, или спам, через роботизированные сети. Такие сети, сокращённо называемые ботнетами, состоят из персональных компьютеров, которые были взломаны и заражены вредоносными программами, позволяющими злоумышленникам управлять системами издалека. Обычно владельцы этих компьютеров даже не подозревают, что их машины захвачены.

Почти все ботнеты, которыми управляли с площадок McColo, были созданы для массовой рассылки незапрошенной рекламной почты, ежедневно переполняющей наши входящие сообщения и спам-фильтры. Однако серверы McColo не создавали и не рассылали спам сами: это привлекло бы слишком много внимания интернет-активистов и западных правоохранительных органов. Вместо этого владельцы ботнетов лишь использовали серверы, чтобы превращать миллионы разбросанных по всему миру персональных компьютеров в изрыгающих спам зомби.

К тому времени, когда медики убрали последствия аварии Коли, жуткие фотографии побоища уже загружали на закрытые российские интернет-форумы, которые посещали друзья и деловые клиенты Макколо. Одними из первых о смерти Коли сообщили обитатели Crutop.nu, русскоязычного хакерского форума, среди восьми тысяч участников которого были крупнейшие спамеры мира. Те

же участники Crutop.nu, которые распространяли фотографии и новости о происшествии, входили в число самых успешных клиентов хостинга McColo. Многие сочли себя обязанными пожертвовать деньги на похороны Коли или сделали это под публичным давлением администраторов форума. Для преступного киберподполья это было крупное событие.

Через несколько дней разношёрстная компания московских спамеров собралась на панихиде, чтобы проститься с ним. Церемония состоялась в той же церкви, где Колю крестили менее двадцати трёх лет назад. Среди присутствовавших были Игорь Гусев по прозвищу Desp и Дмитрий Ступин по прозвищу SaintD, совместные администраторы SpamIt и GlavMed, до недавнего времени крупнейших в мире спонсоров спама[1], а также две фигуры, которым предстоит сыграть ключевые роли в этой книге.

На церемонии присутствовал и Дмитрий Нечволод по прозвищу Gugle, в то время двадцатипятилетний хакер, тесно связанный с ботнетом Cutwail. Cutwail представляет собой огромную преступную машину, которая заразила десятки миллионов домашних компьютеров по всему миру и тайно захватила над ними управление для рассылки спама. Нечволод уже заработал миллионы долларов, используя этот ботнет, чтобы отправлять нежелательную почту GlavMed и SpamIt миллионам людей во всём мире. По сей день Cutwail остаётся одним из крупнейших и наиболее активных спамерских ботнетов, хотя теперь им почти наверняка управляет множество разных людей. Подробнее об этом рассказывается в главе 7 «Знакомство со спамерами».

Почему же важно отметить присутствие этих троих на столь значимом для киберпреступного мира событии? Потому что их работа, как и работа Коли и сотен других людей, ежедневно странным, но весьма существенным образом влияет на каждого из нас - через почтовый спам.

Именно спам стал главным стимулом для разработки вредоносных программ, которые ежедневно поражают такие компьютеры, как наши с вами, а через них наносят удар по нашей личности, безопасности, деньгам, семьям и друзьям. Ботнеты - это виртуальные паразиты, которых необходимо поддерживать и постоянно питать, чтобы они оставались на шаг впереди антивирусных средств и компаний по безопасности, старающихся разрушить эти сети. Чтобы колонии ботов процветали, спамерам, или ботмастерам - эти понятия взаимозаменяемы, - приходится непрерывно распространять и видоизменять поддерживающие их цифровые болезни. Поскольку антивирусы регулярно очищают заражённые персональные компьютеры, используемые для рассылки спама, операторы ботнетов должны постоянно атаковать и захватывать новые машины, а также придумывать новые способы повторного проникновения на уже заражённые.

Эта технологическая гонка вооружений требует разработки, производства и распространения всё более скрытных вредоносных программ, способных обходить непрерывно меняющуюся противовирусную и антиспам-защиту. Поэтому хакеры у рычагов управления огромными ботнетами используют спам ещё и как средство самосохранения. Те же ботнеты, которые извергают обыкновенный спам, обычно применяются для распространения нежелательных писем с новыми версиями вредоносных программ, помогающими расширять заражение. Кроме того, спамеры часто вкладывают доходы от рассылок в создание более совершенных, мощных и незаметных вредоносных программ, способных обходить антивирусы, антиспам-средства и межсетевые экраны. Экосистема спама - это непрерывно развивающаяся технологическая и социальная преступная машина, которая питает сама себя.

До сих пор преступники, ежедневно обрушивающие на мир этот поток цифровой заразы, поразительно успешно подавляют индустрию безопасности. Антивирусные компании сообщают, что им с трудом удаётся классифицировать и отражать атаки в среднем 82 000 новых вариантов вредоносных программ в день. Значительная доля этих штаммов предназначена для превращения заражённых компьютеров в спам-зомби, которыми злоумышленник может удалённо командовать. Гигант индустрии безопасности McAfee заявил, что в четвёртом квартале 2014 года обнаружил свыше двадцати пяти миллионов новых образцов вредоносных программ.

Но и спамерам это обходится недёшево. Для поддержания Cutwail требовались круглосуточные команды разработчиков программного обеспечения и сотрудников технической поддержки. Дело в том, что программы, приводящие в действие такие ботнеты, как Cutwail, обычно сдают в аренду другим спамерам, а те часто требуют изменить код или добавить возможности, чтобы бот-программы исправно работали в их собственной преступной инфраструктуре.

Москвич Игорь Вишневский, которому тогда было чуть больше тридцати, входил в число нескольких хакеров, тесно работавших с Нечволодом над Cutwail. Позднее Вишневский отправился в самостоятельное плавание и создал конкурирующую версию Cutwail, которую тоже использовал для рассылки спама и сдавал в аренду другим спамерам. Он согласился стать нашим виртуальным Вергилием и провести нас по этому странному, незнакомому миру спамеров, поэтому будет появляться на протяжении всей книги. «У нас был офис для Gugle [Нечволода, чьё прозвище произносится как Google] с программистами и поддержкой. Иногда я туда заходил, но сам там не работал», - вспоминал Вишневский в беседе через службу мгновенных сообщений. По его словам, в офисе Gugle постоянно работали не менее пяти программистов и примерно столько же сотрудников поддержки, которые посменно дежурили круглые сутки и по выходным, чтобы лучше выполнять требования клиентов.

Хостинговые компании вроде McColo привлекали таких клиентов, как создатели Cutwail, потому что продолжали работать вопреки серьёзному давлению со стороны отечественных и иностранных правоохранительных органов, требовавших отключить размещённые там сомнительные или незаконные сайты. По словам Вишневского, серверы McColo были легендарными благодаря стабильно высокой скорости и своей «пуленепробиваемости», то есть невосприимчивости к требованиям отключения со стороны других интернет-провайдеров или иностранных правоохранителей.

Вскоре после смерти Коли McColo поспешила заверить киберпреступное сообщество, что, хотя самый узнаваемый участник организации ушёл из жизни, хостинг-провайдер продолжит работать как обычно. Партнёр Коли Алексей распространил это сообщение на нескольких ведущих форумах, благожелательных к киберпреступности, стремясь убедить клиентскую базу компании, что происшествие не вызовет никаких перебоев в обслуживании.

Киберпреступное сообщество почти не пришлось уговаривать остаться. Услуга предоставлялась главным образом с площадок в Соединённых Штатах и была дешёвой, надёжной и быстрой. В течение года после смерти Николая Нечволод и большинство ведущих владельцев спамерских ботнетов продолжали держать управляющие серверы в McColo.

Так продолжалось до вечера 11 ноября 2008 года, когда разоблачительная статья в *Washington Post* о высокой концентрации вредоносной деятельности у этого хостинг-провайдера побудила двух поставщиков подключения McColo к глобальному Интернету одновременно отключить компанию. Объём спама во всём мире мгновенно упал на величину до 75 процентов: миллионы спам-ботов потеряли связь с управляющими серверами и рассеялись на все четыре стороны, словно овцы без пастуха.

Ликвидация McColo напрямую ударила по кошелькам таких владельцев ботнетов, как Нечволод и Вишневский. Спамеры, арендовавшие ботнеты, заполнили Crutop.nu и другие подпольные мошеннические форумы жалобами на потерю значительных вложений и требованиями объяснить, что теперь будет сделано.

«В McColo мы держали серверы в США, где была хорошая скорость, - вспоминал Вишневский. - Когда McColo отключили, нам пришлось арендовать гораздо более медленные серверы в Китае и других странах, которые никуда не годятся», - сказал он, имея в виду их неспособность выдерживать жалобы на злоупотребления.

О том, насколько мало кто верил, что деятельность McColo когда-либо прекратится даже после смерти Коли, говорит тот факт, что многие спамеры хранили прямо на серверах компании ещё одну важную и дорогостоящую часть своих операций - огромные списки адресов электронной почты.

«Все потеряли там свои списки», - сказал Вишневский, отметив, что после ликвидации он и Нечволод лишились особенно большого и ценного списка, содержавшего более двух миллиардов адресов электронной почты.

Гибель Коли и распад McColo стали поворотными событиями: они обозначили начало конца эпохи, когда спамерам и повелителям киберпреступного мира позволялось действовать незаметно и почти безнаказанно. В то время более 90 процентов всей электронной почты в мире составляли незапрошенные сообщения, основная масса которых рекламировала сайты интернет-аптек, исчезавших так же быстро, как появлялись. В последующие четыре года череда аналогичных ликвидаций мошеннических интернет-провайдеров, хостинговых компаний и крупных спамерских ботнетов заметно сократила мировой объём нежелательной почты и совпала с арестом или заключением нескольких ведущих спамеров.

Однако конец McColo одновременно ознаменовал рассвет новой эпохи спама: началась затяжная и дорогостоящая война за сферы влияния, которую мы рассмотрим в этой книге. Наблюдатели из мира киберпреступности и кибербезопасности назвали её «фармацевтическими войнами». Она вылилась в ожесточённую вражду между двумя крупнейшими спонсорами фармацевтического спама, а ничего не подозревавшие пользователи вроде нас с вами оказались между двух огней.

На одной стороне сражались уже упомянутые Дмитрий Ступин и Игорь Гусев с родственными аптечными предприятиями GlavMed и SpamIt. На другой стороне находилась Rx-Promotion, конкурирующая мошенническая интернет-аптека, основанная бывшим деловым партнёром Гусева, тридцатипятилетним москвичом Павлом Врублевским.

Официально Врублевский был высшим руководителем ChronoPay, одной из крупнейших российских компаний по обработке сетевых платежей, которую они с Гусевым основали вместе.

Втайне он был глубоко связан с преступным киберподпольем: помогал сетевым злоумышленникам всех мастей организовывать обработку платежей по кредитным картам для сомнительных предприятий и получал солидную долю выручки. Врублевский также был сооснователем и администратором популярного спамерского форума Crutop.nu и ещё одной ключевой фигурой в кибервойнах, из-за которых сегодня мы превратились в нацию спама, а в действительности - в целый мир спама.

К 2010 году я уже больше года расследовал предполагаемые недобросовестные деловые практики Врублевского и писал о них, а также о его предполагаемых связях со спамерами, работавшими на мошенническую аптечную программу Rx-Promotion. Сначала я занимался этим как журналист-расследователь *Washington Post*, а затем - на собственном новостном сайте о кибербезопасности KrebsOnSecurity.com. Но чем глубже я копал, тем больше мне хотелось понять проблему почтового спама и кибербезопасности: кто ею движет и как её решить. Было ясно, что этим вопросом задаюсь не только я.

До войны на истощение между королями спама, которую исследует эта книга, в открытом доступе находилось поразительно мало надёжных сведений, позволяющих ответить на самые основные вопросы, связанные с проблемой спама:

• Кто покупает товары, рекламируемые в нежелательных письмах, например Viagra, рецептурные лекарства и даже сумки Gucci? Что заставляет людей покупать и принимать таблетки, навязываемые этими назойливыми и неизвестными торговцами?
• Эти лекарства настоящие или бесполезные, а возможно, и смертельно опасные подделки?
• Кто получает прибыль от рассылки спама? Как делятся доходы и куда уходят деньги?

• Почему фармацевтическая отрасль, один из богатейших и наиболее влиятельных видов бизнеса в мире, выглядит бессильной перед повальным воровством и присвоением её товаров, товарных знаков и клиентов?
• И почему вообще настолько легко расплачиваться кредитной картой за эти подделки, которые совершенно открыто рекламируют через спам?
• Взламывают ли счета кредитных карт клиентов или перепродают ли сведения о них после покупки у спамеров? А если человек ничего у них не покупает? Ему всё равно угрожает опасность?
• И что могут сделать потребители, законодатели и правоохранительные органы, чтобы взять эпидемию киберпреступности под контроль?

Именно такие вопросы задавали люди, когда я рассказывал, что пишу книгу о спаме. Поначалу в ответ я мог предложить лишь наиболее правдоподобные догадки. Даже обращаясь за советом к предполагаемым специалистам по спаму, я обнаружил, что твёрдых ответов нет и у некоторых ведущих мировых авторитетов в этой области. Многие давали шаблонные объяснения, которые, по-видимому, основывались на нескольких избитых тематических исследованиях, причём отдельные работы финансировали крупные фармацевтические компании, компании по безопасности или те и другие вместе.

Утёкшие базы данных аптечного спама, которые во время фармацевтических войн мне удалось получить из Rx-Promotion и GlavMed-SpamIt, полностью изменили положение дел: они позволили изнутри и во всех подробностях увидеть почти каждую существенную сторону деятельности крупнейших спамерских организаций мира. Возможно, в этом есть ирония: заглянуть в их сомнительные дела, ежедневно затрагивающие каждого из нас, позволили сами спамеры.

Верные Гусеву и Врублевскому хакеры передали эти сведения отдельным представителям правоохранительных органов и мне, пытаясь навредить друг другу. Вместо этого их базы данных дали беспрецедентное представление о повседневной работе и прибылях этих скрытных международных наркокартелей, которые объединяли в слабо связанную сеть спамеров, создателей вирусов, таинственных поставщиков и перевозчиков. Сведения из этих баз также легли в основу моих репортажей, использованных во многих частях книги.

Что ещё важнее и тревожнее, этот массив документов содержал демографические, медицинские и финансовые сведения о миллионах покупателей. В основном это были потребители из Соединённых Штатов, купившие рецептурные лекарства в спамерских сетях после получения предложения по нежелательной почте или после самостоятельного поиска рецептурных препаратов в Интернете.

Базы данных без прикрас показывали скрытый, но стремительно растущий спрос на дешёвые рецептурные лекарства. Судя по всему, значительную его часть создавали американцы, искавшие более доступные препараты, которые можно приобрести без лишней огласки.

Учитывая растущую угрозу почтового спама и связанных с ним атак на кибербезопасность, которые непосредственно затрагивают потребителей и компании, вы, возможно, недоумеваете, почему правительства, правоохранительные органы и корпорации не занимают более твёрдую и решительную позицию, чтобы остановить обрушившуюся на всех нас приливную волну спама и киберпреступности. Примером такой атаки стала крупная новость, которую я первым сообщил средствам массовой информации в декабре 2013 года: взлом базы данных кредитных карт Target, поставивший под угрозу финансовые сведения миллионов американцев и вынудивший ещё большее число людей получить новые кредитные карты.

Одна из причин, по которым интернет-сообщество до настоящего времени столь вяло отвечает на эпидемию вредоносных программ и спама, состоит в том, что многие законодатели и специалисты по киберпреступности склонны считать спам всего лишь неприятностью. По их мнению, её можно устранить или хотя бы уменьшить до приемлемого уровня правильным сочетанием технологий и правоохранительной деятельности. Для многих из нас спам почти превратился в избитую шутку

из-за тесной связи с таблетками для увеличения мужского полового органа и средствами против эректильной дисфункции, такими как Viagra и Cialis. Мы полагаем, что спам нас не касается, если мы не открываем письма и ничего по ним не покупаем.

К сожалению, такое отношение подчёркивает распространённый, но в корне ошибочный расчёт угрозы, которую спам представляет для каждого из нас. Не учитывается огромная разрушительная сила ботнетов и заблуждающихся программистов, поддерживающих их работу. Ботнеты, созданные и управляемые участниками SpamIt, Rx-Promotion и других спамерских партнёрских программ, применялись не только для распространения спама. Сетевые преступники постоянно арендуют доступ к этим машинам, чтобы скрыть своё настоящее местонахождение в Интернете: ботнеты позволяют злоумышленникам пропускать сетевой трафик через бесчисленное множество заражённых систем, происхождение которого почти невозможно отследить.

Преступники, управляющие этими ботнетами, также регулярно используют их для сбора имён пользователей и паролей с заражённых персональных компьютеров. Они крадут всё: от реквизитов доступа к банковским счетам до цифровых ключей, способных открыть ценные корпоративные тайны как крупных, так и небольших компаний. Более того, злоумышленники у руля некоторых наиболее активных ботнетов мира уже управляют тысячами систем-зомби внутри компаний из списка Fortune 500. Благодаря этому они могут рассылать спам с более мощных корпоративных серверов и выкачивать конфиденциальные и служебные данные из внутренних систем компаний.

Ботнеты несут и другие серьёзные угрозы. Их часто сдают в аренду как мощную наёмную силу для масштабных схем интернет-вымогательства, известных как распределённые атаки типа «отказ в обслуживании», или DDoS. В ходе таких нападений преступники требуют от компаний десятки тысяч долларов за «защиту». Если владельцы бизнеса отказываются платить, хозяева ботнета приказывают армиям заражённых персональных компьютеров обрушить на сайт выбранной компании столько мусорного интернет-трафика, что он больше не способен обслуживать настоящих посетителей. Подвергшаяся вымогательству компания либо платит, либо остаётся вне сети, пока атакующие не отступят. Если у компании достаточно средств, она может нанять законного поставщика защиты от DDoS, который поможет отразить атаки.

Политически или идеологически мотивированные DDoS-атаки способны отключать от сети целые государства и заставлять умолкнуть критиков или участников протестов по определённым вопросам. В 2008 году продолжительная политически мотивированная DDoS-атака на чрезвычайно зависимую от сетей бывшую советскую республику Эстонию на несколько дней вывела из строя большинство правительственных сайтов, на несколько часов нарушила работу электронных банковских услуг, ненадолго парализовала крупнейшую сотовую сеть страны и нарушила работу национальной сети, от которой жители Эстонии зависят при экстренных медицинских ситуациях.

Такая огневая мощь привлекла внимание и вызвала тревогу правительства и вооружённых сил США. Кибератаки были признаны сильной и непосредственной угрозой современной сетецентрической военной машине. В важнейшей речи в Белом доме в мае 2009 года президент Обама назвал киберугрозу одной из наиболее серьёзных проблем, стоящих сегодня перед экономикой и национальной безопасностью Америки.

Несмотря на обеспокоенность правительства, политический ответ на весь организационный и технологический механизм, приводящий в действие эпидемию спама, в лучшем случае остаётся вялым, а кое-где почти полностью отсутствует. Перед нами угроза, способная нарушать инфраструктуру целых стран, ослаблять жизненно важные сети связи, отравлять людей распространяемыми поддельными потребительскими товарами и питать развитие целой незаконной подпольной экономики. И всё же правительства разных стран сделали очень мало, чтобы защитить своих граждан от вторжения этих киберармий.

Многие законодатели в Соединённых Штатах и других странах пользуются эпидемией киберпреступности, чтобы добиваться изменения законов, регулирующих сбор полицией и

федеральными властями данных о гражданах. Но более суровые наказания за киберпреступления почти не сдерживают ни злоумышленников, ни деятельность спамеров, рассылающих рекламу таблеток ради обогащения, ни современных электронных воров. Большинство недавно предложенных и принятых в Соединённых Штатах законов об интернет-безопасности сосредоточено на расплывчатых инициативах по укреплению защиты критической информационной инфраструктуры страны, то есть компьютеров и взаимосвязанных систем, управляющих всем - от производственных предприятий и сооружений водоочистки до электросетей.

Недавние законодательные попытки борьбы с киберпреступностью в Соединённых Штатах также встретили решительное сопротивление защитников неприкосновенности частной жизни и широкой общественности. Когда Конгресс США попытался принять закон, который заставил бы интернет-провайдеров прекращать подключение сайтов, признанных нарушителями прав на товарные знаки из-за торговли пиратскими или поддельными товарами, законодатели столкнулись ни много ни мало с народным восстанием против этой идеи. Основная часть сопротивления была организована и осуществлена в виде искусно спланированных сетевых демонстраций.

Тем временем несколько важных арестов и разрушительных операций против спамерских ботнетов и ведущих участников преступного киберподполья, по-видимому, дестабилизировали отрасль сильнее любого из выдвинутых до сих пор недоделанных законопроектов. Как показывают многочисленные примеры из этой книги, правительства разных стран, вероятно, могут сильнее всего повлиять на киберпреступность не новыми законами и не ужесточением наказаний за различные преступления в сети, а более строгим исполнением уже существующих законов. Кроме того, они могут творчески сочетать давление на глобальные корпорации со стимулами, побуждающими их решать проблему способами, отвечающими собственным интересам и расширяющими возможности отечественных правоохранительных органов.

Это не означает, что борьба со спамом и ботнетами лежит исключительно на правительствах мира. Напротив, далее в книге мы увидим, что некоторые из самых действенных ударов по этим двум бедствиям наносили корпорации, защищавшие собственные финансовые интересы, клиентов, товарные знаки и общественный образ, а также сами потребители.

В конечном счёте спам и все сопутствующие ему беды почти не отступят без более согласованного, совместного натиска со стороны некоторых богатейших и влиятельнейших сил мира. В их число входят фармацевтическая отрасль, сектор кредитных карт и банки, законодатели и правоохранители разных стран, а также такие люди, как вы и я, которые в большинстве своём ежедневно становятся ничего не подозревающими мишенями и жертвами этих спамеров и хакеров. Пора что-то сделать с этой глобальной эпидемией, чтобы защитить наши личности, банковские счета, семьи и жизни, пока не стало слишком поздно.

Сноски

[1] [назад] Следует отметить, что Гусев публично отрицал рассылку спама и руководство SpamIt, хотя в моих беседах с ним лично этого не отрицал.

Глава 2. Пуленепробиваемый

Чтобы понять, какую угрозу почтовый спам представляет для всех нас, прежде всего необходимо заглянуть в тёмные уголки кибермира и разобраться, что там скрывается. Похищения людей. Подкуп. Вымогательство. Шантаж. Коррупция. Эти приёмы ведения дел были обычными для людей, создававших первые убежища киберпреступности - виртуальные пиратские бухты Интернета.

Такие хостинговые предприятия, в большинстве своём находившиеся в России и бывших советских республиках, часто называли «пуленепробиваемыми сетями» или «пуленепробиваемыми хостинг-провайдерами». Различными способами, как законными, так и незаконными, они обеспечили себе достаточную политическую и оперативную защиту и стали практически недосягаемы для закона. Их влияние было столь велико, что зачастую они оставались в сети даже под сокрушительным давлением иностранных правительств и правоохранительных органов, требовавших отключить их самих и их клиентов. Последние неизменно торговали в Интернете сомнительными или незаконными товарами и услугами.

Один из лидеров, McColo Corp., владел этим искусством в совершенстве. Николай, молодой предприниматель, чью насильственную смерть в автомобильной аварии мы наблюдали в начале главы 1, разумеется, не изобрёл бизнес по привлечению и размещению в сети киберпреступных предприятий. Подобно новаторам в других областях, он стоял на плечах предшествовавших ему гигантов киберпреступности и совершенствовал освящённую временем деловую модель, сосредоточившись на эффективности: избавлялся от посредников, резко снижал цены и вкладывал средства в более надёжные и быстрые сети.

Больше всего McColo выделялась репутацией пуленепробиваемого хостинг-провайдера с первоклассной технической поддержкой и обслуживанием клиентов. Первые пионеры этого бизнеса обычно упускали из виду подобные качества, вероятно, потому, что почти не сталкивались с конкуренцией.

Но, чтобы понять, как McColo стала господствовать в преступном киберподполье, полезно узнать, почему потерпели неудачу её предшественники. Пуленепробиваемые хостинг-провайдеры, заложившие фундамент предприятия молодого Николая, оказались также тесно связаны с началом карьеры двух королей киберпреступности, чья долгая вражда образует основную сюжетную линию этой книги. И одна сеть более всех остальных подготовила почву для возвышения McColo, фармацевтических войн и многих методов нежелательной почты и киберпреступности, которые сегодня угрожают нам и нашей безопасности в сети.

К середине 2007 года Russian Business Network (RBN), таинственный хостинговый конгломерат из Санкт-Петербурга, прочно заслужил среди специалистов по безопасности репутацию эпицентра преступной деятельности в Интернете. Раз за разом, когда следователи по компьютерным преступлениям шли по следу денег и улик от сайтов, торговавших детской порнографией или пиратскими программами, в деле неизменно каким-либо образом оказывались замешаны интернет-ресурсы RBN. Когда сетевые сыщики пытались закрыть сайты, распространявшие колонии компьютерных вирусов и фишинговые схемы, в которых письма выдавались за сообщения банков и заманивали людей вводить пароли от счетов на поддельных банковских сайтах, нарушитель чаще всего оказывался клиентом RBN.

RBN воплощал собой первых пуленепробиваемых хостинг-провайдеров - виртуальные убежища, где клиенты хостинга могли демонстрировать и предлагать почти любые материалы, какими бы незаконными или оскорбительными они ни были, пока продолжали платить непомерную арендную плату, способную вырасти без предупреждения. Обычный веб-сервер в RBN стоил от шестисот до восьмисот долларов США в месяц, более чем в десять раз дороже, чем большинство законных

хостинговых компаний в то время брало с обычных клиентов.

Эти платежи не просто набивали карманы пуленепробиваемых провайдеров: без них те не смогли бы выжить. Например, часть дохода от высоких сборов стекала от главарей RBN к местным властям и коррумпированным политикам региона. Некоторые из них были более чем готовы закрыть глаза, когда правоохранители из других стран задавали вопросы о размещённых в сетях RBN сайтах, рекламировавших незаконную деятельность.

Французский исследователь безопасности Давид Бизёль, который в период расцвета RBN в середине 2007 года подготовил чрезвычайно подробный анализ сети, рассказал, что у RBN была специальная группа по работе с жалобами на злоупотребления. Однако единственной её задачей было создать видимость, будто RBN похож на законного интернет-провайдера.

«У RBN есть доступная группа по борьбе со злоупотреблениями, которая нужна, чтобы придать компании респектабельный вид, и для рассмотрения жалобы или требования об отключении эта группа попросит вас предоставить обвинительный акт российского суда, - писал Бизёль в 2007 году. - Разумеется, получить такой документ чрезвычайно трудно. Разве это не рай для мошенников?»

Точное происхождение Russian Business Network окутано тайной. Возможно, именно поэтому специалисты индустрии компьютерной безопасности годами приписывали почти всю вредоносную деятельность в Интернете главарям RBN независимо от того, была ли у неё хоть какая-то очевидная связь с печально известной хостинговой сетью.

И всё же, если для многих RBN превратился в своего рода цифровое пугало, такую репутацию он заслужил. По сообщениям прессы и словам источников, знакомых с компанией, RBN возник из потребности киберпреступников в более устойчивом и надёжном хостинге для разнообразных незаконных предприятий, прежде всего для экстремальной и детской порнографии. Корни RBN действительно уходят в индустрию детской порнографии и организованные преступные группировки из Минска, Беларусь.

На заре нового тысячелетия способного двадцатидвухлетнего белоруса Александра Рубацкого готовили к тому, чтобы он пошёл по стопам отца, уважаемого подполковника белорусской милиции. Но Рубацкого гораздо сильнее интересовали компьютеры, к работе с которыми он имел большие способности, и в конце концов он бросил милицейскую академию.

Виктор Чамковский, белорусский кинематографист и журналист-расследователь, задокументировавший начало карьеры Рубацкого, рассказывал, что его таланты сделали молодого человека ценным приобретением для местных организованных преступных группировок. Те увидели большие деньги в обработке платежей для интернет-предприятий, особенно порнографических. По словам Чамковского, в 1995 году Рубацкий начал проводить время с Геннадием Логиновым, молодым громилой, чей брат возглавлял военизированную организованную преступную группировку из Минска, известную как The Village. Задача Рубацкого состояла не в том, чтобы запугивать людей силой, а всего лишь в поиске баз данных, которые можно разграбить, и счетов кредитных карт, с которых можно вывести деньги или которые можно продать за наличные.

Весной 2001 года Рубацкий начал искать настоящую работу и устроился специалистом по компьютерам в CyberPlat, в то время крупнейшую российскую компанию по обработке сетевых платежей. В рамках своей должности он получил средства и полномочия нанять более десятка других программистов. Ему поручили собрать команду, способную создать следующее поколение платёжной платформы CyberPlat.

Как отмечала белорусская газета *БелГазета*, CyberPlat также платила Рубацкому за строгую проверку систем компании на уязвимости, из-за которых могла произойти утечка данных. Однако впоследствии компания заявила, что он злоупотребил доступом, скачав копию базы данных клиентов. Рубацкий сообщил прокуратуре, что забрал данные исключительно для демонстрации обнаруженных его командой слабых мест в защите. Но работодатель этому объяснению не

поверил. Местная милиция провела обыск в коттедже, где работали Рубацкий и его хакеры, и вывезла достаточно улик, чтобы предать его суду за кражу. В конце концов белорусский суд встал на сторону CyberPlat и приговорил Рубацкого к шести месяцам заключения. Позднее исполнение приговора было приостановлено.

Но Рубацкий отомстил. Ещё до окончания суда список клиентов CyberPlat просочился к правоохранительным органам. Следователи по киберпреступлениям из Соединённых Штатов и других стран давно подозревали, что большая часть платежей сайтам, торговавшим детской порнографией, обрабатывалась через счета продавцов, связанные с CyberPlat и её московским партнёром, банком «Платина». Теперь у властей появилось неопровержимое доказательство.

К середине 2002 года CyberPlat оказалась втянута в международный скандал: российское новостное издание *Коммерсантъ* сообщило, что среди клиентов CyberPlat были десятки сайтов, продававших доступ к изображениям и видеозаписям с детской порнографией. После скандала CyberPlat уволила 40 процентов сотрудников, включая высших руководителей.

Тем временем Рубацкий получил возможность и дальше работать на чрезвычайно прибыльном рынке обработки платежей за детскую порнографию для сомнительных сайтов, которые её предлагали. Одновременно силовик Рубацкого Логинов решил укрепить оперативную и физическую безопасность предприятия. Местная милиция больше никогда не должна была с такой лёгкостью провести обыск в хакерской хижине.[1]

Предвосхищая свою будущую деятельность пионера пуленепробиваемого хостинга, Рубацкий стремился обеспечить защиту на местах и физическую охрану, чтобы его предприятие могло работать без перерывов и вмешательства. Если бы местная милиция решила провести ещё один обыск, Рубацкий по крайней мере заранее увидел бы её приближение и успел спрятать или уничтожить уличающие свидетельства своей деятельности.

Согласно документальному фильму Чамковского «Операция Консорциум» и другим российским новостным источникам, Логинов и его сообщники оборудовали коттедж разнообразными средствами безопасности, включая камеры замкнутого видеонаблюдения и сигнализацию. Команда Логинова также обзавелась огнестрельным оружием, милицейскими радиостанциями и формой. Они даже прошли боевую подготовку под руководством бывшего офицера российского КГБ, тайной полиции и разведывательной службы Советского Союза.

Сообщалось, что банда Логинова прошла ускоренный курс полевой службы КГБ, включавший целый ряд испытаний физической и психологической выносливости, а также специальное обучение разнообразным медицинским и техническим навыкам. «Сначала им даже приходилось сдавать [письменные] экзамены, - рассказывал в документальном фильме Чамковского сотрудник Министерства внутренних дел Беларуси Игорь Пармон. - Их наказывали даже за пропуск занятий».

В статье 2004 года в *Белорусской деловой газете* описывалось, как группа Логинова отреагировала, узнав, что местный предприниматель Евгений Петровский по прозвищу Pet создаёт собственное предприятие по обработке платежей кредитными картами для индустрии детской порнографии - компанию Sunbill, позднее переименованную в BillCards. Организованная преступная группировка решила применить недавно полученную боевую подготовку, устранив или по крайней мере запугав конкурента. Предполагаемое участие Петровского в организации карточного процессинга для сайтов с детской порнографией было также задокументировано в 2004 году Центром исследования компьютерной преступности, некоммерческой организацией из Одессы, Украина, которая собирает сведения о транснациональной киберпреступности.

Петровского остановил в машине человек, выдававший себя за местного милиционера. Когда Петровский по его приказу вышел, люди в масках похитили его. Добравшись до убежища на окраине Минска, похитители связались с партнёрами Петровского и потребовали миллион долларов США за его безопасное возвращение. Но денег они не получили. Когда местные власти

начали приближаться к их местонахождению, нападавшие вместе с Петровским бежали в Москву. К ноябрю 2002 года российские и белорусские власти нашли убежище банды Логинова и арестовали похитителей. Петровского обнаружили живым и почти невредимым.[2]

По словам Чамковского, Рубацкий был всецело поглощён взломом сетевых магазинов и разграблением хранившихся там финансовых данных и ничего не знал о военизированной деятельности своих товарищей. Но, получив известие, что правоохранительные органы схватили группу Логинова за похищение и вымогательство, он бежал из Беларуси в Санкт-Петербург.

Как сообщалось, из арендованного офиса в центре Санкт-Петербурга Рубацкий вместе со знакомыми в московском Альфа-Банке создал совершенно новую платёжную систему Alfa-Pay. Она предназначалась для обработки платежей за детскую порнографию и защиты предприятия от сбоев и любопытных глаз. Как рассказывалось в статье 2006 года в белорусской газете *Вечерний Минск*, предприятие опиралось на сеть холдинговых компаний. Они служили посредниками для сотрудников, остававшихся в Беларуси и занимавшихся всем - от фотографирования моделей подросткового и предподросткового возраста до распространения материалов и выплаты комиссионных перепродавцам фотографий.

«С помощью Рубацкого был создан огромный холдинг, который охватывал всё: от фотосъёмки и распространения порнографии до административной работы холдинговой компании, [включая] регулярные платежи, выставление счетов и комиссионные, - писал Чамковский. - Ноу-хау Рубацкого применительно к... сайтам, посвящённым детской порнографии, заключалось в создании типовой системы, которую можно было легко клонировать».

Всё это могло казаться обособленной проблемой России и Восточной Европы, где подобным таинственным киберпреступным компаниям позволяли существовать. Но в действительности подавляющее большинство клиентов предприятия составляли американцы, готовые платить более сорока долларов в месяц за подписку с доступом к сайтам детской порнографии. В подполье их называли клубничными сайтами и сайтами Lolita, причём последнее название отсылало к одноимённому роману русского писателя Владимира Набокова. Согласно сообщениям прессы об этой операции, сеть сайтов Рубацкого с детской порнографией привлекала свыше 100 000 посетителей в день и приносила почти 5 миллионов долларов в месяц.

Но вскоре Alfa-Pay вновь вступила в противоборство с предприятием Петровского BillCards, обрабатывавшим платежи. К тому времени Петровский объединился с Игорем Гусевым по прозвищу Desp. Ходили слухи, что тот был администратором закрытого сетевого форума Darkmasters.com, обслуживавшего веб-мастеров, или владельцев сайтов, которые продавали чрезвычайно жёсткую порнографию, в том числе детскую.[3]

Как рассказал сооснователь и владелец ChronoPay Павел Врублевский, вскоре Alfa-Pay Рубацкого и BillCards Петровского уже соперничали, стремясь уничтожить друг друга. Упомянутая в главе 1 российская компания ChronoPay начала работу в 2003 году с обработки платежей для веб-мастеров сайтов для взрослых. В том же году Гусев присоединился к Врублевскому в качестве равноправного сооснователя ChronoPay, которая позднее обошла CyberPlat и стала крупнейшим российским обработчиком сетевых платежей.

«Alfa-Pay вступила в огромную схватку с BillCards. Обе стороны начали проводить компьютерные атаки друг на друга, пытаться возбуждать друг против друга уголовные дела, рассылать средствам массовой информации всевозможный компромат и устраивать всю эту дрянь, - вспоминал Врублевский в интервью 2010 года, которое зловеще предвосхитило уже шедшую тогда борьбу между ним и Гусевым за господство на рынке поддельных лекарств в Интернете. - В результате оба предприятия развалились, и разразился большой скандал».

Тогда Рубацкий решил, что пора перейти в другой, прибыльный, но менее опасный вид деятельности - веб-хостинг. По словам Врублевского, белорус организовал встречу с

руководителями Eltel, местного интернет-провайдера, сети которого соединяли значительную часть Санкт-Петербурга с общедоступным Интернетом.

Врублевский утверждает, что руководство Eltel приобрело для своего предприятия политическую защиту у сотрудников российской Федеральной службы безопасности (ФСБ), преемницы советского КГБ. Такое покровительство, названное в источнике словом krusha, то есть русской «крышей», считалось необходимым для любого предприятия, способного приносить солидную прибыль: подобные доходы делали бизнес уязвимым для преступного и государственного вмешательства и даже насилия.

По словам Вадима Волкова, автора книги *Violent Entrepreneurs: The Use of Force in the Making of Russian Capitalism* («Силовые предприниматели: применение силы при становлении российского капитализма»), сотрудников ФСБ часто внедряют в штат российских компаний, официально для того, чтобы помогать бороться с вымогателями, которые могут попытаться украсть прибыль предприятия.

Волков пишет, что российское законодательство позволяет действующим сотрудникам ФСБ «с согласия руководителей направляться для работы на предприятия и в организации... Это положение позволило тысячам действующих сотрудников органов безопасности занимать должности в частных компаниях и банках в качестве, как скромно называлась эта должность, „юрисконсультов“. Пользуясь связями с государственными организациями и информационными ресурсами ФСБ, они выполняли функции, которые стали называть „крышей“: защищали от вымогательства и обмана со стороны преступных группировок и облегчали отношения с государственной бюрократией. По оценкам экспертов, до 20 процентов сотрудников ФСБ участвуют в неофициальном бизнесе „крыш“».

«Ребята из Eltel прославились полным безумием: они размещали детскую порнографию и подобную дрянь, потому что хорошо ладили с местными ментами, - сказал Врублевский в телефонном интервью. - Но провайдеры вышестоящего уровня постоянно заносили сайты Eltel в чёрные списки, поэтому [чтобы обойти эту проблему] Рубацкий придумал установить прямое соединение с крупными [поставщиками магистрального интернет-доступа], такими как Telia и Tiscali».[4] Получив прямой канал, пуленепробиваемые хостинг-провайдеры больше не зависели бы от небольших провайдеров-посредников, которых можно было принудить отключить RBN при малейшем проявлении интереса со стороны правоохранительных органов.

Чтобы обойти это препятствие, «этот парень Рубацкий в конце концов потратил грёбаную кучу денег, чтобы [Eltel] получила собственный канал Интернета из-за границы, - вспоминал Врублевский. - И они назвали его Russian Business Network, сокращённо RBN».

По словам Врублевского, Рубацкий назначил руководителем проекта RBN умного молодого технического специалиста Евгения И. Сергеенко, двадцатилетнего хакера, более известного в подполье под псевдонимом Flyman.

Вскоре Flyman стал неразрывно ассоциироваться и с RBN, и с глобальной эпидемией спама, поскольку RBN превратился в мировой эпицентр вредоносной кибердеятельности, охватывавшей всё - от фишинговых схем до ежедневно обрушивающегося на каждого из нас спама с рекламой увеличения полового члена.

• * *

К 2007 году RBN превратился в киберпреступную силу, внушавшую страх. Мошеннический хостинг-провайдер стал огромным магнитом для всевозможных преступных схем в сети. Исследователи из научных учреждений и частных компаний по интернет-безопасности уже больше года били тревогу по поводу RBN, выпуская бесчисленные отчёты об огромных объёмах фишинговых схем, спама со средствами увеличения мужского достоинства и сайтов с вредоносными программами, которые исходили от проблемного провайдера и заражали миллионы

подключённых к Интернету систем по всему миру. Однако большинство этих отчётов представляло собой довольно технический анализ лишь одной или двух сторон многоликого зла, исходившего от RBN: нового изобретения во вредоносных программах, центра управления ботнетом или очередного сада вредоносных сайтов, выросшего на заднем дворе RBN.

Я понял, что никто не свёл воедино все разрозненные исследования RBN и не попытался объединить их в одном отчёте, раскрывающем всю происходившую там вредоносную деятельность. К тому времени различные публикации уже постепенно ослабили инфраструктуру поддержки, удерживавшую сеть RBN в Интернете. Поэтому мне казалось, что крупное разоблачение в широко читаемом издании может раз и навсегда опрокинуть всё предприятие.

Незадолго до этого я выделил киберпреступность в отдельное направление своей журналистской работы в *Washington Post* и стремился собрать сведения о RBN в одном материале, который, как я надеялся, привлечёт широкое внимание к масштабу угрозы. Я твёрдо верил, что киберпреступное сообщество совершило крупную стратегическую ошибку, сосредоточив столько зла в одном месте. Если бы остальное интернет-сообщество каким-то образом изгнало RBN и отказалось иметь с ним дело, множество киберпреступных предприятий оказалось бы отключено от сети.

Специалисты по кибербезопасности, с которыми я обсуждал эту мысль, говорили, что подобная мера может увеличить расходы преступных предприятий и затруднить поиск устойчивого пристанища. Одним из возможных последствий стало бы значительное сокращение спама для обычных пользователей, а также сайтов, распространяющих вредоносные программы или торгующих детской порнографией. На мой взгляд, положительные последствия могли быть огромны. Удалось бы не только сократить или, возможно, искоренить нежелательную почту и все сопутствующие ей вирусы, вредоносные программы и прочие проблемы безопасности, но и, вероятно, почти уничтожить незаконную и чудовищную индустрию, причинявшую вред детям ради извращённого удовольствия небольшого меньшинства взрослых.

В июне 2007 года я начал настойчиво требовать у десятков источников количественные данные о продолжавшейся в RBN вредоносной деятельности. За следующие четыре месяца журналистская часть материала сложилась почти сама собой: факты, поступавшие из разных источников о местонахождении вредоносных и чудовищных сайтов, начали создавать поистине пугающую картину этого мошеннического хостинга и того, как он забивал наши сети разрушительным почтовым спамом.

Почти одинаковые обвинительные заключения о RBN поступили в виде компрометирующих данных от некоторых наиболее известных компаний индустрии безопасности. Среди них были Cisco, Dell SecureWorks, FireEye, HostExploit, Marshall/M86, SANS Internet Storm Center, Shadowserver, Sunbelt Software, ныне GFI, Symantec, Team Cymru, Trend Micro и Verisign, если назвать лишь некоторые.

Кен Данэм, в то время руководивший группой быстрого реагирования подразделения киберразведки iDefense компании Verisign, рассказал, что его команда изучила все интернет-ресурсы, размещённые в RBN, и не нашла там ни одного положительного качества. «Мы всё просмотрели, сопоставили все сведения и не нашли в RBN ничего хорошего, - сказал Данэм. - В прошлом мы уже видели виртуальные убежища преступных группировок, но у этого хостинг-провайдера практически всё всегда было незаконным или вредоносным». Иными словами, не существовало ни одной уважительной причины оставлять этого преступного интернет-провайдера в сети.

Возможно, из-за тайны и ореола российской организованной преступности, окружавших RBN, убедить источники открыто и прямо рассказать всё, что им было известно о работе провайдера, оказалось гораздо сложнее. Один из источников, научный сотрудник, который ежедневно снабжал следователей Федерального бюро расследований досье о торговле детской порнографией и другой преступной деятельности в RBN, сказал, что опасается за собственную физическую безопасность, если публично расскажет о своих знаниях.

«За RBN стоит русская мафия, а у них большие пушки и очень мало нравственных принципов, - объяснил учёный. - Я с удовольствием стал бы вашим „экспертом“, но совершенно не хочу, чтобы мою семью прикончили».

Это была одна из десятков откровенных цитат, источник которых я не мог назвать, а мне отчаянно требовались специалисты, готовые официально заявить известные им сведения о RBN, чтобы разоблачить вредоносную сеть, влиявшую на жизнь миллионов ничего не подозревавших людей. После долгих уговоров мне наконец удалось убедить достаточно экспертов рассказать правду. 13 октября 2007 года *Washington Post* опубликовала материал «Таинственную российскую компанию считают проводником киберпреступности» в основной части газеты и разместила его на видном месте своего сайта.

Вскоре после этой статьи *Post* опубликовала в блоге Security Fix ещё два подкрепляющих материала. В них подробно описывалась вредоносная деятельность RBN и прямо назывались интернет-провайдеры, соединявшие RBN с остальным Интернетом. Игра была окончена. Теперь, когда их имена стали известны всем, провайдерам пришлось бы объяснять, почему они принимают деньги RBN. Защитить такую позицию было невозможно, учитывая чудовищную репутацию RBN как убежища для любых материалов, какими бы незаконными или оскорбительными они ни были.

В следующие несколько недель десятки тысяч интернет-адресов, прежде выделенных Russian Business Network, постепенно опустели. Киберпреступные предприятия, некогда занимавшие эти «киберучастки», исчезли и рассеялись по новым пуленепробиваемым хостинг-провайдерам в Италии, Китае, Корее и других странах. В результате на короткое время спам-боты продолжали рассылать рекламный мусор и ссылки на заражённые вредоносными программами сайты, но сами рекламируемые в письмах сайты не отвечали. На первый взгляд это была пустая победа, однако многие представители сообщества безопасности приветствовали предупредительный выстрел, сообщавший преступному киберподполью, что индустрия сетевой безопасности наконец начала сопротивляться.

Такое развитие событий обрадовало не всех. Раньше RBN представлял собой скопление известных вредоносных хостингов, которые интернет-провайдеры могли легко заблокировать или отфильтровать несколькими правилами межсетевого экрана. После того как сайты RBN рассеялись по десяткам сетей, блокировать их стало гораздо труднее. Теперь провайдерам приходилось раскидывать сети защиты шире, чтобы вредоносные сайты, ботнеты и спамеры не могли проскользнуть. Зато интернет-провайдеры, государственные чиновники и корпорации наконец начали замечать преступное киберподполье, разраставшееся у них под ногами.

Но это была лишь вершина айсберга. В августе 2008 года, почти через год после того, как RBN развеяли по ветру, я написал серию статей о киберпреступной деятельности, которая сосредоточилась несколько ближе к дому, у таинственного интернет-провайдера Atrivo. Подобно McColo молодого Николая, это был хостинг-провайдер из Северной Калифорнии, который также игнорировал требования правоохранительных органов и сообщества безопасности отключить нарушавшие правила сайты. Компания стала синонимом размещения ботнетов и огромного числа сайтов, созданных для навязывания вредоносных программ. Я опирался на те же доказательства, которые собрали некоторые компании по безопасности, изучавшие RBN, и особенно на отчёт HostExploit, организации пользующихся международным уважением специалистов по Интернету, посвятивших себя исследованию и разоблачению киберпреступности и распространению знаний о ней.

Эта серия, а также растущее внимание других средств массовой информации и специалистов по безопасности привели к постепенному изгнанию Atrivo из Интернета. Партнёров компании среди интернет-провайдеров, соединявших её и её киберпреступных пользователей с глобальной сетью, публично стыдили до тех пор, пока примерно за две недели они один за другим не разорвали с ней отношения.

Одним из важных последствий отключения Atrivo стало ускорение гибели червя Storm, печально известного ботнета, который проник в миллионы персональных компьютеров американцев и захватил их. Как я объяснял 17 октября 2008 года в блоге Security Fix газеты *Washington Post*, когда-то он «отвечал за рассылку более 20 процентов всего спама». Atrivo размещала несколько главных серверов червя Storm. Последний поток спама червь выпустил за три дня до того, как последний остававшийся интернет-провайдер Atrivo принудительно отключил компанию от сети.

Через неделю после исчезновения Atrivo из сети со мной связался надёжный источник, знакомый со многими сомнительными личностями преступного киберподполья. Он сказал, что должен передать сообщение от неназванного киберпреступника, которому организованное мною изгнание Atrivo причинило небольшие неудобства и одновременно внушило невольное уважение.

«Передай Кребсу: „Хорошая работа с Atrivo“, - сказал моему источнику таинственный злоумышленник. - Но если он думает следующим заняться McColo, то слишком испытывает судьбу».

Я не знал, как понимать это сообщение, похожее на насмешливое замечание, подкреплённое скрытой угрозой. Но к тому времени, когда источник передал его, поворачивать назад было уже поздно. Я по колено увяз в расследовании McColo, компании интернет-провайдера под руководством Николая Макколо по прозвищу Коля. Это было логичным продолжением работы, главным образом потому, что многие злоумышленники и владельцы ботнетов, державшие инфраструктуру своих ботнетов и преступных программ в Atrivo, размещали отдельные её части и в McColo. После изгнания Atrivo из Интернета McColo стала ещё более важным пуленепробиваемым провайдером для преступного киберподполья.

Днём 11 ноября я отправил накопленные за несколько месяцев сведения, подробно описывавшие нарушения McColo, двум партнёрам-провайдерам, которые соединяли компанию с глобальным Интернетом: Global Crossing и Hurricane Electric. Штаб-квартиры обеих находились в Соединённых Штатах. Сведения были представлены в виде карты, показывавшей, что управляющие серверы всех пяти наиболее активных спамерских ботнетов, то есть подключённых к Интернету программ, отвечавших за рассылку большей части нежелательной почты в мире, размещались всего на нескольких серверах хостингового центра McColo в Северной Калифорнии. Я предполагал, что, увидев перечень происходившей там вредоносной деятельности, интернет-партнёры McColo разорвут деловые отношения с хостинг-провайдером и фактически парализуют его.

Через несколько часов мне позвонил источник, который ежедневно следил за глобальной активностью спама и знал, что я работаю над материалом о McColo.

«Кребс, что вы сделали? - со смехом и одобрением спросил источник. - Я почти больше не вижу спама, и, похоже, McColo отключили от Интернета!»

Не помню, сказал ли я спасибо или попрощался. Помню лишь, как громко выругался, бросил трубку и немедленно начал звонить с мобильного телефона нескольким другим источникам. Все они подтвердили одно и то же: McColo исчезла, ни один из её интернет-адресов не был доступен ни из одной точки Всемирной паутины. Задача была выполнена - по крайней мере на время.

Звонок Бенни Нгу, директору по маркетингу Hurricane Electric, раскрыл причину. В тот день провайдер разорвал отношения с McColo.

«Мы немного изучили вопрос, увидели размер и масштаб проблемы, о которой вы сообщали, и сказали: „Ничего себе!“ - рассказал Нг. - В течение часа мы отключили все наши соединения с ними».

Через несколько минут после подтверждения ликвидации я написал и опубликовал в блоге сообщение об отключении McColo. По непосредственному мировому воздействию оно быстро стало одной из крупнейших историй о киберпреступности на тот момент. Затем я начал готовить

более подробный материал о происшествии, который на следующий день планировалось опубликовать на сайте *Washington Post* и, возможно, в «издании из мёртвых деревьев», как мы, интернет-журналисты, ласково называли печатную версию.

В тот вечер и далеко за полночь я работал в домашнем кабинете над продолжением статьи, а закончив материал около рассвета, уснул в пижаме прямо за клавиатурой.

Позднее тем же утром текст отредактировали и опубликовали на washingtonpost.com. Некоторое время он находился «над сгибом», то есть на видном месте среди самых популярных материалов сайта за тот день. Так продолжалось, пока статью не обнаружил юрист washingtonpost.com и не пришёл в крайнюю ярость. Очевидно, никто не попросил юристов высказать мнение, и теперь они требовали снять материал с сайта, пока факты не перепроверят трижды, а отдельные формулировки о предполагаемой незаконной деятельности в McColo не смягчат.

Редакторы *Washington Post* и других крупных изданий обычно требуют, чтобы готовящийся материал «прошёл через юристов», если в нём содержатся утверждения о фактах или обвинения, способные позднее привести к правовым неприятностям, особенно со стороны названных в статье людей и организаций, которые могут предъявить иск о клевете. Одному юристу washingtonpost.com было чрезвычайно неуютно от любых формулировок, хотя бы намекавших на незаконную деятельность владельцев McColo, которые раз за разом игнорировали просьбы дать комментарий. О сомнительности дел McColo говорит то, что единственными указанными на её сайте средствами связи были анонимные учётные записи служб мгновенных сообщений. В конце концов, не существовало доказательств, что кому-либо из связанных с McColo предъявляли обвинение в преступлении. На каком же основании мы об этом заявляли?

Здесь важно сделать замечание. В опубликованной тем утром статье было множество ссылок на подкреплявшие её доказательства незаконной деятельности в McColo, собранные бесчисленными специалистами индустрии безопасности. К сожалению, юрист washingtonpost.com, первоначально возразившая против публикации, читала материал на мобильном телефоне, где не отображались гиперссылки. По ним читатели могли перейти к объёмным сторонним отчётам и доказательствам упомянутой преступной деятельности. Юристу же казалось, что статья бросает в McColo всевозможные безосновательные и потенциально клеветнические обвинения, когда предприятие к тому моменту выглядело почти разорённым.

Юрист потребовала убрать статью о McColo с сайта washingtonpost.com. После непродолжительного сопротивления новостная редакция сайта уступила, не спросив меня ни о точности материала, ни о доказательствах, подкреплявших мою работу. Статью просто выдернули с сайта, ничего не объяснив десяткам тысяч читателей, которые встречали неработающие ссылки и в конце концов перенаправлялись к моему первоначальному сообщению в блоге о ликвидации. Мой почтовый ящик быстро заполнили письма озадаченных читателей, спрашивавших, куда исчез материал.

Почти пять мучительных часов продолжение одной из важнейших на тот момент историй о киберпреступности находилось в редакционном и юридическом подвешенном состоянии. Юристы разбирали текст строка за строкой, изменяя или удаляя потенциально спорные фрагменты.

В конце концов статью вновь опубликовали позднее тем же вечером, хотя в сокращённом и сильно отредактированном виде. Но с того дня любой мой материал, где хотя бы слегка пахло сведениями о предполагаемой преступной деятельности в Интернете, приходилось пересылать как минимум одному старшему редактору washingtonpost.com и часто прогонять через целую череду юристов. Поскольку своей темой я считал киберпреступность, обычно это происходило несколько раз в неделю.

После неразберихи вокруг McColo журналистские расследования, на подготовку которых уходили недели, а иногда месяцы, могли столько же пролежать в почтовых ящиках начальников, чьё

одобрение требовалось для публикации. В некоторых случаях редакторы washingtonpost.com, юристы или те и другие откладывали следующие статьи на неопределённый срок.

Одним из таких материалов было расследование, которое я готовил и писал шесть месяцев. Оно рассказывало о схеме киберпреступной деятельности, след которой вёл к ChronoPay Врублевского. В то время самой быстрорастущей и прибыльной киберпреступной схемой в мире было распространение поддельных антивирусов. Такое программное обеспечение, также известное как scareware, использует вводящие в заблуждение всплывающие предупреждения и другие уловки, чтобы напугать ничего не подозревающих пользователей Интернета и заставить их купить бесполезную защитную программу. В довершение неприятностей поддельные защитные программы часто поставляются вместе с вредоносным кодом, который превращает заражённые машины в спам-зомби.

Специалисты по безопасности, внимательно следившие за бедствием scareware, рассказывали мне, что почти всегда платежи кредитными картами в подобных мошеннических схемах обрабатывала ChronoPay. По их данным, основатель компании, россиянин Павел Врублевский, по-видимому, был глубоко и лично вовлечён в создание таких схем и получение прибыли от них.

До конца 2008 года я почти ничего не знал о Врублевском. Тогда российский источник, который останется неназванным, посоветовал мне найти регистрационные документы ChronoPay в Нидерландах, где была основана компания. Из документов следовало, что ChronoPay создали в 2003 году как равноправное партнёрство Врублевского и Игоря Гусева. Те же источники, которые вывели меня на регистрационные данные, рассказали, что в 2005 году эти двое разошлись. В 2006 году Гусев основал партнёрство мошеннических интернет-аптек GlavMed-SpamIt. Врублевский не пожелал уступать: годом позже он стал сооснователем конкурирующей мошеннической интернет-аптеки Rx-Promotion.

В то время я ничего не знал ни о связях Врублевского с Rx-Promotion, ни даже о том, кто такой Игорь Гусев. Зато мне было известно, что совсем недавно ChronoPay связывали с червём Conficker, компьютерной заразой, которая остаётся одним из самых агрессивных и тщательно исследованных образцов вредоносных программ, когда-либо выпущенных в мир. Ранняя версия червя приказывала миллионам заражённых компьютеров загружать мошеннический антивирус с Trafficconverter.biz, сетевого предприятия, зарабатывавшего десятки миллионов долларов, выплачивая мошенникам вознаграждение за навязывание владельцам персональных компьютеров поддельных антивирусов. Обработкой платежей для TrafficConverter занималась ChronoPay.

В марте 2009 года я представил первую версию разоблачительного материала о ключевой и прибыльной роли ChronoPay в распространении поддельных антивирусов. В статье также приводились доказательства того, что Врублевский основал, создал и владел Crutop.nu, таинственным сетевым форумом для спамеров и мошенников, присутствовавших на похоронах Макколо.

Материал ссылался на опубликованные исследования нескольких уважаемых специалистов по безопасности, посвящённые истории ChronoPay. Тем не менее он месяцами оставался в редакционном подвешенном состоянии, переходя от одного старшего редактора washingtonpost.com к другому. Редакторы были уверены, что ChronoPay подаст на *Washington Post* в суд, и их можно было понять. Во время телефонного интервью Врублевский обещал, что его компания именно так и поступит, если мы опубликуем статью.

Та же нерешительность задержала ещё один крупный эксклюзивный материал, связанный со статьёй о ChronoPay. После отключения McColo значительная часть размещавшейся там незаконной деятельности быстро переместилась к другому хостинг-провайдеру Северной Калифорнии, Triple Fiber Networks, известному в подполье как 3FN. Те же управляющие серверы спамерских ботнетов, которые годами называли McColo своим домом, после её гибели начали пользоваться 3FN. Изучение сообщений на сетевом форуме Spamdot, тщательно охраняемом

виртуальном воровском логове, где в то время собиралось большинство самых успешных российских спамеров, показало, что владельцы 3FN активно подбирали оставшихся без пристанища клиентов McColo после прекращения её деятельности в ноябре 2008 года.

В то время 3FN также была крупнейшим в Интернете хостингом сайтов, распространявших поддельные антивирусы. Сайт 3FN зловеще напоминал сайт McColo. И снова единственным способом связаться с владельцами компании был протокол мгновенных сообщений ICQ, чьё название произносится как *I seek you*. На протяжении многих лет он фактически служил основным средством связи для многих российских хакеров.

Я настаивал, чтобы эти материалы увидели свет. Разоблачив вредоносную деятельность, которая в конце концов привела к отключению RBN, Atrivo и McColo, я считал, что *Post* обязана перед читателями и всем миром продолжать освещать интернет-провайдеров, дававших убежище огромной части киберпреступного сообщества. Негативные публикации о таких компаниях в крупных средствах массовой информации заставили бы больше правоохранительных органов принять против них меры и тем самым уменьшить угрозу, которую они представляли для американцев и людей по всему миру. Однако мои редакторы совсем не хотели повторения истории McColo, хотя та и не привела ни к судебным искам, ни к другим проблемам для *Post*.

Когда в начале 2009 года на редакционном совещании я сообщил, что 3FN стала главным объектом американского правоохранительного расследования киберпреступности, мне настоятельно посоветовали получить подтверждение как минимум от двух источников. Иначе следовало ждать официального комментария правоохранительных органов о расследовании или доказательств начала судебного разбирательства против хостинг-провайдера, прежде чем публиковать материал с обвинениями 3FN. Документы дела были запечатаны федеральным судьёй, а мой источник в правоохранительных органах был единственным знакомым мне человеком, который вообще слышал о 3FN. Статью отложили.

Затем, 2 июня 2009 года, более пятнадцати тысяч сайтов, размещённых в 3FN, отключили после того, как Федеральная торговая комиссия США (FTC) убедила судью окружного суда Северной Калифорнии приказать вышестоящим интернет-провайдерам компании прекратить маршрутизацию её трафика. FTC утверждала, что 3FN действовала «как мошеннический интернет-провайдер, или провайдер в „чёрной шляпе“, который привлекал клиентов, заведомо размещал и активно участвовал в распространении незаконных, вредоносных и опасных материалов», включая управляющие серверы ботнетов, детскую порнографию и мошеннические антивирусные продукты.

Действия FTC дали мне опору, необходимую для того, чтобы наконец заручиться достаточной поддержкой и продолжить расследование Врублевского, ChronoPay и их роли в развитии рынка поддельных антивирусов. Этот рынок мучил миллионы потребителей и угрожал их личностям, деньгам и безопасности. Crutop.nu также размещался в 3FN и даже был назван в иске FTC. Комиссия охарактеризовала Crutop как место, «где преступники делятся друг с другом приёмами и стратегиями», и русскоязычный сайт, «содержащий различные форумы, обсуждения на которых посвящены получению денег с помощью спама». Изучение многочисленных веток обсуждения на российском форуме веб-мастеров сайтов для взрослых показало, что более восьми тысяч активных участников Crutop составляли крупнейшую отдельную группу клиентов 3FN.

Что весьма показательно, сразу после ликвидации 3FN, но ещё до публикации на washingtonpost.com статьи о связях ChronoPay с индустрией мошеннических антивирусов, главную страницу Crutop.nu заменили длинной гневной тирадой о действиях FTC против 3FN. Так я впервые познакомился с эпическими разглагольствованиями Врублевского. В сообщении, среди прочего, говорилось:

> И в заключение мы хотели бы добавить: хотя раньше пункт 1 наших правил никто не принимал всерьёз и он был написан как шутка, в связи с последними событиями мы хотели

> бы узнать, как могло случиться, что пять (5!) уважаемых экспертов-агентов из США, включая специалистов NASA и господина Брайана Кребса, где каждый десятый говорит по-русски, источник: Wikipedia, не сумели понять, что обсуждения в подфоруме SPAM на Crutop.nu не имеют никакого отношения к почтовому спаму или другим киберпреступлениям?

Статья о ключевой роли Врублевского и ChronoPay в 3FN наконец вышла более чем через четыре месяца после того, как я её представил. Ни он, ни ChronoPay не подали в суд. Однако редакторы *Washington Post* сказали, что по-прежнему глубоко обеспокоены моей сосредоточенностью на сетевых преступниках. Руководство *Post* нервировало то, что я писал на насыщенную преступностью тему, где обычных форм документальных доказательств, как правило, не существует. Кроме того, оно считало, что моя специализация на киберпреступности слишком узка по сравнению с более широкой темой вроде потребительских технологий или технологической политики, и что я слишком сблизился с источниками, чтобы сохранять объективность.

До некоторой степени я разделял их опасения. Ни один журналист не хочет зависеть от горстки источников, исключая все остальные: так можно публиковать материалы, лишённые широты взгляда и равновесия. Но я знал, что решение состояло лишь в поиске большего числа более качественных источников, особенно тех, кто активно участвовал в киберпреступном сообществе. Я также был убеждён, что история 3FN слишком важна, чтобы её бросить. Отложить её значило упустить прекрасную возможность разоблачить и, возможно, остановить значительный объём киберпреступной деятельности.

На встрече в середине 2009 года редакторы washingtonpost.com объяснили: хотя мой блог Security Fix привлекал преданную и похвально большую для столь узкой темы аудиторию, ракурс моих материалов не вполне соответствовал новой стратегии *Post*: стать главным источником новостей «для Вашингтона, округ Колумбия, и о нём».

Эта формулировка выражала суть новой стратегии, ставшей центральным элементом долгих и болезненных попыток объединить раздельную работу печатной газеты *Washington Post* и редакции washingtonpost.com, главным образом ради сокращения расходов.

Руководство *Post* решило, что одним из способов сэкономить будет изменить освещение новостей в газете и на сайте, сильнее сосредоточившись на местных событиях в столице страны и объясняя читателям, как происходящее в Вашингтоне влияет на остальной мир. Компания также решила закрыть несколько крупных американских бюро новостей и чаще полагаться на информационные агентства вроде Associated Press и Reuters при освещении срочных событий.

Редакторы надеялись, что большую часть времени я стану писать о технологической политике, особенно о регулировании технологий и государственной политике или о будущем технологических инноваций в связи с политикой. Но я совсем не хотел отвлекаться от киберпреступности. В начале своей карьеры в *Post* я несколько лет освещал технологическую политику и счёл эту работу утомительной и отупляющей.

Возвращение к технологической политике также означало бы отказаться от результатов четырёх лет, потраченных на поиск осведомлённых и располагающих связями источников как в индустрии безопасности, так и в киберпреступном сообществе. Я находился в середине годичной серии материалов о всё более дорогостоящих и изощрённых кибератаках, ежемесячно совершавшихся против бесчисленных малых и средних организаций по всей стране. После всех тщательных исследований и расследований я наконец оказался в первом ряду и мог наблюдать за повседневной деятельностью крупных организованных киберпреступных группировок из Восточной Европы.

За несколько месяцев мне удалось узнать, кем были эти преступники, где они работали, чем занимались в свободное время и на кого нападали, причём часто ещё до того, как сами жертвы

узнавали о краже сотен тысяч, а иногда и миллионов долларов. Банковскими счетами большинства малых предприятий и организаций управляют обычные мужчины и женщины, которые не способны противостоять организованным киберпреступным группировкам. Я отчаянно хотел продолжать рассказывать людям об этой всё более распространённой и дорогостоящей разновидности сетевого ограбления.

Кроме того, я начинал понимать, что ChronoPay и Врублевский были лишь вершиной айсберга, самыми заметными фигурами преимущественно российского и восточноевропейского подпольного сообщества, участники которого, казалось, все знали друг друга и друг на друга полагались.

Поэтому через четырнадцать лет после прихода в *Washington Post* меня уволили, выплатив выходное пособие за шесть месяцев. Этого времени как раз хватало, чтобы придумать следующий шаг в карьере. Помню, тогда мне казалось очень важным с ходу приступить к новой работе 1 января 2010 года. Вот только какой именно будет эта новая работа, я ещё не знал.

Об увольнении я рассказал лишь нескольким родственникам и двум надёжным источникам, больше никому. Поэтому я был озадачен, когда меньше чем через месяц и задолго до официальной даты увольнения обнаружил на Crutop.nu длинную ветку обсуждения под заголовком «Кребса уволили из *Washington Post*», участники которой по очереди праздновали новость и издевались надо мной.

«Для тех, кто не знает: он автор Security Fix в WP и любил писать об Atrivo, McColo, EstDomains, UkrTeleGroup, [и] 3FN. Именно он помог их закрыть», - написал участник Crutop, открывший ветку. Другие приветствовали известие возгласами вроде «Спасибо, Санта!» и «Санта получил наши письма!». Было жутко и тревожно видеть, как настолько личные и закрытые сведения раскрываются на общедоступном форуме, которым управляли одни из самых активных спамеров, разоблачить которых я старался. Но это лишь укрепило мою решимость продолжать работу.

Всего за две недели до появления той ветки на Crutop я анонимно зарегистрировал доменное имя KrebsOnSecurity.com, но ещё не решил, искать ли обычную должность в другом крупном новостном издании или самостоятельно вести блог. Я слышал от коллег из других крупных средств массовой информации, что их увольняли, принудительно отправляли в неоплачиваемые отпуска или переводили на более привлекательные для рекламодателей направления. Поэтому мне не хотелось снова искать место в крупной газете или сетевом издании. Но мысль о самостоятельной работе и необходимости ею зарабатывать казалась пугающей, временами даже ужасала.

В то же время часть меня стремилась добиться успеха на собственных условиях и собрать аудиторию исключительно благодаря своим оригинальным материалам. Когда я прочитал ветку Crutop, она показалась почти личным вызовом, и я решил его принять. Вскоре произошло обнадёживающее событие: со мной связались российские читатели, которым ветка на Crutop внушала отвращение. Они хотели поделиться документами, способными доказать масштаб участия ChronoPay в преступном киберподполье. Я подозревал, хотя тогда не мог знать наверняка, что за этой уловкой стоял бывший деловой партнёр Врублевского, ставший его заклятым врагом, Игорь Гусев. Но в тот момент мне не хотелось делать ничего, что могло бы помешать источникам поделиться известными им сведениями.

«Не заблуждайтесь, - предупредил в электронном письме источник под псевдонимом Борис, обещавший передать огромный объём уличающих доказательств нарушений в ChronoPay. - Эти парни и, вероятно, Врублевский жёстко на вас набросятся, и зрелище может оказаться неприятным».

Но Борис и другие сдержали и обещания, и предупреждения. Анонимные угрозы начались всего через несколько дней после того, как в мои руки попала настоящая виртуальная сокровищница уличающих писем и документов ChronoPay. Последние сомнения насчёт самостоятельной работы исчезли. Пора было браться за дело.

Сноски

[1] [назад] Мне не удалось разыскать Рубацкого, однако, по сведениям Белорусского телеграфного агентства, государственного национального информационного агентства, в настоящее время он скрывается от правосудия и разыскивается Интерполом, международной организацией уголовной полиции.
[2] [назад] Позднее Логинова и нескольких его сообщников привлекли к ответственности и признали виновными в похищении человека и других преступлениях. Согласно сообщению *Ecommerce Journal*, предполагается, что Петровский скрывается где-то на Украине.
[3] [назад] В интервью по электронной почте Игорь Гусев признал, что человек с его необычным псевдонимом Desp был указан как администратор на главной странице Darkmasters.com, но отрицал, что когда-либо сам был администратором Darkmasters. По словам Гусева, он лишь согласился за деньги предоставить сайту своё имя и одобрение по просьбе настоящего администратора, другого веб-мастера материалов для взрослых под псевдонимом Master. Врублевский, напротив, настаивает, что это служит «доказательством» тесной связи Гусева с Russian Business Network.
[4] [назад] Сегодня Telia входит в состав TeliaSonera. Это была ведущая шведская телекоммуникационная компания, работавшая по всей Европе и Азии. Tiscali - итальянская телекоммуникационная компания, которая предоставляет услуги внутри страны, а прежде работала по всей Европе и в Гонконге.

Глава 3. Фармацевтические войны

Утро 14 мая 2010 года началось с бессвязного и тревожного письма, ожидавшего во входящих. Анонимный автор прочитал в моём блоге сообщение о только что завершившемся публичном выступлении по теме киберпреступности на севере штата Нью-Йорк. В письме говорилось:

> Брайан,
>
> Вы удивительная загадка. Ваша жена, по-видимому, позволяет Вам вести себя как подросток. Мне хотелось бы увидеть, как Вы повзрослеете.
>
> Мы любим Вас. Но Ваша жена права. Пора передать Ваш необычный талант в руки профессионалов. Последний отчёт о том, как Вы разъезжали по северу штата Нью-Йорк, побуждает меня отправить Вам эту последнюю мольбу, прежде чем...
>
> Ваша многострадальная, но любящая жена должна получить право заключить договор с профессионалом, возможно женщиной, но Ваша покорная супруга съест её глаза вместе с хлопьями на завтрак ещё до того, как Вы подниметесь из подвала, если та начнёт к Вам приставать.
>
> Так зачем я пишу? Всё просто. Мне нравится то, что Вы делаете, и гораздо большему числу людей это тоже понравилось бы, если бы они только знали о Вас. Но, подобно многим художникам, Вы думаете, будто все видят то же, что и Вы. Это не так.
>
> Поэтому следующий ход за Вами. Я бы начал с Вашей жены. Я бы спросил, что она думает об этом письме.
>
> Затем я бы нанял адвоката. Он Вам понадобится, когда она «влюбится».

Послание было образцовым Врублевским: злобным, бессвязным, наглядным и переполненным искалеченными метафорами. Именно такие тирады я часто видел от имени предполагаемой личности Врублевского RedEye на Crutop.nu, российском форуме веб-мастеров сайтов для взрослых, который он помог основать и который служил учебным центром для спамеров. Как заявила Федеральная торговая комиссия США (FTC), ликвидируя хостинг-провайдера 3FN, Crutop «содержит различные форумы, обсуждения на которых посвящены получению денег с помощью спама».

Врублевский приобрёл известность ещё в начале своей деловой карьеры, создав сеть сайтов для взрослых, специализировавшихся на экстремальной и жестокой порнографии, преимущественно видеозаписях изнасилований, инцеста и скотоложства. Его имя и адрес ChronoPay присутствуют в регистрационных документах компании Red & Partners BV. Согласно юридическим документам, полученным автором у правительства Нидерландов, Врублевский создал эту компанию, которая была материнским предприятием его партнёрской программы для веб-мастеров сайтов для взрослых. Кроме того, как я отмечал в статье 2009 года в *Washington Post*, сайты ChronoPay.com и Red & Partners (re-partners.biz) использовали одни и те же серверы доменных имён и один код Google Analytics для отслеживания посетителей, хотя ChronoPay отрицала связь между компаниями. Многие веб-мастера Crutop были партнёрами, зарабатывавшими на перепродаже подписок на порнографические сайты Врублевского и других участников форума.

Однако, если не считать странного и несколько угрожающего языка, письмо почти не содержало других подсказок в поддержку моего подозрения, что его написал Врублевский. Это было лишь чутьё, но время отправки вызывало подозрение.

За шесть месяцев до того я решил работать самостоятельно и запустил собственный сайт KrebsOnSecurity.com, ежедневный новостной блог с журналистскими расследованиями киберпреступности, призванный расширять осведомлённость общества и побуждать его к борьбе.

Письмо пришло всего через два дня после того, как я сообщил Врублевскому о подготовке статьи, основанной на обвинениях в киберпреступности, которые выдвинул против него Илья Пономарёв, член подкомитета Государственной думы России по развитию высоких технологий. Пономарёв направил российским следователям письмо, повторявшее многие обвинения из моих прежних материалов о ChronoPay и Врублевском для *Washington Post*.

В письме Пономарёва содержалась и новая для меня крупица информации, которая впервые позволила заглянуть в широко распространённую коррупцию и отсталость российской политики. Невероятно, но Врублевского, который, по словам нескольких источников, к тому времени управлял одной из самых печально известных программ фармацевтического спама в Интернете, Rx-Promotion, выбрали председателем рабочей группы по борьбе со спамом российского Министерства связи и массовых коммуникаций. Президент России Дмитрий Медведев поручил этому органу консультировать правительство по новым законам, ограничивающим нежелательную почту. По существу, Пономарёв хотел добиться ухода Врублевского.

Когда я обратился к нему за комментарием по поводу послания Пономарёва, Врублевский публично отверг связи с Rx-Promotion или спамом, а затем обвинил меня в том, что его враги подкупили меня ради негативных публикаций о нём. Он снова пообещал подать на меня в суд и на этот раз действительно предпринял шаги для исполнения угрозы. К моменту нашего разговора он уже начал процесс. Но, как я позднее узнал, адвокат и руководители ChronoPay в конце концов его отговорили: шансы на победу были невелики, дело могло тянуться годами, а в случае суда ещё большая часть деятельности Врублевского и ChronoPay могла выйти на свет.

Как я обо всём этом узнал, если Врублевский не говорил ничего, кроме угроз подать на меня в суд? К тому времени в мой почтовый ящик десятками начали приходить утёкшие письма между Врублевским и русскоязычным адвокатом, которого он нанял в вашингтонской юридической фирме Duane Morris LLP. Впоследствии переписка показала, что ради моего молчания Врублевский был полностью готов заплатить свыше 100 000 долларов за иск о клевете в связи с моими статьями о его роли в индустриях мошеннических антивирусов и интернет-аптек.

Эти внутренние письма стали первыми среди множества скомпрометированных материалов, или компромата, как говорят в России, которые на протяжении года я получал от неустановленных и анонимных хакеров, очевидно решивших разоблачить ChronoPay и Врублевского. Когда такие материалы только начали поступать, обычно в виде ссылки на архив в бесплатной файлообменной службе, я допускал, что кто-то мог подделать письма и документы, придав им вид похищенных из ChronoPay. Но в конце концов огромный объём, сложность и взаимосвязанность документов ясно показали, что они подлинные.

Несколько месяцев спустя Врублевский сам признал это в телефонном разговоре со мной. Неизвестные хакеры или сотрудники ChronoPay передали огромные массивы внутренней переписки его компании, десятки тысяч писем и бухгалтерских документов, а также сотни часов телефонных разговоров Врублевского с другими людьми, которые он записывал. Сведения кропотливо документировали весь масштаб участия ChronoPay в предприятиях мошеннических интернет-аптек и поддельных антивирусов. Для них потребовалось создать сложную сеть подставных компаний и офшорных банковских счетов, полностью задокументированную в хорошо организованных таблицах Microsoft Excel, а в отдельных случаях описанную собственным голосом Врублевского.

Этот массив похищенных документов содержал не только доказательства нарушений со стороны ChronoPay и её руководителей, но и сложные, порой непристойные подробности о некоторых самых влиятельных людях преступного киберподполья.

На чтение всех материалов ушло много месяцев, но ещё важнее и труднее было обнаружить самые значимые письма и документы. Отчасти сложность заключалась в том, что почтовые ящики сотрудников ChronoPay, к которым мне предоставили автономный доступ, по иронии судьбы сами

были завалены спамом. Из-за этого при поиске определённых терминов, способных раскрыть участие ChronoPay в создании подставных компаний и партнёрских программ и управлении спамерскими операциями, возникало множество ложных совпадений.

Кроме того, почти все послания были написаны по-русски, а у отдельных выражений и собственных имён часто существовало несколько кириллических и транслитерированных вариантов или сокращений. Для каждого приходилось выполнять отдельный поиск, а порой требовались оба подхода.

К счастью, за четыре года до этого я самостоятельно начал изучать язык. Работая в *Washington Post*, я обнаружил, что провожу необычно много времени на русскоязычных подпольных форумах, которые не только враждебно относились к людям с Запада, но и часто отчитывали или исключали участников за непростительный грех общения по-английски. Чтобы преодолеть препятствие, я взял в местной библиотеке шестидесятичасовой курс русского языка на компакт-дисках. К 2008 году я наконец овладел русским достаточно хорошо, чтобы читать большинство форумов без помощи сетевой службы перевода. Для такого журналиста-расследователя, как я, это было жизненно важно: так я мог не допустить ошибочного толкования полученных сведений. Кроме того, исследования пошли гораздо быстрее.

Просматривая документы, я обнаружил сотни писем между Врублевским и Станиславом Мальцевым, бывшим следователем российского Министерства внутренних дел. В 2007 году Мальцев отвечал за расследование обвинений Врублевского в незаконной предпринимательской деятельности. Но вскоре Врублевский нанял Мальцева руководителем своей службы безопасности, и дело против него быстро заглохло.[1]

Стало также ясно, что руководители ChronoPay безуспешно пытались отделить «чёрные» проекты компании, например программу аптечного спама Rx-Promotion и предприятие поддельных антивирусов, от более законной клиентской базы. Утёкшие письма ChronoPay показывают, что в августе 2010 года сооснователь Павел Врублевский разрешил выплатить 37 350 российских рублей, около 1 200 долларов, за многопользовательскую лицензию на сетевую службу отслеживания и управления разработкой проектов MegaPlan.

Сотрудники ChronoPay использовали учётные записи MegaPlan для учёта проблем с обработкой платежей, объёмов заказов клиентов и рекламных партнёрств этих чёрных программ. Словно персонажи фильма Квентина Тарантино *Бешеные псы*, они взяли любопытные псевдонимы: Mr. Kink, Mr. Stranger, Mr. Templar и Ms. Gandalfine.

Однако в классическом провале оперативной безопасности многие сотрудники настроили автоматическую пересылку сообщений и паролей MegaPlan на свои рабочие адреса ChronoPay, которые в итоге попали в массив утёкшей почты. Организационная схема на главной странице MegaPlan компании ChronoPay показывала, что бывшего милиционера Мальцева, также известного как Mr. Heppner, назначили заместителем руководителя Rx-Promotion непосредственно под «большим боссом» Врублевским, также известным как RedEye.

Наконец у меня появился ключ, который я искал. Учётные записи MegaPlan стали крупнейшим единым хранилищем сведений о масштабах участия ChronoPay в развитии рынков мошеннических антивирусов, или scareware. Эти вредоносные программы показывают обманные предупреждения о несуществующих угрозах безопасности на персональном компьютере жертвы, а затем удерживают машину в заложниках, пока пострадавший не найдёт способ удалить вредоносную программу или не заплатит за лицензию на поддельное средство.

Подобные программы затрагивают десятки миллионов людей по всему миру и приносят поразительную прибыль. Большинству владельцев персональных компьютеров было бы трудно утверждать, что они никогда не встречали таких сообщений. И это лишь самый заметный признак того, что вашу машину захватил удалённый спамер или другая, более скрытная вредоносная

программа. Что бы вы ни делали, никогда не нажимайте на такие сообщения! Постарайтесь немедленно удалить вредоносную программу с помощью специалиста по антивирусной защите или обратитесь к эпилогу за советами о том, как не усугубить подобную неприятную ситуацию.

Утёкшие документы показывают, что подразделение высокорисковых, или «чёрных», проектов ChronoPay усердно старалось оставаться на переднем крае индустрии scareware. В марте 2010 года компания начала обрабатывать платежи для icpp-online.com, новаторского мошеннического сайта, который отнимал деньги у жертв, запугивая их необходимостью выплатить «досудебное урегулирование» в счёт «штрафа правообладателю».

Как в то время отмечала компания по безопасности F-Secure, жертвам мошенничества сообщали, что «сканер Фонда борьбы с пиратством» обнаружил в их системе пиратские фильмы и музыкальные файлы, а отказ заплатить 400 долларов кредитной картой может привести к тюремному заключению и огромным штрафам. Схема была гениальна в своей простоте. Многие люди когда-либо смотрели или слушали пиратские материалы, поэтому у них не было причин не доверять сообщению. В результате обманули тысячи человек.

Но вот самое важное: много лет scareware представляло проблему лишь для владельцев персональных компьютеров, просматривавших Интернет на машинах под управлением Microsoft Windows. Однако в мае 2011 года распространители scareware впервые начали атаковать пользователей операционной системы Apple Mac OS X. От спама и вредоносных атак больше не был защищён никто.

Утёкшие внутренние документы ChronoPay раскрыли участие компании и в этом новшестве. Через несколько дней после появления первых атак опытные пользователи Mac на форумах поддержки Apple начали сообщать, что новые разновидности вредоносных программ для Mac направляют пользователей на домен mac-defence.com, чтобы те заплатили за программу. Другие обнаружили поддельное средство защиты Mac, поступавшее с macbookprotection.com. Впервые взглянув на регистрационные записи этих доменов, я не удивился, обнаружив отчётливый отпечаток ChronoPay.

В регистрационных данных обоих доменов был указан контактный адрес fc@mail-eye.com. Утёкшие документы ChronoPay показывали, что компания владела доменом mail-eye.com и платила за виртуальные серверы в Германии, на которых он работал. Записи также указывали, что адрес fc@mail-eye.com принадлежал финансовому контролёру ChronoPay, тогдашней сотруднице Александре Волковой. Неопровержимое доказательство было найдено, и настало время сообщить о нём обществу.

• * *

После публикации статьи о Пономарёве Врублевский начал звонить мне по телефону не реже раза в день, часто без всякой очевидной причины. Почти каждый звонок поступал с нового мобильного номера. Когда я спросил, почему его звонки всегда приходят с разных российских номеров, Врублевский невозмутимо ответил, что сейчас у него не меньше девяти мобильных телефонов. По его словам, это была обычная тактика успешных российских предприятий, желавших уклониться от слежки назойливых сотрудников российского правительства.

Сначала мне казалось, что он ведёт себя театрально или страдает чрезмерной паранойей. Позднее я узнал, что он действительно был объектом наблюдения российского правительства. «Гусев опубликовал в своём блоге имя сотрудника ФСБ, который работает над делом Врублевского, - сказал мне генеральный директор ChronoPay в одном телефонном разговоре, говоря о себе в третьем лице. - Они прослушивают мой телефон и знают, что я постоянно общаюсь с тобой».

Я быстро обнаружил, что этот человек наслаждался звуком собственного голоса сильнее всех, кого я когда-либо встречал. Несмотря на всё известное мне о нём и на то, что он часто был невероятно

груб, насмешлив и нередко переходил к прямым оскорблениям, я также находил его обезоруживающе обаятельным, забавным и приятным. Он с той же готовностью смеялся над собой, что и над другими, и обладал, казалось, неиссякаемым запасом историй о влиятельных российских посредниках, политиках и киберпреступниках. Без всякой подсказки Врублевский возбуждённо перескакивал с одной красочной истории на другую, словно описывал сложную мыльную оперу, у которой, правда, никогда не было ни центрального сюжета, ни развязки.

Москва опережает Вашингтон, округ Колумбия, находящийся в восточном часовом поясе, на восемь часов. Поэтому Врублевский обычно звонил мне, когда шофёр вёз его из офиса ChronoPay домой. Иными словами, Павел часто был готов расслабиться и поболтать именно тогда, когда я собирался сосредоточиться и начать рабочий день. Большинство разговоров заканчивалось тем, что я вешал трубку: он отказывался понимать намёки на то, что у меня есть и другие дела, кроме многочасового выслушивания его болтовни.

Сначала я думал, что своими телефонными разговорами он пытается добиться от меня публикации чего-нибудь, оправдывающего его нарушения, которых с каждым днём я обнаруживал всё больше. В каждой беседе Врублевский старательно изображал себя борцом с киберпреступностью, решившим уничтожить индустрию спама и добиться ареста и осуждения всех спамеров.

Врублевский постоянно намекал, что я ничего не понимаю в киберпреступности, а полностью разобраться в тонкостях темы невозможно без хотя бы символического визита в Россию. В одном разговоре он предложил оплатить мне перелёт в Москву, чтобы я собственными глазами увидел, что он действительно один из хороших парней.

«Я предлагаю вам приехать в Москву, а если у вас нет денег... Я понимаю, что журналисты в Америке не настолько богаты... Мы с радостью заплатим», - сказал Врублевский в телефонном разговоре 8 мая 2010 года.

Когда я вежливо отклонил приглашение, Врублевский рассмеялся и сказал, что я ошибочно воспринимаю происходящее как подкуп или запугивание, хотя именно так я и думал.

«Довольно забавно, что вы считаете, будто, прилетев на встречу со мной в Москву или в офис ChronoPay, можете оказаться в какой-либо опасности и я вас убью, - сказал Врублевский, в точности угадав мои мысли. - Приезжайте в Москву и убедитесь сами. Возьмите блокнот, приходите ко мне в офис. Сядьте передо мной и осмотритесь. Потому что информация, которую вы получаете, если честно, не соответствует действительности». В конце концов я сделал именно то, к чему призывал Врублевский, как мы увидим в главе 9 «Встреча в Москве».

Примерно через месяц ежедневных, а иногда и происходивших дважды в день звонков Врублевского я понял, что он снабжает меня наполовину достоверными сведениями о других киберпреступниках в надежде отвлечь на их исследование и статьи вместо него самого.

Настоящая проблема этих бесед, помимо их склонности пожирать половину моего рабочего дня, заключалась в необходимости отделять крупицы истины и факты от размышлений Павла, параноидальных теорий заговора и попыток отвлечь внимание от собственных дел. Когда я прямо спросил его о своей теории, согласно которой он старался отвести от себя свет прожектора, развлекая меня замысловатыми историями о соперниках-предпринимателях из российского подполья, Павел на мгновение выронил телефон и около минуты безостановочно хохотал.

«Знаешь, Брайан, иногда ты меня удивляешь. Действительно удивляешь. Вот почему я просто охренеть как тебя люблю, - сказал он, подняв телефон, всё ещё фыркая и потешаясь надо мной. - Почему я это говорю? Забавно, но порой я не уверен, что ты очень-то умён. А потом ты вдруг выдаёшь что-нибудь подобное. Чёрт побери, Кребс, иногда ты, мать твою, гораздо умнее, чем кажешься».

Однако Врублевский бывал и переменчивым: был склонен к резким перепадам настроения, принимался бормотать или выкрикивать ругательства. А иногда голос на другом конце линии

звучал словно у совершенно иного человека - тихо и сравнительно безмятежно. Часто это происходило поздно вечером, когда его трое детей и жена Вера уже лежали в постели, а он, возможно, выпил несколько рюмок или принял что-нибудь ещё, чтобы снять напряжение.

В одном марафонском телефонном разговоре вскоре после того, как я сообщил Врублевскому о получении компромата, он пребывал в одном из мрачных настроений и довольно прямо предложил заплатить мне 30 000 долларов за передачу всех полученных материалов. Я рассказал ему об утёкших документах, потому что полагал: он и так хорошо представляет, какие сведения были похищены. Очевидно, будущая гарантия моего молчания интересовала его сильнее, чем возвращение контроля над компроматом. Я вежливо отклонил денежное предложение и сказал, что польщён, но всё равно собираюсь продолжать расследования.

Вскоре я понял, что в своём крестовом походе за восстановление положительного образа ChronoPay Врублевский нацелился на другую, гораздо более крупную мишень: Игоря Гусева, бывшего делового партнёра по ChronoPay, который теперь возглавлял аптечную партнёрскую программу, непосредственно конкурировавшую с Rx-Promotion Врублевского. Врублевский был убеждён, и, думаю, справедливо, что внутренние письма ChronoPay и другие уличающие документы передал Гусев или один из его приспешников.

Примерно тогда же, когда утекла первая порция компромата ChronoPay, Адам Дрейк, источник из сообщества борцов со спамом, которому я рассказывал кое-что о странных звонках Врублевского, написал мне о только что полученном причудливом сообщении. Таинственный корреспондент Дрейка под псевдонимом Despduck утверждал, что имеет доступ к базе данных GlavMed и SpamIt, родственных программ, отвечавших за огромную долю мировой проблемы спама. Часть Desp в псевдониме обыгрывала прозвище Игоря Гусева, человека, который в 2003 году вместе с Врублевским основал ChronoPay, а два года спустя ушёл и самостоятельно создал SpamIt и GlavMed.

Дрейк писал:

> Брайан,
>
> Недавно вы писали о расследовании российским правительством деятельности SpamIt («По следу денег, часть II» - krebsonsecurity.com).
>
> Со мной связался человек из России, который называет себя другом бывшего участника партнёрской группы SpamIt-GlavMed. У него много сведений, которыми я хочу конфиденциально поделиться с вами.
>
> Я говорю об этом, потому что хотел узнать ваше мнение. Он утверждает, будто знает, каким образом вам передали часть сведений для той статьи, и мне хотелось услышать ваши мысли по этому поводу.
>
> Кроме того, он утверждает, что располагает довольно большим объёмом необработанных данных, связанных с несколькими местами их встреч. Если они покажутся подлинными, я передам их правоохранительным органам. С прошлого года я работаю с оперативной группой, в которую входят сотрудники Интерпола и ФБР и которая расследует деятельность этой группы, поэтому почти ничего не мог публиковать открыто.
>
> Если всё это не относится к вашей области или выходит за круг интересов, дайте знать, но мне показалось, что вам это может пригодиться. Та же группа, вероятно, стоит и за валом мошеннической антивирусной дряни, которая сейчас повсюду распространяется.
>
> Надеюсь, во всём остальном у вас всё хорошо.

Я сразу узнал в этой уловке руку Врублевского и попросил Дрейка переслать копию письма Despduck. Читая сообщение, я едва верил своим глазам: оно выглядело так, словно кто-то записывал под диктовку Врублевского одну из его возбуждённых бессвязных историй, которыми он

потчевал любого готового слушать. Письмо насчитывало более двух тысяч слов и было переполнено сложными теориями о том, кто стоял за атаками на ChronoPay, компанию, о которой Despduck отзывался исключительно восторженно.

Я рассказал Дрейку о подозрении, что Врублевский теперь преследует и его. Дрейк признался, что его знакомый правоохранитель, хорошо знавший Врублевского и тоже видевший письма Despduck, независимо пришёл к тому же выводу.

В письмах Despduck оставалось ещё что-то, чего я никак не мог уловить. Через неделю я вернулся к своей прежней переписке с Врублевским и сравнил её с письмами Despduck, которые получал мой источник из сообщества борцов со спамом. Одна общая черта немедленно бросилась в глаза на экране. И Despduck, и Врублевский писали английские слова You и Your с прописной Y независимо от их положения в предложении и количества повторений. Ни одно другое слово, которое не следовало писать с прописной, подобным образом в письмах не выделялось.

Тогда я задумался: а как насчёт письма с угрозой «съесть глаза», полученного сразу после звонка Врублевскому за комментарием к статье об обвинениях Пономарёва? Разумеется, там обнаружилась та же особенность регистра. Части головоломки начали складываться.

Но зачем Врублевский прикладывал столько усилий к многовекторной кампании, одновременно пытаясь привлечь меня на свою сторону и принудить к сотрудничеству? Ответ дал мой источник из сообщества борцов со спамом, поделившийся несколькими письмами Despduck. Они показывали, что Врублевский считал, будто я получил деньги от его соперника на рынке фармацевтического спама Гусева в обмен на статьи о деяниях Врублевского. По-видимому, он был также убеждён, что я состою в сговоре с таинственными фигурами, стоявшими за Russian Business Network (RBN), империей пуленепробиваемого хостинга, подробно описанной в первой половине главы 2.[2]

Despduck писал, снова используя прописную Y в слове You:

> 1. Хотите верьте, хотите нет, но парни из RBN, главным образом GlavMed, действительно заплатили Брайану Кребсу за публикацию его исследований. В действительности все его сведения основаны на том факте, что офисным адресом re-partners.biz был указан адрес ChronoPay, а это, разумеется, полная чушь. Любой человек может где угодно указать какой угодно адрес.
>
> 2. Затем Илья Пономарёв, который НЕ является ведущим российским политиком, написал российским ментам письмо, пытаясь как-то поиметь Врублевского на основании сведений Кребса. Глупая попытка, вероятно лишь видимость работы, чтобы получить от Desp больше денег. Разумеется, ничего не произошло, потому что у ChronoPay чрезвычайно сильный образ и бренд в России. ChronoPay скоро подаст на Кребса в суд, а Пономарёв уже изменил своё мнение и направил ментам ещё одно письмо, объяснив, что не преследовал Врублевского.
>
> 3. Всё это произошло потому, что Врублевский занимает должность в российском правительстве и борется со спамом, а что ещё важнее, защищает образ России за рубежом. За это спамеры его ненавидят. Расскажу подробнее, когда у Вас появятся вопросы.

Despduck снова восторженно описывал Врублевского как борца с киберпреступностью, которого средства массовой информации и деловые соперники несправедливо обвиняли в организации злодеяний, с которыми тот якобы сражался. Теперь я был как никогда уверен, что Despduck и есть Врублевский.

12 июля 2010 года анонимный источник, с которым я переписывался по электронной почте, прислал мне ещё одно огромное хранилище компромата, похищенного из ChronoPay. Источник, использовавший в переписке только имя Борис, сказал, что делится данными из-за разочарования

российскими властями. По его словам, те считали Врублевского едва ли достойным труда вытряхнуть из него взятки, не говоря уже о расследовании.

> Брайан,
>
> Этот файл содержит полные сведения о преступной деятельности ChronoPay и лично Павла Врублевского по легализации вне-законных денег [так в оригинале]. Мы испробовали все доступные в России методы, но абсолютная коррупция российской милиции тормозит [так в оригинале] уголовное дело, и оно топчется на месте. Надеемся, вы сможете эффективно использовать эти сведения в борьбе за чистоту Интернета. Тот же файл две недели назад был передан ФБР.
>
> Удачи,
> Борис

Письма ChronoPay, переданные Борисом, та самая «сокровищница документов», упомянутая в конце главы 2, показывали, что Врублевский нанял хакера под именем Nooder Tovreance для взлома SpamIt Гусева и кражи платёжных документов и данных клиентов организации. В переписке, начавшейся 8 апреля 2010 года и закончившейся в начале июня, Tovreance предложил продать Врублевскому базу за 20 000 долларов, но сообщил, что из-за её размера передачу придётся разбить на несколько меньших частей.

В конце концов они сошлись на цене 15 000 долларов с оплатой в WebMoney, виртуальной валюте, популярной в России и Восточной Европе. Первые 7 500 долларов следовало перевести на указанный Tovreance кошелёк WebMoney в обмен на половину файлов, а оставшуюся сумму выплатить после получения Врублевским всей базы. Последующая переписка показывала, что Врублевский заплатил первые 7 500 долларов, но отказался от второго платежа, получив обещанную базу. Во время нашей беседы Tovreance подтвердил, что Врублевский нанял его добыть данные GlavMed и SpamIt и действительно обманул на половину обещанной суммы.

• * *

Примерно через неделю после того, как злоумышленники передали компромат ChronoPay, Дрейк позвонил с новостью: Despduck прислал ему копию базы SpamIt и GlavMed. К тому времени я начал думать, что Врублевский прячется за личностью Despduck, передавая базу клиентов GlavMed-SpamIt, а Гусев, в свою очередь, пользуется личностью Бориса, снабжая меня похищенными у ChronoPay сведениями.

База GlavMed-SpamIt попала ко мне на следующий день после того, как я опубликовал в блоге первую срочную новость о новом, чрезвычайно сложном компьютерном черве, который, по-видимому, превратили в оружие шпионажа. Это была первая широко прочитанная статья о вредоносной программе беспрецедентной сложности, позднее получившей название Stuxnet. Впоследствии специалисты установили, что этот компьютерный червь был кибероружием, созданным разведывательными службами Израиля и США в ходе успешной попытки задержать осуществление ядерных устремлений Ирана.

Но статью о Stuxnet я опубликовал, как раз отправляясь на недельный отдых с женой и матерью в Йорк, штат Мэн, и пообещал отдохнуть от работы. Для дальнейшего освещения Stuxnet потребовались бы десятки телефонных бесед. А изучать эксклюзивные сведения, переданные источником из сообщества борцов со спамом, можно было так, чтобы семья не узнала о моём возвращении к работе.

Дрейк создал для меня учётную запись на своём веб-сервере и поместил туда копию архива SpamIt. Файл содержал почти десять гигабайт данных. Чтобы представить объём: если бы базу SpamIt напечатали в книгах в мягкой обложке толщиной три дюйма, для них потребовалась бы книжная полка примерно с футбольное поле.

Я уже был завален гигабайтами увлекательных внутренних материалов ChronoPay и вынужден был удалить данные с диска своего MacBook, чтобы разместить архив SpamIt. Сидя с ноутбуком на коленях на задней террасе дома для отдыха на побережье Мэна и слушая рёв океанского прибоя, я начал осознавать огромный масштаб стоявшей передо мной задачи. Мне предстояло разобраться в необработанных разведывательных данных от двух крупнейших спонсоров спама на планете и тем самым, возможно, навлечь на себя гнев самых могущественных и мстительных киберпреступников мира.

Сноски

[1] [назад] Врублевский утверждал, что обвинения были сфабрикованы и представляли собой не более чем организованное его врагами законное вымогательство. Однако компания, которую «вымогатели» пытались потрясти, управляла созданной им виртуальной валютой, помогавшей его веб-мастерам и спамерам получать плату, не оставляя официального денежного следа в российских банковских сетях.
[2] [назад] Хотя Врублевский делал вид, будто не имеет никакого отношения к RBN, сайты аптечного спама и партнёрские программы поддельных антивирусов, которыми он управлял, в полной мере пользовались хостингом под вывеской RBN.

Глава 4. Знакомство с покупателями

Хотя моей конечной целью было разоблачить владельцев ботнетов, получавших деньги за рассылку большей части нежелательной почты в мире, я понимал, что на изучение данных двух конкурирующих мошеннических аптечных программ уйдут месяцы, возможно годы. Пока я обнаружил лишь отдельные фрагменты преступной деятельности. Чтобы построить против этих людей неопровержимое дело и раскрыть их вредоносные действия, требовалось гораздо более глубокое исследование и расследование. Я решил сосредоточить ближайшие усилия на людях, непосредственно пострадавших от киберпреступников: покупателях, которые приобретали и принимали таблетки из спамерской рекламы.

Почти все мы когда-либо получали спам о таблетках или аптечный спам: письма во входящих, спам-фильтрах и папках нежелательной почты, предлагающие дешёвые рецептурные лекарства или средства для улучшения возможностей организма. Вряд ли кого-то поразит, что около 70 процентов операций через мошеннические аптечные сайты, рекламировавшиеся SpamIt Гусева и Rx-Promotion Врублевского, приходилось на средства для увеличения мужских возможностей, такие как Viagra и Cialis. Даже клиенты GlavMed, не заказывавшие лекарства от эректильной дисфункции, обычно всё равно получали таблетки для потенции. Аптеки настолько верили в силу своего ассортимента средств от эректильной дисфункции, что постоянно вкладывали в каждый заказ от двух до четырёх бесплатных образцов таких таблеток.[1]

Тем из нас, кому и в голову не придёт заказать что-либо в неизвестной аптеке, это может показаться очевидным и совершенно ненужным риском. Почему просто не воспользоваться обычной аптекой? Мне действительно было чрезвычайно интересно узнать, что заставляло людей заниматься столь явно рискованным делом и были ли они довольны покупками или считали себя обманутыми. Я думал: если опросить достаточно покупателей и установить, что в целом они не получили ожидаемого, обнародование такой реакции поможет сократить спрос и в конце концов лишить спамеров дела.

Благодаря утечкам данных из Rx-Promotion и GlavMed-SpamIt у меня были имена, телефонные номера, адреса и номера кредитных карт более чем миллиона людей, купивших лекарства из спамерской рекламы. Некоторые заказы были довольно свежими. Поэтому я стремился поговорить с покупателями, у которых могли ещё оставаться таблетки и которые могли прислать их мне для исследования в квалифицированной лаборатории, чтобы выяснить, что в действительности получали потребители.

Я намеренно не звонил клиентам, которые искали и покупали поддельные Viagra и Cialis. Отчасти я считал, что люди, пришедшие в эти аптеки-однодневки за лекарствами от более серьёзных заболеваний и состояний, расскажут более интересные, вызывающие сочувствие истории, которые помогут добраться до сути: кто покупал лекарства и почему? Но было бы нечестно отрицать, что на мой подход повлиял и случай, произошедший с собеседником в самом начале общения с покупателями.

Всего через несколько дней после того, как я начал звонить покупателям лекарств GlavMed, я набрал номер клиента-мужчины, заказавшего Viagra. Вместо него ответила жена. Когда я объяснил, что несколькими месяцами ранее её муж купил непатентованный Cialis, она расплакалась. Она ничего об этом не знала и сказала, что не может представить ни одной причины, по которой он мог ему понадобиться. После этого, к счастью, короткого разговора я решил больше не звонить покупателям, заказывавшим только препараты от эректильной дисфункции.

За два месяца я позвонил более чем четырёмстам людям, покупавшим таблетки в SpamIt. Большинство тех, с кем удалось связаться, либо бросали трубку, либо отказывались от разговора. Но мне удалось опросить по меньшей мере сорок пять покупателей, заказывавших всё - от

сердечных лекарств и антидепрессантов до таблеток от заболеваний щитовидной железы. Я начал яснее понимать, кем были эти люди, что ими двигало и как их поступки влияли на всех нас, даже на тех, кто не открывает спамерские письма и тем более ничего по ним не покупает.

Многие люди, особенно борцы со спамом, по понятным причинам неодобрительно относятся к потребителям, покупающим товары из нежелательной почты. Рассуждение таково: если люди перестанут покупать на сайтах, которые рекламирует ежедневно переполняющий наши ящики спам, то индустрия спама и многие связанные с ней угрозы нашей личности и безопасности, вероятно, значительно уменьшатся. Но, вопреки распространённому мнению, большинство покупателей спамерских товаров не глупы и не безумны. Как правило, это не слишком искушённые в технологиях люди, которые делают рациональный, хотя, возможно, рискованный выбор на основании одной или нескольких основных причин:

• **Цена и доступность.** Почти все покупатели лекарств, не предназначенных для увеличения мужских возможностей, говорили, что откликнулись на спам с рецептурными препаратами либо из-за отсутствия медицинской страховки, либо потому, что те же лекарства по их плану страхования стоили в два-пять раз дороже предложений этих вызывавших доверие канадских аптечных сайтов. В действительности спамеры лишь заимствовали хорошую репутацию законных канадских аптек. Как мы увидим в главе 5, лекарства, которые отправляла каждая партнёрская программа, производились главным образом в Индии и Китае, а продававшие их сайты чаще всего размещались на взломанных персональных компьютерах-ботах, которыми спамеры пользовались для рассылки нежелательной почты.
• **Конфиденциальность.** Покупатель хочет приобрести определённые препараты тихо и без огласки из-за смущения или застенчивости либо потому, что считает необходимым что-то скрыть от супруга или близкого человека. Большинство опрошенных мною клиентов в этой группе делилось на два лагеря: люди, самостоятельно лечившие венерические заболевания, и те, кто заказывал средства от импотенции ради секса с любовником или супругом. К сожалению, история заказов показывает, что некоторые покупатели неоднократно относились сразу к обеим категориям.
• **Удобство.** Заказать лекарства в Интернете без рецепта и получить их у двери чрезвычайно удобно. Кроме того, очень многие мои собеседники говорили, что всего лишь покупали препараты, которые им уже назначали при сходном или связанном заболевании. По существу, эти люди сами выписывали себе лекарства и не видели смысла платить за визит к врачу или мириться с более высокими ценами местных аптек.
• **Развлечение или зависимость.** Покупатели этой категории приобретали преимущественно лекарства, продажа и использование которых в Соединённых Штатах ограничены, обычно из-за возможности злоупотребления. Прежде всего это были обезболивающие, такие как непатентованные оксикодон, гидрокодон и трамадол; средства для снижения веса вроде фентермина, мощного стимулятора; и снотворные, такие как Soma и Lunesta. Возможно, из-за способности некоторых препаратов вызывать зависимость покупатели этой категории становились самыми верными, прибыльными постоянными клиентами.

Цена

Клиенты SpamIt покупали рекламируемые спамом лекарства по разным причинам, но чаще всего я слышал об их доступной цене, особенно от покупателей препаратов для лечения хронических заболеваний.

Не случайно большинство клиентов SpamIt живёт в Соединённых Штатах, стране с самыми высокими в мире ценами на рецептурные лекарства. Стоимость фармацевтических препаратов в США значительно выше, чем в Канаде, Индии, Великобритании и многих других странах, во многом потому, что там установили государственное регулирование цен на лекарства. В 2010 году

потребители и страховые компании платили в среднем 13,14 доллара за рецепт на один из пятидесяти наиболее популярных непатентованных препаратов. В 2014 году они платили уже 62,10 доллара, что означает рост на 373 процента. За последние годы стремительно выросли и цены фирменных лекарств. Исследование Bloomberg News 2014 года показало, что с конца 2007 года цены многих фирменных препаратов в Соединённых Штатах росли гораздо быстрее инфляции. Издание обнаружило семьдесят четыре бренда, у которых американская цена хотя бы одной дозировки за этот период поднялась не менее чем на 75 процентов.

К другим причинам удорожания рецептурных препаратов относятся резкий рост спроса на них за последнее десятилетие; активное продвижение среди потребителей и врачей более дорогих фирменных лекарств; попытки производителей возместить значительные расходы на исследования и разработку; а также дорогостоящая игра в кости, которой является вывод нового препарата на рынок Соединённых Штатов. Согласно исследованию Центра изучения разработки лекарств Университета Тафтса за 2014 год, производители могут потратить более 2,5 миллиарда долларов за десять и более лет до получения разрешения продавать новое рецептурное средство.

Но это ещё не всё. В знаковом исследовании экономики мошеннических интернет-аптек 2011 года учёные Калифорнийского университета в Сан-Диего (UCSD) нашли способ изучить бесчисленные записи о покупках в сетевых магазинах таблеток, связанных с EvaPharmacy, ещё одной мошеннической аптечной партнёрской программой, которая напрямую конкурировала с подобными Rx-Promotion и SpamIt. Исследователи обнаружили существенные различия в выборе лекарств американцами и покупателями из Канады и Западной Европы. При анализе таблетки EvaPharmacy разделили на две широкие категории: препараты образа жизни, например средства от эректильной дисфункции и таблетки гормона роста человека, и препараты, не связанные с образом жизни, в том числе лекарства от тревожных расстройств, инфекций носовых пазух, высокого артериального давления, выпадения волос, рака и бесплодия.

Исследователи обнаружили, что американские покупатели в 33 процентах случаев выбирали товары, не связанные с образом жизни. Покупатели из Канады и Западной Европы, напротив, почти всегда приобретали препараты образа жизни: лишь 8 процентов товаров в их корзинах относились к другой категории. Иными словами, гораздо больше американцев обращалось в эти спамерские аптеки за рецептурными средствами для лечения серьёзных заболеваний, а не для повышения удобства или удовольствия от жизни.

«Мы полагаем, что это различие может быть обусловлено особенностями систем здравоохранения. Препараты, необходимость которых легко обосновать врачу, могут полностью оплачиваться государственными планами медицинского страхования в Канаде и Западной Европе, оставляя внешнему рынку лишь товары, связанные с образом жизни, - писали исследователи. - В Соединённых Штатах, напротив, отдельные клиенты без страховки или с недостаточным страховым покрытием могут считать рекламируемые спамом аптеки, где не требуется рецепт, конкурентным рынком для удовлетворения своих медицинских потребностей».

Интересно, что десятки опрошенных мною клиентов SpamIt говорили: полученные таблетки невозможно отличить от тех же препаратов, купленных в местных аптеках, за исключением того, что заказанные в Интернете обходились гораздо дешевле. Многие покупатели были настолько довольны заказами, что месяц за месяцем возвращались на тот же сайт.

Сорокадвухлетний калифорнийский агент по недвижимости Генри Уэбб к моменту моего первого звонка почти три года покупал лекарства в сетевых аптеках, хотя, по его словам, до нашего разговора понятия не имел, у кого именно их приобретает. Большую часть взрослой жизни Уэбб боролся с депрессией, пока около десяти лет назад врач не назначил ему рецептурный антидепрессант Lexapro. Годами Уэбб платил почти 500 долларов за запас препарата на девяносто дней.

Но однажды он открыл незапрошенное письмо, рекламировавшее Lexapro почти вчетверо дешевле. С тех пор он заказывал на нескольких разных сайтах «канадских аптек» и утверждал, что пока не столкнулся ни с одним неприятным случаем.

«Таблетки выглядят в точности как те, за которые я платил пятьсот долларов в аптеке: такая же блистерная упаковка и всё остальное, - сказал Уэбб. - Могу лишь заметить, как печально, что мы живём в этой стране и вынуждены искать доступные лекарства за пределами Соединённых Штатов».

Когда через несколько месяцев после первого разговора я снова связался с Уэббом, он сказал, что перестал заказывать в Интернете после неприятного случая с препаратами, от которых ему стало плохо. Уэбб также столкнулся с тем, что рано или поздно ожидает почти каждого покупателя рекламируемых спамом товаров: непрерывными звонками агрессивных продавцов сетевых аптек, пытавшихся снова наполнить его запас лекарства или продать другие препараты.

«Они не оставляют меня в покое и звонят по нескольку раз в день, - сказал Уэбб. - Я не могу сменить номер, потому что он связан с моей работой. Эти люди прибегают к очень коварным приёмам, например подменяют номер звонящего, чтобы казалось, будто звонят из моего района. И я отвечаю, потому что должен оставаться на связи с клиентами по недвижимости».

Проблему цен для потребителей усугубляет малоизвестная, но широко распространённая практика, при которой крупнейшие производители лекарств платят конкурентам, выпускающим непатентованные препараты, за задержку появления более дешёвых средств. По данным Федеральной торговой комиссии США (FTC), в 2010 финансовом году фармацевтические компании заключили беспрецедентное число подобных сговоров. FTC установила, что их количество взлетело более чем на 60 процентов: с девятнадцати в 2009 финансовом году до тридцати одного в 2010-м. В 2013 году производители фирменных и непатентованных лекарств заключили не менее двадцати девяти соглашений «плата за задержку», совокупный годовой объём продаж по которым в США составлял около 4,3 миллиарда долларов.

Крейг С., ныне вышедший на пенсию продавец страхования жизни из Северной Каролины, не понаслышке знает, что чувствуешь, когда производитель лекарств или медицинская страховая компания внезапно перестаёт предлагать непатентованные препараты. По словам Крейга, раньше работодатель, у которого он прослужил двадцать лет, предлагал медицинский план с щедрым покрытием лекарств. Но за год до нашей беседы работодатель отказался от страховой компании и перевёл всех сотрудников на медицинские сберегательные счета (HSA), внося на них всего тысячу долларов в год. Врач давно назначил Крейгу фирменный препарат Actos для лечения диабета второго типа, а Крейг покупал его непатентованный вариант.

Но вскоре он обнаружил, что программа HSA не предлагает непатентованный Actos. Как ни странно, при этом ему удалось воспользоваться кредитной картой HSA, чтобы за 178 долларов с учётом доставки и обработки купить в магазине таблеток GlavMed запас на девяносто дней.

«Лекарство, которое врач хочет заставить меня принимать, стоит 212 долларов в месяц, и я сказал ему, что этого просто не будет, - рассказал Крейг. - Теперь оно обходится примерно в треть того, что я ежемесячно платил бы за фирменный вариант по своему медицинскому плану».

Когда его спросили, тревожат ли его качество, эффективность и безопасность приобретаемых у спамеров лекарств, Крейг ответил: «Не особенно». По его словам, он по-прежнему посещал врача каждые девяносто дней, и заказываемые в GlavMed препараты, судя по всему, удерживали диабет под контролем.

Главным образом он опасался, что однажды заказанные таблетки просто не придут по почте. Однажды такое едва не случилось: заказ прибыл на неделю позже положенного. Но пока поставщики лекарств через Интернет, похоже, навели порядок с доставкой. Крейг рассказал, что раз в несколько месяцев, примерно за три недели до окончания запаса, ему начинают звонить

люди с индийским акцентом и спрашивают, готов ли он снова заказать лекарства.

• * *

Житель Иллинойса под вымышленным именем Стив подозревал, что девушка ему изменяет, но окончательно поверил в это лишь в тот день, когда получил потрясающую новость в текстовом сообщении.

«Мне понадобились лекарства от синдрома изменившей девушки», - смущённо объяснил Стив причину покупки во время нашей беседы. «Однажды она написала, что у неё гонорея и мне тоже следует провериться».

Месяц выдался для Стива тяжёлым. Девушка не только переспала с коллегой, бросила его и наградила, к счастью, излечимым венерическим заболеванием. Работодатель, компания по экологическим исследованиям, только что его уволил, и медицинской страховки у него не было.

«Я мог бы получить страховку COBRA, но это триста-четыреста долларов в месяц, - объяснил Стив. - Когда у тебя нет дохода, но есть аренда, платёж за машину и всё остальное, это не настоящий вариант».

Бывшая девушка услужливо прислала название препарата, который врач назначил ей для излечения: полный курс таблеток эритромицина по 500 миллиграммов. Стив нашёл лекарство в Интернете на сайте, утверждавшем, что продаёт препараты из Канады. В действительности сайт, где Стив сделал покупку, размещался через GlavMed в Китае, а лекарства отправили из Индии. Через семь дней и шестьдесят долларов антибиотики были у Стива, и он направлялся к жизни без венерического заболевания.

Несмотря на обстоятельства покупки, Стив сказал, что в целом остался доволен GlavMed и купил бы там снова, если бы болезнь когда-нибудь обострилась.

«Сделал бы я это снова? Конечно. Зачем платить доплату и семьдесят пять долларов за рецепт, если в Интернете можно получить лекарство гораздо дешевле и с меньшими хлопотами? Таблеток, которые они прислали, хватило бы на лечение пяти человек. По такой цене их предложение не превзойти».

Как показывают истории этих покупателей, очень многие американцы обращаются к рекламируемым спамом лекарствам, потому что альтернатива в несколько раз дороже или страховка не покрывает назначенные препараты. Положительный опыт Стива с таблетками, заказанными для однократного курса, по-видимому, встречается довольно часто. Но постоянные покупатели лекарств от хронических заболеваний рано или поздно, скорее всего, получат плохую партию.

Как мы увидим в главе 5, причина в том, что рекламируемые спамом аптеки обычно получают дешёвые таблетки из десятков разных источников по всему миру. Некоторые из них, по-видимому, почти или совсем не несут ответственности за безопасность и эффективность препаратов. Низкосортные и некачественные лекарства могут всего лишь вызвать у покупателя болезнь, как случилось с Генри. В крайних случаях, которые мы увидим в главе 5, таблетки ненадлежащего качества могут отправить покупателя в больницу или, что ещё хуже, в морг.

Конфиденциальность

Вашингтонский житель под вымышленным именем Джон, по профессии юрист, проводил слишком много времени за столом и искал быстрый и простой способ нарастить мышцы. Изучив несколько сетевых форумов о бодибилдинге, он начал принимать юридически сомнительные стероиды с одного из сайтов, рекомендованных опытными качками. Через несколько месяцев и после

короткого цикла тренировок в зале таблетки для набора массы помогли прибавить несколько фунтов мышц к его худощавому телу.

Но однажды в феврале 2010 года Джон почувствовал припухлость и чувствительность вокруг сосков. Опасаясь, что это мог быть отсроченный побочный эффект таблеток для набора массы, и не желая обсуждать с врачом недавний курс, Джон вернулся за советом товарищей-качков на форумы бодибилдеров.

Участники форума сказали, что он страдает вызванной стероидами гинекомастией: аномальным увеличением молочных желёз у мужчины, из-за которого растёт грудь.

«Медицинское сокращение для этого состояния произносится как guyno, но большинство парней на форумах просто называет их „сучьими сиськами“, - рассказал Джон. - Парни говорили, что, если не исправить это лекарствами, придётся делать пластическую операцию на груди, а мне этого не хотелось».

По словам новых друзей Джона с форумов, его состояние лечилось курсом дополнительных препаратов, предназначенных для противодействия гормонам, вызывающим guyno. Среди них было лекарство Femara, которое чаще всего назначают пациенткам в постменопаузе с ранней стадией рака молочной железы.

Джон поискал в сети и в итоге купил на сайте GlavMed elitepharmacy.com двухнедельный курс таблеток Femara по 2,5 миллиграмма за 136 долларов. Он ждал лекарства три недели, но они не пришли. Тогда Джон отменил заказ в GlavMed и заказал их в другой сетевой аптеке, не связанной с GlavMed. По воспоминаниям Джона, оба сайта выглядели почти одинаково. Первый сайт извинился за задержку и вернул уплаченную сумму на его кредитную карту.

Препараты со второго сайта пришли в жёлтом конверте с индийским обратным адресом. Сами таблетки находились в запечатанном блистере, а название бренда Novartis было безукоризненно напечатано множество раз на серебряной фольге поверх них.

По словам Джона, таблетки выглядели настоящими, уменьшили чувствительность и припухлость сосков и тем самым подавили его надутую мужскую грудь в самом зародыше.

«Сначала я немного опасался всего происходящего, но средство сработало, - сказал Джон. - Кроме того, мне казалось, что отменять заказ бесполезно. Я в некотором роде считал это сомнительным предприятием... но они вернули деньги».

Опыт Джона показывает, насколько далеко готовы зайти мошеннические аптечные программы ради удовлетворения покупателя. Их цель не обязательно в том, чтобы клиент остался доволен. Скорее управляющие такими предприятиями готовы почти на всё, лишь бы покупатели не инициировали возвратный платёж, то есть отмену списания под предлогом мошенничества или другого нарушения со стороны сетевого магазина. Продавцы, получающие слишком много возвратных платежей, платят гораздо более высокую комиссию за обработку, а в конечном счёте могут быть оштрафованы, лишиться счетов или столкнуться с обоими последствиями.

Данные из клиентской базы GlavMed показывают, что в программе круглосуточно трудились десятки сотрудников поддержки. По телефону и через сетевой чат они отвечали на тревоги и вопросы покупателей по существующим заказам.

Спамер Вишневский, о котором говорилось в главе 1 и который работал с GlavMed-SpamIt, помогая финансировать разработку ботнета Cutwail, в беседе через службу мгновенных сообщений сказал, что покупатель аптечного сайта всегда может вернуть деньги. Для этого достаточно позвонить по бесплатному номеру программы и подать жалобу.

«Банк трахнет любого продавца, у которого возвратные платежи составляют больше 1 процента продаж, - сказал Вишневский. - Поэтому никто не станет рисковать [счётом обработки карт], отказываясь возвращать деньги, и каждый, кто попросит [службу поддержки аптечной партнёрской

программы] вернуть средства, их получит».

Самостоятельное назначение лекарств

Кимберли из Виргинии была покупательницей GlavMed, которая сама назначила себе лекарство, но получила возврат, пожаловавшись на покупку. Они с мужем не могли зачать ребёнка. Муж часто надолго уезжал на военную службу, и она очень хотела забеременеть до его следующей годичной командировки за границу. Кимберли, работавшая медсестрой, сказала, что решила заказать препарат от бесплодия Clomid через Интернет, поскольку знала, что именно его назначил бы репродуктолог.

«В сущности, я знала, как им пользоваться и что нужно делать. Вместо того чтобы платить врачу кучу денег за объяснение того, что я уже умею, я решила сделать всё сама, - объяснила Кимберли. - Я не просто заказала на первом попавшемся сайте. Я поискала и увидела, что множество других сайтов ссылается на один определённый».

Через несколько недель по почте пришёл коричневый конверт с индийской маркировкой. Таблетки Clomid находились в знакомой блистерной упаковке, но Кимберли заметила, что указанный срок годности уже истёк. Она потребовала вернуть деньги и немедленно их получила. По иронии судьбы всего через несколько дней после возврата она узнала о беременности: таблетки не понадобились.

Но с момента заказа лекарств её почтовый ящик, по её словам, переполнял спам. Она по-прежнему опасалась, что управляющие сетевой аптекой люди проведут мошеннические списания с кредитной карты.

«С тех пор они присылали мне спам миллион раз, - сказала Кимберли. - Я понимаю, что заказывать эти лекарства в Интернете было не лучшей идеей, но тогда я была в отчаянии. Очень рада, что не стала принимать препарат. Наверное, он повредил бы ребёнку, который уже был во мне».

Вишневский подтвердил, что после заказа по предложению из нежелательной почты или ответа на него людей часто заваливают спамом. Причина в том, что адреса известных покупателей являются ценным товаром, который часто перепродают или просто похищают другие хакеры и спамеры. Вспомним, как собственный список Вишневского с двумя миллиардами адресов остался на серверах McColo. Скачать его мог любой человек, случайно обнаруживший правильную ссылку на файл.

Но, по словам Вишневского, распространено ошибочное мнение, будто заказ на сайте сетевой аптеки приведёт к мошенничеству с кредитной картой. Ни один спамер SpamIt, GlavMed или другой программы аптечного спама не позволяет партнёрам просматривать карточные данные клиентов, поскольку владельцы хотят сохранить эти сведения для себя.

«Их видят только администраторы аптечной программы, а им невыгодно допускать мошенничество с картой, потому что из-за роста возвратных платежей и заявлений о мошенничестве продавец рискует потерять [счёт обработки карт]», - сказал он.

Зависимость и пристрастие

Большинство покупателей, с которыми мне удалось связаться и которые относились к этой категории, отказались от разговора. Кроме того, все они заказывали на сайтах партнёров Rx-Promotion Врублевского. Эта программа заняла нишу одной из немногих мошеннических аптечных партнёрских программ, рекламировавших и продававших обезболивающие, стимуляторы

и другие вещества, распространение которых строго контролируется властями Соединённых Штатов и других стран. Документы показывают, что в первые два года существования GlavMed тоже предлагала контролируемые таблетки, но к началу моей работы над проектом уже перестала их продавать.

Горан, сорокаоднолетний бывший военнопленный из Восточной Европы, который теперь жил в Соединённых Штатах, почти двадцать лет назад сильно повредил спину. Врачи давно перестали выписывать ему гидрокодон, поэтому он тратил от 250 до 500 долларов в месяц, покупая его вместе с трамадолом в Интернете, хотя в его штате это считалось тяжким преступлением. Утёкшие документы Rx-Promotion показывают, что на протяжении 2010 года Горан совершил несколько покупок.

Горан рассказал, что пока доволен покупками и что они подавляют боль примерно так же хорошо, как назначенные врачом лекарства. По его словам, сетевые препараты обычно отправлялись из Гонконга и приходили в блистерах, завёрнутых в герметичный пакет с застёжкой.

Без обезболивающих он, по его словам, не смог бы управлять своим транспортным предприятием. «Знаете, кто ты в этой стране, если не работаешь? - спросил он. - Бездомный».

Возможно, Горан принимал таблетки от настоящей боли в спине, но я подозревал, что многие другие делали это не по медицинским причинам. Интересно, что база GlavMed содержит явные признаки злоупотребления среди покупателей контролируемых веществ в годы, когда партнёрская программа их продавала. Я поделился клиентскими данными GlavMed с Гэри Уорнером, руководителем исследований компьютерной криминалистики в Алабамском университете в Бирмингеме. Он выполнил ряд запросов к базе, чтобы проверить, не проявятся ли очевидные закономерности.

«Мы установили, что, если клиент GlavMed делал более пяти заказов, с вероятностью 80-85 процентов он покупал трамадол или Soma, - сказал Уорнер. - Вопрос в том, приобретал ли он их для себя или для перепродажи. На улице такие таблетки стоят около пяти долларов за штуку. Это означает, что, заказав флакон в GlavMed и продав таблетки по одной, можно получить около 1 300 долларов прибыли с каждого флакона».

Исследователи UCSD, с которыми я поделился данными о продажах Rx-Promotion, тоже нашли убедительные признаки того, что значительную часть дохода мошеннической аптеке приносили постоянные покупатели. Команда установила, что продажа обезболивающих и других строго ограниченных в Соединённых Штатах препаратов обеспечивала 48 процентов всей выручки программы Rx-Promotion.

«То, что подобные лекарства представлены в непропорционально большой степени и в Rx-Promotion, и, применительно к Soma и трамадолу, в SpamIt, подтверждает гипотезу о том, что злоупотребление может быть важным источником этой части спроса», - написала команда UCSD в исследовательской работе о своих выводах.

По большей части мне не удалось узнать непосредственно у собеседников об эффективности и безопасности лекарств, полученных с сайтов GlavMed или Rx-Promotion. Почти каждый обещал прислать одну-две таблетки из полученной упаковки, но обещание выполнил лишь один человек. В посылке находились поддельная Viagra и другой препарат, лежавшие в одном пакете: они раздробились, смешались и оказались сильно загрязнены.

Таким образом, я получил полезные сведения о том, почему люди заказывали лекарства и тем самым поддерживали проблему спама. Но, чтобы разобраться в партнёрских и клиентских данных GlavMed и Rx-Promotion, мне требовалась помощь Уорнера и нескольких других известных научных исследователей, располагавших возможностями и лабораториями для проверки препаратов. Тогда я не знал, что они сами пытались выяснить то же самое, но упирались в километры бюрократической волокиты и сопротивление самой фармацевтической отрасли. Кроме того, мне

только предстояло узнать о гораздо более мрачных и зловещих последствиях выбора покупателей сетевых лекарств.

Сноски

[1] [назад] Хотя утёкшие письма ChronoPay снова свидетельствуют об обратном, Врублевский отрицает совместное владение Rx-Promotion, но признаёт, что ChronoPay обрабатывала платежи аптечной программы. Гусев публично отрицал руководство SpamIt, однако доказательства и здесь говорят об обратном.

Глава 5. Русская рулетка

Менее чем через двадцать четыре часа после Рождества 2006 года Марсия Бержерон умерла от ядов, примешанных к нескольким лекарствам, которые она заказала через Интернет в аптеке, предположительно канадской. Её тело обнаружил сосед, а в доме нашли более ста таблеток непатентованных препаратов, в том числе успокоительное, противотревожное средство и ацетаминофен.

За несколько дней до смерти у Бержерон, пятидесятисемилетней жительницы острова Куадра в канадской провинции Британская Колумбия, начали выпадать волосы и ухудшилось зрение. В заключении коронера говорилось: «Госпожа Бержерон страдала от целого ряда симптомов. В электронных письмах подруге она описывала непрекращающуюся тошноту, диарею, боли в суставах и другие проблемы. Жившие поблизости друзья знали, что у неё выпадают волосы и возникают проблемы со зрением. В дни непосредственно перед смертью она испытывала крайнюю слабость и была больна».

Вскрытие показало, что Бержерон медленно отравляли чрезвычайно опасные химические вещества, содержавшиеся в таблетках, которые, по данным Службы коронеров Британской Колумбии, были заказаны в интернет-аптеке.

Токсикологические анализы показали, что во многих таблетках содержались опасно высокие концентрации тяжёлых металлов: вероятно, их использовали в качестве наполнителя либо они попали туда как следовые элементы из-за загрязнения производственного оборудования. Среди обнаруженных в таблетках веществ были уран и свинец; даже в малых дозах оба могут привести к смерти или причинить тяжёлый вред.

До сих пор неясно, какая именно мошенническая аптечная интернет-программа поддерживала сайт, где Бержерон сделала заказ. Лекарства, приобретённые через GlavMed и другие мошеннические аптечные партнёрские программы, рекламируют так, будто они поступают из аптек Канады, известной во всём мире доступными ценами на лекарства. Однако, по всей видимости, большинство препаратов GlavMed отправлялось из полудюжины аптек или от поставщиков в Индии, которая сейчас также относится к крупнейшим мировым источникам законных фирменных и непатентованных лекарств. Остальные, судя по всему, поступали более чем от сорока производителей и поставщиков из Китая, Индии и Пакистана. Некоторые из них, по-видимому, перепродавали законные фирменные препараты по бросовым ценам, а некоторые - нет. Тот, услугами которого воспользовалась Бержерон, явно этого не делал.

В Индии есть специалисты, рабочая сила и инфраструктура, позволяющие ежегодно производить огромное количество таблеток. Страна создала бурно развивающуюся фармацевтическую отрасль с оборотом 10 миллиардов долларов в год, хотя регулярно отказывала в патентной защите многим лекарствам западных производителей.

Как писали Викас Баджадж и Эндрю Поллак в *New York Times* в марте 2012 года, конфликт Индии с западными фармацевтическими компаниями из-за патентов восходит к 1970 году, когда страна перестала выдавать патенты на лекарства. Она возобновила их выдачу в 2005 году в рамках соглашения со Всемирной торговой организацией, но действие соглашения не распространялось на лекарства, созданные до 1995 года.

С тех пор, отмечает *Times*, Индия превратилась во всемирную аптеку и в последние десятилетия была крупнейшим поставщиком дешёвых непатентованных жизненно важных лекарств для бедных стран по всему миру. Западные производители лекарств утверждают, что, ограничивая в отдельных случаях действие патентов и поощряя разработку недорогих непатентованных копий, индийское правительство и фармацевтическая промышленность страны подавляют инновации и сокращают прибыль, без которой невозможно продолжать исследования и разработку жизненно

важных препаратов. Индийские фармацевтические компании заявляют, что благодаря их практике более бедные страны сохраняют доступ к недорогим лекарствам против таких бедствий, как ВИЧ и рак.

Так, в одном получившем широкую огласку судебном противостоянии индийские производители лекарств сошлись со швейцарским фармацевтическим гигантом Novartis в споре о том, могут ли индийские компании продолжать выпускать непатентованные копии Gleevec - препарата, эффективно лечащего некоторые виды лейкемии. Как отмечает *New York Times*, Gleevec может стоить до 70 000 долларов в год, тогда как индийские непатентованные версии продавались примерно за 2500 долларов в год. В конце марта 2013 года Верховный суд Индии постановил, что патент, которого добивалась Novartis для Gleevec, не представляет собой подлинного изобретения.

Проблема в том, что достойная восхищения, пусть и небескорыстная борьба Индии за производство доступных непатентованных лекарств для остального мира не решает вопроса о безопасности и эффективности этих препаратов, продаваемых не под фирменными марками. Но если послушать американскую фармацевтическую отрасль, то любое рецептурное лекарство, произведённое вне так называемой «одобренной цепочки поставок», как минимум является поддельным, вероятно, не соответствует стандартам, а вполне возможно, вредно или смертельно опасно. Так ли это всегда или нет, в одном американские производители лекарств правы: большинство препаратов, продаваемых мошенническими фармацевтическими интернет-компаниями, выпускается на нерегулируемых предприятиях и потому представляет серьёзную опасность для каждого, кто решит их принимать.

Статистика мошеннической фармацевтической отрасли и её последствия для здоровья клиентов поистине ужасают. По данным Всемирной организации здравоохранения, около 8 процентов лекарственных субстанций, ввозимых в Соединённые Штаты, являются поддельными, неодобренными или не соответствующими стандартам, а на поддельные лекарства приходится 10 процентов мировой фармацевтической торговли, или 21 миллиард долларов. В исследовании, проведённом под руководством *International Journal of Clinical Practice* (IJCP) и опубликованном в 2012 году, названа сумма более чем втрое выше. По оценке авторов исследования IJCP, мировые продажи поддельных лекарств удвоились за пять лет с 2005 по 2010 год и теперь превышают 75 миллиардов долларов. По оценке Альянса безопасных интернет-аптек, в любой момент времени работают от 30 000 до 40 000 активных интернет-продавцов лекарств, и лишь небольшая их доля действует законно.

Фармацевтический гигант Merck недавно проанализировал более 2500 интернет-аптек и обнаружил, что свыше 80 процентов этих сайтов продавали лекарства, не требуя рецепта. Интернет-аптеки, которыми управляли аптечные партнёрские сети вроде Rx-Promotion и GlavMed-SpamIt, никогда не просили покупателей предъявить рецепт, хотя закон требует, чтобы законные интернет-аптеки, продающие американцам рецептурные препараты, запрашивали его. Более того, Merck обнаружила, что почти шестьсот таких аптек продавали препараты дешевле самой низкой средней оптовой цены на любом рынке мира. Это убедительно указывало на то, что лекарства были поддельными и вполне могли оказаться небезопасными.

Многие покупатели интернет-аптек, связанных с Rx-Promotion и SpamIt, удивлялись, получив таблетки в упаковках, из которых следовало, что товар отправили непосредственно из Индии и Китая. Но, согласно отчёту Счётной палаты США (GAO) за 2010 год, именно там производится и подавляющее большинство лекарств, которые вы покупаете в ближайшей аптеке. GAO установила, что примерно 80 процентов исходных компонентов для всех фармацевтических препаратов - включая товары мошеннических интернет-аптек, одобренных интернет-аптек и даже обычных розничных сетей вроде CVS и Walgreens - поступает с химических предприятий Индии и Китая.

Проблема не в том, что эти лекарства для потребителей из США и Канады производят за пределами Северной Америки. Вопрос в том, поставляют ли компании, услугами которых

пользуются мошеннические аптечные предприятия вроде SpamIt и Rx-Promotion, фирменные и непатентованные лекарства также в цепочку поставок таблеток, продаваемых в законных и одобренных аптеках Соединённых Штатов и других стран, а главное - безопасны ли производимые ими препараты.

Например, аптеки SpamIt полагались на таблетки, которые крупными партиями отправляли не менее сорока разных поставщиков, однако подавляющее большинство лекарств, продававшихся через рекламируемые спамом сайты программы, поступало от полудюжины поставщиков прямой доставки из Индии и Гонконга. Согласно сведениям, собранным из базы данных партнёров SpamIt и интернет-переписки Ступина, в число крупнейших поставщиков SpamIt входили Sai Balaji Enterprises и Hemant Pharma, работавшая под названием Chinmay Overseas, - обе из Мумбаи, Индия. Среди других основных поставщиков SpamIt были гонконгская Trans Atlantic Corp. и Shri Kethlaji Traders из индийского Сумерпура.

Беда в том, что система исполнения заказов GlavMed-SpamIt, по-видимому, автоматически выбирала поставщиков и компании прямой доставки в зависимости от того, кто недавно предложил самую низкую цену на нужную покупателю категорию лекарств. Спамерские фармацевтические компании понятия не имеют, безопасны ли эти препараты для употребления и вообще настоящие ли это лекарства, а не подделки, начинённые возможными ядами и токсинами вроде тех, что убили Марсию Бержерон.

Короче говоря, покупатели заказываемых через спам лекарств, возможно, играют в опасную русскую рулетку.

Продолжив поиски, я обнаружил, что GlavMed скрупулёзно регистрировала жалобы и обращения в службу поддержки. В утёкшей базе данных GlavMed находились тысячи жалоб клиентов, однако лишь сравнительно немногие касались качества доставленных лекарств. В основном люди жаловались на задержки с получением заказанных препаратов, на то, что им прислали не те лекарства, или на неподходящую упаковку.

Одним из исключений была покупка Деборы Г., жительницы Великобритании. Дебора заказала препараты для снижения веса и другие товары на pillaz.com - сайте, который рекламировал спамер, работавший на партнёрскую программу Игоря Гусева GlavMed. Согласно базе данных клиентских жалоб GlavMed, заказанные Деборой таблетки привели её в отделение неотложной помощи. Эта жительница Лондона описывала себя как сорокатрёхлетнюю женщину весом более двухсот фунтов, которая не страдала аллергией и в тот момент не принимала никаких лекарств. В 2010 году она заплатила 437,39 доллара, не считая доставки, за целую домашнюю аптечку рецептурных препаратов, в которую входили:

• Сто восемьдесят таблеток по 20 миллиграммов препарата против ожирения Acomplia.
• Шестьдесят доз Xenical - препарата, блокирующего усвоение жиров из некоторых продуктов.
• Трёхмесячный запас Hoodia - органической добавки для снижения веса.
• Четыре тюбика крема с третиноином для борьбы с угревой сыпью.

Вскоре после того, как Дебора начала принимать новые таблетки, она впала в глубокую депрессию, а затем почувствовала тошноту, и её пришлось госпитализировать. Заподозрив, что таблетки из интернет-заказа могли быть загрязнены, она отнесла лекарства в лабораторию для профессионального анализа.

«При проверке выяснилось, что они целиком и полностью поддельные», - написала Дебора в жалобе, отправленной по электронной почте в службу поддержки GlavMed. По её словам, лабораторные анализы показали, что некоторые таблетки содержали разнообразные неактивные и откровенно опасные ингредиенты, включая яды, цемент и тальк.

Позднее Дебора оставила на сайте, где сделала заказ, жалобу с угрозой.

«Я хочу, чтобы мне вернули ВСЕ деньги. Я с готовностью отправлю таблетки обратно, и никаких дальнейших действий не последует, - написала она в комментарии, сохранившемся в базе данных SpamIt. - Однако, если я не получу деньги, у меня не останется иного выхода, кроме как обратиться в полицию и во все таможенные органы, занимающиеся поддельными лекарствами, и поверьте, я добьюсь вашего уголовного преследования. Я требую немедленно и полностью вернуть деньги за все ваши яды».

Документы показывают, что аптечный сайт, связанный со SpamIt, подчинился и полностью вернул деньги на кредитную карту Деборы. Повторюсь: меньше всего эти мошеннические интернет-аптеки хотят попасть в поле зрения правоохранительных органов или получить от недовольных клиентов возвраты платежей, которые могут лишить аптеку возможности принимать кредитные карты, что погубит её бизнес, а также повлечь крупные штрафы.

Учитывая объём поддельных фармацевтических препаратов, ежегодно наводняющих рынки Северной Америки и Европы, а также ущерб брендам и упущенную прибыль из-за мошеннических аптек, можно было бы ожидать, что могущественная и влиятельная фармацевтическая отрасль употребит свою силу, чтобы показать, насколько опасны эти препараты. И действительно, историю смерти Бержерон почти всегда пересказывают в той или иной форме, когда связанные с фармацевтической отраслью специалисты говорят о необходимости искоренить мошеннические интернет-магазины таблеток.

И всё же ни Управление по санитарному надзору за качеством пищевых продуктов и медикаментов США (FDA), ни гиганты фармацевтической отрасли, по-видимому, не предприняли конкретных шагов для борьбы с этими мошенническими интернет-конкурентами, хотя было бы несложно установить, содержат ли предлагаемые ими препараты вредные вещества или хотя бы опасно низкие либо высокие уровни действующих веществ по сравнению с законными версиями тех же таблеток.

Джон Хортон, президент компании LegitScript, которая ведёт доступную для поиска базу данных тысяч одобренных и «мошеннических» аптечных сайтов, рассказал, что FDA время от времени публикует результаты химических анализов пищевых добавок и некоторых рецептурных препаратов, приобретённых в интернет-аптеках, однако всесторонних исследований проводилось мало.

«Справедливо будет сказать, что анализов крайне не хватает, - сказал Хортон, с 2002 по 2007 год работавший в администрации президента Джорджа Буша-младшего помощником Белого дома по вопросам наркополитики. - Думаю, одна из возникающих проблем состоит в дороговизне таких анализов. Кроме того, препараты, заказанные в мошеннических аптеках, трудно изучать научными методами и анализировать их химический состав, поскольку эти аптеки постоянно меняют поставщиков».

По данным LegitScript, в Интернете действует более 35 610 аптек, но лишь 212 из них являются одобренными и законными интернет-магазинами таблеток. Иными словами, если вы делаете заказ в одной из них, вероятность попасть на незаконный, неодобренный сайт превышает 99 процентов. Компания относит аптеку к законным, если та соответствует набору критериев, в том числе зарегистрирована в Управлении по борьбе с наркотиками США и обладает действительной лицензией на отпуск лекарств. Но важнее всего то, что до отправки рецептурных препаратов американцам магазин таблеток должен запросить и получить настоящий рецепт, выписанный врачом.

Положение усугубляется тем, сказал Хортон, что многие из более чем 35 000 мошеннических интернет-аптек полагаются на нескольких поставщиков. Это означает, что качество и безопасность отправляемых ими препаратов могут меняться день ото дня вместе с колебаниями цен на оптовом рынке и рынке прямых поставок.

«У большинства таких аптечных партнёрских программ не один поставщик, - сказал Хортон. - У некоторых крупных программ их десятки. Поэтому, если сегодня конкретный препарат из определённой аптечной программы при проверке окажется настоящим, это не означает, что в следующий раз при чьём-то заказе придёт такой же настоящий препарат».

Но, по мнению Хортона, едва ли не главная причина, по которой ни FDA, ни фармацевтическая отрасль не прилагают особых усилий к проведению анализов, заключается в опасении: анализы могут показать, что препараты, которые продают многие так называемые мошеннические аптеки, в целом по химическому составу неотличимы от товаров одобренных аптек.

«Откровенно говоря, это своего рода палка о двух концах, - сказал Хортон. - Допустим, вы проверите препараты Rx-Promotion и окажется, что они настоящие, химически равноценные тем, которые вы получили бы в местной аптеке. Не получится ли тогда, что, опубликовав эти результаты, вы тем самым почти безоговорочно одобрите продавший их сайт?»

Таким образом, основная работа по анализу таблеток, продаваемых мошенническими аптеками, легла на учёных, которые пытаются получить данные о безопасности и эффективности рецептурных препаратов, заказанных через спам. Стефан Сэвидж, профессор группы систем и сетей Калифорнийского университета в Сан-Диего (UCSD), возглавил исследовательскую группу, которая на протяжении многих месяцев 2011 года сделала более восьмисот контрольных заказов в магазинах таблеток, рекламировавшихся с помощью нежелательной почты.

«Общепринятое мнение состояло в том, что такие аптечные лавки забирают ваши деньги, обчищают кредитную карту, а вы вообще ничего не получаете, - сказал он. - Мы хотели узнать, получаете ли вы на самом деле хоть что-нибудь, если заказываете в этих магазинах, и если да, то откуда оно поступает, кто обрабатывает платёж и всё остальное».

Сэвидж рассказал, что группа с удивлением обнаружила: во всех приобретённых и проверенных ими лекарствах, судя по всему, содержались нужные действующие вещества примерно в правильных количествах. Однако исследователи не могли проверить препараты на наличие загрязняющих примесей, которые могли угрожать здоровью покупателей.

«По юридическим причинам мы не можем покупать все препараты, да и оборудования для всесторонних анализов у нас нет, - сказал Сэвидж. - Но в лекарствах, которые мы проверили, нужное действующее вещество присутствовало в нужном количестве. Поэтому по поведению участников этого бизнеса и их общению между собой действительно складывается впечатление, что они считают свой товар равноценным» тому, который потребители в ином случае получили бы в местной аптеке, сказал он.

В 2012 году Сэвидж и его коллеги-исследователи из UCSD совместно с учёными Международного института компьютерных наук и Университета Джорджа Мейсона изучили массивы данных, отражавшие повседневные финансовые операции GlavMed, SpamIt и Rx-Promotion. Результатом стал, возможно, самый подробный на сегодняшний день анализ экономического обоснования эпидемий вредоносных программ и спама, которые продолжаются до сих пор. Исследователи установили, что для прибыльности любой мошеннической аптеки критически важны постоянные покупатели. На повторные заказы приходилось 27 процентов среднего дохода программы GlavMed и 38 процентов дохода SpamIt. У Rx-Promotion доля дохода от повторных заказов достигала 23 процентов общего дохода.

«Это говорит о многом, и в частности о том, что многие покупатели этих программ остались довольны», - сказал Сэвидж, отметив, однако, что немало постоянных клиентов приобретали контролируемые рецептурные препараты, вызывающие привыкание, в том числе обезболивающие. «Возможно, купленные лекарства оказывали прекрасный эффект плацебо, но, как мне кажется, это довольные клиенты, и именно поэтому они возвращались».

• * *

Безусловно, самый важный вопрос о таблетках, которые навязывает спамерский бизнес, - их эффективность и безопасность. Я опросил сотни жителей США, покупавших рецептурные препараты на аптечных сайтах из рекламы SpamIt, и получил множество самых разных ответов об эффективности этих таблеток. Но никто из опрошенных не мог ничего сказать ни о безопасности лекарств, ни об их чистоте.

Чтобы выяснить это, я надеялся заручиться помощью химиков и исследователей. Гэри Уорнер, руководитель исследований в области компьютерной криминалистики Университета Алабамы в Бирмингеме (UAB), пытался провести во многом такое же исследование, но на каждом шагу сталкивался с бюрократическими препятствиями. Поэтому вскоре после получения копии данных GlavMed-SpamIt я поделился ею с Уорнером. Тот, в свою очередь, попытался заинтересовать разные фармацевтические компании в использовании данных для начала более широкого, хорошо финансируемого расследования деятельности этих мошеннических интернет-аптек. Но большого успеха его усилия не принесли.

Обширный кампус UAB известен также как «университет, проглотивший Бирмингем», и нетрудно понять почему. В Бирмингеме живёт менее четверти миллиона человек, и примерно каждый десятый из них учится в этом университете.

На четвёртом этаже невзрачного кирпичного здания в самом центре кампуса находится лаборатория компьютерной криминалистики UAB. Там Уорнер проводит по восемь-десять часов в день вместе со студентами бакалавриата, магистратуры и докторантуры, которые, как и я, словно заражены страстью к преследованию интернет-злодеев.

Уорнер стоит перед доской во всю стену, покрытой уравнениями, связанными с математическим алгоритмом, над которым пытаются работать двадцатилетние умники из компьютерной лаборатории. Он указывает на ряды компьютерных серверов и систем Mac OS X вдоль обеих стен помещения с климат-контролем и строгой системой безопасности. В частности, здесь работают студенты университета, которые в рамках гранта Управления перспективных исследовательских проектов Министерства обороны США (DARPA) создают и изучают вредоносные программы в лабораторных условиях.

Уорнер, неисправимый и нисколько этого не стесняющийся любитель кофеина, прихлёбывает третью за день диетическую Mountain Dew. Он с воодушевлением рассуждает об опасности заказов в нелицензированных интернет-аптеках независимо от того, настоящие ли сами таблетки и равноценны ли они по химическому составу тем, которые покупатели в ином случае приобрели бы в местной аптеке.

По словам Уорнера, отчасти проблема состоит в том, что многие нелицензированные интернет-аптеки охотно отправляют разнообразные препараты, использование которых в Соединённых Штатах запрещено или строго ограничено из-за их склонности вызывать опасные побочные эффекты, но при этом не предоставляют никаких предупреждений или инструкций по применению лекарств.

Например, фармацевтический гигант Roche решил убрать с американского рынка препарат против угревой сыпи Accutane после того, как суды присяжных присудили миллионы долларов компенсаций людям, ранее принимавшим этот препарат. Установлена тесная связь между ним и врождёнными пороками у детей, чьи матери принимали его во время беременности. Поэтому в 2005 году американское FDA распорядилось продавать Accutane только женщинам, которые подпишут обязательство неоднократно проходить тесты на беременность и во время приёма препарата использовать по меньшей мере два способа контрацепции. Но Accutane по-прежнему можно приобрести через мошеннические аптеки из спама.

Это ещё один пример риска, на который идут покупатели таких мошеннических аптек: они не получают жизненно важной информации о серьёзной опасности для здоровья, с которой могут

столкнуться при приёме определённых препаратов при определённых состояниях или в сочетании с другими лекарствами. Законные аптеки, напротив, делают всё возможное, чтобы покупатели поняли эти риски до того, как им выдадут рецептурные препараты.

«Многие из этих мошеннических аптек до сих пор рекламируют целый ряд снятых с производства, запрещённых или очень строго ограниченных препаратов, - сказал Уорнер. - И они определённо не передают предупреждений о том, как следует применять эти лекарства, даже когда в обычной аптеке покупателю при заказе непременно поставили бы строгие условия».

Самым очевидным примером обычного риска, создаваемого таблетками из аптек GlavMed и SpamIt, были от двух до четырёх бесплатных поддельных таблеток Viagra или Cialis, которые отправлялись с каждым заказом. Их вкладывали во все посылки, даже если клиент покупал такие препараты, как нитраты, способные образовать смертельную смесь при совместном приёме со средствами от эректильной дисфункции. Врачи давно предостерегают от одновременного приёма средств от эректильной дисфункции и лекарств для снижения высокого артериального давления, поскольку это может привести к опасно низкому давлению - состоянию, которое нередко провоцирует сердечный приступ.

Лаборатория компьютерной криминалистики UAB идеально подходит для анализа препаратов, купленных через спам. Этажом ниже логова Уорнера доктор Элизабет Гарднер проводит большую часть времени за анализом новых «легальных наркотиков». Это изменяющие сознание вещества, созданные на основе синтетических версий химических соединений, использование и распространение которых в Соединённых Штатах ограничены. Некоторые из этих легальных наркотиков довольно безобидны, например продающиеся на автозаправках таблетки «для повышения возможностей», которые намекают на якобы присущую им способность увеличивать выносливость мужчины в постели.

«В большинстве из них просто много кофеина и благих пожеланий», - шутит Гарднер.

В четверг после полудня в середине июня 2012 года Гарднер изучает результаты химического анализа местного образца наркотика под названием «соли для ванн». Частицы препарата поступают в большой белый ящик, напоминающий лазерный принтер-переросток. Это масс-спектрометр - прибор, с помощью которого лаборатория ищет и идентифицирует действующие вещества в разных контролируемых препаратах. Почти бесшумно он автоматически извлекает и анализирует крошечные стеклянные пробирки с химическими образцами, подаваемые внутрь аппарата.

Аппарат выдаёт данные и передаёт их на стоящий рядом компьютер, который на их основе строит линейный график с несколькими отчётливыми всплесками вверх.

«Видите вот эти всплески? - говорит Гарднер, указывая на два особенно высоких пика графика. - Это химические маркеры мефедрона, действующего вещества этих солей».

Несмотря на все усилия, мне не удалось убедить никого из покупателей интернет-аптек прислать полезные образцы таблеток для анализа в лаборатории Гарднер. Впрочем, это всё равно ничего бы не изменило: UAB так и не смог получить юридическое разрешение на такую работу.

Как ни удивительно, исследователи UAB имеют официальное разрешение федеральных регуляторов и правоохранительных органов проверять и использовать строго контролируемые и незаконные вещества, такие как кокаин, героин и метамфетамин, но к тому времени ещё не получили разрешения FDA и Управления по борьбе с наркотиками США на анализ таблеток, заказанных через нежелательную почту.

Отчасти проблема связана с тем, что в 2008 году Конгресс изменил закон, приняв закон Райана Хейта, который прямо запрещает кому бы то ни было заказывать рецептурные препараты через Интернет без рецепта. Кроме того, даже если у американца есть действительный рецепт на лекарство, ему запрещено заказывать его в аптеке за пределами Соединённых Штатов и ввозить

обратно в страну.

«Мы вроде бы почти со всем разобрались, - сказал Уорнер. - У нас готовы меморандумы о взаимопонимании, полностью подготовлены абонентские ящики и получено одобрение высшего руководства университета. Но нам всё ещё нужно преодолеть одно крошечное административное препятствие». Им по-прежнему требовался зелёный свет от федеральных регуляторов.

Уорнер даже заручился участием регионального банка, готового предоставить исследователям предоплаченные карты, с помощью которых можно было бы тайно покупать препараты у GlavMed-SpamIt и Rx-Promotion.

«Банк был готов выделить деньги на финансирование наших операций, но нам всё ещё требовалась составленная на официальном бланке правительственная записка, которая, по сути, подтверждала бы, что за это никто не попадёт в тюрьму», - сказал Уорнер. Университет должен был получить грант FDA на исследование мошеннических аптек, однако грант предоставлялся на жёстких условиях.

«По существу, нам сказали, что никакую часть этих денег нельзя использовать для приобретения препаратов, а если хоть сколько-нибудь грантовых средств пойдёт на анализ лекарств, заказанных через спам, грант отзовут, - сказал Уорнер. - Что изменилось между предварительным предложением гранта со стороны FDA и появлением этих условий? Никто не может сказать. Они просто заявили: „Закон не позволяет нам разрешить вам покупать лекарства“. Поэтому Управлению по соблюдению требований FDA пришлось вернуться к документам и изменить грант так, чтобы мы лишь оценивали сайты из спамерских писем, а покупать таблетки нам больше не разрешалось».

Уорнер и UAB не впервые столкнулись с препятствиями в попытке ради исследования проанализировать таблетки, заказанные через спам. Незадолго до того, как я поделился с ним данными GlavMed, Уорнер встречался с руководителями и специалистами по расследованию мошенничества из Pfizer. Фармацевтический гигант проявил интерес к сотрудничеству с UAB в исследовании препаратов, приобретённых через мошеннические аптечные партнёрские программы. В конце концов, продажи подделок его сверхпопулярного препарата Viagra составляли более 40 процентов операций как Rx-Promotion, так и GlavMed.

Но финансирование такого проекта сопровождалось бы определёнными условиями. «Pfizer сказала, что готова работать с нами над этим проектом, если получит право закрыть его в случае, если препараты окажутся настоящими, - вспоминал Уорнер. - Microsoft обсуждала с нами и Pfizer, не могли бы UAB и Microsoft сделать что-то вроде сайта pilldangers.org и предупреждать людей об опасности покупки таблеток через Интернет. А мой химик спросил: „Но что, если лекарства настоящие?“»

«В ответ представитель Pfizer сказал: „Тогда мы ничего не захотим публиковать“. Я объяснил им, что мы очень дорожим академической свободой и не сможем принять такое условие, - вспоминал Уорнер. - Я сказал ему, что мы захотим иметь возможность заявить, например: „Итак, в 25 процентах полученных нами аптечных заказов товар был настоящим“. Они ответили: „Нет, нет, так нельзя. Мы хотим, чтобы вы публиковали сведения только о поддельных таблетках“».

Затем, уже получив копию данных GlavMed, Уорнер смог поговорить с другим Уорнером - Марком Уорнером, директором разведывательной службы Pfizer и ветераном ФБР с двадцатиоднолетним стажем. Уорнер из UAB рассказал, что Уорнер из Pfizer позвонил обсудить возможное сотрудничество по поиску в данных GlavMed сведений, которые американские правоохранители могли бы затем представить российским властям, чтобы помочь остановить затрагивающий всех поток спама.

«Я закончил разговор, так толком и не поняв, кто он такой, но этот тип держался как старорежимный коп-дуболом, - вспоминал об этом разговоре Уорнер из UAB. - Он ньюйоркец, так что всё было примерно так:

„Что ж, мистер Уорнер, вы только послушайте. Я занимаюсь этим гораздо дольше вас. И вот как всё будет: русские для нас ни хуя не сделают. Нам нужно найти партнёров-спамеров, которые находятся в Соединённых Штатах, и посадить их. Забудьте о русских. До русских нам никогда не добраться. Русские пуленепробиваемы. Мы не можем их тронуть. Так что давайте просто найдём парней в США, посадим их в тюрьму и пойдём дальше“».

С одной стороны, в словах Уорнера из Pfizer был смысл: по мнению большинства опрошенных мною для этой книги специалистов правоохранительных органов, вероятность того, что русские сделают по этому поводу хоть «хуя», была почти нулевой. Начать с того, что хакеров в России обычно оставляют в покое, пока они не охотятся на компании или граждан собственной страны. Но Уорнер из UAB сказал, что такой ответ его ошеломил. В конце концов, более 40 процентов продаж GlavMed приходилось на поддельные версии сверхпопулярного препарата Pfizer Viagra, поэтому сотрудничество отвечало бы интересам самой фармацевтической компании.

«Я просто не мог поверить, что у этого типа настолько пещерное мышление, - вспоминал Уорнер в телефонном интервью. - Я подумал: да, возможно, он проработал в ФБР двадцать один год, но это не означает, что он хоть что-нибудь понимает в киберпреступности. При этом поддельные версии главного источника дохода его компании с огромным отрывом занимали первое место среди отдельных препаратов, продававшихся GlavMed. Именно Pfizer находится в идеальном положении, чтобы жаловаться на фармацевтический спам, но кто знает? Возможно, 100 миллионов долларов прибыли SpamIt и GlavMed от подделок - ничто для компании, которая зарабатывает десятки миллиардов в год».

Уорнер из UAB рассказал, что начал впадать в уныние: у него на руках было столько сведений о масштабном преступном киберзаговоре, а правоохранительные органы, по-видимому, почти не интересовались тем, чтобы воспользоваться этим массивом данных.

«Я участвовал в рабочей группе ФБР по фармацевтическому мошенничеству и был ужасно разочарован, потому что почти никто из крупных фармацевтических компаний не приходил на совещания, - сказал Уорнер. - По крайней мере, на тех совещаниях, где бывал я, за столом сидели представители семи фармацевтических компаний, и ни об одной из них я прежде не слышал. Не было Roche, не было Bayer, не было Pfizer. Не было Merck. Возможно, на одном из совещаний присутствовала AstraZeneca. Но заинтересовать никого не удавалось».

Впрочем, могла существовать ещё одна причина, по которой Pfizer была не настроена помогать ФБР. Незадолго до того, как Уорнер получил данные GlavMed-SpamIt, ФБР завершило уголовное расследование в отношении Pfizer, связанное с продвижением применений её самых продаваемых препаратов не по утверждённым показаниям и выплатой вознаграждений врачам за их рекламу. Правительство утверждало, что торговые представители Pfizer вводили людей в заблуждение маркетинговыми заявлениями о применении препаратов компании. Например, как утверждалось, представителей призывали обучать врачей тому, как строить разговоры о назначении Viagra женщинам, испытывавшим трудности с достижением оргазма.

Pfizer отрицала обвинения, но всё же согласилась выплатить 2,3 миллиарда долларов в рамках урегулирования дела - на тот момент это была крупнейшая отдельная сумма, когда-либо взысканная Министерством юстиции США по делу о мошенничестве. Она примерно равнялась ежегодному доходу Pfizer от продаж Viagra. Неудивительно, что фармацевтический гигант не хотел вовлекать ФБР в очередное расследование, даже если оно отвечало его интересам.

Со своей стороны, Pfizer предпочла преследовать спамеров и изготовителей подделок с помощью гражданских исков. За последние пять лет компания потратила миллионы на расследования и оплату юридических услуг, преследуя продавцов поддельной Viagra и других препаратов. (Pfizer неоднократно отклоняла просьбы дать интервью для этой книги.)

Уорнер был разочарован тем, что не смог получить разрешение на анализ рецептурных препаратов, приобретённых у Rx-Promotion и GlavMed-SpamIt. Но он, казалось, искренне надеялся, что клиентских баз данных обеих мошеннических аптечных сетей будет достаточно, чтобы помочь ликвидировать деятельность некоторых крупнейших в мире спамеров и хозяев ботнетов. Почти все они работали на одну из этих партнёрских программ или сразу на обе, а их персональные и финансовые данные были рассеяны по утёкшим документам каждой программы.

Тот же активист по борьбе со спамом, который поделился со мной базой GlavMed, рассказал, что отправил её копию своим контактам в ФБР. На протяжении нескольких недель в конце 2010 года сразу несколько правоохранительных ведомств боролись за ведущую роль в расследовании. В конечном счёте было решено, что дело лучше всего расследовать как нарушение прав на товарные знаки, и его передали межведомственной оперативной группе Иммиграционной и таможенной полиции США (ICE), входящей в Министерство внутренней безопасности.

Эта оперативная группа, известная как Национальный координационный центр по правам интеллектуальной собственности (NIPR), привлекает ресурсы гражданских и уголовных расследований по меньшей мере двадцати отдельных ведомств, среди которых ФБР, Интерпол, Служба почтовой инспекции США, Национальное управление по аэронавтике и исследованию космического пространства (NASA) и Королевская канадская конная полиция.

Расследование в NIPR было частью более широкой кампании администрации Обамы против нарушений прав интеллектуальной собственности в Интернете, в том числе продаж мошеннических аптек и незаконной торговли пиратскими фильмами, музыкой и программным обеспечением. Примерно в то же время представители администрации объявляли результаты операции «Пангея» - ежегодной международной кампании правоохранительных органов под руководством Интерпола, направленной на пресечение фармацевтической преступности. Недельная операция привела к закрытию не менее 290 мошеннических интернет-аптек, конфискации почти 11 000 посылок, содержавших более миллиона таблеток, а также к аресту или началу расследования в отношении не менее семидесяти шести человек, связанных с этими фармацевтическими магазинами.

Многие сайты, закрытые в ходе операции «Пангея», были интернет-витринами, которые рекламировали спамеры, работавшие на программу Врублевского Rx-Promotion. Непосредственно перед закрытиями Управление по санитарному надзору за качеством пищевых продуктов и медикаментов США направило партнёру Врублевского Юрию «Hellman» Кабаенкову письмо с предупреждением. Ведомство сообщало, что выявило 294 сайта, продававших без рецепта вызывающие зависимость, строго контролируемые рецептурные препараты, например обезболивающие. Казалось, американские власти наконец начали давать отпор.

Rx-Promotion, по существу, лишь пожала плечами. По словам Врублевского, почти никто в программе не заметил закрытий, число которых, по иронии судьбы, примерно равнялось среднему количеству сайтов, еженедельно исчезавших в результате обычных зачисток, проводимых группами по борьбе со спамом и хостинговыми компаниями.

«Было очень забавно читать новости о гигантской международной операции, результатом которой стало закрытие сотен незаконных аптек в Интернете, - сказал Врублевский. - А потом заходишь на форумы спамеров и хакеров и видишь, как эти парни спрашивают друг друга: „Чувак, ты это почувствовал?“ и „Чувак, ты это заметил?“ Похоже, всем было всё равно и никто толком ничего не заметил».

Врублевский рассказал, что за несколько недель до операции группа американских компаний, главным образом правообладателей из индустрии развлечений, созвала совещание с депутатами Государственной думы, нижней палаты российского парламента. Оно было частью кампании индустрии развлечений против музыкального и кинопиратства в России. Её лозунг можно было примерно перевести как «Скажи вору нет!».

Утёкшие электронные письма ChronoPay показывают, что компания негласно оплачивала работу по меньшей мере одного сотрудника Российской ассоциации электронных коммуникаций (РАЭК), отраслевой торговой группы. Согласно счетам ChronoPay, компания платила «ежемесячное вознаграждение за консультации по связям с общественностью» в размере 16 666,66 евро Дмитрию Захарову, тогдашнему директору РАЭК по связям с общественностью. (Это был ещё один долг, по которому Врублевский и ChronoPay впоследствии не расплатились. Во внутренней почте ChronoPay множество писем от взыскателей долгов РАЭК, безуспешно добивавшихся от сотрудников ChronoPay выплаты десятков тысяч евро просроченных «консультационных» гонораров.) Я попросил господина Захарова прокомментировать эту предполагаемую договорённость, но ответа не получил. Это вызывало досаду и было иронично отчасти потому, что в 2010 году Захаров покинул РАЭК и теперь занимает должность заместителя директора департамента внешних коммуникаций российского Министерства связи и массовых коммуникаций.

В телефонном интервью через месяц после операции «Пангея» Врублевский рассказал мне, что связался с руководителями РАЭК, чтобы высмеять их участие в форуме по вопросам авторских прав и товарных знаков.

Неудивительно, что правообладатели, особенно представители киноиндустрии, пригрозили таким членам РАЭК, как «ВКонтакте», российский аналог Facebook, и Mail.ru, поставщик услуг веб-почты: если те не удалят все материалы, нарушающие права, вмешаются правоохранительные органы, рассказал Врублевский. «Я услышал об этом, позвонил этим типам из РАЭК и сказал: „Эй, сколько же нужно иметь мозгов, чтобы не ходить на встречу с правообладателями под названием «Скажи вору нет!»?“»

Позднее в 2010 году РАЭК направила официальное письмо Виктории Эспинель, координатору администрации Обамы по обеспечению соблюдения прав интеллектуальной собственности. В письме, которое также направили высшим руководителям Google, Microsoft, Национальной ассоциации фармацевтических советов и LegitScript, российская индустрия высоких технологий предлагала помощь в борьбе со спамом и в будущих инициативах по искоренению мошеннических интернет-аптек.

В письме утверждалось, что в 2009 году экономический ущерб от спама в России составил 450 миллионов долларов и что поэтому страна усиленно разрабатывает собственные законы против спама. РАЭК не упомянула, что человек, ставший одним из основателей мошеннической интернет-аптеки, против которой была направлена недавняя американская операция «Пангея», одновременно возглавлял комитет российского правительства, отвечавший за рекомендации по разработке этих законов против спама.

В завершение письма представители РАЭК предложили организовать защищённую видеоконференцию с должностными лицами администрации Обамы и представителями технологической отрасли, «в ходе которой мы могли бы обсудить имеющиеся результаты исследований, текущие вопросы, инициативы и возможности совместных действий, направленных на стабилизацию ситуации в сфере киберпреступности в целом и в отношении фармацевтического спама в частности».

Президент LegitScript Джон Хортон рассказал, что, получив копию письма, первым делом связался с FDA и Эспинель.

«Я сказал: „Уверен, вы знаете, что происходит с ChronoPay“, и оказалось, что они знали, - сообщил Хортон. - Я также написал Виктории [Эспинель] по электронной почте и сообщил, что мой неофициальный совет - не отвечать на письмо».

В середине августа 2010 года Эндрю Дж. Клейн, старший советник президента Обамы по обеспечению соблюдения прав интеллектуальной собственности, пригласил руководителей крупнейших регистраторов и реестров доменных имён на трёхчасовое совещание в Белом доме,

чтобы обсудить добровольные способы закрытия сайтов, продающих поддельные рецептурные препараты.

Приглашение разослали по электронной почте десяткам руководителей и юристов крупнейших интернет-компаний мира, среди которых были Google, Microsoft, PayPal, Visa и Yahoo! Получателям предлагалось 29 сентября встретиться с высокопоставленными должностными лицами Белого дома и членами кабинета, в том числе с Викторией Эспинель.

«Цель настоящего совещания состоит в обсуждении незаконной деятельности, осуществляемой через Интернет в целом, и, в частности, добровольных протоколов противодействия незаконной продаже в Интернете поддельных рецептурных препаратов, не относящихся к контролируемым веществам», - говорилось в приглашении.

Несколько участников мероприятия назвали его скорее засадой, чем совместной встречей умов ради решения сложной проблемы, и рассказали, что Эспинель, по существу, заявила собравшимся: им необходимо выработать добровольный подход, иначе последствия не заставят себя ждать.

«По сути, она собрала в одной комнате владельцев множества крупных брендов, чтобы заявить: „Вы, ребята, должны что-то с этим сделать, иначе что-то сделают с вами“», - сказал Сэвидж из UCSD, вспоминая разговор с одним из участников.

Хотя тогда об этом мало кто знал, одну из приглашённых компаний, Google, Министерство юстиции США уже расследовало по уголовному делу за активное привлечение поддельных канадских аптек, в том числе множества мошеннических интернет-аптек, созданных SpamIt и Rx-Promotion, к размещению рекламы лекарств для поставки в Соединённые Штаты.

Последствия этого дела были огромны. Одним из способов продвижения аптечных сайтов партнёрами GlavMed был взлом чужих сайтов. Партнёры вставляли во взломанные сайты десятки ссылок и даже целые веб-страницы, перенаправлявшие посетителей на площадки, торговавшие поддельными рецептурными препаратами. Чем больше взломанных законных сайтов ссылалось на аптечные магазины партнёров, тем выше те оказывались в выдаче крупнейших поисковых систем, когда потребители искали конкретные названия лекарств. Этот процесс, известный в подполье как «чёрная поисковая оптимизация», или сокращённо «чёрное SEO», был одним из главных источников аптечных продаж для партнёров как Rx-Promotion, так и GlavMed-SpamIt.

Постоянные манипуляции спамеров с поисковой выдачей Google были уже достаточно плохи. Но то, что Google к тому же получала деньги от нерегулируемых интернет-аптек, потенциально связанных со спамерами, переходило все границы. По данным Министерства юстиции, Google ещё в 2003 году знала, что канадские аптеки незаконно отправляют рецептурные препараты в Соединённые Штаты.

Позднее Google урегулировала уголовные обвинения по этому делу и согласилась выплатить ошеломляющий штраф в размере 500 миллионов долларов. Этот штраф, одна из крупнейших конфискационных выплат, когда-либо поступавших Министерству юстиции, должен был соответствовать сумме рекламных доходов компании от канадских аптек и доходов самих аптек от американских покупателей контролируемых препаратов.

Менее чем через два месяца после совещания в Белом доме Эспинель встала за трибуну на пресс-конференции там же. По обе стороны от неё находились генеральный прокурор США Эрик Холдер и тогдашний министр внутренней безопасности Джанет Наполитано. Эспинель объявила о создании новой некоммерческой организации для борьбы с мошенническими интернет-аптеками.

«Сегодня группа партнёров-учредителей из частного сектора объявила, что они создадут новую некоммерческую организацию, чтобы совместно друг с другом и правительством США избавить Интернет от незаконных интернет-аптек», - объяснила Эспинель, назвав членами организации American Express, eNom, GoDaddy, Google, MasterCard, Microsoft, Network Solutions, Neustar, PayPal, Visa и Yahoo.

«Эта группа компаний предприняла выдающийся и беспрецедентный шаг для борьбы с незаконными интернет-аптеками, - заявила Эспинель переполненному пресс-залу и камерам CNN. - Мы считаем, что это окажет на незаконные интернет-аптеки быстрое и решительное воздействие. Это изменит правила игры и даст ясно понять, что законные компании не будут взаимодействовать с преступниками».

Во всём объявлении была лишь одна проблема. Мало кто в названных компаниях мог припомнить, чтобы они соглашались создать такую некоммерческую организацию.

«До той пресс-конференции представители этих компаний провели круглый стол по телефону, чтобы всё обсудить, но никто не начинал тот разговор с намерением согласиться на создание такой группы, - сказал Уорнер. - Люди, с которыми я говорил и которые смотрели объявление о том, что они согласились создать эту группу, после него спрашивали: „Мы согласились?“»

Спустя восемнадцать месяцев после создания некоммерческой организации, о которой Эспинель впервые объявила на встрече в Белом доме, группа всё ещё не провела первого совещания. Одновременно закрывалось дело NIPR. Предупреждение руководителя службы безопасности Pfizer оказалось пугающе пророческим. По словам источников в двух разных федеральных правоохранительных ведомствах, которые попросили не называть их имён, потому что не имели полномочий делать официальные заявления, расследование в отношении ключевых спамеров и хакеров, нанятых GlavMed и SpamIt, прекратили отчасти потому, что большинство преступников предположительно находилось в России и бывших советских республиках. Эти страны, как правило, неохотно сотрудничали с западными правоохранительными органами, пытавшимися задержать киберпреступников на их территории.

Поскольку федеральные регуляторы не проявляют интереса к систематическим анализам лекарств, заказанных в этих аптеках-однодневках, по-прежнему неясно, содержит ли основная масса препаратов достаточное количество действующих веществ и нет ли в них одновременно вредных загрязняющих примесей, способных нанести вред или даже убить принимающих их людей.

Такое бездействие, по-видимому, устраивает фармацевтическую отрасль, которая опасается проводить анализы и получить результаты, способные показать, что подавляющее большинство заказанных через спам рецептурных препаратов гораздо дешевле и не менее безопасно, чем те же таблетки из местной аптеки.

К сожалению, отсутствие объективных данных о безопасности и эффективности заказанных через спам рецептурных препаратов почти не ослабляет спрос, но по-прежнему подвергает потребителей опасной игре в русскую рулетку.

Глава 6. Партнёр(к)и в (дез)организованной преступности

В знаменитом изречении из трактата Сунь-цзы «Искусство войны» выражена мысль, которая применима к моему исследованию и к побуждению написать эту книгу: «Знай своего врага». Итак, получив некоторое представление о том, что движет этими спамерскими аптеками и их покупателями, пора рассмотреть, как на самом деле устроена деятельность по рассылке спама. Движущая сила успеха таких программ, как GlavMed и Rx-Promotion, и механизм, приводящий в действие практически любое совместное предприятие киберпреступников, - это схема, известная в России как «партнёрка», буквально «партнёрство». Такие партнёрки, как GlavMed и Rx-Promotion, стремятся свести сомнительных рекламодателей с компаниями, готовыми покупать веб-трафик, который можно создать с помощью спама.

Многие законные предприятия, ищущие новых покупателей, главным образом малые компании из России и Восточной Европы, пытаются повысить известность своих товаров или услуг и спрос на них, нанимая спамера. Хотя использование взломанных компьютеров для рассылки нежелательной почты формально незаконно в России, многие законные предприятия страны либо не знают об этом запрете, либо его не боятся.

И действительно, как мы увидим в главе 7, нашим «Вергилием» в подпольном мире спамеров стал финансист ботнета Cutwail Игорь Вишневский. Он начал заниматься спамом, когда начальник велел ему придумать, как привлечь больше посетителей на сайт своей компании по продаже отопительного оборудования.

Более того, когда спамерский ботнет Cutwail используется для отправки спама на адреса электронной почты, заканчивающиеся на «.ru», в сообщениях очень часто указывается российский телефонный номер, по которому получатели могут узнать, как заказать спамерскую рекламу для собственных товаров и услуг.

«Я видел, как таким способом рекламировали почти всё - от электронных сигарет и офисных помещений до курортов», - сказал исследователь Калифорнийского университета Бретт Стоун-Гросс, много лет изучавший работу ботнета Cutwail.

В типичной спамерской партнёрке управляющие ею люди, то есть спонсоры, берут на себя координацию и поддержку почти всех сторон бизнеса: от веб-контента и обслуживания клиентов до переговоров с поставщиками и настройки веб-серверов и доменных имён, необходимых для рекламы продаваемого товара.

Единственная задача спамеров, которых иногда называют «адвертами» или «трафферами», - направлять трафик на сайты, где продаются рекламируемые в спаме товары; при этом они могут в любой момент выйти из сделки. Как правило, спамеры получают комиссию в размере 30-35 процентов от общей суммы продаж, обеспеченных их трафиком. Для них это довольно прибыльный бизнес, при условии что трафик действительно приводит платящих покупателей.

Такая динамика партнёрских систем позволяет спонсорам сохранять безопасную дистанцию, по крайней мере теоретически, от более противозаконных сторон спамерского бизнеса, который обычно задействует тысячи взломанных персональных компьютеров для ретрансляции спама и размещения аптечных сайтов. Адверты выигрывают благодаря возможности быстро отключить свой трафик от одной партнёрской программы в пользу другой, предлагающей более привлекательные условия: более высокие комиссионные, лучшее обслуживание покупателей и более широкий выбор товаров, которые повышают вероятность привлечь покупателей с помощью спама. Существует множество видов партнёрств: одни торгуют точными копиями часов, порнографией, поддельными дизайнерскими сумками и фальшивыми антивирусными

программами, другие - рекламируемыми спамом аптечными товарами. Когда спамерские письма появляются во входящих или попадают под блокировку брандмауэра, спам-фильтра или антивирусной программы, вероятно, они пришли из одной из таких партнёрок.

Специалисты по технологиям и безопасности любят называть эти партнёрки «организованной киберпреступностью». Но, по словам Стефана Сэвиджа из UCSD, партнёрские системы точнее описывать как «дезорганизованную преступность», то есть слабо связанные сети независимых подрядчиков, каждый из которых, по существу, стремится заработать для себя и продолжает партнёрство лишь до тех пор, пока оно остаётся экономически жизнеспособным и конкурентоспособным.

«Для обеих сторон это действительно блестящая бизнес-модель, - сказал Сэвидж, соавтор нескольких многолетних исследований разных сторон экономики партнёрок, от спама до ботнетов. - Партнёру не требуется разбираться во всём, что касается обработки платежей и исполнения заказов; ему нужно лишь понять, как получить трафик. К тому же у вас огромная свобода: если одна партнёрская программа прекращает работу или у другой оказываются более выгодные ставки, можно перейти к кому-то ещё. Поэтому модель партнёрки действительно даёт партнёру невероятную мобильность, ведь он ни к чему не привязан».

Сэвидж сказал, что сами партнёрские программы выигрывают от такой схемы, поскольку им не приходится иметь дело с возможными рисками формальной связи с ботнетами и другими изобретательными, но потенциально вредными и юридически сомнительными способами создания трафика, которые могут придумать их спамеры.

«Партнёрская программа выигрывает, потому что ей не нужно делать ставку на лучший способ получения трафика, - сказал он. - Партнёрская программа рассуждает так: „Большинство этих парней [спамеров] прогорят, но мне всё равно, потому что я плачу только комиссионные. Кто-нибудь сделает всё правильно, и тогда я на этом заработаю“».

Из-за такой динамики партнёрок большинство спамеров также не хранит верность какой-либо одной аптечной партнёрской программе. Например, почти все ведущие спамеры как GlavMed, так и Rx-Promotion сотрудничали по меньшей мере ещё с полудюжиной аптечных партнёрок, в числе которых были EvaPharmacy, Bulker.biz, Rx-Partners и Mailien. Эта динамика создаёт, пожалуй, самую досадную из всех проблем для борцов со спамом, пытающихся остановить поток нежелательной почты. Если сдавить надутый воздушный шар, он не уменьшится, а воздух лишь переместится в новые выпуклости. Точно так же кампании против спама, которым удаётся закрыть одну партнёрку или важную составляющую её деятельности, часто приводят лишь к тому, что самые успешные партнёры переносят спамерский трафик к конкурирующим партнёркам.

Как отметил специалист SophosLabs Canada по безопасности Дмитрий Самосейко в своей основополагающей работе «Партнёрка: что это такое и почему вас это должно волновать?», все партнёрки жёстко конкурируют друг с другом.

«Верность завоёвывают более щедрыми комиссионными ставками, более короткими периодами „удержания“, поддержкой более широкого спектра платёжных систем, более качественными рекламными материалами, лучшей поддержкой и так далее», - писал Самосейко. Обычно партнёрки удерживают комиссионные на одну-две недели, чтобы застраховаться от необходимости одновременно платить всем партнёрам и не допустить выплаты партнёрам комиссионных за продажи, которые позднее отменят системы обработки платежей по кредитным картам.

По словам Самосейко, партнёрки часто используют конкурсы и другие уловки для привлечения новых партнёров, то есть спамеров. «Многие устраивают для своих участников дорогие вечеринки, рассылают щедрые подарки к праздникам, проводят лотереи, в которых лучший производитель выигрывает роскошный автомобиль, и так далее», - писал он.

Эти стимулы также увеличивают объём получаемого нами почтового спама. Например, в 2008 году Ступин и Гусев, основатели и администраторы GlavMed и SpamIt, решили провести конкурс среди своих ведущих спамеров с крупными денежными призами для тех адвертов, чей спам обеспечит наибольшее количество продаж. Каждый участник получил список примерно из 20 000 адресов электронной почты, а конкурс начался 4 июля 2008 года, в День независимости США.

Три первых участника получили призы от 1000 до 3000 долларов и статус «Повелитель входящих» на Spamdot.biz, закрытом форуме, принадлежавшем администраторам SpamIt. (Победителем конкурса стал хакер по прозвищу Engel - тот самый россиянин, который предположительно стоял за спамерским ботнетом Festi, чрезвычайно заразной и мощной машиной для рассылки спама, подробно описанной в главе 7. Между прочим, Engel и его ботнет в конце концов подтолкнут Врублевского и его самого к опасному столкновению с законом, как мы увидим в главе 12.)

В своей основополагающей работе «PharmaLeaks: понимание бизнеса партнёрских программ интернет-аптек» исследователи из Калифорнийского университета в Сан-Диего (UCSD), Международного института компьютерных наук и Университета Джорджа Мейсона изучили массивы данных о повседневных финансовых операциях GlavMed, SpamIt и Rx-Promotion. В совокупности за четыре года эти программы обработали заказы на сумму более 170 миллионов долларов от покупателей, искавших более дешёвые и доступные лекарства, которые можно было приобрести с большей конфиденциальностью.

Результатом стал, возможно, самый подробный на сегодняшний день анализ экономического обоснования эпидемий вредоносных программ и спама, продолжающихся и по сей день. Исследователи пришли к выводу, что спам и все сопутствующие ему бедствия останутся распространённой и неотступной проблемой, поскольку потребительский спрос на товары, чаще всего рекламируемые с помощью нежелательной почты, остаётся неизменным.

«Рынок рекламируемых спамом лекарств и близко не насыщен, - сказал профессор UCSD Стефан Сэвидж. - Количество новых покупателей, ежедневно приходивших в эти программы, объясняет, почему люди рассылают спам. Ведь рассылка спама всем жителям планеты постоянно приносит вам новых покупателей, а значит, никуда не исчезнет».

Партнёры глубоко это понимают и, подобно региональным наркоторговцам, делящим огромные участки интернет-территории, часто ссорятся друг с другом из зависти или неприязни либо мстят за какую-нибудь мнимую обиду. Эти виртуальные войны за территорию могут быстро стать весьма грязными и дорогостоящими для всех участников. Особенно это верно, когда споры разгораются между конкурирующими партнёрками, поскольку большинство ведущих партнёров - крупные спамеры, в распоряжении которых находятся чрезвычайно мощные ботнеты.

Такие споры обходятся дорого ещё и из-за связанных с ними альтернативных издержек. Разрушительные атаки проводят с помощью ботнетов: ресурсы, которые обычно используются для рассылки спама, перенаправляют на отправку бесполезного интернет-трафика, пока целевой сайт не окажется перегружен и не перестанет обслуживать законных посетителей, то есть потенциальных покупателей.

В своей работе «PharmaLeaks» исследователи UCSD обнаружили, что всего на 10 процентов самых высокооплачиваемых партнёров приходилось от 75 до 90 процентов общего дохода программ во всех трёх партнёрских сетях.

«Подрыв деятельности всего нескольких партнёров оказал бы значительное влияние на итоговую прибыль программы», - писали исследователи.

Теневые боссы во главе разных партнёрских программ рано распознали в этой слабости угрозу самому существованию бизнеса. Чтобы устранить её, криминальные боссы попытались создать виртуальный картель аптечных интернет-партнёрок, призванный предотвращать междоусобные споры, ценовые войны и мгновенное массовое бегство партнёров из одной аптечной программы в

другую. Боссы партнёрок полагали, что такое соглашение сократит накладные расходы и периодические падения общего объёма спама, а в конечном счёте обеспечит более стабильный поток нежелательной почты в ящики по всему миру.

Для этого 4 сентября 2007 года Дмитрий Ступин сообщил своему партнёру Игорю Гусеву, что хотел бы видеть SpamIt и GlavMed участниками аптечного картеля вместе с другими партнёрскими программами. Неделю спустя Гусев организовал встречу для обсуждения этой идеи с Леонидом Куваевым, осуждённым спамером и одним из администраторов Rx-Partners, конкурирующей программы фармацевтического спама.

Примерно тогда же Павел Врублевский, как сообщалось, создавал собственное мошенническое аптечное предприятие Rx-Promotion вместе с коллегой и давним другом Юрием «Hellman» Кабаенковым. Врублевский отрицает, что играл активную роль в Rx-Promotion, но, согласно утёкшим письмам ChronoPay, он встречался с Лео Куваевым из Rx-Partners и партнёром Куваева Владиславом Хохолковым, чтобы обсудить участие Rx-Promotion в пока ещё формировавшемся картеле. В утёкших письмах Врублевский утверждает, что отказался участвовать в картеле, но говорит, что Mailien, SpamIt и ещё одна крупная программа, EvaPharmacy, согласились установить предельные цены на лекарства и ограничить комиссионные партнёров уровнем 40 процентов.

Журналы переписки, которые российские следователи в конце концов изъяли с компьютера Ступина, показывают, что картель прилагал настойчивые усилия, чтобы склонить на свою сторону EvaPharmacy. Ниже приведена запись разговора Ступина с представителями Eva, известной также как Bulker.biz. Их переписка была переведена с русского на английский.

> **СТУПИН:** Мне не нравятся условия, которые мы даём адвертам. Некоторые требуют 45 процентов. Мы страдаем из-за низких цен, а некоторые ещё и просят сократить удержание до одной недели. Я хочу их приструнить и платить себе больше, чем им ;) Мы никому не предлагаем удержание меньше двух недель. Просто из-за задержек платежей от Shaman и островов (офшора) остатки на наших счетах уменьшаются.[1] Я ни о чём вас не прошу, просто говорю, что вы тоже можете установить минимальный срок удержания в две недели, и тогда у адвертов не будет выбора, потому что мы предложим одинаковые условия. Думаю также, что с удержанием вам будет легче платить, чем без него, потому что, если адверты увеличат объём работы, вам придётся держать в банках слишком много наличности. Если подвести итог, моя утопия - картельное соглашение о снижении комиссионных адвертов до 30-35 процентов, как в западных партнёрских программах.
>
> **BULKER.BIZ:** У нас тоже действует двухнедельное удержание. Однако для лучших адвертов мы делаем исключение [из этого ограничения]. Снизив цены, вы заставили многих наших адвертов перейти к вам. Поэтому у нас не осталось иного выбора ;) Соглашение - прекрасная идея, но, чтобы оно работало, в него должны войти Mailien и другие. Иначе спамеры продолжат перебегать к ним. Конечно, 45 процентов - просто возмутительно! Из-за этого партнёрка зарабатывает втрое меньше!
>
> **СТУПИН:** Да, и единственный довод в пользу требования 45 процентов состоит в том, что Eva столько платит ;)
>
> **BULKER.BIZ:** Некоторые платят даже 50 процентов и ещё сильнее убивают рынок. Хочу также сказать, что знаю, о каком адверте вы говорите. У него вообще нет удержания, но это не означает, что каждый день он обходится нам во весь остаток средств.
>
> **СТУПИН:** Знаю, он мне всё рассказал.
>
> **BULKER.BIZ:** Послушайте, мы готовы заключить соглашение и установить одинаковые условия для адвертов, но лишь после того, как проверим новых поставщиков и сможем снизить цены, чтобы сравняться с вашими или приблизиться к ним, только когда наши

конкурентные условия станут сопоставимыми.

По словам Вишневского, который активно участвовал в разработке ботнета Cutwail, вывод исследователей UCSD о том, что основную часть доходов партнёрских программ создаёт примерно горстка партнёров, верен. Вишневский сказал, что очень немногие партнёры, ещё не владевшие значительными ресурсами для рассылки спама, могли рассчитывать на большой заработок из-за затрат на создание таких ресурсов.

Самая дорогая часть любой спамерской операции - приобретение ботов для ретрансляции нежелательной почты. Почти без исключений самые высокооплачиваемые партнёры управляли собственными очень крупными ботнетами - преступными машинами, с помощью которых рассылали свой спам и которые сдавали в аренду другим партнёрам.

Вишневский рассказал, что партнёры, арендующие ресурсы ботнетов у других спамеров, часто делают это, покупая «инсталлы», то есть заражая заранее оговорённое количество ботов дополнительной вредоносной программой, которая рассылает спам для партнёра. Партнёры, арендующие ботов у коллег, нередко расплачиваются за эти ресурсы простым перечислением доли своих комиссионных с каждой продажи, обеспеченной спамом арендованных ботов. По словам Вишневского, хозяева ботнетов очень часто требовали до 50 процентов комиссионных партнёра-клиента.

Но полноценная сеть для рассылки спама состоит далеко не только из ботов. Если сравнить спамерскую сеть с фабрикой, то боты можно представить как станки, отвечающие за сборку составных частей продаваемого товара. А эффективность спамерского ботнета не может быть выше эффективности программного обеспечения, которое управляет повседневной работой этих станков. Современные персональные компьютеры чрезвычайно мощны, но могут быстро оказаться перегружены, если одновременно потребовать от них слишком много операций. Хорошая спамерская программа распределяет нагрузку между тысячами заражённых машин и не позволяет завалить отдельные компьютеры объёмом работы, с которым они не справятся.

Одновременно хорошая спамерская программа должна учитывать, сколько писем успешно доставлено и сколько получателей перешло на рекламируемый сайт. От программы также ожидают, что она будет автоматически удалять, или «вычищать», из спамерских списков адреса электронной почты, которые больше не действуют или отказываются принимать входящие письма. Спамеры часто подменяют, или фальсифицируют, адрес в поле «От кого:» нежелательного письма. Когда спам отправляют в неактивные ящики, сообщения об ошибке часто возвращаются не спамерам, а ничего не подозревающему человеку, чей адрес использовали для подмены отправителя! (Наверняка и вам приходило нечто подобное от друга, коллеги или родственника, чью учётную запись электронной почты взломали либо чей адрес подменили.) Такие возвраты заставляют сбитых с толку и обеспокоенных интернет-пользователей жаловаться своему поставщику услуг Интернета, электронной почты или обоим сразу, а те в ответ могут принять более строгие меры для блокировки подобных заблудших сообщений в будущем.

Наконец, партнёру, у которого ещё нет хороших списков адресов, придётся купить их у кого-то другого, если он не способен написать собственную программу для непрерывного сбора новых адресов электронной почты со случайных сайтов.

По словам Вишневского, партнёр может рассчитывать, что потратит от 20 до 30 процентов своего дохода на аренду программного обеспечения и списков адресов.

«Не должно удивлять, что большинство спамеров зарабатывают немного, если им приходится всё это арендовать», - сказал он.

Невозможно сказать, сколько организации по всему миру тратят на борьбу с нежелательной почтой от таких отправителей, как партнёры Rx-Promotion, GlavMed и SpamIt, но почти наверняка во много-много раз больше, чем скромная прибыль, которую выжимают администраторы и основатели

этих программ.

Поразительно, что, подсчитав прямые и косвенные расходы этих программ за одиннадцать месяцев с мая 2009 по апрель 2010 года, исследователи UCSD установили: чистая прибыль программ составляла около 20 процентов валового дохода.

«Во всём этом удивительно то, что в конечном счёте речь идёт не о таких уж больших деньгах, - сказал Сэвидж из UCSD. - Парни, управляющие фармацевтическими программами, не Дональды Трампы, однако их деятельность оказывает реальное и существенное финансовое влияние на повседневную жизнь десятков миллионов людей. Иными словами, чтобы эти парни нажили скромное богатство, нам нужна многомиллиардная индустрия безопасности для борьбы с ними».

Сэвидж и его исследовательская группа также получили возможность изучить множество утёкших разговоров Гусева с его деловым партнёром Ступиным. По словам Сэвиджа, в переписке было полно примеров того, как эти парни постоянно искали способы повысить ценность своих предложений для потребителей. Такие люди, как администраторы SpamIt, добивались успеха, потому что понимали свой основной рынок: они продавали недорогие товары с конфиденциальной доставкой, от интернет-порнографии до таблеток для потенции, которые многим взрослым в иных обстоятельствах было бы стыдно покупать.

Как показывает переписка, однажды Ступин и Гусев задумались об использовании своей спамерской инфраструктуры для продвижения куда более сомнительного потребительского товара: устройств для удлинения пениса.

«Это с огромным отрывом самый забавный разговор во всей коллекции, - вспоминал Сэвидж. - По существу, Гусев спорит со Ступиным о том, следует ли им добавить в свои интернет-магазины устройства для удлинения пениса. Гусев полностью за эту идею. Он говорит что-то вроде: „Да, американцы действительно хотят прибавить дюймы“, но Ступин не убеждён. И именно это я стараюсь объяснить людям [на основании] всех наших исследований этой причудливой подпольной экономики.

Фармацевтические дельцы и спамеры в принципе совершенно не считают себя преступниками. Думаю, в их представлении они продают качественный товар аудитории, которая его требует. Да, на пути могут стоять какие-то законы, но эти законы - инструменты западной властной структуры и буржуазная чушь об интеллектуальной собственности; просто Система мешает их рынку».

• * *

Если Сэвидж прав и партнёрки представляют собой «дезорганизованную киберпреступность», то роль по созданию и поддержанию порядка во всём этом преступном хаосе выпадает форумам киберпреступников. Это интернет-сообщества, где большинство спамеров, мошенников и аферистов встречаются, заключают сделки, зарабатывают и поддерживают «заслуживающую доверия» репутацию в подполье.

Форумы киберпреступников служат нескольким основным целям. Прежде всего, они дают сравнительно неизвестным и начинающим преступникам возможность завоевать репутацию надёжного продавца или покупателя услуг, которому можно доверять. Если такие новички хотят создать новое киберпреступное предприятие, например спамерский ботнет, но им не хватает знаний или ресурсов для разработки отдельной части этого бизнеса, они могут просто приобрести недостающие компоненты или сведения у других участников. Или обратиться за советами и ответами на вопросы к старшим участникам и размещённым на форумах руководствам для самостоятельного обучения.

Таким образом, преступные форумы почти повсеместно снижают порог входа для потенциальных киберпреступников. Они также дают мошенникам с разными навыками место для рекламы и проверки своих услуг и товаров, а заодно для покупки у других незаконно полученных товаров и услуг.

Существуют форумы почти для каждого крупного языка и направления киберпреступности, но большинство преступных форумов ведётся либо на русском, либо на английском языке. Кроме того, большинство имеет сходную структуру: главную страницу со ссылками на подфорумы, посвящённые широкому спектру направлений киберпреступности, включая спам, мошенничество в интернет-банкинге, схемы «обналичивания» банковских счетов, разработку вредоносных программ, кражу личных данных, мошенничество с кредитными картами, злоупотребление доверием и чёрное SEO, то есть методы мошеннического воздействия на положение сайта в выдаче Google и других интернет-поисковиков.

Даже форумы, посвящённые конкретному виду киберпреступности, например спаму, обычно следуют той же структуре подфорумов. В 2011 году исследователи из Калифорнийского университета в Санта-Барбаре и Рурского университета в Бохуме, Германия, опубликовали подробный анализ ботнета Cutwail «Подпольная экономика спама: взгляд хозяина ботнета на координацию крупномасштабных спамерских кампаний». В ходе расследования исследователи получили серверную базу данных ныне закрытого преступного форума Spamdot.biz, тщательно охранявшегося сообщества киберпреступников, и в конечном счёте согласились передать мне полную информацию сайта для работы над этой книгой. В 2007 году владельцами Spamdot стали Игорь Гусев и Дмитрий Ступин, совместные администраторы родственных аптечных партнёрок GlavMed и SpamIt.

Из этих материалов было ясно: хотя среди участников Spamdot были одни из самых опытных и успешных спамеров мира, на форуме состояли и десятки людей, основной специализацией которых было предоставление вспомогательных киберпреступных услуг - от пуленепробиваемого веб-хостинга и массовой регистрации доменных имён до продажи огромных списков адресов для рассылки спама и программ, помогавших спамерам «вычищать» из имеющихся списков недействующие адреса и адреса, которыми пользовались активисты по борьбе со спамом и охранные компании.

Эти активисты часто усевают Интернет подставными адресами электронной почты в надежде, что спамеры найдут их и отправят на них спам. Затем и самодеятельные борцы, и охранные компании используют пришедший на подставные адреса спам для сбора образцов новейших вредоносных программ или фишинговых схем, распространяемых через нежелательную почту. Они помогают оценить размер и местонахождение крупных спамерских ботнетов, после чего борцы со спамом обычно могут повысить эффективность спам-фильтров. Но поскольку такая деятельность со временем снижает прибыльность и устойчивость любой спамерской операции, более опытные спамеры понимают долгосрочную ценность очистки своих списков рассылки от этих адресов-приманок. Это непрерывная игра в кошки-мышки.

Подфорумы обычно модерируют известные киберпреступники, хорошо разбирающиеся в соответствующей специализации. Нередко один и тот же киберпреступник модерирует одинаковый подфорум сразу на нескольких самостоятельных преступных форумах. Например, печально известный российский мошенник по прозвищу Severa выступает или выступал модератором спамерского подфорума по меньшей мере на четырёх разных крупных форумах киберпреступников, в том числе на Spamdot. Как будет подробнее рассказано в главе 7 «Знакомство со спамерами», Severa - автор нескольких самых продуктивных и «успешных» спамерских ботнетов из когда-либо созданных. Благодаря этому он знает практически всех значимых участников спамерской отрасли и обладает широкими познаниями в этой области, а потому идеально подходит для модерирования посвящённых ей дискуссионных форумов.

Такие деятели, как Severa, - живой «клей», скрепляющий эти киберпреступные сообщества. Они обладают огромными знаниями о своей отрасли и умело сводят новичков с более опытными участниками, которые ищут партнёров или субподрядчиков. Поэтому ключевые злоумышленники вроде Severa представляют привлекательные цели для правоохранителей: их устранение часто

дестабилизирует мошенническую экосистему.

Многие преступные форумы, особенно новые и только начинающие работу, разрешают открытую регистрацию и принимают всех желающих. Но форумы, участниками которых являются самые опытные и обладающие обширными связями киберпреступники, обычно создают для новичков разнообразные препятствия. Они призваны отделить полезных и талантливых хакеров от прихлебателей или, что ещё хуже, возможных сотрудников правоохранительных органов, пытающихся проникнуть внутрь и собрать доказательства незаконной деятельности спамеров. В качестве такой меры безопасности большинство известных преступных форумов требует от новых кандидатов назвать в качестве поручителей, или «ваучей», по меньшей мере двух действующих участников форума, пользующихся доверием. Это означает, что один или несколько действующих участников готовы поручиться за навыки и порядочность кандидата и пригласили новичка подать заявку на вступление.

Как правило, новые кандидаты также должны внести невозвратный залог, обычно в цифровой валюте вроде WebMoney или биткоинов. Если поручители подтверждают, что знают кандидата и могут ручаться за его навыки, тот получает ограниченный доступ к форуму. С его помощью он может представиться более широкому сообществу, обосновать своё право на членство и перечислить уникальные способности, которыми обогатит форум в качестве полноправного участника.

Во время испытательного срока действующие участники могут подвергать кандидата дедовщине или словесным оскорблениям либо проверять его знания программирования и взлома или навыки в заявленной области интересов и специализации. Так отсеиваются самые слабые новички. Однако в конечном счёте многие форумы демократичны: постоянное членство кандидата утверждается голосованием, в котором все полноправные участники могут, хотя и не обязаны, принять участие.

Так что же побуждает вступать в эти форумы и почему они так популярны среди спамеров? Подобно тому как некогда замок защищал своих обитателей от мародёров и разбойников, преступные форумы дают полноправным участникам некоторую защиту, или по меньшей мере основание для иска, от обмана. Мошенники особенно уязвимы перед обманом, действуя самостоятельно, поскольку не могут сообщить местным властям, что стали жертвой. В конце концов, заключаемые ими сделки в большинстве случаев незаконны. Для борьбы с таким «кидаловом» форумы насаждают строгий этический кодекс, поэтому участников, пойманных на попытке обмануть коллег, быстро изгоняют или блокируют.

Прежде всего, большинство известных форумов за небольшой процент от суммы сделки предлагают услугу условного депонирования: средства покупателя удерживаются, пока он не удостоверится, что продавец выполнил свою часть договора. Законные по меркам форума и давние участники обычно настаивают на использовании такого депонирования во всех сделках, а скряги и менее опытные участники пренебрегают этой возможностью на свой страх и риск.

Подобно тому как интернет-аукцион eBay призывает пользователей оставлять положительные или отрицательные отзывы в зависимости от качества сделок с другими участниками, положение участника мошеннического форума отчасти определяется количеством очков репутации, или «репы», накопленных за время пребывания на нём. Участники могут заработать очки репутации, просто регулярно и активно участвуя в дискуссиях разных разделов, то есть делясь знаниями и опытом по разнообразным темам компьютерной преступности. Очки репутации начисляют или снимают известные участники и модераторы форума, заслужившие право присваивать или отзывать такие показатели статуса.

Эта система на удивление эффективно регулирует преступные действия мошенников друг против друга. Алексей Михайлов, уроженец России и специалист по информационной безопасности, всесторонне изучивший документы, переписку и другие материалы, утёкшие с форума Spamdot, рассказал, что угроза единственной отрицательной публикации на форуме заставляет этих парней

мирно улаживать разногласия на десятки тысяч долларов. Доступ к форуму и их «положение» на нём заботят каждого. Без защиты и подотчётности, которые обеспечивают эти преступные убежища, спамеры, мошенники и прочие интернет-негодяи подвергаются гораздо большему риску быть обобранными своими же собратьями.

Участникам, которых администраторы форума признали виновными в многочисленных или серьёзных нарушениях правил, могут присвоить звание «оленя» или ещё более серьёзную метку «кидала». Метка оленя обычно указывает на нового участника, нарушившего правила форума случайно или потому, что ещё недостаточно с ними знаком. Обладателей статуса оленя принято считать бестолковыми новичками; этот статус предупреждает остальных участников, что общение с ними может доставить больше хлопот, чем принести пользы.

Кидалами называют тех, кто, как было доказано, «кинул» другого участника, не завершив ранее согласованную сделку: либо отказался платить за услугу или товар, либо не предоставил обещанное. Пострадавшая сторона должна доказать администраторам форума, что её обманули, обычно открыв обсуждение в подфоруме под названием «чёрный список». Очень часто для этого публикуют длинные журналы прежней интернет-переписки, документирующие предполагаемое нарушение. Интересно, что такие добровольно опубликованные записи нередко представляют бесценные доказательства и разведывательные сведения для работающих под прикрытием правоохранителей и исследователей безопасности, которые часто таятся на подпольных преступных форумах.

Хотя на обычном преступном форуме много участников, иногда десятки тысяч, большинство самых активных площадок существует для того, чтобы приносить деньги администраторам, руководителям подфорумов и продавцам готовых услуг или решений для остального сообщества. Лучшие продавцы платят за закрепление своих торговых обсуждений, чтобы предложения оставались наверху соответствующих подфорумов и с большей вероятностью попадались на глаза людям, ищущим помощь в этих областях киберпреступности. В зависимости от форума такие закрепления продаются на год или на месяц и стоят от ста до нескольких тысяч долларов в месяц.

За последние несколько лет количество новых форумов киберпреступников резко возросло, демонстрируя бурный рост спроса на преступные услуги и ожесточённую конкуренцию за покупателей. И хотя многие новые преступные сообщества исчезают или угасают вскоре после создания, другие существуют уже более десяти лет. Это говорит о значительной зрелости киберпреступной отрасли, где каждая торговая площадка располагает собственными уникальными средствами самоконтроля, налаживания связей и быстрого обмена информацией.

Попытки активистов по борьбе со спамом закрыть наиболее зрелые из этих киберпреступных сообществ, обычно путём давления на их хостинг-провайдеров, регистраторов доменов или тех и других, в конечном счёте приводят к обратному результату. Форумы просто переносят домены к другому, более пуленепробиваемому и изолированному хостинг-провайдеру, часто попутно вводя более строгие меры безопасности, чтобы тщательнее проверять новых и действующих участников на признаки соглядатаев, сотрудников правоохранительных органов и исследователей.

Но надежда есть: некоторые из самых успешных попыток обуздать эпидемии спама и вредоносных программ были сосредоточены на выявлении и задержании ведущих спамеров мира и уничтожении их преступных машин, как мы увидим в следующей главе и в главе 11 «Ликвидация».

Сноски

[1] [назад] Имя Shaman в этой переписке означает прозвище Николая Викторовича Ильина, сорокатрёхлетнего компьютерного специалиста, стоявшего за Gateline.net. Gateline была системой обработки платежей по кредитным картам, которую SpamIt, GlavMed, Rx-Promotion и другие партнёрки, по-видимому, особенно ценили за возможность обрабатывать операции MasterCard. Ступин и Гусев считали Shaman ключевым и равноправным партнёром своего бизнеса.

Глава 7. Знакомство со спамерами

Игорь Вишневский не знал бы, где и как начать заниматься спамерским бизнесом, если бы не связи, которые он завёл, проводя бессчётные часы на нескольких крупнейших в то время форумах киберпреступников. В девятнадцать лет он поступил в московский университет и мечтал получить работу программиста в законной компании. Но довольно скоро деньги закончились.

«Я проучился три года, а потом родители перестали платить за моё образование, потому что у них не было денег», - рассказал Вишневский в интервью.

Немногочисленные познания Вишневского в компьютерах восходили к подростковым годам, когда родители купили ему Sinclair ZX Spectrum - ранний домашний компьютер, один из первых массово продававшихся в Европе. В юности Вишневский самостоятельно изучил всё, от BASIC до более сложных языков программирования на ассемблере. Позднее он приобрёл подержанный персональный компьютер и освоил PASCAL - язык программирования, предназначенный для обучения студентов созданию более сложных программ.

Сообразительный молодой хакер зарабатывал от 200 до 300 долларов в месяц, создавая порнографические сайты в рамках партнёрской программы Врублевского Crutop.nu. Но для жизни в Москве этого было совершенно недостаточно, поэтому он устроился в местную компанию, продававшую отопительное и климатическое оборудование и услуги. Он и представить не мог, что это приведёт его к спаму.

Однажды начальник попросил его помочь с рекламой услуг компании с помощью не вполне законных средств.

«Однажды мой начальник заказал у кого-то спам, сказал, что это круто, и велел мне выяснить, как самому рассылать спам, - вспоминал Вишневский. - Конечно, я ответил ему, что спам - это плохо, бла-бла-бла, но он сказал, что у нас мало заказов и я должен это сделать [чтобы привлечь больше клиентов]».

Исследуя для начальника спамерскую отрасль, Вишневский пришёл на Carderplanet.com, который в то время был чрезвычайно популярным русскоязычным форумом киберпреступников. Carderplanet привлекал тысячи участников со всего мира, обменивавшихся знаниями и советами обо всём - от управления спамерскими ботнетами до обналичивания средств со взломанных банковских счетов и кредитных карт.

Основанный на Украине в 2001 году Carderplanet.com был самым дерзким собранием кардеров, то есть мошенников, торговавших краденными кредитными картами, хакеров и киберворов из всех, какие когда-либо видел Интернет. Как пишет Джо Мэнн в книге «Фатальная системная ошибка», законы против компьютерных вторжений на Украине практически не исполнялись, поэтому группа чувствовала себя в достаточной безопасности, чтобы устраивать вечеринки и рекламировать хакерские услуги в открытом Интернете. Carderplanet стал образцом почти для каждого будущего преступного форума с подфорумами для всех мыслимых специализаций компьютерной преступности.

Именно на Carderplanet Вишневский познакомился с Вартаном Кушниром, тридцатипятилетним печально известным спамером, который управлял American Language Center (ALC), законной московской компанией, обучавшей россиян английскому языку. Кушнир предложил помочь Вишневскому начать рассылать спам, если тот в ответ согласится использовать часть своих ресурсов для нежелательных писем с рекламой услуг ALC.

«Он предложил мне достаточно денег, чтобы арендовать серверы, и вскоре я зарабатывал вчетверо больше, чем мне платила климатическая компания, - рассказал Вишневский. - Но я продолжал там работать, потому что не был уверен в стабильности спама как источника денег.

Через пару месяцев я уже довольно хорошо умел рассылать спам».

Рассылая спам для своего наставника Кушнира, Вишневский познакомился с Дмитрием «Гугл» Нечволодом.

«Гугл был другом Вартана и постоянно приходил к нему обсуждать всякое дерьмо, - сказал Вишневский. - В какой-то момент я тоже начал общаться с [Гуглом]».

Но настоящий шанс выпал Вишневскому после того, как его наставника в спамерском ремесле внезапно и жестоко убили. Однажды утром мать Кушнира обнаружила окровавленное тело сына на полу в ванной: его череп был проломлен. Как подробно рассказывалось в статье *Wired.com* 2007 года, спамерское предприятие Кушнира ежедневно отправляло более двадцати пяти миллионов незапрошенных нежелательных сообщений. Большинство рекламировало услуги ALC и рассылалось по российским почтовым ящикам. По данным *Wired* и Вишневского, открытое и постоянное пренебрежение Кушнира жалобами на спам с рекламой ALC могло стать одной из основных причин его убийства.

Не испугавшись ужасной смерти Кушнира, Вишневский и Гугл объединили ресурсы и основали собственный спамерский бизнес.

К октябрю 2011 года я решил, что в утёкших данных SpamIt и Rx-Promotion уже достаточно сведений, чтобы начать устанавливать личности и составлять профили ведущих спамеров мира, а следовательно, и людей, отвечавших за создание и поддержку крупнейших спамерских ботнетов. Среди гигабайтов внутренних документов ChronoPay скрывалась электронная таблица Microsoft Excel с безобидным названием «Регистрационные данные». Она стала Розеттским камнем, позволившим установить личности многих из этих злоумышленников.

Сопоставив информацию из таблицы с уже собранными мною данными о доходах и контактах из утечки SpamIt, я понял: по неизвестным причинам кто-то в ChronoPay составил этот список самых активных спамеров. Большинство спамеров как Rx-Promotion, так и SpamIt получали деньги через WebMoney - уже упоминавшуюся виртуальную валюту наподобие PayPal, популярную в России и Восточной Европе и широко используемую в хакерском подполье.

Учётные записи WebMoney можно оформить под псевдонимом, как торговые счета или с официальным аттестатом. Для двух последних типов заявитель должен предъявить копию паспорта в уполномоченном пункте WebMoney, прежде чем получит аттестат для счёта. WebMoney не публикует эти сведения, но, по-видимому, сотрудник ChronoPay заплатил своему человеку внутри WebMoney, чтобы тот раскрыл имя и другие контактные данные, связанные с каждым счётом ведущих партнёров SpamIt. Как выяснилось, многие из этих людей также рассылали спам для Rx-Promotion.

Из 163 счетов WebMoney, перечисленных в таблице, примерно треть имела официальный аттестат или относилась к торговым счетам. В таблице содержались идентификатор WebMoney партнёра, имя, адрес, телефонный номер, дата рождения, адрес электронной почты, номер паспорта и почтовый адрес государственного учреждения, выдавшего паспорт.

Многие из этих счетов WebMoney были созданы за несколько лет до того, как их владельцы начали рассылать спам или участвовать в какой-либо киберпреступной деятельности. Но один особенно привлёк моё внимание. Среди описанных в таблице аттестованных счетов был кошелёк WebMoney, созданный в январе 2002 года пользователем, указавшим псевдоним Software Seller. За продвижение аптечных сайтов SpamIt на этот счёт поступило более 175 000 долларов. С него я и решил начать.

Гугл

Потребовалось много недель, чтобы изучить бесчисленные утёкшие записи разговоров между этим пользователем, который применял псевдоним «Гугл» и в системе мгновенных сообщений ICQ, и на Spamdot.biz, и администраторами аптечной партнёрки SpamIt. В конечном счёте мне удалось установить, что именно этот человек управлял Cutwail - безусловно, крупнейшим и самым активным спамерским ботнетом того времени. (Он и сейчас весьма активен.)

В строке таблицы с соответствующим идентификатором WebMoney рядом с хозяином ботнета по имени Гугл был указан Дмитрий Сергеевич Нечволод, родившийся 9 июля 1983 года и живший в Москве. Когда я увидел данные Нечволода в документе, что-то в них напомнило мне о разговоре с Врублевским в начале того же года. Тогда я не осознал значения этого разговора, поскольку ещё не вполне понимал роль Гугла.

Это было в конце 2010 года. Врублевский только что позвонил мне и взволнованно пересказывал разведывательные сведения, полученные через его сеть контактов в правоохранительных органах. Ему сообщили, что следователи по киберпреступлениям из Национального управления США по аэронавтике и исследованию космического пространства (NASA) едут в Москву на встречу с сотрудниками российской ФСБ. Сотрудники NASA, которые носят оружие и жетоны и обладают такими же следственными полномочиями, как другие американские правоохранительные ведомства, собирались обсудить сотрудничество с российскими властями в расследовании против Нечволода.

К тому времени следователи NASA уже связали Нечволода с Гуглом и строили против него уголовное дело по обвинению в заражении бесчисленных компьютеров NASA вредоносной программой Cutwail.

«Американцы приехали в Москву в поисках владельца Cutwail, известного под псевдонимом „Гугл“, - возбуждённо и гордо рассказал мне Врублевский в телефонном интервью о человеке, входившем в число ведущих спамеров и Rx-Promotion, и SpamIt. - Они правильно выяснили его псевдоним и даже настоящее имя, но так и не смогли его поймать. Честно говоря, думаю, его кто-то предупредил. Знаете, Брайан, уровень коррупции в российских правоохранительных органах, связанной с киберпреступностью, на самом деле довольно высок».

Я до сих пор не уверен, зачем Врублевский всё это мне рассказал. Возможно, хотел похвастаться, что имел настолько хорошие связи с российскими правоохранителями в области киберпреступности, что мог спасти одного из лучших спамеров Rx-Promotion от передачи в руки американских федеральных агентов. Думаю, Врублевский также хотел, чтобы следователи NASA знали: он оставил их в дураках. В конце концов, те же следователи NASA убедили Федеральную торговую комиссию США отключить пуленепробиваемого хостинг-провайдера 3FN. Это отключение причинило множество хлопот и расходов Врублевскому и его сети веб-мастеров экстремальных сайтов для взрослых, продавцов поддельных антивирусов и спама.

По словам источника, помогавшего NASA вести то расследование, коррумпированные сотрудники ФСБ заранее предупредили Врублевского о визите. За несколько дней до назначенной встречи NASA с ФСБ Нечволод бежал из России на Украину.

«Гугл и Павел были деловыми партнёрами и друзьями, - сказал мой источник в правоохранительном подразделении NASA на условиях анонимности, поскольку не имел права обсуждать дело. - Именно Павел предупредил Гугла, что [NASA] встречается с ФСБ по поводу Cutwail. Как сообщается, теперь Гугл на Украине и не высовывается».

Согласно сайту российской программной компании Digital Infinity Developers Group, Нечволод входил в команду первоклассных программистов, которых можно было нанять для работы через diginf.ru. На ныне закрытой странице Diginf Team этого сайта Дмитрий Нечволод был указан как «администратор систем на базе UNIX», «администратор маршрутизаторов Cisco» и «специалист по программному обеспечению для информационной безопасности». Судя по резюме Нечволода и его

команды, совместная квалификация этой группы программистов позволяла им взломать или обойти практически любую систему связи или безопасности.

Группа Нечволода поддерживала базовую версию кода ботнета Cutwail и сдавала её в аренду другим злоумышленникам на подпольных форумах, где спамерская система была известна под названием «0bulk Psyche Evolution».

Во многих отношениях Нечволод - образцовый современный киберпреступник. Эта профессия похожа на торговлю наркотиками тем, что создаёт постоянный денежный поток. Незаконные средства необходимо либо отмывать, вкладывая в недвижимость или другие материальные активы, либо тратить. По словам Вишневского, Нечволод, как и многие его коллеги, предпочитал сорить деньгами, ведя роскошную и стремительную жизнь с быстрыми автомобилями, доступными девушками, красивой одеждой и наркотиками.

«Он всегда очень хорошо одевался, а когда разбил свой седан Lexus за 100 000 долларов, пошёл и купил совершенно новый BMW», - рассказал Вишневский.

К 2008 году спамерский бизнес Нечволода процветал. Его ботнет Cutwail разросся до более чем 125 000 заражённых компьютеров и мог ежедневно обрушивать на мир шестнадцать миллиардов спамерских сообщений. Довольно скоро рост компании заставил его найти и нанять нескольких новых программистов. Чтобы вы поняли, кого именно он искал, ниже приведено объявление, которое он разместил на Crutop.nu в поисках талантливого программиста с опытом создания веб-приложений.

Тип работы: местный офис в Москве (социальный пакет предоставляется), полный рабочий день (9 часов в день, 5 дней в неделю).

ТРЕБОВАНИЯ:

• Отличное знание Perl и PHP.
• Отличное знание SQL.
• Знание AJAX, JavaScript.
• Умение быстро писать скрипты без ошибок.
• Возраст не менее 22 лет.
• Ответственность.

Заработная плата на испытательный срок: 1,5 тыс. долларов (1 месяц), после него - от 2 тыс. долларов.

Полная занятость, социальный пакет и возможности для карьерного роста. Чего ещё может желать предприимчивый молодой программист? И хотя 23 500 долларов в год были бы очень хорошей зарплатой для начинающего программиста, живущего в Москве, для разработчиков из провинции, способных убедить начальника разрешить им работать удалённо, это было воплощением мечты. Предложение Нечволода о работе - ещё одна иллюстрация того, как киберпреступные предприятия в некоторых частях света напрямую конкурируют со многими законными компаниями за талантливых программистов.

Cosma

Утёкшие документы как GlavMed-SpamIt, так и Rx-Promotion показывают, что одним из самых успешных спамеров обеих партнёрок был хакер, пользовавшийся множеством псевдонимов, среди которых «Cosma», «Тарелка», «Bird» и «Adv1». Для простоты здесь мы будем называть его Cosma. За три года он и все связанные с ним учётные записи SpamIt заработали более 3 миллионов долларов комиссионных в аптечной программе.

Его спамерской машиной был ботнет Rustock, разновидность вредоносной программы, впервые выпущенной в Интернет в 2006 году. Название ботнета происходило от его первоначальной цели: помогать совершать одну из форм мошенничества с ценными бумагами, известную как биржевая схема «накачка и сброс». В таких схемах мошенники скупают множество дешёвых акций микрокапитализации, цена которых обычно составляет от долей цента до нескольких центов за штуку, рассылают миллионы спамерских писем, рекламирующих эти акции как чрезвычайно выгодную покупку, а затем сбрасывают свои бумаги, как только цена немного поднимется благодаря простачкам, попавшимся на уловку.

В 2007 году исследователи начали замечать, что заражённые Rustock компьютеры наряду с письмами о «накачке и сбросе» стали рассылать фармацевтический спам. Специалисты Dell SecureWorks тогда оценивали, что Rustock заразил более 150 000 персональных компьютеров и был способен выбрасывать до тридцати миллиардов спамерских сообщений в день.

Появление фармацевтического спама из Rustock совпадает со временем, когда Cosma зарегистрировался как партнёр SpamIt. Те же три партнёрских имени, которыми хозяин Rustock пользовался в SpamIt, - Cosma2k, Bird и Adv1 - были зарегистрированы с той же учётной записью ICQ в Rx-Promotion Врублевского. Утёкшие данные ChronoPay показывают, что в 2010 году эти три учётные записи сообща заработали около 200 000 долларов комиссионных за продвижение аптечных сайтов Rx-Promotion.

В нескольких разговорах Cosma размышляет, что делать с десятками тысяч взломанных, но в остальном бездействующих персональных компьютеров под его управлением. Из всех бесед Ступина с Cosma ясно, что у Cosma был доступ к внутренним ресурсам SpamIt, недоступным другим спамерам, и что он по меньшей мере отчасти влиял на направление бизнеса.

В одном разговоре от 14 октября 2008 года Cosma сообщает Ступину, что решил несколько приглушить свой публичный образ после того, как привлёк нежелательное внимание других преступников. Cosma рассказывает, что на него напали и взяли в заложники бандиты, выбравшие его жертвой из-за новейшего Porsche Cayenne - внедорожника, который в Москве стоит значительно дороже 100 000 долларов. После побоев Cosma отдал похитителям ключи от Porsche. Он жалуется Ступину, что после случившегося решил заменить украденный Cayenne менее броским BMW 530xi.

Cosma оставил множество ключей к своей настоящей личности. В программе SpamIt он зарегистрировался с адресом электронной почты ger-mes@ger-mes.ru. В 2010 году сайт исчез, но его сохранённая копия показывает, что прежде на главной странице находились весьма любопытные сведения. Там было резюме программиста, получившего образование в Белоруссии, а рядом фотография молодого шатена с кружкой в руке. Над изображением стояло имя «Сергеев Дмитрий А.». В самом верху страницы находилось простое сообщение: «Я хочу работать в Google». Под резюме был указан адрес электронной почты автора, за которым следовали слова: «Жду вашу работу!»

Если бы бандиты, укравшие Porsche Cosma, знали, кто он такой, они могли бы передать его Microsoft. В июле 2011 года Microsoft объявила постоянную награду в размере 250 000 долларов за сведения, которые приведут к аресту и осуждению хозяина Rustock. Cosma по-прежнему находится на свободе.

Severa

Cosma вёл бизнес биржевого спама вместе с другим киберпреступником, хакером по прозвищу Severa. В обвинительном заключении, вынесенном федеральным судом США в 2007 году, этот

спамер был назван обвиняемым и главным партнёром Алана Ральского, американского спамера, которого в 2009 году признали виновным в том, что он платил Severa и другим спамерам за продвижение биржевых схем «накачки и сброса». Но, хотя Severa предъявили обвинение, его так и не арестовали, и дело по-прежнему не закрыто. Отчасти это объясняется тем, что он, по-видимому, всё ещё находится в России - стране, которая традиционно не выдаёт предполагаемых киберпреступников для суда в Соединённых Штатах или Европе.

Спамерскую машину Severa приводил в действие сложный компьютерный червь Waledac. Эта зараза впервые появилась в апреле 2008 года, но многие специалисты считают Waledac всего лишь обновлённой версией червя Storm, механизма огромного спамерского ботнета, впервые появившегося в 2007 году.

Waledac и Storm были крупными распространителями фармацевтического спама и нежелательных писем с вредоносными программами. На пике Waledac ежедневно отправлял 1,5 миллиарда нежелательных писем. По данным Microsoft, всего за один месяц около 651 миллиона спамерских писем, приписываемых Waledac, направили на учётные записи Hotmail. Среди них были предложения и мошеннические схемы, связанные с интернет-аптеками, поддельными товарами, работой, бросовыми акциями и многим другим. Ботнет червя Storm также ежедневно отправлял миллиарды сообщений и заразил, по оценкам, один миллион компьютеров по всему миру.

Waledac и Storm были чрезвычайно новаторскими: в обоих имелись механизмы самозащиты, специально предназначенные для противодействия исследователям безопасности, которые могли попытаться уничтожить преступные машины. Традиционными ботнетами управляют интернет-серверы, которые можно закрыть так же, как McColo или Atrivo. Но Waledac и Storm получали обновления и другие команды через одноранговую систему связи, похожую на популярные сервисы обмена музыкой и файлами. Прелесть такого подхода в том, что, даже если исследователям безопасности или правоохранителям удавалось захватить серверы внутренней системы управления ботнетом и очистить огромное количество заражённых персональных компьютеров, ботнеты могли возродиться, передавая обновления программ с одного заражённого компьютера на другой.

Согласно документам SpamIt, за три года Severa обеспечил выручку в размере 438 000 долларов и заработал 145 000 долларов комиссионных, рассылая спам с рекламой сайтов мошеннических интернет-аптек. Он также был модератором Spamdot.biz.

Ещё больше Severa зарабатывал, сдавая ботнет в аренду другим спамерам. За 200 долларов проверенные пользователи могли нанять его ботнет для отправки одного миллиона спамерских писем. Кампании нежелательной почты, рекламировавшие работу или мошеннические схемы с «денежными мулами», стоили 300 долларов за миллион, а фишинговые письма можно было разослать через ботнет Severa по выгодной цене 500 долларов за миллион.

Утёкшие разговоры SpamIt содержат множество доказательств того, что Severa управлял спамерским ботнетом Waledac. 27 августа 2009 года Severa отправил личное сообщение пользователю Spamdot.biz по имени IP-server. Из переписки следует, что тот продал Severa доступ к услугам так называемого пуленепробиваемого хостинга, который выдерживал многократные жалобы о злоупотреблениях от других поставщиков интернет-услуг. Сообщения показывают, что Severa заключил с IP-server сделку о приобретении выделенных серверов, использовавшихся для управления работой ботнета Waledac.

В личном сообщении Severa написал IP-server (перевод с русского): «Здравствуйте, пишу вам в ICQ, вы не отвечаете. Один из серверов не работает уже 5 часов. Тот, адрес которого заканчивается на .171. В чём проблема, он заработает или нет и когда?» Затем Severa вставил сообщение об ошибке, отправленное проблемным веб-сервером. Должно быть, IP-server устранил сбой, потому что интернет-адрес, на который жаловался Severa, 193.27.246.171, днём позже был отмечен аналитиками вредоносных программ и назван управляющим сервером ботнета Waledac.

В федеральном обвинительном заключении имя Severa указано как «Пётр Севера», но эта фамилия может быть псевдонимом. По данным активистов Spamhaus.org, борющихся со спамом, настоящее имя Severa - Пётр Левашов.[1]

Почему кого-то должно волновать, кто такой Severa на самом деле? Как и за его близкого соратника Cosma, хозяина ботнета Rustock, за голову Severa также могли назначить награду в 250 000 долларов. Червь Conficker, глобальная зараза, выпущенная в 2009 году и быстро распространившаяся, по оценкам, на девять-пятнадцать миллионов компьютеров по всему миру, вызвал беспрецедентную международную реакцию специалистов по безопасности. Эта группа специалистов, получившая прозвище «Кабала Conficker», тщетно пыталась сдержать распространение червя.

Но, хотя Conficker заразил огромное количество систем Microsoft Windows, его ни разу не использовали для рассылки спама. В действительности заражённые Conficker системы только загружали и распространяли новую версию ботнета Waledac. Позднее в том же году Microsoft объявила о награде в 250 000 долларов за сведения, которые приведут к аресту и осуждению автора или авторов Conficker. Некоторые специалисты по безопасности считают это доказательством связи между Severa и Conficker.

За годы совместной работы в бизнесе биржевого спама Severa и Cosma встречались несколько раз и, по-видимому, знали друг друга достаточно близко, чтобы обращаться по именам. Среди переданных мне архивных документов Spamdot.biz находится ряд личных сообщений, которыми Cosma и Severa обменялись 25 и 26 мая 2010 года. В них Severa называет Cosma «Димасом», фамильярной формой имени «Дмитрий». В свою очередь, Cosma обращается к Severa как к «Петьке», распространённой русской уменьшительной форме имени «Пётр».

И Severa, и Cosma остаются на свободе и весьма активно участвуют в мире спама и вредоносных программ. Severa по-прежнему администрирует спамерские подфорумы нескольких подпольных площадок и рекламирует там свои услуги рассылки спама, что примечательно, почти по тем же ценам, которые предлагал в 2008 году. Поддерживаемые Severa спамерские ботнеты продолжают наводнять почтовые ящики нежелательными письмами с рекламой товаров-однодневок и распространять вредоносные программы.

GeRa

Согласно утёкшим данным SpamIt, вторым по успешности партнёром программы был участник по прозвищу GeRa. За три года его реклама и реклама привлечённых им партнёров обеспечили не менее 80 000 продаж поддельных фармацевтических препаратов, принесли SpamIt выручку более 6 миллионов долларов, а ему и его приятелям - свыше 2,7 миллиона долларов.

Разнообразные данные указывают на то, что GeRa был ведущим хакером, стоявшим за Grum - спамерским ботнетом, который до своей ликвидации в 2012 году мог отправлять более восемнадцати миллиардов писем в день.

GeRa и Ступин почти ежедневно разговаривали в ICQ, обычно потому, что GeRa жаловался на неполадки в какой-нибудь части своей спамерской инфраструктуры. Ступин даже говорил, что среди всех ведущих спамеров программы GeRa доставлял больше всего хлопот, сообщив другому администратору SpamIt: «Ни Доцент [хозяин Mega-D], ни Cosma [хозяин Rustock] не могут сравниться с ним по количеству проблем с хостинг-провайдерами».

В нескольких утёкших разговорах Ступина GeRa указывает на проблемы с конкретными интернет-адресами, которые позднее были отмечены как управляющие серверы ботнета Grum. Например, в разговоре со Ступиным 11 июня 2008 года GeRa размещает ссылку на адрес

206.51.234.136. Затем, проверив сервер, он сообщает Ступину, сколько заражённых персональных компьютеров в тот момент связывалось с этим адресом. Тот же сервер давно известен как управляющий узел ботнета Grum.

К тому времени Grum превратился в настолько известную угрозу, что был упомянут в работе исследователя Dell SecureWorks Джо Стюарта «Разоблачение ведущих спамерских ботнетов». 13 апреля 2008 года, всего через пять дней после публикации анализа Стюарта, GeRa разместил ссылку на него в разговоре со Ступиным и написал: «Ха-ха, я тоже в списке!»

Разговоры GeRa со Ступиным показывают, что в какой-то момент GeRa переметнулся от SpamIt к рассылке спама для Rx-Promotion. Исследователи Калифорнийского университета в Сан-Диего (UCSD), изучившие утёкшие данные партнёров Rx-Promotion, отметили, что в исходном коде всех аптечных сайтов Rx-Promotion имелся параметр site_id, однозначно определявший магазин для последующего начисления рекламных комиссионных. Исследователи обнаружили: когда Grum рекламировал сайт Rx-Promotion, этот идентификатор всегда был одним и тем же - 1811. Согласно утёкшей базе данных Rx-Promotion, данный партнёрский идентификатор принадлежал пользователю «gera».

«Это не доказывает, что GeRa владел Grum, - сказал Стефан Сэвидж, профессор группы систем и сетей UCSD и соавтор исследования. - Но показывает, что, когда Grum рекламировал Rx-Promotion, он продвигал сайты, комиссионные за которые выплачивались человеку по прозвищу GeRa».

Согласно платёжным документам из утечек GlavMed и Rx-Promotion, GeRa получал комиссионные по всем этим учётным записям на кошелёк WebMoney с идентификатором 112024718270. По словам источника, имевшего возможность просматривать данные о личности, привязанные к счетам WebMoney, в 2006 году этот кошелёк создал человек, который пришёл в московское отделение WebMoney и предъявил российский паспорт. В паспорте было указано имя двадцатишестилетнего Николая Алексеевича Костогрыза. (Мои попытки связаться с Костогрызом, чтобы подтвердить, действительно ли он был GeRa или его личность украли, не увенчались успехом.)

Записи разговоров Ступина и личные сообщения GeRa на Spamdot.biz рисуют воинственного и задиристого хакера, который, казалось, вечно злился на то, что кто-то его обманул. GeRa долго враждовал с FTPFire, участником SpamIt, которого сам привёл в программу. В одном из разговоров со Ступиным GeRa заявил, что хочет найти этого парня и «разобраться» с ним «по-итальянски». Он сообщил Ступину, что держит на жалованье нескольких полицейских и попросил их разыскать FTPFire.

GeRa также рассказал, что его обокрали на 30 000 долларов, когда закрылась мошенническая антивирусная партнёрка, с которой он работал. Это преступное предприятие под названием BakaSoftware занималось лжеантивирусами и засыпало жертв всё более тревожными предупреждениями об угрозах безопасности и вирусах на их компьютерах. Предупреждения не прекращались, пока жертва не платила за лицензию на почти бесполезную защитную программу или не находила способ удалить назойливое приложение.[2]

Хотя неясно, действует ли GeRa по-прежнему на спамерской сцене, его вклад в мир нежелательной почты продолжает жить. Исходный код его ботнета Grum был продан нескольким другим спамерам, которые, по-видимому, изменили его для собственных целей и сейчас используют для массовой рассылки нежелательной почты.

Engel

Мало кто из хозяев ботнетов был настолько зол и мстителен, как Engel - псевдоним, выбранный осуждённым российским спамером Игорем А. Артимовичем и его братом Дмитрием. Предположительно Engel поддерживал ботнет Festi и некоторое время рассылал спам как для Rx-Promotion, так и для SpamIt. Но в 2009 году ряд происшествий и столкновений с администраторами SpamIt навсегда настроил его против программы и превратил в близкого союзника Павла Врублевского. По иронии судьбы этот союз в конечном счёте погубил Врублевского и Rx-Promotion.[3]

Festi, впервые замеченный осенью 2009 года, быстро превратился в серьёзную угрозу среди ботнетов. По данным словацкой компании ESET, производящей антивирусные средства и средства безопасности, в то время Festi относился к самым мощным и активным ботнетам для рассылки спама и проведения распределённых атак типа «отказ в обслуживании» (DDoS). Громкий и зачастую воинственный участник форума Spamdot.biz, Engel называл свой ботнет «Topol Mailer». Это название было завуалированной отсылкой к российской межконтинентальной баллистической ракете «Тополь-М» - подходящее имя для ботнета, который одно время доставлял треть всего спама в почтовые ящики по всему миру, главным образом американцам.

В профиле Engel на Spamdot.biz был указан адрес электронной почты support@id-search.org. Этот домен больше не работает, но archive.org показывает, что Engel использовал его как базу для бота, единственной задачей которого был сбор адресов электронной почты с миллиардов веб-страниц. Публично Engel утверждал, что бот был всего лишь исследовательским проектом, однако в частных разговорах хвастался участникам Spamdot, что его поисковый бот может одновременно прочёсывать сотни сайтов и быстро собирать «сотни мегабайт» списков адресов.

Вскоре после начала работы на SpamIt Engel заподозрил, что Гусев и Ступин «сбривают» его комиссионные, то есть, по существу, выплачивают не все деньги, причитавшиеся ему за продажи фармацевтических препаратов на сайтах, которые он продвигал спамом из ботнета Festi. Гусев и Ступин из SpamIt отрицали, что сбривают комиссионные, и это отрицание было правдивым, но утёкшая личная переписка Ступина показывает, что правда была лишь частичной.

Из разговоров следует, что хозяин Cutwail Гугл, Дмитрий Нечволод, каким-то образом захватил часть трафика Festi и перенаправил спам, предназначавшийся для аптечных сайтов Engel, в собственные магазины таблеток. Гусев и Ступин знали об этом, но, казалось, не хотели ничего предпринимать, главным образом потому, что сильно недолюбливали Engel и уже подозревали его в слишком тесном союзе с Врублевским.

К 2009 году Engel настолько ожесточился из-за постоянных обвинений в недоплате комиссионных, что начал активно рекламировать на форуме Spamdot.biz собственную новую аптечную партнёрку и форум Spamplanet.net. Вскоре ему удалось переманить нескольких ведущих хозяев ботнетов, в том числе Cosma, управлявшего Rustock.

Гусев и Ступин решили, что эта деятельность в сочетании со всё более публичными и агрессивными обвинениями Engel в сбривании комиссионных неприемлема, и заблокировали его на своём форуме. Когда администраторы SpamIt проигнорировали требования Engel снова включить его учётную запись, тот использовал ботнет Festi для долгой серии сокрушительных DDoS-атак на SpamIt и её сеть магазинов таблеток, снизив доходы всех участников партнёрки.

Описанные в этой главе спамеры создавали и поддерживали некоторые из самых мощных и разрушительных спамерских ботнетов мира, а потому отвечают или отвечали за огромную долю ежедневно рассылаемой по всему миру нежелательной почты. За минувшие годы их ботнеты в совокупности заразили десятки миллионов компьютеров и попутно поглотили личные и финансовые данные бесчисленных потребителей.

Каждый из этих мастеров нежелательной почты заработал своими усилиями несколько миллионов долларов, но они заставили компании и потребителей потратить ещё сотни миллионов на

укрепление цифровой обороны для борьбы с ежедневным потоком преступных программ.

Но эти спамеры были лишь вассалами и баронами, управлявшими враждующими феодами. Подлинные творцы этой экономической асимметрии - воротилы, создавшие аптечные партнёрки, - использовали спамеров как пешки в шахматной партии с высокими ставками. Этот дорогостоящий конфликт обитатели цифрового подполья вскоре назовут «фармацевтическими войнами».

Сноски

[1] [назад] Я связался с Severa по адресу системы мгновенных сообщений, который он указывал на нескольких форумах киберпреступников, где являлся главным модератором обсуждений нежелательной почты и услуг по рассылке спама. Ответивший по этому адресу человек сказал, что не знает никакого Severa, никогда не использовал ботнеты для массовых почтовых кампаний и проводил для клиентов только небольшие целевые рассылки.
[2] [назад] Стоит отметить, что основным обработчиком платежей по кредитным картам для BakaSoftware была ChronoPay.
[3] [назад] По данным *New York Times* за 2013 год, Артимович не отрицает, что пользовался псевдонимом Engel, но отрицает использование ботнетов или рассылку спама и говорит, что ChronoPay наняла его только для помощи в создании антивирусного продукта.

Глава 8. Старые друзья, заклятые враги

В начале лета 2008 года двадцатисемилетний совладелец SpamIt Игорь «Desp» Гусев отдыхал с молодой женой и грудной дочерью в Марбелье, на живописном побережье юга Испании. Ему только что предложили должность российского государственного служащего - помощника чиновника Министерства экономического развития, но он не был уверен, что хочет уехать из Испании и принять предложение.

К тому времени SpamIt и GlavMed превратились в крупнейшую на планете программу мошеннических интернет-аптек и привлекли почти всех ведущих спамеров мира. Обе программы только что достигли будущего пика своей доходности и ежемесячно приносили почти 6 миллионов долларов выручки.

Несмотря на успех спамерского предприятия, Гусев всерьёз размышлял о том, чтобы согласиться на государственную должность и навсегда оставить жизнь босса киберпреступников. Он ещё не поднимал эту тему со своим деловым партнёром Дмитрием Ступиным, но в какой-то момент должен был сообщить новость. Вдвоём они с нуля превратили GlavMed и SpamIt в процветающий бизнес, однако в последнее время между ними возникло ожесточение. Гусев стремился к более осмысленной, законной и стабильной жизни с семьёй. Тем временем Ступин всё сильнее негодовал из-за того, что Гусев постоянно путешествовал и оставлял его одного разбираться с повседневными трудностями управления бизнесом, который в основном полагался на преступников.

Следующий разговор взят из переписки Гусева со Ступиным, записанной летом 2008 года и переведённой на английский язык носителем русского Алексеем Михайловым. Он показывает копившуюся обиду Ступина из-за того, что его оставили одного. Здесь также звучит тема, проходившая через многие их беседы: Ступин вечно придумывал новые способы заработать, а Гусев, казалось, тосковал по более респектабельному, пусть и более обыденному образу жизни.

ГУСЕВ: Мне очень нравится в Испании :) Однако всё удовольствие омрачает будущая «работа»; посмотрим, что это за говнище.

СТУПИН: Какая «работа»? О чём ты?

ГУСЕВ: Я собираюсь поступить в Министерство экономического развития помощником заместителя министра.

СТУПИН: Хм... ты всё-таки решил это сделать? Если хорошенько подумать и вложить своё время и силы в то, что у нас уже есть, мы можем увеличить прибыль в два-три раза, а для тебя это означает несколько дополнительных миллионов долларов в год.

ГУСЕВ: Конечно, если твоя цель - зарабатывать деньги :) Письменно объяснять слишком долго. Давай как-нибудь пообедаем в Москве, и я объясню тебе, зачем хочу пойти на эту работу. Но вот короткая версия: в нашей стране главное не заработать деньги. Самое важное - сохранить их, приумножить и сделать так, чтобы никто их не отнял. Сейчас наш основной источник дохода - полулегальный бизнес. Если нас захотят уничтожить, сделают это так же легко, как раз-два-три. Выскочить из него будет нелегко даже с теми двумя-тремя политическими связями, которые у меня сейчас есть. Главная цель - не потерять уже имеющееся и не позволить себя уничтожить.

СТУПИН: Если речь о том, чтобы не потерять, просто купи недвижимость за границей. Она более «мобильна», чем ты думаешь. Если дерьмо попадёт на вентилятор, мы сможем поддерживать всё силами четырёх-пяти человек. Все остальные нужны только для развития бизнеса.

ГУСЕВ: Я говорю не о деньгах. Речь о самом бизнесе. Если у нас с тобой возникнут проблемы, вся эта «мобильность» исчезнет. Поэтому я хочу устроить всё так, чтобы создать проблемы тебе и мне было непросто. Ты должен признать, что без нас с тобой бизнес сам себя не поддержит. Андрей, Марго, Сашка, Стратос самостоятельно с этим не справятся.

СТУПИН: В последнее время мне кажется, что я разговариваю со стеной. Я действую тебе на нервы?

ГУСЕВ: Нет, почему ты так решил?

СТУПИН: Ты ведёшь себя иначе. Общения больше нет.

ГУСЕВ: С моей стороны всё не так уж изменилось. Я что-то пишу и не получаю ответов. Ты лишь время от времени пишешь «ладно» :)

СТУПИН: Я больше не считаю тебя «работником», человеком, с которым можно работать. Я постоянно общаюсь с Андреем и Сашкой и всё с ними обсуждаю. А тебя либо нет, либо ты ничего не делаешь (как мне кажется). Это не действует мне на нервы и не раздражает. Просто я больше не считаю тебя человеком, с которым мне нужно или можно работать.

ГУСЕВ: Что касается работы, у тебя уже давно все полномочия. Так эффективнее.

СТУПИН: Мне удобнее почти не общаться с тобой, потому что иначе я начинаю задумываться, зачем ты нам вообще нужен. Будет лучше, если ты начнёшь что-нибудь делать, иначе я буду всё меньше и меньше с тобой обсуждать.

ГУСЕВ: Знаешь, спасибо за откровенность, но я дал тебе возможность подняться от простого программиста до партнёра не для того, чтобы в будущем ты говорил мне, что я больше не нужен. Если бы мы тогда не встретились и я не позволил тебе управлять компанией, ты был бы ведущим разработчиком в какой-нибудь крупной фирме с зарплатой пять-семь тысяч и не смог бы купить дом в Турции. Подумай об этом на досуге. Деньги ослепляют людей и создают ложное ощущение полной власти.

СТУПИН: Разве я сказал, что ты стал не нужен? Это твоя собственная мысль. Если бы ты подумал чуть дальше, то понял бы: всё работало так надёжно и основательно именно благодаря тому, что я стал тем человеком, которым ты позволил мне стать.

ГУСЕВ: Давай поговорим вечером. Я немного остыну.

СТУПИН: Без проблем. У меня нет претензий.

Но эту вражду пришлось отложить, потому что на первый план вышла более неотложная проблема. Пока Гусев ещё находился на юге Испании, его засыпал срочными сообщениями друг Алексей - хакер, на которого Гусев полагался в получении разведывательных сведений об интересе правоохранителей к деятельности спамеров.

ЛЁХА: Эй. Ты здесь? Я тебя искал.

ГУСЕВ: Извини, был в Испании с семьёй.

ЛЁХА: Тебе нужно узнать кое-что плохое. Просто выслушай меня, а потом делай собственные выводы.

Лёха объяснил, что несколькими вечерами ранее столкнулся с Юрием «Hellman» Кабаенковым, равноправным партнёром Врублевского по Rx-Promotion. Как часто бывало, Кабаенков был пьян, и именно тем вечером Лёха услышал, как тот хвастался своей ролью в подкупе местной полиции ради возбуждения уголовного дела против бизнеса Гусева.

ЛЁХА: Так вышло, что на прошлой неделе я столкнулся с пьяным Hellman. И то ли просто чтобы похвастаться, то ли потому, что он тупой дебил, он выложил всё начистоту. Он

спросил: «Ты продолжаешь общаться с Desp [Гусевым]?» Это определённо был вопрос с подвохом. Я сразу ответил: «А почему ты спрашиваешь?»

Hellman намекнул, что «здравомыслящие люди» начнут задумываться, не отдалиться ли им от Гусева, и что он собственными глазами видел документы по делу, в которых говорилось, что Гусева должны обвинить в отмывании денег.

ГУСЕВ: Что они пытаются на меня повесить?

ЛЁХА: Статью уголовного кодекса о легализации доходов, полученных преступным путём. Я не уверен, существует уголовное дело уже на самом деле или нет, а лишь передаю то, что услышал. Я сам потрясён настолько тупым поведением. Очевидно, это Паша [Павел Врублевский] всё затеял, но особенно нелепо, что Hellman в это ввязался.

ГУСЕВ: Спасибо, Лёха. Ты вовремя меня предупредил.

ЛЁХА: Hellman хотел купить машину. Если помнишь, он хвастался этим у меня на дне рождения... Но в какой-то момент сказал, что пришлось отложить покупку, потому что ему для чего-то понадобилось много денег. И теперь, пока был пьян, выболтал, для чего именно они были нужны.

ГУСЕВ: Ты случайно не знаешь, какая прокуратура ведёт дело?

ЛЁХА: Понятия не имею, какая прокуратура и кто возбудил дело. Я даже не уверен, что оно существует. Я его не видел.

ГУСЕВ: Но зачем Hellman платить за уголовное дело против меня? Что я ему сделал?

ЛЁХА: Полная бессмыслица. Понятия не имею, какая у него может быть причина. Я спросил, а он ответил: «А почему бы и нет?» Паша [то есть Врублевский] - ебаный мудак. Творить такую херню - это уже слишком.

ГУСЕВ: Забавно, что он до сих пор должен мне деньги.

ЛЁХА: Столько хвастовства. Говорит, что на него в таких делах работают полковники и генералы полиции. Hellman тоже подхватил эту дурь. Говорит, что всё держит под контролем.

ГУСЕВ: Если сможешь попытаться выяснить, какая прокуратура ведёт дело, найти его будет гораздо легче.

ЛЁХА: У меня очень хуёвое предчувствие насчёт этого, Игорь. У тебя есть какой-нибудь способ решить проблему?

ГУСЕВ: Сейчас начну этим заниматься. Я не уверен на сто процентов, но попрошу помощи у очень серьёзных людей. Как ты знаешь, стопроцентной гарантии решения всех проблем не даёт даже Бог.

Так начались фармацевтические войны - долгая, публичная и в конечном счёте очень дорогостоящая распря между владельцами крупнейших на тот момент аптечных партнёрок мира, навсегда изменившая путь спамерской отрасли. Расследование, которое Врублевский и Hellman предположительно купили против Гусева и его бизнеса, запустило разрушительную череду событий: двое мужчин принялись соревноваться, кто потратит больше денег на подкуп чиновников, чтобы погубить другого.

И оба добились успеха.

Гусев считает, что Врублевский и Hellman оплатили уголовное дело против него, потому что подозревали его в причастности к недавней финансовой катастрофе, уничтожившей более 7 миллионов долларов, принадлежавших одному из их предприятий. Потерянные деньги находились на условном депонировании для некоторых самых искусных российских хакеров, и последствия их

исчезновения быстро сделали RedEye, то есть Врублевского, персоной нон грата как среди веб-мастеров сайтов для взрослых, так и среди спамеров.

В телефонном интервью Гусев сказал, что неприятности с Врублевским начались вскоре после того, как тот стал жертвой рейдерского захвата, который привёл к разграблению миллионов долларов, предположительно причитавшихся от Врублевского российским веб-мастерам сайтов для взрослых. Многие западные читатели наверняка знакомы с понятием обычного корпоративного рейда, также известного как враждебное поглощение, при котором приобретают значительную долю в компании, а затем используют полученное право голоса
для проведения изменений, например замены высших руководителей или ликвидации компании.

Однако в России враждебное поглощение слишком часто становится насильственным событием и может произойти как с помощью подкупленных судей или политиков, так и под дулом оружия. По данным Knowledge@Wharton, издания Уортонской школы бизнеса, ежегодно жертвами рейдерских атак становятся ошеломляющие 70 000 российских компаний.

«В середине 1990-х годов слишком часто появлялись сообщения о вооружённых АК-47 людях в масках, которые врывались в штаб-квартиры развивающихся компаний, захватывали имущество и заставляли владельцев подписывать разнообразные документы о передаче собственности», - написали пять слушателей выпуска 2010 года Института Лаудера при Уортонской школе, ставшие авторами статьи.

«Однако после [российского] финансового дефолта 1999 года тактика рейдеров и их агентов стала гораздо сложнее. Сегодня самый распространённый сценарий предполагает, что заинтересованная сторона заказывает рейдерской группе захват выбранной компании. Обычно рейдеры начинают с приобретения миноритарной доли в целевой фирме и используют её для возбуждения против компании необоснованных исков. Затем посредством сложной игры в юридический арбитраж они нарушают работу компании и резко обесценивают её акции. Эти действия приводят к возможному банкротству и почти неизбежному захвату рейдером».

Предприятием, ставшим целью рейда против Врублевского, была Fethard Finance - ныне закрытая система виртуальной валюты, в которой Врублевский владел контрольным пакетом. Через основанное им юридическое лицо Red & Partners Врублевский создал сеть сайтов с экстремальной порнографией. Основанный Врублевским, также известным как RedEye,[1] интернет-форум Crutop.nu был идеальным местом для рекламы сайтов Red & Partners российским веб-мастерам сайтов для взрослых, которые могли получать комиссионные за продажу месячных подписок. (Напомним, что наш «Вергилий» в этом спамерском преисподнем, Вишневский, в молодости неплохо зарабатывал рекламой партнёрских сайтов Crutop.) Когда этим веб-мастерам-партнёрам платили, они получали вознаграждение не в долларах или российских рублях, а в единицах виртуальной валюты Fethard, быстро ставшей в российском киберподполье признанной формой оплаты товаров и услуг.

Fethard и порнографическая империя Врублевского, казалось, прекрасно работали до сентября 2007 года. Тогда Врублевский, точнее администратор Crutop RedEye, сообщил более чем восьми тысячам российских веб-мастеров сайтов для взрослых, чьи деньги находились в виртуальной валюте, что Fethard стала очередной жертвой рейдерского захвата и совершенно разорена.

По словам Гусева, мозгом рейда был Михаил Жиленков, муж Марии Окуловой, внучки первого президента России Бориса Ельцина. Любопытно, что отец Окуловой Валерий Окулов - бывший генеральный директор «Аэрофлота», крупнейшей российской авиакомпании, которой вскоре предстояло радикально изменить направление жизни Врублевского.

«В 2007 году у системы Fethard было два основных акционера: Павел и Жиленков, который является известным рейдером и имеет хорошие связи в полиции и [российской ФСБ]», - вспоминал Гусев в телефонном интервью. И действительно, Александр Хинштейн, журналист российского

издания «Московский комсомолец», подробно описал действия «РостИнвеста» - инвестиционной фирмы Жиленкова, замешанной во множестве рейдерских скандалов второй половины прошлого десятилетия.

Гусев полагает, что жажда власти Врублевского и стремление быть связанным с каждым, у кого она имелась, ослепили его бывшего делового партнёра и не позволили увидеть грядущее. Жиленков воспользовался влиянием владельца 50 процентов компании, чтобы получить контроль над повседневным управлением Fethard. Это дало ему прямой доступ ко всем партнёрским счетам Fethard.

12 сентября 2007 года Врублевский получил два удара исподтишка. Первым стала новость о том, что почти все средства со счетов Fethard выведены и переведены в разные офшорные банки. Вторым было известие о том, что российская полиция возбудила уголовное дело против него и Fethard, назвав компанию незаконной банковской системой.

«Павел либо не видел, либо не тревожился об этой стороне Жиленкова, потому что расхаживал гоголем и хвастался, что заполучил такого важного человека в новые партнёры и что это даст ему все связи и власть», - сказал Гусев в интервью автору этой книги.

Рейд против Fethard был важным событием, потому что Врублевский убедил себя: его организовал Гусев. (Гусев яростно отрицает какую-либо причастность, и я поверил этому заявлению.) Решив нанести ответный удар предполагаемому обидчику, Врублевский начал вместе с уже упоминавшимся сооснователем Rx-Promotion Юрием «Hellman» Кабаенковым строить планы по возбуждению уголовного дела против Гусева.

«Это дело затеял Жиленков, - сказал Гусев. - Так он предупреждал Павла, чтобы тот не пытался вернуть деньги. Жиленков предельно ясно дал понять: если Павел попытается вернуть украденные у Fethard деньги, у него возникнет ещё больше проблем, а уголовное дело получит ход. Но Павел всё это время ошибочно подозревал, что я каким-то образом к этому причастен».

Нетрудно понять почему. Во многих отношениях Гусев и Врублевский не могли бы отличаться сильнее. Гусев вдумчив, эрудирован, нетороплив, самоироничен и скуп. Врублевский, напротив, груб, импульсивен, словоохотлив, самовлюблён и расточителен. Гусев называет себя «золотым мальчиком», выросшим в богатой семье - его дед был министром строительства в Советском Союзе, - и получил классическое образование в одной из лучших российских школ. Врублевский, который выглядит по меньшей мере на десять лет старше своего настоящего возраста, то есть человека тридцати с небольшим лет, рос не в таких тепличных условиях, и в юности его выгнали из нескольких школ.

Гусев рассказал, что начал работать в интернет-индустрии в 1998 году, когда местный предприниматель нанял его создать сайт для торговли спортивными памятными вещами. Гусев узнал всё, что сумел, об HTML и веб-программировании и заработал за свои усилия двести долларов. Вскоре он решил, что сможет получить гораздо больше в порнографическом бизнесе, и нанял программиста, который помог создать программу для сбора списков ведущих порносайтов, использовавшихся в так называемых операциях «circle jerk».

«CJ, как их называют, представляют собой систему, где разные сайты со множеством порнографических изображений перенаправляют зрителя, который нажимает на картинку, с одного сайта на другой, - сказал Гусев. - Идея CJ в том, что вас перенаправляют столько раз, что в конце концов вы настолько устаёте искать материалы, что действительно нажимаете на одну из реклам спонсоров и покупаете подписку. Эта система предназначена для того, чтобы измотать людей, и она работала довольно хорошо, по крайней мере некоторое время. Но могу сказать вам вот что: впервые этот трюк испробовали в Соединённых Штатах. Его изобрели не в России!»

Гусев и Врублевский впервые встретились благодаря общей связи с порнографией довольно экстремального характера. В 1998 году Гусев администрировал российский интернет-форум для

веб-мастеров, продававших фильмы и изображения со скотоложеством и сексом с сельскохозяйственными животными. Рынком Врублевского, который он обслуживал через холдинговую компанию Red & Partners, были любители жестокой порнографии, главным образом изображений и коротких фильмов с изнасилованием или другими формами принудительного секса, инцестом и содомией.[2]

Гусев мог получать прибыль от этого бизнеса, поскольку владел компанией по расчётам с кредитными картами Digital Internet Billing, сокращённо DiBill. Она полагалась на связи с нидерландской банковской системой, где, по словам Гусева, благополучно находилась значительная часть рынка товаров его компании.

Однажды Гусев получил мгновенное сообщение от Врублевского с предложением встретиться, обсудить объединение усилий и создать единую компанию по обработке платежей для обслуживания бурно развивавшейся порнографической индустрии, которая возникла практически за одну ночь благодаря широкому распространению коммерческого Интернета на Западе.

«Мы несколько раз говорили в Москве, и он казался таким увлечённым и заинтересованным в новом бизнесе ChronoPay и предложил мне присоединиться, - сказал Гусев. - Тогда я подумал, что это может стать очень хорошим шагом в моей карьере. Хотел бы я быть немного умнее и отказаться от его предложения».

В 2003 году они оформили всё официально. Red & Partners объединилась с фирмой Гусева DPNet, чтобы создать в Нидерландах новую корпорацию, и так родилась ChronoPay. Среди инвесторов был Владимир Цастин, генеральный директор эстонского регистратора интернет-доменов EstDomains. Цастин и Врублевский быстро подружились, и в следующие пять лет EstDomains Цастина стал самым популярным регистратором доменов среди российских веб-мастеров, особенно распространявших спам и вредоносные программы.[3]

Недолгое время Гусев и Врублевский работали бок о бок в одном офисе. Но меньше чем через год оба мужчины начали постоянно пререкаться о том, в каком направлении должна развиваться фирма. После затяжного спора о том, кому следует разрешить купить долю Гусева в ChronoPay, Гусев продал DPNet российскому предпринимателю Леониду Михайловичу Терехову и занялся созданием GlavMed и SpamIt.

«Мы сидели в одном офисе друг напротив друга, и, полагаю, поэтому нас следует считать какими-то друзьями или деловыми партнёрами, - сказал Гусев в интервью 2011 года. - Но это работало лишь первые пять-шесть месяцев. Затем у нас начались проблемы с общением. Проблема была в том, что я не поддерживал его решения, а он не поддерживал мои».

Тем временем в ChronoPay происходило нечто странное. Компания начала привлекать законные предприятия: не только порносайты, но и известные российские фирмы, стремившиеся помочь покупателям найти альтернативные способы оплаты товаров. В то время мало кто из российских трудящихся пользовался кредитной картой или вообще имел её. И хотя интерес к электронной торговле рос, на удивление немногие работавшие в России компании хотели и могли помогать потребителям оплачивать интернет-покупки с банковских счетов.

К 2006 году клиентами ChronoPay стали несколько крупнейших российских брендов, включая операторов мобильной связи МТС и Skylink, и даже более ориентированные на Запад некоммерческие организации вроде Всемирного фонда дикой природы. Миллионы россиян внезапно получили возможность оплачивать через ChronoPay счета за отопление или телефон, покупать билеты на концерты и самолёты.

Привлекая этих крупных законных клиентов, Врублевский, возможно, обеспечивал чёрным и серым предприятиям постоянный доступ к банковским системам, готовым обрабатывать более рискованные операции, например покупки в интернет-аптеках и карточные платежи за вымогательские продажи мошеннических антивирусов, сказал Гусев.

«Главная причина, по которой ChronoPay так долго и успешно работала во всех этих серых и чёрных предприятиях, заключалась в пуле белых клиентов, бизнес которых прикрывал серые и чёрные сделки, - сказал Гусев. - Они использовали это, чтобы получать более выгодные тарифы на обработку платежей от [банков-эквайеров], потому что говорили: „Мы принесём вам операции крупнейших российских компаний на миллионы долларов, а вам нужно лишь помочь нам обработать кое-что ещё“».

Профессор Калифорнийского университета в Сан-Диего Стефан Сэвидж, совершивший сотни законных покупок лекарств через аптеки GlavMed, Rx-Promotion и десятков других партнёрок, сказал, что ChronoPay в действительности была не обработчиком кредитных карт, а продавцом и перепродавцом платёжных услуг, что в отрасли называется поставщиком платёжных услуг, или PSP.

«У них не было собственных отношений с банками, но они работали с другими компаниями, у которых такие отношения имелись. У них было множество соглашений с другими людьми, помогавшими проводить деньги, - сказал Сэвидж. - От имени клиентов они представляли банкам поддельных клиентов, продававших лекарства, и по кругу проводили бизнес Rx-Promotion через созданные ими подставные компании. А позднее, когда банки выясняли, что происходит, ChronoPay отрицала всякое знание о действиях своих подставных компаний».

Иными словами, ChronoPay и Врублевский сыграли ключевую роль в создании организационного, юридического и технического прикрытия, необходимого спамерам, чтобы принимать номера кредитных карт за рекламируемые таблетки. ChronoPay и Врублевский использовали те же методы сокрытия, чтобы скрыть свою важнейшую роль в обработке десятков миллионов долларов карточных платежей от американцев и европейцев, пострадавших от мошенничества с лжеантивирусами. Как мы увидим в главе 9 «Встреча в Москве», Врублевский утверждает, что был связан с этими схемами лишь как консультант, помогавший создавать подставные компании и платёжные системы, чтобы вся операция выглядела законной для компаний кредитных карт.

По словам Сэвиджа, предоставлявшаяся ChronoPay услуга известна в отрасли как «факторинг». Компания брала нескольких клиентов, обеспечивала им обработку кредитных карт, а затем привязывала их операции к счетам подставных фирм, которые представляла банкам настоящими клиентами. После этого Врублевский и другие причастные сотрудники ChronoPay просто расплачивались с этими клиентами из собственного кармана.

Короче говоря, сомнительные организации обращались к ChronoPay главным образом тогда, когда других возможностей почти не оставалось.

«Они были готовы принимать всех этих по-настоящему тёмных клиентов, которых больше никто не согласился бы обслуживать, и управлять ими, - сказал Сэвидж. - С несколькими банковскими партнёрами велось множество игр, и ChronoPay очень хорошо умела в них играть».

Эти партнёрские отношения, прежде всего с финансовыми учреждениями бывших советских республик Азербайджана, Грузии и Латвии, были главным источником господства ChronoPay в обработке операций мошеннических интернет-аптек и схем с лжеантивирусами, скрывавшихся за законным фасадом компании. К счастью для Врублевского и Гусева, некоторое время эта деятельность в значительной мере оставалась незаметной на фоне гораздо более крупных объёмов операций сравнительно законных российских компаний.

«С одной точки зрения ChronoPay - уникальная компания, потому что в России она известна [связью] с крупнейшими брендами страны, - сказал Гусев в интервью 2010 года. - Но все знают, кому принадлежит компания, чем он занимался до неё и что делает сейчас».

• * *

Через два года после того, как Врублевский и Гусев разошлись как сооснователи ChronoPay, Гусев сам добился успеха. GlavMed и SpamIt приносили миллионы долларов в месяц и нанимали одних

из лучших компьютерных программистов, которых могла предложить Москва.

Не желая уступать сопернику, в 2007 году Врублевский и Hellman запустили Rx-Promotion и попытались переманить множество ведущих спамеров SpamIt. Rx-Promotion выходила на уже переполненный рынок, где действовало около двух десятков других мошеннических аптечных партнёрок. Но с самого начала у неё было преимущество перед конкурентами: она специализировалась на предложении строго ограниченных и вызывающих зависимость рецептурных препаратов, например гидрокодона и Valium, любому покупателю независимо от наличия рецепта, одобренного врачом.

Гусев сказал, что первоначально GlavMed также предлагала контролируемые препараты, но вскоре решила, что рынок этих таблеток слишком изменчив и опасен.

«Когда GlavMed начала работать в 2006 году, там были некоторые контролируемые вещества, но тогда мы не понимали, во что ввязываемся, - сказал Гусев. - Через пару лет мы приняли стратегическое решение не иметь никакого отношения к контролируемым препаратам. В конце концов, если продаёшь Viagra, серьёзного вреда здоровью нет. Но контролируемые препараты... если продавать их через Интернет, чаще всего продаёшь наркозависимым. А я, честно говоря, не хочу быть своего рода наркоторговцем».

Хронология Гусева не вполне совпадает с утёкшими документами SpamIt и GlavMed: они показывают, что две партнёрки продолжали продавать некоторые контролируемые рецептурные препараты по меньшей мере до середины 2009 года.

• * *

Всё указывает на то, что, несмотря на раннее предупреждение Врублевского о направленных против него политических и юридических махинациях, Гусев недооценил решимость бывшего партнёра либо не сумел найти союзников с нужными связями в российском политическом и правовом аппарате, чтобы сорвать медленно набиравшее силу уголовное дело против него и его предприятий. Во-первых, Гусев начал принимать меры, чтобы обойти Врублевского, лишь в начале 2010 года, когда наконец признал, что российские сотрудники ФСБ ведут против него расследование и пытаются изобразить его «спамером номер один в России».

Дело против Гусева совпало с кампанией тогдашнего президента России Дмитрия Медведева по привлечению иностранных инвестиций в «Сколково». Проект представлял собой амбициозный технологический парк, строившийся за пределами Москвы и призванный стать российским аналогом Кремниевой долины, крупнейшего американского инкубатора высокотехнологических инноваций. Проект «Сколково» набрал силу в марте 2010 года после того, как производитель интернет-оборудования Cisco Systems Inc. пообещал вложить в него 1 миллиард долларов, а венчурная компания Кремниевой долины Bessemer Venture Partners обязалась за два года инвестировать 20 миллионов долларов.

Но Медведев и другие руководители понимали: чтобы успешно привлечь больше инвестиций из западных стран, придётся исправить репутацию России как государства, которое неохотно преследует киберпреступников на своей территории. Гусев был идеальным первым козлом отпущения. Ему предстояло стать первой громкой целью Национального антикоррупционного комитета в сфере киберпреступности. Этот орган должен был помогать государственным ведомствам и министерствам очищаться от коррумпированных чиновников, которые часто закрывали глаза на преступления в обмен на взятки или «пожертвования».

Словно подтверждая правильность выбора антикоррупционного комитета, первым ответом Гусева на активно разворачивавшееся против него уголовное дело стала попытка подкупить государственных чиновников, чтобы они задерживали расследование, сообщали ему подробности о его ходе и создавали препятствия от его имени.

9 января 2010 года Гусев связался по интернет-чату с Дмитрием Ступиным, своим соадминистратором GlavMed-SpamIt, чтобы обсудить способы избежать или отсрочить уголовное преследование. Гусев сказал Ступину, что, возможно, сможет купить защиту от обвинений, направив деньги ключевым российским политикам, способным влиять на следователей.

В частности, Гусев предложил приобрести спонсорство Федерации волейбола России. Цена составляла официальный спонсорский взнос в 10 миллионов рублей, около 350 000 долларов, плюс 150 000 долларов наличными. Официальный руководитель федерации Николай Патрушев - влиятельный человек в российских правоохранительных органах. С 1999 по 2008 год Патрушев возглавлял российскую ФСБ, организацию-преемницу КГБ. С 2008 года он занимает должность секретаря Совета безопасности России.

По словам Гусева, российские спортивные лиги и благотворительные организации обычно используются как средства направления денег в карманы людей, принимающих политические решения.

«В России спорт в действительности не является бизнесом. Это способ решать деловые вопросы, - сказал Гусев в телефонном интервью. - У меня есть друг, довольно известный хоккеист. Однажды он рассказал, что в [хоккейной] лиге всего две команды могут что-то зарабатывать, а остальные несут лишь убытки. Спорт в России - это своего рода... с одной стороны, возможность встретить новых людей и завязать отношения на будущее, а с другой - получить некоторую защиту. Потому что во всех лигах, будь то баскетбол, футбол, хоккей или что угодно, есть люди из правительства, которые каким-то образом их контролируют».

Описанное Гусевым явление хорошо задокументировано. Один пример приводится в книге Леннарта Дальгрена, бывшего руководителя российского подразделения шведского производителя мебели IKEA. В книге «Вопреки абсурду: как я покорил Россию, пока она покоряла меня» Дальгрен пишет, что ему пришлось выплатить российским благотворительным организациям взятки на 30 миллионов рублей, или 1 миллион долларов, а те помогли направить деньги бюрократам и высокопоставленным чиновникам.

В телефонном интервью в мае 2011 года Гусев рассказал мне, что стал платным спонсором российской волейбольной лиги в надежде убедить кого-нибудь остановить уголовное дело против него. Гусев был убеждён, а другие утёкшие документы, по-видимому, подтверждают его подозрения, что интерес правоохранительных органов к его деятельности оплатил Павел Врублевский, бывший деловой партнёр, ставший конкурентом.

И действительно, в конце 2010 года Врублевский обеспечил ChronoPay спонсорство Российской федерации баскетбола. Федерацию возглавляет Сергей Иванов, бывший сотрудник КГБ, которого президент России Владимир Путин назначил заместителем председателя правительства. ChronoPay даже использовала связи с Ивановым как рекламу своего успеха и влияния. В серии фотографий руководителей ChronoPay в корпоративном блоге есть снимок, на котором Врублевский и Иванов стоят в первом ряду на баскетбольном матче, болеют за свою команду, оба в деловых костюмах и широко улыбаются.

Неясно, сколько Врублевскому пришлось заплатить за это спонсорство, однако несколько признаков указывают на сумму более 1 миллиона долларов. В статье печатного выпуска российской ежедневной газеты «Коммерсантъ» за март 2011 года говорилось, что благодаря взносам спонсоров - ChronoPay, российской инвестиционной группы ВТБ и российского автопроизводителя Sollers - бюджет баскетбольной федерации вырос примерно до 6 миллионов долларов. В статье приводятся слова Иванова о том, что ВТБ внёс более половины бюджета, а вторую половину обеспечили ChronoPay и Sollers.

«Если Павел хочет, чтобы меня назвали спамером номер один в мире, он платит большие деньги, чтобы дать мне это звание, но, знаете, я никогда не пытался проводить исследования и выяснять,

кто на самом деле был спамером номер один», - сказал Гусев. Он имел в виду только что опубликованную работу исследователей UCSD, установивших, что спамеры Rx-Promotion рассылали более чем вдвое больше спама, чем участники любой другой программы, включая SpamIt.

«Я думал, что это должны быть владельцы крупнейших ботнетов, и полагал, что большинство из них работает со SpamIt, - сказал Гусев. - Но это исследование показывает, что 25 процентов спама приходилось на сайты Rx-Promotion. Павлу очень трудно даже со всей этой информацией, деньгами и влиянием убедить людей, что большая проблема связана не с ним».

Записи разговоров конца января 2010 года показывают, что Гусев и Ступин отправили из своей компании Despmedia первоначальные «пожертвования» в размере 210 000 и 115 000 долларов Федерации волейбола. В другом интернет-разговоре месяц спустя Гусев сообщает Ступину, что общие расходы на взятки российским правоохранителям превысили 400 000 долларов.

В разговоре от 19 февраля 2010 года Гусев сообщает, что только что заплатил 20 000 долларов: 5000 посреднику и 15 000 человеку из Генеральной прокуратуры, правоохранительного органа, расследовавшего его деятельность, - за сведения и «затягивание» дела. В той же переписке Гусев говорит, что нашёл человека, чрезвычайно способного мужчину, юриста и решальщика, который может предоставить «полный набор услуг» для решения «проблемы RedEye».

Гусев получил от этого человека обещание, что пожертвование должного размера практически гарантирует заключение Врублевского под стражу и уничтожение разных сомнительных предприятий последнего. Но цена гарантии была высокой: 1,5 миллиона долларов.

Гусев говорит, что встретился с решальщиком, и просит Ступина посоветовать, как договориться с ним помимо выплаты 1,5 миллиона. Условие посредника состояло в том, что Гусев и Ступин должны согласиться помочь давнему общему знакомому создать конкурирующую программу мошеннических интернет-аптек.

«Я нашёл человека, который готов помочь мне в этой ситуации с RedEye, - пишет Гусев. - У этого парня есть проверенная схема, потому что он очень сильный юрист. Настоящий решала. За свои услуги, помимо очень большой суммы денег, он просит кое-что взамен: помочь его другу, очень известному веб-мастеру, который столкнулся с проблемой, похожей на нашу, и был спасён этим человеком. Сейчас этот „друг“ ничем не занимается. Юрист просит нас помочь ему создать программу интернет-аптек. Я не в восторге от идеи усилить конкуренцию, но из всех людей, с которыми я говорил, лишь этот парень предложил структурированное решение проблемы, давшее нам надежду».

Затем Гусев переходит к спонсорству волейбольной федерации - условному обозначению направления денег коррумпированным сотрудникам ФСБ для создания препятствий. Он говорит: «Люди из волейбольной ассоциации могут и будут прикрывать нас, используя свои связи в ФСБ, но почти ничего не могут сделать с прокуратурой. Они способны лишь затянуть судебное разбирательство. Они также не смогут привлечь Red к ответственности. Человек, которому нас просят помочь, - мой давний знакомый Pet, владелец „лолного“ [разговорное слово, произносится как „лол-нава“ и означает сайты с Лолитой или детской порнографией], где расчёты проводятся через BillCards». Почти наверняка здесь Гусев говорит о Евгении «Pet» Петровском, белорусском владельце компании обработки платежей Sunbill/BillCards, которого похитила банда Логинова в главе 2.

После того как Гусев сообщает, что юрист-решальщик просит 1,5 миллиона долларов и личную услугу, Ступин восклицает: «О боже! Что он обещает за это?»

«Он обещает, что Red останется в тюрьме и не сможет откупиться, - ответил Гусев. - Кроме того, тот потеряет значительную часть бизнеса и останется без денег на войну».

В телефонном интервью в середине 2011 года Гусев так объяснил свои действия: «Я хотел лишь поговорить с кем-нибудь из ФСБ, кто создавал это [дело] для Павла, и убедить их прекратить весь конфликт, пока не стало слишком поздно, - сказал он. - К сожалению, это мне почти не помогло».

Летом 2010 года неизвестные инсайдеры или злоумышленники, взломавшие сеть компании, слили десятки тысяч писем и внутренних документов ChronoPay, содержавших бессчётные примеры деятельности, организацию которой Врублевский отрицал годами.

Когда я спросил Гусева, отвечал ли он за этот инцидент, тот отрицал, но затем признал, что его участие было логичным предположением с учётом войны на истощение, которая ранее застала его врасплох.

«Павел опережает меня на год, потому что я совершенно не ожидал, что он обнародует всё это обо мне и нашем бизнесе, - сказал Гусев. - Теперь я своего рода киберпреступник, и он своего рода киберпреступник. Самым логичным решением было бы тихо всё уладить, но он так отчаянно хочет причинить мне вред, что принимает решения, не понимая последствий».

Убеждённый в том, что за утечкой документов и писем ChronoPay стоял Гусев, Врублевский заплатил местному хакеру за взлом и публикацию клиентской базы данных SpamIt и GlavMed.

Следующая запись разговора датирована 28 августа 2010 года, всего через несколько дней после того, как внутренняя база SpamIt попала к американским правоохранительным органам. В этой беседе Ступин и Гусев обсуждают, не закрыть ли SpamIt.

> **ГУСЕВ:** Похоже, я в глубокой заднице. Red передал нашу базу американцам.
>
> **СТУПИН:** Каким американцам?
>
> **ГУСЕВ:** Пока не могу сказать точно. Вероятно, ФБР или Секретной службе. Ты читал в блоге Кребса о совещании в Белом доме по проблеме незаконных аптек в Интернете?
>
> **СТУПИН:** Нет.
>
> **ГУСЕВ:** krebsonsecurity.com
>
> **СТУПИН:** Может, вернёшься в Россию?
>
> **ГУСЕВ:** Я собираюсь так и сделать. Теперь я по-настоящему беспокоюсь.
>
> **ГУСЕВ:** Думаешь, «закрытие» поможет? Просто пойми: у них ВСЯ наша база... Там 900 000 записей. Что мы будем с ними делать? Для обвинительного приговора и пяти лет тюрьмы достаточно доказать всего одну операцию! Что хуже всего? Приговоры складываются, и можно получить пять пожизненных сроков.
>
> **ГУСЕВ:** Я тоже думаю, что нужно остановить работу, потому что это абсолютная катастрофа!
>
> **ГУСЕВ:** Что касается закрытия, думаю, сначала нужно закрыть SpamIt. Через месяц или половину месяца - GlavMed.

Гусев и Ступин закрыли SpamIt.com в конце сентября 2010 года, заменив главную страницу Spamdot.biz следующим сообщением партнёрам:

> Из-за многочисленных негативных событий, произошедших в прошлом году, и возросшего внимания к нашей партнёрской программе мы решили с 1.10.2010 [1 октября 2010 года] прекратить принимать трафик. Мы считаем это решение наиболее подходящим в данной ситуации. Оно позволит избежать внезапной остановки работы, ведущей к краху программы и невыплате вашей прибыли.
>
> В нашем случае вся прибыль будет выплачена в обычном порядке. Любое возможное мошенничество исключено. Просим до 1.10.2010 перевести свой трафик в другие

> партнёрские программы.
>
> Благодарим за сотрудничество! Мы очень ценим ваше доверие!

Сразу после закрытия SpamIt объём нежелательной почты, рассылавшейся по всему миру, заметно сократился, по разным оценкам, на 20-40 процентов: работавшие на программу спамеры пытались перенести трафик в другие партнёрства, которые могли платить за их услуги. Специалисты, отслеживавшие ведущие спамерские ботнеты, использовавшиеся для продвижения «канадских» аптечных сайтов SpamIt, быстро заметили, что большинство крупных ботнетов, в том числе Grum, Rustock и Cutwail, по существу несколько недель стояли на нейтрали, пока их хозяева искали новые способы зарабатывать с помощью преступных машин.

Благодаря статье *New York Times*, источником которой, согласно утёкшим письмам ChronoPay, отчасти стала информационная работа сотрудников по связям с общественностью Российской ассоциации электронных коммуникаций (РАЭК), Гусев превратился в крупнейшего спамера мира, хотя сам утверждает, что никогда не был спамером в обычном смысле. К тому времени, когда московская полиция обыскала его квартиру, Гусев уже бежал из России с женой и маленькой дочерью и, как сообщалось, направлялся в Испанию.

Но Гусев не собирался сдаваться без боя. В ноябре он запустил redeye-blog.com, сайт, где публично каталогизировал яркое прошлое Врублевского, и даже нанял носителя английского языка для перевода блога западной аудитории. Вскоре многочисленные враги Врублевского последовали его примеру и начали вывешивать грязное бельё RedEye в комментариях к блогу. Сотни веб-мастеров сайтов для взрослых, хорошо помнивших причинённое им Врублевским зло, принялись документировать в блоге миллионы долларов, которые тот всё ещё был им должен после катастрофы Fethard.

«Москва - хорошее место для жизни, когда у тебя есть деньги и хорошие друзья, способные помочь с проблемами, - сказал Гусев в телефонном интервью в ноябре 2010 года. - Я пытаюсь разрушить его ChronoPay, потому что, если у него не будет денег, надеюсь, он прекратит всё это».

Вскоре после этого интервью с Гусевым Врублевский наконец признал, что фармацевтические войны, как многие называли их вражду, прошли точку невозврата. Вернее, как иронично выразился Врублевский, ни одну сторону, по-видимому, не удерживало «взаимно гарантированное уничтожение». Он имел в виду доктрину военной стратегии, при которой обе стороны гонки ядерных вооружений воздерживаются от первого удара, поскольку знают, что действие агрессора неизбежно вызовет равный ответ.

«Проблема в том, что Гусев не пытается ударить меня своим оружием, а пытается напугать, - сказал Врублевский во время одного из многочисленных звонков автору. - Его заявление о том, что он навсегда остаётся за границей, - вся эта чушь предназначена его веб-мастерам и, конечно, звучит как история о Джеймсе Бонде, но так никто не скрывается. В действительности Гусев ждёт, что я позвоню и скажу: „Ладно, приятель, давай прекратим эту войну“. Но в том компромате ChronoPay нет ничего, что могло бы меня остановить или теперь спасти его. Это лишь способ, с помощью которого он, как ему кажется, сможет шантажировать меня каждые несколько месяцев, и ничего больше».

Тем временем потребители по всему миру наслаждались краткой передышкой от шквала спамерских писем и переносимых ими вредоносных программ, которые грозили заразить компьютеры и украсть личные данные. Империя почтового спама балансировала на грани краха. Когда я спросил Гусева, не тревожит ли его, что попытки опозорить Врублевского и доставить ему неприятности способны ещё сильнее повредить отрасли, которую он помог построить и которая сделала его весьма богатым, Гусев ответил, что вынужден пойти на этот риск.

«По крайней мере, мы оба потеряем много времени, сил и денег, и победителя здесь не будет, - сказал Гусев по телефону из нераскрытого места за границей. - Я всё ещё готовлю некоторые

отчёты, чтобы продолжать этот конфликт, лишь по одной причине. Потому что, если я остановлюсь сейчас, через год или два Павел найдёт возможность снова ударить меня чем-нибудь другим, а я не хочу ему это [позволять]».

Я верил Гусеву, когда он рассказывал факты о своей жизни, бизнесе и конфликте с Павлом. Возможно, он не всегда говорил мне всю правду, но у меня было мало причин сомневаться в его версии событий. Врублевский, напротив, во время наших интервью часто лгал мне или растягивал истину далеко за пределы правдоподобия. И всё же он обещал быть откровеннее, если я встречусь с ним на его территории, а мне не терпелось услышать его сторону истории. Пришло время обновить паспорт.

Сноски

[1] [назад] Обратите внимание: Врублевский отрицает, что является RedEye, и всегда говорит о RedEye как о «господине RedEye», что выглядит несколько шутливо. Блог Гусева о Павле называется redeye-blog.com.
[2] [назад] Врублевский отрицает даже связь с материнской компанией, владеющей всеми этими сайтами, хотя регистрационные документы указывают тот же адрес в Нидерландах, который ChronoPay использовала в своих регистрационных документах. Более того, сайт Red & Partners много месяцев размещался в диапазоне интернет-адресов, выделенном ChronoPay европейскими органами распределения интернет-адресов.
[3] [назад] Цастин назвал «чепухой» утверждения о том, что EstDomains заигрывала со спамерами и распространителями вредоносных программ. Тем не менее позднее интернет-регуляторы лишили его компанию возможности выдавать новые доменные имена после публикации *Washington Post*, рассказавшей, что в Эстонии его признали виновным, среди прочего, в сговоре с целью мошенничества с кредитными картами, отмывании денег и подделке документов. После этого EstDomains прекратила существование, но Цастин и ещё шесть сообщников предположительно продолжили незаконные схемы. В 2011 году эстонские власти арестовали его в ходе международной операции правоохранительных органов по уничтожению троянской программы DNSChanger. Этот огромный ботнет заразил более четырёх миллионов персональных компьютеров по всему миру вредоносной программой, которая захватывала поисковую выдачу и отключала защитные программы, и принёс Цастину и его деловым партнёрам более 14 миллионов долларов. Цастину и его коллегам предъявили обвинения в мошенничестве с использованием электронных средств связи и отмывании денег, но в конце 2013 года эстонский суд их оправдал. На момент написания книги мужчины ожидают экстрадиции из Эстонии, чтобы предстать перед судом в Соединённых Штатах по обвинениям в кибермошенничестве.

Глава 9. Встреча в Москве

Замёрзшая Москва-река хрустела и стонала, бурля под двумя двигателями, с постоянной скоростью толкавшими наш изящный современный круизный ледокол. На дальнем берегу над покрытой инеем чёрной водой возвышалось грозное и прекрасное здание Кремля. Через открытую дверь за моей спиной в пронизывающий ночной воздух врывалась какофония пульсирующей русской поп-музыки, звона бокалов и грохота столовых приборов о тарелки.

Февраль трудно назвать самым тёплым месяцем для поездки в Россию, но приглашение в пресс-тур 2011 года от российской компании по безопасности «Лаборатория Касперского» оказалось слишком своевременным, чтобы от него отказаться. Я хотел застать Врублевского врасплох и не был уверен, что он ещё долго останется на свободе, поэтому с готовностью принял приглашение.

Я изучал русский язык и культуру, а также их грязное киберпреступное подполье уже больше пяти лет и давно мечтал побывать в стране. Но о предстоящем визите сообщил лишь немногим и никому не раскрыл настоящую причину поездки: встретиться с Павлом Врублевским в Москве и, возможно, с Игорем Гусевым во время отдельной поездки по Европе, которая так и не состоялась. Тогда мне казалось, что их вражда могла стать интересной историей, и мне не терпелось встретиться с каждым лицом к лицу.

Я хотел встретиться с этими печально известными киберпреступниками именно тогда, поскольку считал, что это может оказаться единственной возможностью взять у них личное интервью без присутствия тюремных охранников. Я готовил цикл статей о фармацевтических войнах Гусева и Врублевского, потому что вдвоём они, вероятно, отвечали за 75 процентов спама на планете. Я был уверен: после начала публикации цикла ни один из них не захочет много со мной разговаривать.

«Брайан! Идёмте, представление начинается», - проревел широко улыбавшийся и махавший рукой Евгений Касперский, которого едва было слышно за мощными турбинами корабля и треском речного льда. Последовав за ним через дверь с кормы в главный зал, я чуть не врезался в труппу молодых мужчин в небесно-голубых комбинезонах. Они делали перевороты и исполняли традиционный русский народный танец на деревянном танцполе между баром и обеденными столиками.

Круиз на ледоколе с Касперским состоялся за день до моего отъезда из Москвы. После ужина мы с ним выпили по рюмке ледяной русской водки, и он начал рассказывать о своей работе в области криптографии в 1980-х годах для бывшего советского института, который поддерживали Министерство обороны СССР и КГБ, тогдашний российский аналог Федерального бюро расследований США.

Выяснилось также, что мы оба заинтересовались компьютерной безопасностью после взлома. Евгений стал одержим вирусами, обнаружив в 1991 году вредоносную программу на своём компьютере. Я принялся изучать всё, что мог, о компьютерах и интернет-безопасности десятилетие спустя, когда мою домашнюю сеть захватил «червь li0n» - зараза, выпущенная ныне известным китайским хакером. Она лишила меня доступа к собственным системам и уничтожила несколько серверов.

Наблюдая, как танцоры проносятся из одного угла корабля в другой, я мысленно вернулся к дню прибытия в Москву, когда сразу же добился встречи с Врублевским. После беседы с печально известным деятелем киберпреступного мира я не сомкнул глаз и вновь и вновь прокручивал в голове события того дня.

Мой рейс в Москву проходил через Международный аэропорт имени Джона Кеннеди в Нью-Йорке, где я столкнулся с Полом Робертсом, журналистом и аналитиком по вопросам безопасности, который незадолго до этого начал работать на Касперского. Робертс также участвовал в пресс-туре.

Я прежде не бывал в России, но при подлёте к Международному аэропорту Шереметьево увидел Москву именно такой, какой до этого её представлял: пасмурной, холодной, снежной и ветреной.

Ожидая приземления, я внезапно осознал, насколько мало в действительности готовился к поездке, и впервые немного испугался. Перед отъездом родственник, служивший в дипломатическом ведомстве, дал мне несколько непрошеных советов о том, как обеспечить безопасность в Москве. В основном это были очевидные вещи: «назначайте все встречи в общественных местах», «никуда не ходите в одиночку» и «не садитесь в машины к незнакомцам». Тем не менее меня поразило, как скоро после прибытия в Москву мне придётся пренебречь всеми этими советами.

В аэропорту нас с Робертсом должна была ждать машина, чтобы отвезти в гостиницу, но сильный ветер задержал вылет нашего рейса из Нью-Йорка. Когда мы прибыли в Россию, нанятой машины нигде не было.

Стоило нам выйти из главного терминала на покрытый снежной кашей тротуар, как в нас сразу распознали американцев и окружили около полудюжины мужчин, предлагавших «дешёвую» поездку на такси из аэропорта. К сожалению, гостиница находилась примерно в тридцати километрах, и поездка обещала быть какой угодно, только не дешёвой.

Очень скоро после выхода из терминала меня начало мутить, причём настолько, что я был уверен: завтрак вот-вот окажется на таксистах, которые постоянно лезли мне в лицо и не понимали слова «нет». Я отступил к покрытой снегом металлической скамье, чтобы перевести дух и прийти в себя. Таксисты, казалось, поняли, что могут пожалеть, если подойдут слишком близко, и милосердно оставили меня в покое на пару минут. Вскоре Робертс направился ко мне, осмотрев весь тротуар перед аэропортом в поисках признаков заранее заказанной машины.

«Мне эта идея тоже не очень нравится, но, похоже, придётся нанять одного из этих парней», - сказал он, щурясь сквозь плотный снегопад.

Пять минут спустя мы теснились на заднем сиденье чёрного компактного автомобиля российского производства, мчались по раскисшим улицам и лавировали между более медленными машинами, заполнявшими Ленинградское шоссе - главную трассу из аэропорта в центр Москвы. Я воспользовался возможностью проверить заранее оплаченную услугу беспроводного Интернета. Я редко подключаюсь к незащищённым общественным сетям Wi-Fi и тем более не хотел делать этого в Москве, поэтому стремился не зависеть от беспроводных сетей кафе и гостиниц. Я заранее договорился приобрести доступ в Интернет у компании XCom Global. Непосредственно перед отъездом она присылает USB-модем, который теоретически должен обеспечивать беспроводной доступ к 3G почти в любой точке выбранного города.

Однако, подключив модем к MacBook на заднем сиденье такси, я с огорчением обнаружил, что сигнал невозможно удержать дольше нескольких секунд. Сначала я подумал, что причина в нашем движении по шоссе со скоростью 120 километров в час, но позднее выяснил: услуга работала столь же ненадёжно и в кафе рядом с гостиницей, в самом центре Москвы. Те немногие планы, которые я составил перед поездкой, стремительно рушились.

Через сорок пять минут и сумму, равную 170 долларам, мы с Робертсом вышли из такси и зарегистрировались в гостинице Marriott Grand на Тверской улице - широкой торговой магистрали, идущей от Красной площади через центр Москвы. За стойкой регистрации привлекательная молодая женщина попросила мой паспорт. Когда я его предъявил, она забрала документ, сухо сказала, что я смогу получить его позднее в тот же день, и исчезла в служебном помещении.

Мне совершенно не нравилась мысль расстаться с паспортом, но особого выбора не было. Вскоре беспокойство превратилось в страх. Я пробыл в гостинице всего пять часов, когда меня встревожило новостное оповещение Google, настроенное для отслеживания публикаций в Интернете с моим именем. Оно вело на короткое сообщение в российском блог-сервисе LiveJournal, раскрывавшее моё точное местонахождение. В публикации говорилось: «Американский блогер по кибербезопасности Брайан Кребс сейчас находится в России и остановился в московском Marriott Grand».

Я помчался наверх, запер дверь просторного гостиничного номера и сразу задумался, не совершил ли огромную ошибку, приехав в Россию. В конце концов я убедил себя в обратном, напомнив, что это интервью необходимо для завершения всей моей работы по разоблачению спамеров. Через несколько часов я наконец набрался храбрости позвонить Врублевскому. Он ответил на третий из имевшихся у меня номеров мобильного телефона.

«Чува-а-а-а-а-ак! - проревел он в трубку. - У вас семь утра. Кто умер?»

Я сообщил Врублевскому, что на самом деле нахожусь в его часовом поясе и нам следует встретиться как можно скорее. После ещё одного протяжного «Чува-а-а-а-а-ак!» Врублевский пообещал прислать машину, если я подожду в вестибюле гостиницы. Он сказал, что вместе с водителем отправит свою секретаршу Веру. Затем описал Веру как чудовищно толстую, непривлекательную пожилую даму, но, мол, она говорит по-английски и умеет обращаться с западными людьми, поэтому приедет именно она.

Через пятнадцать минут я сидел в вестибюле, нервно ждал Веру и наблюдал, как входящие гости стряхивают снег и тяжело проходят через вращающуюся дверь гостиницы. Потягивая горячий чай, я с трудом удерживался от взглядов на великолепную стройную молодую брюнетку в обтягивающих джинсах и дутой белой куртке, которая нервно стояла у двери. После некоторого времени безуспешных попыток не смотреть в её сторону было трудно не заметить, что она тоже старается не глазеть на меня.

Примерно через пять минут этого танца молодая женщина подошла и спросила, не Брайан ли меня зовут. На мгновение я встревожился, ведь тогда почти никого не знал в Москве, пока она не представилась Верой. Тут я с улыбкой вспомнил, почему почти ничему из сказанного Врублевским нельзя доверять.

Шутка получила продолжение, когда после примерно двадцати минут ползучего московского часа пик ради поездки на пару миль мы прибыли в офис ChronoPay и я столкнулся с той же девушкой, но в другой одежде. Оказалось, у Веры есть сестра-близнец, которая тоже работает в компании.

В тот вечер Врублевский был особенно возбуждён и явно обрадовался моему неожиданному визиту. Как и следовало ожидать, почти сразу после моего приезда он пустился в пространный рассказ. Оказалось, кто-то организовал полицейский рейд на «Золотую вечеринку» Rx-Promotion, которая прошла четырьмя вечерами ранее в московском Golden Palace. Обычно это пьяное и непристойное мероприятие устраивали для всех партнёров Rx-Promotion - нескольких сотен людей, рекламировавших аптечные сайты программы. Лучший партнёр должен был выиграть настоящий золотой слиток весом один килограмм, а другим ведущим продавцам таблеток предназначались iPad и iPhone.

К несчастью для партнёров Rx-Promotion, вечеринка прекратилась, когда несколько автобусов с людьми в лыжных масках и с автоматами ворвались внутрь и начали допрашивать гулявших. Врублевский утверждает, что людей направили органы по борьбе с наркотиками. Однако, по словам нескольких участников, описавших случившееся на разных российских форумах, полиция, по-видимому, использовала рейд как предлог, чтобы сопоставить интернет-псевдонимы партнёров Rx-Promotion с настоящими лицами и именами. Про себя я решил, что версия Врублевского маловероятна, но не хотел прерывать рассказ: вдруг он обидится и укажет мне на дверь или

сделает что-нибудь похуже.

Сам Врублевский на собственной вечеринке не появился. По его объяснению, за день до мероприятия жена без понятной причины умоляла его срочно уехать в отпуск на Мальдивы. Более того, у кого-то хватило предусмотрительности убрать все логотипы Rx-Promotion из арендованного помещения за несколько часов до приезда полиции.

«Весь российский Интернет знал, что в Москве должна состояться вечеринка Rx-Promotion, и, разумеется, все ожидали увидеть логотипы Rx-Promotion», - рассказывает мне Врублевский, одну за другой закуривая Marlboro в тесном конференц-зале компании. Там висит огромная устаревшая карта мира, по бокам от которой расположены мечи и гигантский красный флаг советской эпохи.

«И почему-то, - продолжил он, говоря о себе в третьем лице, - все ожидали, что господин Врублевский там появится. Очевидно, господин Врублевский, вероятно, не смог бы контролировать каждого ебаного придурка вокруг с камерой в телефоне. Поэтому господин Врублевский решил там не появляться. Одновременно кто-то другой решил убрать все логотипы Rx-Promotion.

Господин Врублевский летит на Мальдивы в недельный отпуск. Затем ему звонят и сообщают, что пять автобусов российского спецназа по борьбе с наркотиками едут на вечеринку, закрывают Golden Palace и два соседних кафе просто потому, что спецназовцев, собак и камер слишком много. Они входят внутрь и обнаруживают какую-то очень тупую херню: ни господина Врублевского, ни логотипов, снимать на видео совершенно нечего».

История о том, как полиция устроила рейд на вечеринку Rx-Promotion ради компромата на основателей и партнёров, безусловно, была забавной, однако, по-видимому, это оказался всего лишь один из девяти рейдов в казино и почти ста рейдов по «игорным притонам», проведённых в 2011 году новым московским борцом с азартными играми Анатолием Андреевым.

Рассказав эту, казалось бы, случайную историю, Врублевский просит Веру принести кофе, и мы немного беседуем о московском движении и о мужчине, который топает над нами, сгребая с крыши здания огромные кучи снега. Я немного расспрашиваю Врублевского о семье, и тот со знающей улыбкой и саркастическим смехом говорит, что его отец много лет работал исследователем в Nycomed, крупной европейской фармацевтической компании.

Я спрашиваю о происхождении меча, стоящего рядом с советским флагом за моим стулом. Врублевский долго рассказывает, что меч подарил ему глава столицы Дагестана, которого он называет близким другом. Имени он не сообщает, говорит лишь, что этот человек по меньшей мере когда-то был мэром Махачкалы. По данным *Moscow Times*, вероятнее всего, это Саид Амиров, четырежды избиравшийся мэр, который, как утверждается, пережил более пятнадцати покушений и парализован ниже пояса. В июле 2014 года российский суд признал Амирова виновным в подготовке террористического акта и приговорил к десяти годам в колонии строгого режима. Амирова также признали виновным в незаконном хранении оружия, поэтому довольно забавно, что он подарил Врублевскому меч.

«Оказалось, что главным типом среди тех, с кем я там был, был племянник мэра [столицы Дагестана] Махачкалы, - вспоминал Врублевский. - Этот мэр - самый взрываемый человек в мире. Этого мэра взрывали, блядь, раз тринадцать. Они его не убили, он в инвалидном кресле. Но однажды местные террористические группировки взорвали целый квартал, лишь бы попытаться его убить. Не одно здание, а весь квартал».

Врублевский уклоняется от прямых вопросов о том, зачем находился в этой неспокойной горной российской республике - преимущественно мусульманском регионе, граничащем с Грузией и отколовшимися районами Чечни. Но, вероятно, Врублевский проезжал через регион во время отдельной поездки из Баку, Азербайджан. Утёкшие письма ChronoPay показывают, что руководители несколько раз посещали Баку для поддержания отношений с Bank Standard, азербайджанским финансовым учреждением, обрабатывавшим огромные объёмы платежей за

мошеннические антивирусные программы ChronoPay и аптечные сайты Rx-Promotion.

Я меняю тему и спрашиваю Врублевского, удалось ли выяснить, кто слил внутренние документы ChronoPay.

Он отвечает: «Утечку устроили изнутри компании, из ИТ-отдела. Они поняли, что их поймают на краже денег. Поэтому сначала они нарушили работу [внутренней] системы учёта, отчего компромат стал бесполезен для правоохранительных органов, ведь у нас просто нет никакой базы бухгалтерского учёта. Её уничтожили до публикации компромата».

Я пододвигаю через стол к Врублевскому манильскую папку, полную распечатанных писем. «Что ж, кем бы ни был этот человек, он также отправил около 30 000 внутренних писем ChronoPay. Они входили в первоначальный пакет почты ChronoPay с начала 2009-го до середины 2010 года, который мне прислали».

Врублевский лениво перелистывает несколько страниц, пожимает плечами и толкает папку обратно через стол. «Я нисколько не удивлён».

Его неопределённость меня не останавливает. «Это очень богатая коллекция документов. Возможно, она покажется вам интересной. Там много компрометирующего и ничего особенно лестного ни для вас, ни для ChronoPay. Но, полагаю, большинство этих писем вы уже видели».

«Возможно. Там много „но“».

Я продолжаю: «С „но“ или без них, документы показывают, что вы совершенно не были со мной правдивы, Павел».

«Да? В чём?» - неопределённо спрашивает он.

«Во многом. Для начала помните мою первую статью о ChronoPay? Материал 2009 года о мошеннических антивирусах? Вы сказали, что не имеете никакого отношения к этой отрасли».

«Да, и в чём история?»

«Это вы мне скажите! Насколько я понимаю, история в том, что вы, ребята, создали целую киберпреступную отрасль и оплачивали для неё домены и обработку платежей».

«Да, и что? Я уже рассказывал вам об этом: так делают все обработчики платежей, и никто не может раскрыть это вам по очень простой причине. Это нарушает правила Visa и MasterCard. Visa и MasterCard знают, что так делают все, но по правилам это незаконно. Регистрация идентификаторов продавцов - часть предоставляемой вами услуги. Кроме того, вы оказываете связанную с ней поддержку клиентов».

Допивая кофе и закуривая ещё одну сигарету, Врублевский упоминает мою статью 2009 года в *Washington Post*, которая выявила многочисленные связи между ним, ChronoPay и отраслью мошеннических антивирусов.

Я не верил собственным ушам: Врублевский признал, что многие компании, которые ChronoPay якобы представляла как клиентов, на самом деле создали сотрудники ChronoPay и они же ими управляли.

«Вот в чём ваша ошибка. Во время, к которому относится ваша статья, мы не слишком хорошо разбирались в шпионских программах. Но отслеженная вами компания использовалась не только для них. Она использовалась для кучи всякого дерьма. Покопайтесь в Wirecard и Visa Iceland, и найдёте то же самое дерьмо. Причина в том, что при открытии идентификатора продавца его нужно зарегистрировать на компанию, а та должна выглядеть снаружи абсолютно надёжной: иметь законный сайт и так далее. Поэтому большинство поставщиков платёжных услуг, по существу, сами регистрируют компании и контролируют их изнутри».

Я возражаю: «Вы также никогда не говорили мне, что ChronoPay обрабатывала платежи Rx-Promotion...»

«Нет, вы правы. Не говорил».

«Но это правда, верно?»

«Да. Во всяком случае, раньше было правдой».[1]

Я был ошеломлён. «Что вы имеете в виду? Больше нет? С какого времени?»

«Друг мой, если бы я мог рассказать вам это, я был бы чертовски счастлив».

«И всё? В чём там дело, Павел? Вы знаете, что я проделал огромный путь и сильно рисковал собой, чтобы лично взять у вас интервью. Так вести себя совсем нехорошо». Я понимал, что рискую, бросая ему вызов, но мне были нужны ответы.

Снова рассмеявшись, он отвечает: «Мы отказались от них как от клиента. Всё очень просто».

«От Rx-Promotion? Когда?»

«В сентябре 2010 года. Значит, у меня было... полгода, блядь, чтобы принимать хорошие законные деловые решения».

Врублевский кому-то звонит и по-русски просит Веру принести нам ещё кофе.

Я продолжаю: «У людей, опубликовавших документы вашей компании, много сведений о её деятельности».

«Они крали деньги изнутри, очевидно, что сведения у них есть. Но с этим они ничего не добьются».

«Почему?»

«Понимаете, одного компромата недостаточно, чтобы кого-то поиметь. Нужно ещё иметь возможность что-то доказать, а для этого следует понимать, как всё работает. Люди, опубликовавшие сведения, совершили множество ошибок. Я распространяю информацию довольно осторожно. В основном можно увидеть, кто именно её распространял, не из самой информации, а из того, что её окружает. Вы знаете то, чего они не знают. По тому, что человек знает и чего не знает, можно довольно легко понять, кто это делал».

Красавица Вера, нервно улыбаясь нам обоим и каким-то образом почувствовав, что разговор стал напряжённее, осторожно входит в конференц-зал, ставит перед нами чашки кофе и быстро уходит. Ответ Врублевского приводит меня в замешательство, но я не хочу его перебивать. «Ладно, - говорю я. - Продолжайте».

«Брайан, есть ещё одна вещь, не совсем связанная с этим, которая меня удивляет».

«Какая, Павел?»

«Когда речь идёт обо мне... почему вы опять ожидаете, что я буду правдив? Напомните, пожалуйста».

Меня немного ошеломило, как ловко он направил разговор обратно на меня. «Считайте меня старомодным. Полагаю, задавая прямой вопрос, я ожидаю честного ответа».

«Ахахаха. Многие этого ожидают. Но, возвращаясь к теме, я не вижу в компромате ничего такого, что делало бы Rx-Promotion или большую часть прочего дерьма серьёзной проблемой. И я объясню почему: на самом деле я нарушаю не так уж много законов».

При этих словах я смеюсь так сильно и непроизвольно, что только что отпитый кофе едва не вылетает у меня из носа. Мне с трудом удаётся не облить костюм и стол конференц-зала. Мы оба от души смеёмся, и это помогает ослабить напряжение.

Тем не менее я видел, что эта линия вопросов не будет плодотворной. Поэтому попытался изменить подход и достал из портфеля несколько распечатанных писем ChronoPay.

«Я хочу узнать вашу реакцию на это внутреннее письмо ChronoPay, отправленное 16 марта 2010 года руководителем службы безопасности ChronoPay Владимиром Степковым с темой „Общий доход Rx-promotion2“. Оно, по-видимому, описывает ваше совместное владение Rx-Promotion с Юрием „Hellman“ Кабаенковым. Там сказано: „Парни, наш любимый Киселёв передал данные о стоимости технической поддержки. Павел и Hellman делят всё пополам, и...“»

Прерывая меня, Врублевский явно раздражается и больше не улыбается. «Стойте, стойте, Брайан, стойте, подождите! Я, блядь, понятия не имею, что здесь происходит! Я не могу особенно глубоко обсуждать разговоры между другими людьми и мной. Поэтому, пожалуйста, бросьте эту херню со страшными вопросами, и, возможно, лучше перейдём к нормальной беседе».

Несколько минут я молчу. Врублевский продолжает, снова усмехаясь и закуривая очередную Marlboro ещё до того, как погасла предыдущая. Я решаю, что неловкое молчание может заставить его рассказать больше. Но он не поддаётся.

«Я не стану глубоко погружаться в эту херню с Rx-Promotion, а вы сами многого не выясните. То же относится к шпионским программам. Я гораздо лучше исследую то, что касается Гусева. Как говорят полицейские, лучший способ что-то выяснить - когда человек сам это говорит. Я не хочу обсуждать эту тему. Но прежде я обещал дать вам правдивые ответы на некоторые вопросы. Разумеется, не на все, но на некоторые».

«Понятно. Что ж, окажите мне услугу, хорошо? Просто сообщите, когда захотите начать это делать».

Мы разговаривали более трёх часов, и на мои дополнительные прямые вопросы Врублевский давал столь же уклончивые и бессмысленные ответы. Обессилев, я наконец собрал вещи и поблагодарил его за уделённое время. На выходе Врублевский показал мне здание, где размещались офисы ChronoPay и которое, по его словам, представляло историческую ценность.

Когда мы спускались по лестнице в подземную автостоянку, он указал на дверь ровно одним этажом ниже входа в офис ChronoPay. На двери висела табличка «Российская ассоциация электронных коммуникаций». РАЭК - лоббистская организация, главному организатору которой, согласно утёкшим документам ChronoPay, компания ежемесячно платила зарплату. Та самая РАЭК играла ведущую роль в кампании по организации освещения западными СМИ уголовных обвинений против Гусева как «спамера номер один в России».

Через два дня я покинул Россию, отклонив ещё два приглашения Врублевского встретиться. Наша встреча раздражила и выбила меня из равновесия. Предыдущие восемь месяцев я слушал, как он лжёт мне по телефону на разные темы, но увидеть, как он столь нагло и открыто делает это мне в лицо, было крайне неприятно, и рядом с ним я чувствовал себя очень неуютно.

Я не ожидал от Врублевского многого, поэтому его отказ отвечать во время интервью не особенно меня удивил. Однако он подтвердил несколько важных сведений. ChronoPay была глубоко вовлечена не только в обработку платежей для компаний лжеантивирусов и аптечной партнёрки Rx-Promotion, но прежде всего в создание и развитие этих предприятий.

Самоуверенное заявление Врублевского о том, что он в действительности нарушает не так уж много законов, оказалось ошибочным. Через четыре месяца после нашей встречи российские федеральные следователи выдали ордер на его арест в связи с масштабной кибератакой на главного конкурента ChronoPay - российскую компанию обработки платежей Assist. Позднее Врублевского арестовали, судили, признали виновным и приговорили к двум с половиной годам в российской колонии. В мае 2014 года, проведя за решёткой едва год, он по необъяснимым причинам вышел на свободу.

Несмотря на разочарование после встречи с Врублевским, она помогла мне составить более полную картину этой мошеннической экосистемы, что всегда и было моей целью. К тому моменту я опросил десятки покупателей, поддерживавших существование проблемы спама, и разыскал некоторых самых печально известных спамеров мира. Пришло время двигаться дальше и погрузиться в окопы вместе с борцами со спамом на переднем крае этой непрекращающейся войны без границ.

Сноски

[1] [назад] Наконец мы чего-то добились. Признание Врублевского в том, что его компания действительно была тесно связана с Rx-Promotion, подтвердило очевидное из утёкших писем и таблиц ChronoPay за несколько лет. В одном из наших марафонских телефонных разговоров до моего визита в Москву Врублевский фактически признал подлинность утёкших документов и писем, когда неохотно согласился: даже российской ФСБ было бы трудно подделать столько документов, сколько опубликовали после взлома ChronoPay.

Глава 10. Борцы со спамом

Мало какие темы настолько предсказуемо приводят в ярость сообщество спамеров и киберпреступников, как разговоры об «анти» - так в подполье презрительно называют самодеятельных борцов со спамом, которые в одиночку или вместе с другими «анти» мешают работе либо ликвидируют крупномасштабные предприятия нежелательной почты, отравляющие нам жизнь. Утёкшие интернет-разговоры Ступина с сотнями массовых рассыльщиков, работавших на SpamIt, показывают: когда партнёры не занимались спамом, они использовали армии ботов, чтобы вывести из Интернета людей или системы, которые угрожали погубить их преступные предприятия. Очень часто конкурирующие спамеры обращали цифровое оружие друг против друга. Но любимой целью были «анти», в которых спамеры видели реальную и непосредственную угрозу своим бизнес-моделям, и вполне справедливо.

К третьему кварталу 2013 года почти 70 процентов всей ежедневно отправляемой электронной почты составляли незапрошенные массовые письма, передававшиеся через спамерские ботнеты. Чтобы вы могли оценить масштаб проблемы, злоумышленники вроде участников SpamIt и других спамерских партнёрок ежедневно рассылали, по оценкам, восемьдесят пять миллиардов нежелательных сообщений. По данным InternetWorldStats.com, в июне 2014 года Интернетом пользовалось более трёх миллиардов человек, а значит, спамеры ежедневно отправляли примерно по двадцать восемь нежелательных писем на каждого интернет-пользователя.

Некоторые методы борьбы со спамом исходили от независимых активистов, например участников InboxRevenge.com - форума, посвящённого разоблачению спамеров путём отправки регистраторам жалоб на спамерские домены и привлечения внимания к дружественным спамерам пуленепробиваемым хостинг-провайдерам. Одним из самых активных участников InboxRevenge был Адам Дрейк, тот самый борец со спамом, которому Врублевский первоначально слил базу SpamIt, чтобы навредить своему заклятому врагу Гусеву.

По иронии судьбы, чтобы ликвидировать деятельность спамеров, Дрейку и его весёлой банде самодеятельных борцов пришлось воспользоваться методами противника. Они создали ряд автоматизированных инструментов для одновременного размещения фиктивных заказов лекарств на десятках сайтов из спамерской рекламы. Эти программы набивки заказов в быстром темпе заказывали таблетки, используя вымышленные личности и данные кредитных карт. Замысел состоял в том, чтобы затопить базы партнёрок таким количеством мусора, что им придётся вручную проверять каждый заказ. Иногда программы набивки заказов замедляли аптечные сайты почти до полной остановки и мешали заинтересованным покупателям совершать покупки.

«Каждый день мы в среднем отправляли от 20 000 до 30 000 „заказов“ на их рекламируемые спамом домены», - вспоминал Дрейк об инициативе, начатой ими в 2007 году. В ответ спамерские партнёрки создавали всё более сложные системы выявления мошенничества, которые действовали во многом как ненавистные им спам-фильтры, но отсеивали фиктивные заказы. Эти системы «оценивали» вероятность поддельности каждого заказа, ища сочетание характеристик, указывавших на высокий риск. По словам Дрейка, в результате спамеры отклоняли или отменяли великое множество заказов настоящих покупателей. «Мы явно заставили их потерять деньги».

И действительно, система проверки заказов SpamIt и GlavMed постоянно отмечала красным даже слегка подозрительные покупки. Изучение утёкших журналов заказов покупателей этих родственных партнёрок показывает, что тысячи заказов задерживали или отклоняли при малейшем намёке на подделку. Например, многие отклонялись по следующей причине, сопровождавшей тысячи записей в системе обслуживания клиентов SpamIt:

«Этот заказ немного рискованнее, поскольку предоставленный пользователем телефонный номер находится не в том почтовом индексе, который указан в платёжном адресе кредитной карты».

По словам Вишневского, нашего «Вергилия» в подпольном мире спамеров и человека, помогавшего финансировать разработку спамерского ботнета Cutwail, меры по борьбе с мошенничеством также сдерживали спамеров-партнёров, которые пытались создавать поддельные продажи и комиссионные с помощью краденых кредитных карт. Такое мошенничество не только приносило комиссионные за фиктивные продажи, но в конечном счёте привлекало нежелательное внимание к системам обработки кредитных карт партнёрки. Тем грозили крупные штрафы, если количество возвратов платежей по кредитным картам превышало определённый порог, обычно 1 процент всех продаж.

Администраторы SpamIt также предпринимали сложные меры, чтобы группы и активисты по борьбе со спамом не могли с лёгкостью закрывать аптечные сайты из спамерской рекламы. Люди SpamIt использовали взломанные компьютеры, чтобы скрывать настоящее местонахождение сайтов, торговавших таблетками, применяя обходной метод, известный как fast-flux-хостинг. Этот метод - виртуальный эквивалент классического уличного мошенничества, известного как игра в три карты, - предполагает быстрое изменение местоположения сайта, чтобы ни один из адресов не использовался достаточно долго для его изоляции и закрытия.

При схеме fast-flux покупатель, переходящий по ссылке в спамерском письме, мог попасть на другой сайт или интернет-адрес, если снова нажимал на эту ссылку несколько секунд спустя. Потенциальные покупатели таких аптек не замечали никакой разницы, разве что небольшой задержки.

Кураторы SpamIt также пристально следили за расследователями мошенничества из MasterCard, Visa и крупнейших фармацевтических компаний. База данных SpamIt показывает, что они регулярно добавляли интернет-адреса и адреса электронной почты этих расследователей в базу клиентов, которым запрещалось размещать заказы на аптечных сайтах.

Ботмастеры вроде Gugle и Cosma усердно добивались максимальной доставляемости своих писем во входящие и постоянно меняли подходы, чтобы обходить новые средства защиты, добавлявшиеся в антиспамовое программное и аппаратное обеспечение. Этот поток спама стал настолько подавляющим, что многим специалистам по сетевой безопасности, отвечавшим за защиту корпоративных сетей, пришлось дополнять аппаратные и программные средства борьбы со спамом спамерскими «чёрными списками» (их также называют «списками блокировки»).

В самом простом виде чёрный список спама - это перечень диапазонов интернет-адресов, которые чаще всего замечают как источники спама. Как правило, попадающие в чёрные списки интернет-адреса относятся к одной из двух категорий: либо они находятся в сетях и у интернет-провайдеров (ISP), заслуживших репутацию тех, кто закрывает глаза на спамеров в своих сетях, - таких как Atrivo и McColo Corp., - либо это отдельные заражённые вредоносными программами компьютеры-«зомби», извергающие спам.

Самыми распространёнными чёрными списками управляли ситуативно сформированные и скрытные организации с забавными названиями, например Spamhaus, SURBL и URIBL (буквы BL в этих аббревиатурах означают «blacklist», то есть «чёрный список»). Компании, пытавшиеся защитить от спама десятки тысяч сотрудников, обычно встраивали эти чёрные списки в спам-фильтры, блокируя доставку писем с любого из перечисленных интернет-адресов. Нередко невиновные сети, не занимавшиеся спамом, попадали в эти чёрные списки вместе со злоумышленниками. Но большинство организаций охотно мирились с тем, что часть законных писем не дойдёт, если это позволяло сдержать растущий ежедневный поток нежелательных сообщений.

Сообщество спамеров, со своей стороны, вовсе не забавляли эти самоназначенные хранители входящих, и оно настаивало, что «анти» не имеют права решать, какие письма интернет-пользователи должны или не должны получать. В 2011 году копия Spamdot.biz, чрезвычайно закрытого форума, который посещало большинство ведущих спамеров мира, стала

доступна нескольким правоохранительным органам и автору этой книги. Публикации на форуме показывают, что ещё в 2005 году спамеры начали организовывать и проводить крупномасштабные интернет-атаки, призванные наказать и запугать активистов, боровшихся со спамом.

Одной из самых разрушительных и яростных кампаний такого рода стала одна из крупнейших кибератак в истории Интернета, обрушенная на чрезвычайно эффективный антиспамовый стартап Blue Security Inc. Компания придумала изящный способ остановить спам, предназначенный более чем полумиллиону пользователей её программы Blue Frog. Программа просто отправляла ответ в сеть отправителя с просьбой к спамеру прекратить рассылку нежелательной почты её пользователям.

Но поскольку подобные просьбы обычно игнорировали, Blue Security перешла на следующий уровень. Она одновременно обрушивала на спамеров запросы от всех 522 000 своих клиентов. Это создавало столь мощный поток интернет-трафика, что мешало спамерам отправлять письма другим получателям, - парализующий эффект, из-за которого несколько известных спамеров подчинились требованиям.

Однако вскоре ключевые участники спамерского подполья заявили, что с них хватит и Blue Security пора стереть с лица Интернета. Согласно длинной ветке обсуждения на Spamdot.biz, не менее дюжины ведущих спамеров потратили несколько недель и более $15 000, собирая силы для полномасштабной внезапной атаки на клиентов Blue Security.

Участники Spamdot обнаружили, что программа Blue Frog содержала критическую слабость: спамерам, желавшим выполнить требования Blue Frog об удалении адресов, бесплатно предоставлялся инструмент, позволявший очистить их списки от адресов электронной почты пользователей Blue Frog. Хотя Blue Security тщательно шифровала адреса пользователей, включённые в этот инструмент, спамеры могли без труда определить, какие адреса в их списках рассылки принадлежали пользователям Blue Frog. Спамеру требовалось лишь сравнить исходные списки адресов для спама со списками, очищенными инструментом Blue Security. Все адреса, отсутствовавшие в очищенных списках рассылки спамера, принадлежали пользователям Blue Security.

Атака на Blue Security началась с письма с угрозами, отправленного большинству из 522 000 пользователей Blue Frog. Приведённое ниже сообщение выложили для проверки, а затем несколько участников форума Spamdot отредактировали его, прежде чем оно было разослано сообществу Blue Frog:

> Вы получили это письмо, потому что пользуетесь широко известной программой Blue Security «Blue Frog».
>
> Сегодня база данных Blue Security стала известна худшим спамерам всего мира. В течение 48 часов база будет опубликована в Интернете, и ваш адрес электронной почты окажется открыт для них всех. После этого количество спама, поступающего в ваш почтовый ящик, увеличится в 10-20 раз.
>
> Blue Security незаконно атаковала компании, занимающиеся маркетингом по электронной почте, и делала это с вашей помощью. Целями и жертвами стали многие сайты, в том числе не имеющие отношения к спаму. Программа Blue Security была полностью проанализирована и содержит множество вредоносных программных компонентов. Среди них: возможность массово рассылать письма пользователям; возможность атаковать сайты с помощью распределённых атак отказа в обслуживании (DDoS); возможность открывать потайные двери на любом компьютере, где она работает; а также скрытая функция автоматического обновления кода, которая может установить на ваш компьютер что угодно и открыть к нему доступ кому угодно.

> Blue Security указывает в качестве места ведения бизнеса адрес в США, хотя её главный офис находится в Тель-Авиве. Blue Security управляют несколько родившихся в России евреев, которые прежде сами занимались спамом. Когда всё будет кончено, они смогут сбежать, спрятаться и сменить личности, оставив вас расплачиваться. ВЫ НЕ МОЖЕТЕ УЧАСТВОВАТЬ В НЕЗАКОННОЙ ДЕЯТЕЛЬНОСТИ и надеяться, что вам это сойдёт с рук. Это письмо гарантирует, что вы прекрасно осведомлены о ситуации. Вскоре вас признают виновными в компьютерных преступлениях, таких как DDoS-атаки на сайты, преступный сговор и массовая рассылка незапрошенных сообщений обо всём - от виагры до порнографии, - если вы продолжите пользоваться Blue Frog.
>
> Они не берут денег за скачивание своей программы, не берут денег за удаление адресов из своих списков, и у них нет видимого источника дохода. Зато у них ЕСТЬ 500 000 компьютеров, которые сидят и ждут следующей команды. Что они делают сейчас?
>
> 1. Используют ваш компьютер для рассылки спама?
>
> 2. Используют ваш компьютер для атаки на сайты конкурентов?
>
> 3. Выуживают из ваших файлов сведения о вашей личности и банковские данные?
>
> Если вы думаете, что можете просто сменить адрес электронной почты и оставаться в безопасности, продолжая пользоваться Blue Frog, вас ждёт большой сюрприз. Это только начало...

Необычайно активный участник форума Spamdot, взявший псевдоним BoT, изложил коварный план атаки на Blue Security, которая должна была обратить собственную антиспамовую службу компании против её пользователей. Стратегия была простой и изящной. Спамеры собирались зарегистрировать десятки доменных имён, каждое из которых перенаправляло бы посетителей на единственный сайт под их контролем. Затем злоумышленники должны были разослать спам всей базе пользователей Blue Security и отойти в сторону, ожидая неизбежной волны запросов на отписку. Когда запросы на удаление из рассылки хлынули бы обратно на этот единственный сайт, спамеры просто изменили бы его настройки так, чтобы весь входящий трафик перенаправлялся на главную страницу Blue Security, фактически заставив собственную антиспамовую технологию компании атаковать саму себя.

«Так их либо оттрахают в задницу их же собственным оружием, либо на них посыплются жалобы на злоупотребления, - объяснял BoT в публикации на форуме Spamdot непосредственно перед атакой. - Ещё лучше было бы перенаправить трафик на сайты CNN, BBC, Reuters и тому подобные, и тогда эти сайты начнут писать, что из-за „синих лягушат“ Интернет превратился в поле боя».

1 мая 2006 года спамерское сообщество обрушило на интернет-серверы Blue Security серию всё более мощных атак, немедленно лишив законных пользователей доступа к сайту компании. В Blue Security ещё не знали, что стали мишенью, но руководители компании видели, что клиентам трудно попасть на её сайт. В какой-то момент было решено перенаправить трафик, предназначенный для недоступной главной страницы, в корпоративный блог, где разместили сообщение для пользователей Blue Frog с признанием проблемы.

Блог Blue Security находился на блог-платформе компании Six Apart Ltd. из Сан-Франциско, обслуживавшей миллионы сайтов через сервис TypePad. (Позже Six Apart купит российский блог-гигант LiveJournal.ru.) В результате перенаправления основной удар атаки принял на себя блог-сервис Six Apart, и тысячи размещённых там блогов тоже перестали работать. Атака отказа в обслуживании также примерно на двенадцать часов остановила работу Tucows Inc., торонтской интернет-компании, помогавшей управлять сайтом Blue Security. Генеральный директор Tucows Эллиот Носс назвал эту атаку «несравненно крупнейшей из всех, которые когда-либо видела компания», и сказал, что инфраструктура, способная выдержать такой натиск, а тем более более мощный, есть лишь у считаных компаний.

«Эта атака и правда была похожа на попытку убить комара атомной бомбой», - сказал Носс.

Вскоре после этого генеральный директор Blue Security Эран Решеф получил письмо от одного из спамеров, прежде согласившихся прекратить рассылать спам пользователям Blue Security: тот сообщил, как связаться с человеком, руководившим атакой.

В сообщении была ссылка на аптечный сайт, который в то время продвигали спамеры, и указание Решефу просмотреть исходный HTML-код страницы. В нём он должен был найти номер ICQ. ICQ, или I-Seek-You, - технология мгновенного обмена сообщениями, в то время чрезвычайно популярная в сообществе киберпреступников.

Команда Blue Security скачала копию главной страницы аптечного сайта, а затем открыла её в HTML-редакторе, чтобы убедиться, что там нет ловушки с вредоносным кодом. После этого они нашли скрытое сообщение: «preved, stuchis v asku 299650295», то есть «привет, стучись в аську 299650295».

Вскоре после того, как Решеф отправил запрос на чат на этот номер ICQ, ему ответил человек под именем Pharmamaster. Pharmamaster издевался над собеседником и совершенно не собирался торговаться.

> Вторник, 2 мая 2006 года, 16:30:57
>
> [16:02] BLUESECURITY: Вы хотите сейчас обсудить мирное урегулирование сложившейся ситуации? Нам известны ваши опасения, но, как я уже говорил, вопреки тому, что вы думаете, мы не хотим влиять на ваш бизнес. Мы не обычная антиспамовая компания.
>
> [16:07] PHARMAMASTER: Вы начали со мной, с моими людьми и моими сотрудниками, так что сначала пострадаете и почувствуете, кто мы такие. А когда я удостоверюсь, что до вас дошло, кто мы, тогда сможем поговорить. Bluesecurity.com сейчас не работает, но как насчёт того, чтобы мы не давали всем вашим системам работать несколько месяцев?

Решеф отказался от интервью о подробностях атаки. Но источник, помогавший компании противостоять натиску, сказал, что Решеф также получал угрозы в адрес своей семьи.

«Атака достигла такого страшного уровня, что я помню совещание с Эраном и остальными ребятами, - сказал источник на условиях анонимности. - Кроме того, шла личная атака: Эрану присылали фотографии его детей на игровой площадке - снимки, которых он прежде никогда не видел».

Атаки продолжались более двух недель, набирая силу. В какой-то момент нападавшие начали писать сотрудникам Blue Security, утверждая, что у них есть 70 процентов базы электронных адресов пользователей Blue Frog, и предлагая $50 000 за оставшиеся 30 процентов любому сотруднику, готовому передать внутренние данные компании.

14 мая руководство Blue Security встретилось с ФБР, чтобы обсудить возможные варианты, но это было скорее формальностью. Два дня спустя Решеф и Blue Security подняли белый флаг. 17 мая *The Washington Post* опубликовала на первой полосе статью автора этой книги, где сообщалось, что компания признала поражение. Blue Security получила более $4 миллионов венчурного финансирования, но её благодетели решили, что пора сдаться.

В той статье цитировался Тодд Андервуд, в то время директор по эксплуатации и безопасности Renesys Corp., компании, отслеживающей подключение к Интернету. Андервуд назвал атаку «неудивительной, но печальной».

«Когда основатели компании впервые обратились к более широкому антиспамовому сообществу и спросили, что оно думает о бизнес-модели Blue Security, все сказали, что это ужасная идея и в конце концов они нанесут большой сопутствующий ущерб, - сказал Андервуд. - Но это также крайне прискорбно, потому что показывает, насколько сильно спамеры побеждают в этой битве».

Люди, отвечавшие за организацию атаки на Blue Security, по всей видимости, были руководителями одной из крупнейших в то время аптечных партнёрок. Многие планы атаки на Blue Security, изложенные на Spamdot.biz, формировались и поощрялись влиятельным пользователем Spamdot.biz, взявшим псевдоним Mr. Green. По данным Spamhaus, псевдонимом Mr. Green пользовался россиянин Влад Хохолков, уроженец Москвы, предположительно сотрудничавший с печально известным спамером Лео Куваевым.

Атака на Blue Security стала предупредительным выстрелом для борцов со спамом повсюду. В то время почти 90 процентов всей электронной почты составляла нежелательная реклама, и Blue Security затронула глубинное раздражение пользователей, которым осточертел ежедневный потоп. Но ведущие участники Spamdot управляли аптечными партнёрками, приносившими миллионы долларов в месяц, и видели в Blue Security авангард нового вида антиспамовой деятельности, представлявшей серьёзную угрозу дальнейшему успеху их денежных машин. Они не собирались позволять оттеснить себя в сторону, чего бы это ни стоило.

Spamhaus считает, что Куваев и Хохолков управляли аптечными партнёрскими программами Mailien и Rx-Partners. Это подтверждается утёкшей перепиской администратора SpamIt Дмитрия Ступина в системе мгновенных сообщений. В разговоре 2008 года между Ступиным и Joop - таков был псевдоним россиянина, одного из самых высокооплачиваемых партнёров GlavMed, - они обсуждают конкурирующую партнёрскую программу под названием Affiliate Connection.

«Если не секрет, ты знаешь Леонида Куваева и Влада Хохолкова (Mr. Green)?» Когда Ступин замешкался с ответом, Joop извинился и сменил тему. «Я беру свой вопрос обратно. Что-то у меня с головой. Забыл, что их партнёркой [была] Rx-Partners/Stimulcash».

Гражданина России Куваева в 2003 году признали в Массачусетсе виновным в нарушении американских законов против спама и обязали выплатить $37 миллионов за массовую рассылку через ботнет спама, рекламировавшего поддельные копии Microsoft Windows и другого программного обеспечения известных марок. Сообщалось, что после этого он бежал из страны, избежав тюремного срока. Но в какой-то момент после приговора Куваев вернулся в Россию.

Однако в конечном счёте последней посмеялась Microsoft. Софтверный гигант заплатил консультантам из российской компании Group-IB, занимающейся компьютерной криминалистикой, за наблюдение за деятельностью Куваева и передачу сведений российским правоохранительным органам.

В 2011 году Куваева арестовали по обвинению в сексуальном насилии над детьми. Сейчас он находится в российской тюрьме. Полиция провела обыск в доме Куваева после сообщения о том, что он вступал в сексуальные отношения с несовершеннолетними девочками. В его жилище нашли многочасовые видеозаписи, показывавшие, как он насиловал девочек - некоторым было всего четырнадцать лет, - заманенных из расположенного неподалёку московского детского дома. В 2012 году Куваева судили и признали виновным в сексуальном насилии над детьми; сейчас он отбывает двадцатилетний тюремный срок (по данным российского еженедельника MKRU, недавно сокращённый до десяти лет).

Отвечая по электронной почте, Хохолков отрицал свою причастность к атаке на Blue Security. Кто именно отвечал за организацию атаки, остаётся неясным, но утёкшая переписка SpamIt и обсуждения на форуме ясно показывают, что Влад и Лео работали как партнёры и что спамерская группировка Куваева принимала активное участие.

Вскоре после атаки на Blue Security Mr. Green попросил администраторов форума Spamdot удалить все его публикации и данные учётной записи. Но некоторые сообщения с форума сохранились в виде цитат в обсуждениях между другими участниками Spamdot. Они указывают, что Mr. Green тесно сотрудничал при проведении атаки с человеком, называвшим себя сатанистом и использовавшим псевдоним Zliden и адрес электронной почты domains@locu.st. По данным

Spamhaus, это был последний известный адрес электронной почты Лео Куваева.

Куваева многие считают одним из самых откровенных и нераскаявшихся спамеров, когда-либо работавших в этом бизнесе. Но, подобно другим мастерам массовой рассылки, он старался отделять свои многочисленные сетевые личности от своего существования вне Сети, меняя адреса электронной почты и псевдонимы и время от времени удаляя старые публикации, чтобы ускользнуть от расследователей цифровых преступлений и активистов, боровшихся со спамом.

И всё же опыт Куваева (как и его современников вроде Cosma и Nechvolod) показывает: хотя Интернет порой теряет след сетевых личностей, у активистов в области борьбы со спамом и интернет-безопасности память куда длиннее, и они готовы пойти на многое, чтобы привлечь спамеров к ответственности.

DDoS против Spamhaus

Обитатели Spamdot.biz также спланировали и провели несколько мощных атак на Spamhaus, а также на широко используемые чёрные списки спама, которые вели URIBL и SURBL. В сообщении другим участникам в октябре 2008 года администратор Spamdot под псевдонимом Ika опубликовал на форуме заметку, чтобы сообщить группе о ходе сбора денег со спамеров для продолжительной распределённой атаки отказа в обслуживании (DDoS) на сайты всех трёх поставщиков чёрных списков.

В сообщении, в частности, говорилось:

> Уважаемые господа!
>
> Мы собрали в фонд более $3 000, часть которых будет направлена на первые четыре дня DDoS против URIBL и Spamhaus. Мы также купили установку ботов на $1 000 по цене $25 за 1 000 ботов.
>
> Текущие цели DDoS: 1) инфраструктура lists.uribl.com; 2) домашние предприятия [основателя Spamhaus Стива] Линфорда - uxn.com и ultradesign.com, где хранится резервная база данных Spamhaus; 3) оба интерфейса spamhaus.org.

Представитель партнёрки интернет-аптек Affiliate Connection сказал, что его спамеры могут объединить несколько миллионов взломанных компьютеров для масштабной атаки на Spamhaus. Но он отметил, что альтернативные издержки такого нападения будут высоки, поскольку компании, противодействующие злоупотреблениям, быстро выявят и внесут в чёрные списки все дальнейшие сообщения от спамерских зомби, включая будущий спам, приносящий деньги. Более того, сказал руководитель Affiliate Connection, URIBL и SURBL недавно приобрели услуги защиты от отказа в обслуживании у ведущего поставщика средств противодействия DDoS.

Администраторы SpamIt ответили, что этих факторов едва ли достаточно, чтобы заставить их отказаться от планов.

«Ну что же, если они сидят на мощных анти-DDoS-каналах, нам придётся действовать сильно и решительно, чтобы забить их каналы, - заявил Ika. - Им придётся отвечать за огромные объёмы трафика, и это станет для них настоящей проблемой. Это будет дорого, но, думаю, некоторые партнёры могут выделять на это по несколько сотен баксов в день».

Несколько недель спустя ветка Spamdot.biz о планах атаки на Spamhaus разрослась на несколько страниц разговоров, но действий почти не было. Испытывая отвращение к своим коллегам, GeRa - партнёр SpamIt и Rx-Promotion, управлявший спамерским ботнетом Grum, - призвал других спамеров активизироваться и пойти на жертвы ради блага отрасли.

> Я обращаюсь к крупнейшим спамерам: вы, ребята, получающие от $50 000 до $200 000 комиссионных в месяц, неужели не сможете найти $3 000, чтобы решить эту проблему?

Docent, куратор спамерского ботнета Mega-D, ответил, что он и его команда готовы предоставить финансирование для поддержки продолжительной атаки на Spamhaus. Но вскоре обсуждение застопорилось на вопросе о том, кто возьмёт на себя ответственность за руководство и организацию атаки.

Ситуацию осложняло то, что не все на спамерском форуме поддерживали атаку на Spamhaus и других поставщиков чёрных списков. Severa, ботмастер, создавший спамерские ботнеты Waledac и Storm и управлявший ими, рассуждал более философски, замечая, что «Spamhaus - лишь часть [огромного] эволюционного процесса» и что спам-фильтры на самом деле помогали отделять начинающих спамеров от профессионалов и отбивали у неопытных потенциальных спамеров желание осваивать это ремесло.

«Ребята, мы больше НЕ МОЖЕМ жить без антиспамовых фильтров», - рассуждал Severa в ответе в обсуждении на Spamdot. Выступая за дальнейшее широкое использование спам-фильтров, Severa, должно быть, звучал для многих коллег почти как еретик. Но этот спамерский король, по всей вероятности, верно определил неопытных спамеров как бедствие для отрасли и обузу для собственной прибыли. Если спам-фильтры главным образом успешно удерживали мелюзгу на расстоянии, значит, так тому и быть.

«Действительно, они останавливают новичков и ламеров. Представьте, что сейчас отключили бы все фильтры. Вы бы зарабатывали деньги? НЕТ! Это просто убило бы электронную почту как средство связи, и больше ничего. Поэтому Spamhaus не хороший и не плохой; Spamhaus - это просто Spamhaus».

Участник Spamdot по имени Swank сказал, что согласен с общим утверждением Severa, но Spamhaus всё же нужно проучить.

«Severa, ты высказал отличную мысль и совершенно прав, - написал Swank. - Наличие антиспамовых фильтров и прочего полезно для технологий и Интернета, потому что обе стороны - спамеры и борцы со спамом - постоянно приспосабливаются и всё меняют, чтобы обойти последние меры друг друга. В итоге технологии непрерывно совершенствуются, что, как ты и сказал, также позволяет профессионалам продолжать работу и не пускает новичков в бизнес. При этом глупые компании вроде Spamhaus несправедливы к рассыльщикам, которые соблюдают правила. Spamhaus злоупотребляет своими полномочиями, чтобы уничтожать ЛЮБОГО, кто занимается маркетингом по электронной почте, независимо от того, соблюдает этот человек правила или нет. Spamhaus ненавидит всех специалистов по почтовому маркетингу. Эта хрень - полное дерьмо, и это несправедливо по отношению ко всем. Spamhaus должен понять, что он не неуязвим, и скоро он это поймёт».

В октябре 2008 года GeRa объявил участникам Spamdot, что выпускает автоматизированный инструмент атаки, созданный его программистами, чтобы помочь сообществу участвовать в массовом нападении на Spamhaus. Инструмент, который он назвал Anti-Haus v. 1.0, распространили среди владельцев крупных ботнетов, а те установили программу на десятки тысяч контролируемых ими взломанных компьютеров, уже использовавшихся для пересылки спама.

Представитель Spamhaus, назвавшийся лишь Barry, сказал, что организация не помнит конкретно эту атаку октября 2008 года, отметив, что за прошедшие годы Spamhaus потерял счёт числу обрушившихся на него масштабных атак.

В марте 2013 года Spamhaus подвергся атаке, которую ему предстояло запомнить надолго. Более того, некоторые эксперты назвали её крупнейшей скоординированной кибератакой, которую когда-либо видел Интернет. Группа пуленепробиваемых хостинг-провайдеров, объединившихся под знаменем Stophaus, решила атаковать поставщика антиспамовых услуг. Stophaus создала

интернет-форум для координации нападения после того, как Spamhaus внёс в список блокировки одного конкретного пуленепробиваемого хостинг-провайдера - сеть, известную как CB3ROB, или Cyberbunker, поскольку она работала из сильно укреплённого бункера НАТО в Нидерландах.

Связанные со Stophaus нападавшие начали девятидневную цифровую осаду, обрушивавшую на сайт организации до 300 миллиардов бит данных в секунду. Как описывала *The New York Times*, направленный на Spamhaus «пожарный шланг» данных не просто затопил поставщика антиспамовых услуг: поток перелился в соседние сети, из-за чего, по оценке обслуживавшей организацию сети доставки контента CloudFlare, сотни миллионов людей столкнулись в Сети с задержками и сообщениями об ошибках.

Когда связанные со Stophaus нападавшие решили, что не смогут вывести из строя CloudFlare, нанятую Spamhaus для защиты от DDoS-атак, они начали бить по «точкам пиринга», где интернет-сети обмениваются трафиком, включая точки обмена интернет-трафиком в Лондоне, Амстердаме, Франкфурте и Гонконге.

The New York Times сообщала, что позднее власти Испании арестовали Свена Олафа Камфёйса, тридцатипятилетнего голландца, которого считали ответственным за координацию беспрецедентной атаки на Spamhaus. По данным Spamhaus и сообщений СМИ, Камфёйс утверждал, что представляет собственную независимую страну - Республику Cyberbunker. *The Guardian* сообщала, что Камфёйс был экстрадирован в Нидерланды, однако признаков того, что там его преследуют за преступления, нет. Камфёйс отрицал причастность к атаке и говорил, что лишь выступал контактным лицом для прессы от CB3ROB/Cyberbunker. Тем временем в ноябре 2014 года семнадцатилетний юноша признал в Великобритании вину в участии в беспрецедентной атаке на SpamHaus.

Нападение Stophaus стало самым громким и свежим напоминанием о том, что такое оружие массового нарушения работы сегодня легко и бесплатно доступно любому человеку или организации, решившим им воспользоваться. Атака, поразившая Spamhaus, известная как атака отражения и усиления DNS, задействовала неуправляемые серверы системы доменных имён (DNS) в Сети, чтобы создавать огромные потоки трафика, предназначенные для запугивания целей и принуждения их к молчанию.

Чтобы понять значение этого, приведём немного предыстории. DNS-серверы действуют как телефонный справочник Интернета, преобразуя, или «разрешая», удобные для людей доменные имена вроде example.com в числовые сетевые адреса, используемые компьютерами. Обычно DNS-серверы обслуживают только машины внутри доверенного домена, в данном случае example.com. Но атаки отражения DNS опираются на бытовые и корпоративные интернет-маршрутизаторы, настроенные принимать запросы из любой точки Сети. Нападавшие могут отправлять поддельные DNS-запросы на эти так называемые «открытые рекурсивные» DNS-серверы, фальсифицируя запрос так, будто он исходит из сети цели. Поэтому, отвечая, DNS-серверы направляют ответ на поддельный адрес, то есть адресу цели.

Усиливающая часть атаки использует возможность составить DNS-запросы так, чтобы ответы были намного больше запросов. Для этого задействуется расширение стандарта DNS, позволяющее передавать крупные DNS-сообщения. Например, нападавший может составить DNS-запрос размером менее 100 байт, вызывающий ответ в шестьдесят-семьдесят раз больше. Эффект усиления особенно заметен, если преступники одновременно обращаются с такими поддельными запросами к десяткам DNS-серверов.

Хорошая новость состоит в том, что специалисты по Интернету и безопасности давно понимают, как блокировать эти необычайно мощные атаки. «И действительно, ряд специалистов по компьютерной безопасности указал, что атаки были бы невозможны, если бы крупнейшие интернет-компании мира просто проверяли, действительно ли исходящие пакеты данных отправлены их клиентами, а не ботнетами», - писали Джон Маркофф и Николь Перлрот из *The New*

York Times.

Плохая новость состоит в том, что с тех пор, как эти сверхмощные атаки впервые появились более десяти лет назад, изменилось мало, сказал Родни Джоффе, старший вице-президент и старший технолог компании безопасности Neustar, которая также помогает клиентам выдерживать огромные интернет-атаки. По оценке Джоффе, существует приблизительно двадцать пять миллионов неправильно настроенных или устаревших домашних и корпоративных маршрутизаторов, которыми можно злоупотребить в таких цифровых осадах. В основном это домашние маршрутизаторы, предоставленные интернет-провайдерами, или неправильно настроенные корпоративные маршрутизаторы, однако очень многие устройства находятся у интернет-провайдеров в развивающихся странах либо у провайдеров, которые не видят экономической выгоды в том, чтобы тратить деньги ради общего блага Интернета.

«Почти во всех случаях это параметр, который может настроить интернет-провайдер, но нужно заставить провайдера это сделать, - сказал Джоффе. - Многие из этих провайдеров работают с очень низкой маржой и не заинтересованы проходить весь процесс защиты своих конечных пользователей - или, если уж на то пошло, остальных пользователей Интернета».

И именно в этом заключается проблема. Ещё недавно спамеру или хакеру, желавшему начать масштабную интернет-атаку, приходилось собирать огромный ботнет, включавший легионы взломанных компьютеров. Сегодня такому нападающему уже не нужно создавать столь громадную армию ботов. По словам Джоффе, вооружившись всего несколькими сотнями заражённых ботами компьютеров, современные нападавшие могут вывести из строя почти любую цель в Интернете благодаря миллионам неправильно настроенных интернет-маршрутизаторов, которые в любой момент готовы быть мобилизованы для атаки.

«Если плохие парни начнут атаку, они могут сначала злоупотребить 20 000 таких неправильно настроенных серверов, а если цель всё ещё работает и остаётся в Сети, увеличат число до 50 000, - сказал Джоффе. - В большинстве случаев, чтобы отключить более крупные сайты, им достаточно дойти лишь до 100 000, но всего таких доступных серверов двадцать пять миллионов».

Глава 11. Ликвидация

Через девять месяцев после моего круиза-ледокола во время поездки в Россию на встречу с Врублевским я снова смотрел на звёздное ночное небо, стоя на палубе другого большого корабля в чужой стране. На этот раз я находился на верхней палубе стареющего круизного лайнера, пришвартованного в гавани в центре Роттердама.

За покрытыми инеем окнами-иллюминаторами биг-бенд играл на приёме для участников конференции по кибербезопасности GovCert, где ранее в тот день я выступил с докладом о войне за территорию между Гусевым и Врублевским. Вечер был пронизывающе морозным и ветреным, а я ждал, когда меня представят следователям из российской Федеральной службы безопасности (ФСБ). Несколько сотрудников ФСБ, посетивших конференцию, сказали нашим голландским хозяевам, что хотят встретиться со мной, но только в приватной обстановке.

Мои руки замёрзли настолько, что я больше не мог удерживать бокал пива, покрывавшийся льдом. Я поставил бокал на выступ и в то же мгновение услышал, как за моей спиной распахнулась толстая стальная дверь, громко скрипнув петлями. Выйдя в ночной воздух, женщина с конференции подошла ко мне, официально представила троих следовавших за ней мужчин, а затем поспешила обратно, в тепло приёма.

Коренастый мужчина средних лет, представленный старшим офицером ФСБ, говорил по-русски, а молодой джентльмен переводил на английский между затяжками сигареты Marlboro. Они спросили, знаю ли я что-нибудь о московской компании под названием Onelia. Я ответил, что нет, попросил произнести название по буквам и поинтересовался, почему их интересует эта фирма. Высокопоставленный сотрудник ФСБ сказал, что они считают компанию глубоко вовлечённой в обработку платежей для различных организованных киберпреступных предприятий.

Позднее тем же вечером, вернувшись в гостиничный номер, я поискал в Интернете сведения о компании, но ничего не нашёл. Я подумал, не спросить ли у некоторых из лучших своих источников в России, что им известно об Onelia. Но внутренний голос предупредил меня: возможно, сотрудники ФСБ как раз и надеялись, что я это сделаю. Они смогли бы определить, кто мои источники, когда те начали бы наводить справки о загадочной и, вероятно, вымышленной фирме Onelia.

Моя паранойя взяла верх, и я отложил эти сведения в сторону. Так продолжалось до тех пор, пока несколько месяцев спустя я не обнаружил, что Onelia (как оказалось, чаще это название пишут Oneliya) - название общества с ограниченной ответственностью, стоявшего за Gateline.net, процессинговой компанией по кредитным картам, которая обрабатывала десятки тысяч покупательских транзакций для SpamIt и Rx-Promotion.

На Gateline.net говорится, что услугами компании пользуются фирмы из разных отраслей, включая туризм, продажу авиабилетов, мобильные телефоны и виртуальные валюты. Но, согласно платёжным и партнёрским записям, утёкшим как из SpamIt, так и из Rx-Promotion, Gateline также прежде обрабатывала большинство покупок на сайтах мошеннических аптек, которые продвигали спамеры, работавшие на эти две программы.

Связь Gateline со спамерскими программами подтверждается журналами чатов, изъятыми в 2011 году российскими следователями, расследовавшими деятельность SpamIt. Эти журналы содержат сотни разговоров между совладельцем SpamIt Дмитрием Ступиным, известным как SaintD, и администратором Gateline Николаем Викторовичем Ильиным, который использовал псевдоним Shaman (shaman@gateline.net) и которого называли Nikolai или уменьшительным именем Kolya. В журналах насчитывается более 205 разговоров между Shaman и Ступиным с 2007 по 2010 год.

Утёкшие чаты Ступина позволяют предположить, что Shaman имел огромное влияние на повседневную работу SpamIt. У спонсора аптечного спама были большие трудности с

предоставлением покупателям возможности платить картами MasterCard, главным образом потому, что MasterCard, по всей видимости, гораздо бдительнее Visa следила за использованием своих услуг мошенническими интернет-аптеками. Платёжные записи SpamIt указывают, что Shaman получал значительную долю, около 8 процентов, со всех продаж, обработанных аптеками SpamIt, и порой зарабатывал за свои услуги десятки тысяч долларов в неделю.

В следующем чате между Shaman и Ступиным, записанном 23 ноября 2009 года, Shaman отчитывает Ступина за недостаточное внимание к транзакциям, которые они считали контрольными покупками, совершёнными расследователями мошенничества из MasterCard. В начале чата Shaman публикует ссылку на статью об уголовном деле, возбуждённом российскими следователями против SpamIt и партнёра Ступина Игоря Гусева.

SHAMAN: runewsweek.ru

СТУПИН: Ага, ага.

SHAMAN: Я бы посоветовал вам не слишком рекламировать (пиарить) банки.

СТУПИН: Нам это меньше всего нужно.

SHAMAN: Иначе весь бизнес рухнет. Что-то подобное уже было.

СТУПИН: Игорь пытается удалить эти публикации.

SHAMAN: Хорошо. Что там с информационными войнами? Надо как-то это остановить. Вы уничтожите весь бизнес.

СТУПИН: Мы??? От нас не было ни одной публикации. Игорь всё время их удаляет. Больше мы ничего не делаем.

SHAMAN: Перестаньте отвечать ему в публикациях на форуме, и RedEye успокоится.

СТУПИН: Я спрошу Игоря, отвечал ли он. Если отвечал, попрошу его перестать это делать.

SHAMAN: [Указывая адрес электронной почты, который, по всей видимости, принадлежал расследователю мошенничества из MasterCard] Уберите этого мудака - он сотрудник MasterCard. Он совершил покупку. iacva.org

SHAMAN: Будьте внимательнее с партией. Уберите и этих: Charles Wilson, Stephen Carpenter, Fredric Manger, Sandro Racheli...

SHAMAN: Что у вас происходит?

СТУПИН: Наши программисты проверяют, что случилось. Такого не должно происходить.

Когда я встретился с сотрудниками ФСБ, петля вокруг Врублевского уже начала затягиваться, а Гусев давно закрыл SpamIt и фактически затопил GlavMed. Теперь, по всей видимости, ФСБ нацелилась на финансовую инфраструктуру, обслуживавшую обе конкурирующие аптечные партнёрки, а также другие программы мошеннических интернет-аптек.

Фармацевтические войны Врублевского и Гусева обошлись спамерской отрасли чрезвычайно дорого, а их междоусобица дорого стоила всем в этом бизнесе. Теперь обоих повсеместно ненавидят на киберпреступных форумах за то, что они лишили спамеров десятков миллионов долларов прибыли и привлекли внимание правоохранительных органов и специалистов по безопасности к отдельным спамерам.

«Эти два мудака убили спамерский бизнес, - сказал Вишневский в интервью в мае 2012 года. - Для большинства ребят он никогда не был сверхприбыльным; может быть, пять-десять человек зарабатывали на спаме действительно хорошие деньги. Но после того, как Павел и Гусев начали свою войну, все стали думать, что каждый спамер - миллионер, и начали охотиться на спам и спамеров».

Вишневский жаловался, что, когда доходы от его спамерского бизнеса сократились, ему пришлось устроиться на вторую, законную, или «белую», работу, чтобы дополнять свои «чёрные» дела. Он по-прежнему продаёт свою спамерскую программу множеству других спамеров, но теперь также служит системным администратором в местной московской компании, то есть, по существу, получает деньги за защиту от некоторых угроз, которые сам помогает распространять с помощью спамерского бизнеса.

Но его спамерский бизнес определённо сильно сдал со времён золотых лет до и после McColo. Дело не в том, что спам каким-то образом стал в России более опасным занятием. Скорее, Вишневскому трудно привлекать и удерживать талантливых программистов, помогающих поддерживать его спамерский бизнес. В Москве талантливым разработчикам доступно всё больше законных высокотехнологичных и хорошо оплачиваемых программистских вакансий, и многих давних сотрудников Вишневского переманили на законную работу в молодом, но многообещающем технологическом секторе Москвы.

«Многие представители подполья теперь не могут найти хороших программистов, потому что их зарплаты в Москве намного выше того, что можно заработать спамом, - сказал Вишневский. - Этот бизнес пошёл по пизде, когда Пашу [Врублевского] взяли. Если бы Паша и Гусев не начали ту дурацкую войну, все были бы гораздо счастливее».

Критика Вишневского может быть резкой, но преувеличением её едва ли назовёшь. За последние несколько лет спамерская отрасль и правда получила тяжёлый удар. До закрытия SpamIt в октябре 2010 года объём ежедневно рассылавшегося по всему миру спама держался примерно на уровне 5,5 миллиарда сообщений. Однако после закрытия SpamIt ежедневный объём мирового спама заметно сокращался. По данным Symantec, к марту 2011 года уровень спама упал до немногим более одного миллиарда нежелательных сообщений в день и с тех пор оставался на этом пониженном уровне или очень близко к нему.

Спам остаётся серьёзной проблемой, но он ушёл гораздо глубже в подполье, а крупнейшие игроки, похоже, стали намного осмотрительнее в своих действиях. Конечно, война за территорию между Гусевым и Врублевским была лишь одним, пусть и значительным, фактором упадка спамерской экономики. Если спамерская отрасль стала менее привлекательной для потенциальных киберпреступников, это может быть связано с серией целенаправленных ликвидаций крупных спамерских ботнетов за последние несколько лет.

Вот ещё несколько примечательных ликвидаций, целями которых стали операторы ботнетов и их преступные машины:

• В мае 2009 года Федеральная торговая комиссия убедила суд заставить интернет-провайдеров прекратить маршрутизацию трафика для 3FN, хостинг-провайдера в Северной Калифорнии, которого следователи и FTC определили как крупный источник вредоносного контента в Интернете. Форум Врублевского Crutop.nu размещался там и после закрытия 3FN был вынужден искать новый дом.

• В ноябре 2009 года FireEye, компания по безопасности из Милпитаса, штат Калифорния, возглавила скоординированную операцию по ликвидации ботнета Mega-D. Год спустя предполагаемого владельца Mega-D, двадцатичетырёхлетнего Олега Docent Николаенко, арестовали в Лас-Вегасе. В 2013 году он признал себя виновным в распространении вредоносных программ на защищённые компьютеры и был приговорён к уже отбытому сроку и трём годам условного надзора. (До вынесения обвинительного приговора Николаенко уже провёл под стражей двадцать семь месяцев в связи со своим процессом.)

• В январе 2010 года сотрудники компании интернет-инфраструктуры Neustar захватили управление спамерским ботнетом Lethic, извергавшей спам преступной машиной, состоявшей более чем из 200 000 заражённых компьютеров.

• В феврале 2010 года Microsoft представила первую из будущей серии поддержанных судами ликвидаций крупных спамерских ботнетов. Первой целью стал спамерский ботнет Waledac, принадлежавший Severa, который в то время ежедневно рассылал миллиарды спамерских писем через сеть более чем из 60 000 взломанных компьютеров. В ходе этой операции Microsoft убедила федеральный суд США передать софтверному гиганту законное право собственности на 277 интернет-доменов, которыми ботмастер Waledac пользовался для управления своей спамерской империей.

• В октябре 2010 года власти Армении арестовали двадцатисемилетнего россиянина Георгия Аванесова одновременно со скоординированной ликвидацией ботнета Bredolab, спамерского механизма, который с момента появления в 2009 году захватил миллионы компьютеров. По словам экспертов, на пике работы Bredolab ботнет рассылал более трёх миллиардов сообщений в день. Следователи утверждали, что Аванесов зарабатывал более $130 000 в месяц, сдавая свой ботнет в аренду другим спамерам. Согласно сообщению BBC, позднее Аванесова признали виновным в компьютерном саботаже и приговорили к четырём годам в армянской тюрьме. Записи SpamIt указывают, что у него было несколько партнёрских профилей, приносивших ему доход от этой аптечной программы.

• В марте 2011 года Microsoft взялась за Rustock, начав через судебную систему США юридическую внезапную атаку с целью захватить управление доменами, использовавшимися для контроля спамерского механизма Cosma. В то время Rustock работал, по оценкам, на 815 000 компьютеров и ежедневно рассылал огромные объёмы нежелательной почты. В этом деле Microsoft помогала Pfizer, производитель лекарств, чьими продуктами и товарными знаками спамеры злоупотребляли больше всего.

• В июле 2011 года Microsoft объявила о вознаграждении в $250 000 за сведения, которые приведут к аресту и осуждению ботмастера Rustock. Любопытно, что, хотя Spamdot.biz закрылся после того, как в октябре 2010 года российские правоохранительные органы назвали Гусева спамером номер один в мире, спамерский форум не исчез. Он лишь сменил название и местонахождение. Вскоре после того, как Microsoft предложила награду, Cosma, куратор Rustock, к тому времени сменивший псевдоним на Tarelka, мог наблюдаться на новом форуме за просьбами посоветовать, как получить новый паспорт на вымышленное имя.

• В июле 2012 года FireEye и Spamhaus взялись за ботнет Grum, который вошёл в тройку самых активных спамерских машин, отправляя восемнадцать миллиардов сообщений в день. Их совместная ликвидация ненадолго сократила мировой объём спама, но позднее исходный код Grum попал в руки нескольких других злоумышленников, что привело к его возрождению. Grum остаётся активным и сегодня.

• В июле 2013 года Microsoft и ФБР объявили о совместной операции, ликвидировавшей более 1 400 отдельных ботнетов, которые использовали вредоносную программу Citadel для управления заражёнными компьютерами. Citadel преимущественно использовалась преступными группировками, опустошавшими банковские счета с помощью интернет-ограблений.

• В декабре 2013 года Microsoft снова работала с ФБР, а также с европейскими властями, чтобы нарушить работу ботнета ZeroAccess. ZeroAccess часто поставлялся в комплекте с другими угрозами, включая спам-боты и поддельные антивирусные программы, но главным предназначением ботнета был захват результатов поисковых систем на заражённых компьютерах и перенаправление людей на сайты, которые мошеннически взимали с компаний плату за клики по интернет-рекламе.

• В июне 2014 года ФБР совместно с многочисленными международными правоохранительными партнёрами и частными компаниями по безопасности ликвидировало ботнет Gameover Zeus, состоявший более чем из одного миллиона взломанных компьютеров. ФБР также назвало россиянина, тридцатиоднолетнего Евгения Михайловича Богачёва, организатором операции и

главным автором ботнета. По данным Министерства юстиции США, ботнет Gameover использовался для кражи более $100 миллионов у пострадавших компаний. Кроме того, ботнет служил крупной платформой для проведения дорогостоящих интернет-атак с вымогательством против отдельных пользователей компьютеров.

Но война между Гусевым и Врублевским временно разгромила не только спамерскую отрасль. ChronoPay активно участвовала в обработке платежей для партнёрок, продвигавших мошеннические антивирусные продукты, и, когда в 2011 году Врублевский стал фигурантом уголовного расследования, его процессинговые сети развалились. Партнёрские сети мошеннических антивирусов остановились в одночасье, поскольку потеряли связь с сетями кредитных карт. Врублевского арестовали в конце мая 2011 года по не связанным с этим обвинениям, а к августу 2011 года гигант компьютерной безопасности McAfee заметил 60-процентное сокращение числа пользователей, сообщавших о проблемах с поддельными антивирусными программами.

Закрытие доменов и очистка поиска

Ещё один фронт войны со спамом был направлен против аптечных сайтов, рекламировавшихся в нежелательной почте. Как правило, спамеры искали регистраторов доменных имён, закрывавших глаза на регистрацию спамерами сотен и даже тысяч доменов в месяц для использования в кампаниях аптечного спама. Многие годы некоторые крупнейшие игроки индустрии доменных имён отмахивались от просьб антиспамовых групп аннулировать регистрацию доменов, явно созданных ради выгоды от спамерской деятельности.

Джон Хортон, бывший заместитель руководителя в Управлении Белого дома по политике контроля над наркотиками, а ныне президент LegitScript, службы проверки интернет-аптек, годами отслеживал домены мошеннических аптек. Хортон сказал, что довольно долго большинство регистраторов утверждали: проверять, как клиенты используют свои домены, не их работа.

Ситуация начала меняться в конце 2008 года, когда EstDomains, эстонский регистратор доменов, ставший явным фаворитом как спамеров, так и интернет-мошенников, лишился аккредитации Интернет-корпорации по присвоению имён и номеров (ICANN), некоммерческой организации, надзирающей за отраслью регистрации доменных имён. ICANN приняла меры после того, как в статье автора этой книги в *The Washington Post* было отмечено, что генеральный директор EstDomains, эстонский бизнесмен Владимир Цастин, ранее был осуждён за отмывание денег, подделку документов и мошенничество с кредитными картами.

ICANN предприняла действия после того, как моя статья в *The Washington Post* привлекла внимание к малоизвестному положению договоров, которые регистраторы доменных имён вроде EstDomains подписывали с ICANN: регистраторам запрещалось назначать руководителями лиц с уголовным прошлым. Как упоминалось в главе 8, Цастин был одним из первых крупных инвесторов ChronoPay, а в 2011 году его арестовали в Эстонии вместе с шестью другими мужчинами, обвинёнными в управлении огромным ботнетом, охватывавшим более четырёх миллионов машин по всему миру.

По словам Хортона, случай EstDomains напугал многих в бизнесе регистрации доменов. Одним из ближайших партнёров EstDomains был индийский регистратор Directi, который боролся с собственным потоком жалоб на злоупотребления со стороны спамеров, пользовавшихся его услугами.

«Три-четыре года назад никто не приостанавливал доменные имена, участвовавшие в деятельности мошеннических интернет-аптек, если вы не могли также ясно показать, что эти

домены получали выгоду от спама, - сказал Хортон. - Directi был одним из первых регистраторов, заявивших: если нам известно, что сайты продают рецептурные лекарства без рецепта и [эти лекарства] отправляют в другую страну в нарушение законов этой страны, мы примем меры и приостановим домен. После этого мы увидели, как то же самое начали делать GoDaddy, eNom и ещё несколько компаний. Если посмотреть на доли рынка регистраторов, то сейчас примерно 60-70 процентов [рынка] регистраторов действительно принимают меры [для приостановки доменов] на основании таких обвинений».

Если интернет-сообщество не осознавало финансовых рисков чрезмерного погружения в паутину поддельных фармацевтических сайтов, то в августе 2011 года оно получило этот сигнал громко и отчётливо: Министерство юстиции США объявило, что Google согласилась выплатить штраф в $500 миллионов для урегулирования уголовного расследования по поводу того, что компания позволяла предполагаемым канадским аптекам, включая многие мошеннические интернет-аптеки, рекламировать лекарства для распространения в Соединённых Штатах. Сумма в $500 миллионов должна была представлять рекламный доход компании от канадских аптек и выручку, которую аптеки получили от американских покупателей контролируемых препаратов.

Наступление Visa

Вероятно, самым долговременным воздействием на спамерскую экономику за последние два года обладало исследование, опубликованное разношёрстной группой учёных, которые нанесли на карту сети отмывания денег, использовавшиеся почти всеми аптечными партнёрками. Что ещё важнее, исследователи смогли использовать свои выводы, чтобы вынудить ведущие коммерческие бренды оказать давление на Visa и заставить её принять меры против финансовых учреждений, обеспечивающих эту деятельность.

К началу 2010 года в программы мошеннических аптек и распространителей поддельных антивирусов тайно проникла группа исследователей в белых шляпах, университетских преподавателей и аспирантов, надеявшихся показать, что следование за деньгами может значительно усложнить этим предприятиям получение процессинговых услуг для кредитных карт. На протяжении нескольких месяцев исследователи совершили сотни «контрольных покупок» на сайтах сорока разных сомнительных предприятий, торговавших поддельными рецептурными лекарствами, контрафактными программами и фальшивыми антивирусными продуктами. Исследователи из Университета Джорджа Мейсона, Международного института компьютерных наук и Калифорнийского университета в Сан-Диего (UCSD) выдавали себя за покупателей этих товаров.

Группа учёных полагала: если ей удастся найти финансовые учреждения, получавшие прибыль от этой торговли, и привлечь к ним общественное внимание, пострадает вся отрасль. Причина в том, что, хотя сама по себе продажа через Интернет поддельных рецептурных лекарств не является незаконной, иностранным организациям запрещено отправлять рецептурные лекарства в Соединённые Штаты. Такая деятельность нарушает правила обработки карт Visa и MasterCard и может повлечь крупные штрафы.

Как отмечалось в главе 5, профессору UCSD Стефану Сэвиджу и его команде предстояло проделать огромную работу уже для того, чтобы собрать достоверные исходные данные о спамерской фармацевтической экономике.

«Когда мы это начали, то хотели разобраться во всей цепочке создания стоимости спамерской экономики, - сказал Сэвидж. - Одной из крупных её частей были внутренняя обработка и банки, на которые никто не смотрел».

По словам Сэвиджа, поначалу Калифорнийский университет в Беркли отнюдь не заинтересовался их исследованием. Щекотливые этические и юридические вопросы, связанные с фактическим нарушением федерального закона ради проведения в остальном безвредного исследования, мешали продать проект руководству. Университет и исследователи заключили соглашение. Они будут покупать только непатентованные лекарства, доступные в Соединённых Штатах без рецепта, например препарат для аборта RU-486.

Оказалось, что самой трудной частью исследования было найти надёжный способ оплачивать контрольные заказы. Если они снова и снова заказывали лекарства одной и той же кредитной картой, аптечные партнёрки отменяли транзакции и отмечали номер карты как подозрительный. Они остановились на предоплаченных подарочных картах, поскольку эти платёжные инструменты позволяли совершать покупки анонимно. Но одной возможности купить лекарства предоплаченными картами было недостаточно. Команде требовалось уговорить эмитентов карт раскрыть названия банков и номера торговых счетов, использованных для обработки транзакций.

«Мы выяснили, что [использовать] подарочные карты проще всего, потому что в них можно было указать вымышленное имя или что угодно ещё, - сказал Сэвидж. - Но по многим таким подарочным картам, если вы хотели узнать сведения о транзакции, нужно было звонить в какой-нибудь центр поддержки клиентов. И даже у некоторых довольно крупных предоплаченных карт работало всего несколько специалистов по обслуживанию. Они быстро начинали подозревать неладное, потому что, если вы совершали много покупок, вам постоянно приходилось разговаривать с одними и теми же людьми».

Вскоре Сэвидж и другие исследователи нашли идеальную сеть предоплаченных карт, хотя он отказался назвать её, чтобы не испортить аналогичные текущие и будущие исследования. Он сказал лишь, что это предоплаченная карта, выпускаемая довольно крупной сетью продовольственных магазинов в Соединённых Штатах.

«Мы спросили другую группу, которая это исследовала, и они рассказали нам о подарочной карте сети продовольственных магазинов. [Аспирант UCSD] Крис Канич приходит в один из таких магазинов с чем-то вроде $5 000 наличными и покупает целую уйму этих магазинных предоплаченных карт. Там даже глазом не моргнули, - сказал Сэвидж. - Где-то у нас до сих пор лежит их стопка. Но через университет это было действительно трудно протащить: мы собирались взять все эти деньги и превратить их в неотслеживаемые платёжные инструменты, и, конечно, нам нужно было поверить, что мы просто не отправимся на какие-нибудь каникулы в Бразилию или куда-то ещё».

С благословения университета и стопкой предоплаченных карт толщиной в несколько колод игральных карт исследователи принялись покупать поддельные лекарства на сайтах, рекламировавшихся с помощью спама. Сеть предоплаченных карт продуктового магазина безупречно работала во всех интернет-аптеках, и всё, казалось, шло как по маслу. Так продолжалось до тех пор, пока дядя Сэм не решил, что бурно растущий и почти нерегулируемый рынок предоплаченных карт чрезвычайно удобен для злоупотреблений со стороны тех, кто отмывает деньги.

«Всё шло хорошо, пока Конгресс не решил помочь миру этим законом Credit CARD Act 2009 года, - сказал Сэвидж, имея в виду закон, вступивший в силу в 2010 году и содержавший множество ограничений на то, как компании кредитных карт могут взимать плату с потребителей. - Сеть по борьбе с финансовыми преступлениями Министерства финансов США (FinCEN) всегда была очень обеспокоена подарочными картами с точки зрения объёма неотслеживаемых денег, потому что они были просто отличными и прекрасно подходили для отмывания денег. Клянусь, если бы у вас был чемодан таких карт, вы могли бы перевезти многие миллионы долларов, и он был бы чертовски легче нескольких миллионов баксов».

Каким-то образом индустрия предоплаченных карт избежала действия правил «знай своего клиента», регулирующих все финансовые учреждения США. Эти правила требуют от банков предпринимать конкретные шаги для анализа деятельности клиентов на предмет признаков отмывания денег, подозрительных транзакций и финансирования терроризма. Однако после принятия Credit CARD Act сети предоплаченных карт подпали под те же правила.

«Все эти карты можно было пополнять, и на них можно было установить любое имя, какое пожелаете, потому что для сетей предоплаченных карт практически не существовало правил „знай своего клиента“, - сказал Сэвидж. - Внезапно этим сетям понадобилась защита международных транзакций от отмывания денег. Краткосрочным последствием стало то, что все в этой отрасли фактически сказали: „Ладно, больше никаких международных транзакций по предоплаченным картам“, - и мои предоплаченные карты на $5 000 мгновенно превратились в бесполезную кучу дерьма».

Сэвидж сказал, что в тот момент был обескуражен и готов сдаться, но одного из его аспирантов, Криса Канича, это не остановило. Близился конец ноября 2011 года.

«Этот сукин сын полностью проигнорировал меня и начал обзванивать эмитентов кредитных карт без предварительной договорённости. Он просто звонил им и говорил: „Здравствуйте, меня зовут Крис Канич, мы проводим исследование аптечного спама, и нам нужен финансовый продукт, который умеет X, Y и Z“. Он позвонил примерно в пятьдесят банков, пока не нашёл этот маленький банк на Среднем Западе. Человек, с которым он говорил, отнёсся к нему благосклонно и сказал, что генеральный директор банка очень интересуется кибербезопасностью. Они заключили с нами особое соглашение, и после этого стало намного проще».

Исследовательская группа близко познакомилась с различными схемами, которые разные сети мошеннических аптек использовали для отсеивания подозрительных транзакций. Сети мошеннических аптек чрезвычайно опасались любого мошенничества, способного повысить показатели возвратов по их транзакциям или привести к их закрытию, поэтому они обычно полагались на многоуровневые меры борьбы с мошенничеством. Например, они использовали службы геолокации, чтобы проверить, показывает ли интернет-адрес покупателя, что тот находится в том же городе, который указан в платёжном адресе кредитной карты.

«Со временем мы узнали, что каждой транзакции присваивался показатель мошеннического риска на основании ряда критериев, и любые транзакции, превышавшие определённое значение этого показателя, торговые процессоры просто не проводили, - сказал Сэвидж. - Мы узнали, что адрес электронной почты у общедоступного провайдера веб-почты повышал ваш показатель риска. Со временем мы узнали, что вам требовалось имя с настоящим физическим адресом и работающим номером телефона, потому что вам часто перезванивали для подтверждения заказа».

В начале своей серии фиктивных покупок исследователи были разоблачены. Они пытались ежемесячно совершать не менее одной контрольной покупки в каждой из более чем двух дюжин партнёрских программ интернет-аптек, чтобы отслеживать банки-эквайеры, обрабатывавшие транзакции. Они не знали, что большинство партнёрок пользовались одними и теми же финансовыми учреждениями - горсткой банков в Азербайджане, Латвии, на Кипре и в Турции.

«Мы старались не привлекать внимания и размещали по одному заказу в каждой программе в месяц, но, поскольку мы не знали, что все они получают процессинговые услуги из одного места, выходило что-то вроде тридцати пяти заказов в месяц от одних и тех же людей, - сказал Сэвидж. - В какой-то момент Крису Каничу [который по-прежнему участвовал в исследовании, но к тому времени стал доцентом Иллинойского университета в Чикаго] звонят сотрудники клиентской службы одной из партнёрок, и ему приходится соображать на ходу, потому что они хотели узнать, почему столько людей по его адресу заказывают Zyrtec, противоаллергический препарат. И он, по сути, выдумал историю, сказав, что живёт в студенческом общежитии и что у него и всех соседей аллергия, потому что у них у всех аллергия на кошек, а один из ребят держал кошку. Так со

временем мы все научились делать эти фиктивные заказы».

Спамалитика, Microsoft и напалм

Следование по денежному следу выявило поразительный факт: 95 процентов транзакций по кредитным картам за рекламировавшиеся в спаме лекарства и растительные средства, купленные исследователями, обработали всего три финансовые фирмы - одна в Азербайджане, одна в Дании и ещё одна на острове Невис в Вест-Индии. Многим американцам, вероятно, было бы трудно найти эти места на карте, не говоря уже о том, чтобы вспомнить о деловых отношениях с компанией в этих регионах. И всё же огромная доля обработки кредитных карт для спамерской отрасли проходила через финансовые учреждения этих регионов. Специалисты по борьбе со спамом хотели знать, почему банки не могут заметить эту странную концентрацию сомнительной банковской деятельности и положить ей конец.

Исследователи опубликовали результаты в статье «Траектории кликов: сквозной анализ цепочки создания стоимости спама», где описали свой метод «спамалитики», направленный на главную слабость любой спамерской операции - её зависимость от обработки кредитных карт при продаже товаров, рекламируемых в нежелательных сообщениях.

Сэвидж сказал, что через пять дней после статьи *The New York Times* об их работе исследователям позвонили из Белого дома. На линии была Виктория Эспинель, координатор администрации Обамы по обеспечению прав интеллектуальной собственности.

«Она устраивала эту встречу с пристрастием для регистраторов доменных имён, известных брендов и Google, говоря: „Эй, мы все должны что-то делать с этой проблемой спама“. В своей статье мы сказали, что в основном существуют два способа: можно действовать в двустороннем порядке против обслуживающих [аптеки] торговых банков, но это медленно. Либо можно попытаться перекрыть всё со стороны эмитентов кредитных карт, потому что деньги этих фармацевтических сетей в основном были западными. Оглядываясь назад, это была глупая идея, потому что, когда мы поговорили с банками-эмитентами здесь, в Соединённых Штатах, они сказали: „Эй, наши клиенты не жалуются, а мы не занимаемся надзором за тем, что делают наши клиенты, если в записях транзакций это выглядит законным“».

Эспинель связала Сэвиджа и его команду с Международной коалицией по борьбе с контрафактом (IACC), некоммерческой группой, созданной для помощи корпоративным брендам в борьбе с коммерческим пиратством и нарушениями прав на товарные знаки. IACC создавала интернет-портал, где любой правообладатель бренда мог зарегистрироваться и сообщить о нарушении прав на свои товарные знаки непосредственно MasterCard и Visa, которые должны были расследовать заявление и в конечном счёте наложить штрафы на банки, обрабатывавшие связанные с ним транзакции.

IACC опиралась на договоры, которые подписывают все банки как обязательное условие работы с ассоциациями кредитных карт. Они предусматривают, что любая продажа товара должна быть законной не только в юрисдикции, где находится обслуживающий продавца банк, но и в стране проживания покупателя. А поскольку отправка рецептурных лекарств потребителям из-за пределов Соединённых Штатов нарушает американское законодательство, каждое заявление, поданное затронутым правообладателем бренда в Visa или MasterCard через IACC, фактически вызывало дождь штрафов для банков, обрабатывавших платежи аптечных партнёрок.

«Эти условия всегда были в договорах, но почему-то люди не обращали на них внимания, - сказал Сэвидж. - Оказалось, что по-настоящему проблему спама принимают близко к сердцу правообладатели брендов, потому что именно их продукты, авторские права и товарные знаки

подделывают и нарушают. И прелесть такого подхода в том, что это не правовой вопрос уголовного законодательства. Это исключительно договорный вопрос. В сущности, правоохранительные органы в этом процессе вообще не участвуют. Нужно лишь заставить Visa и MasterCard обеспечивать соблюдение собственных договорных правил».

По иронии судьбы, применить дубинку IACC против аптечных спамеров вызвались не фармацевтические компании, а Microsoft. Те же сети, которые извергали спам для продвижения интернет-аптек, использовались и для рекламы сайтов, торговавших контрафактными копиями операционной системы Microsoft Windows, и Microsoft увидела в IACC прекрасную возможность значительно повысить для фальсификаторов стоимость обработки платежей по кредитным картам за поддельные копии Windows.

«Microsoft решила взяться за дело по полной. Они были по-настоящему преданы цели, - сказал Сэвидж. - Идея, как выразился их главный человек, заключалась в „особом подарке ко Дню благодарения“. Они собирались одновременно взяться за каждый банк, использовавшийся в этой программе, за всех регистраторов, регистрировавших домены, и за все хостинговые компании, а затем за короткое время закрыть всё. После этого обратиться в Google и Bing и убрать [спамеров] ещё и из результатов поиска. В какой-то момент они просто сбросили бомбу на всю отрасль. И в подполье происходит этот переход, когда все говорят: „Эй, у нас тут небольшие трудности“».

Сэвидж сказал, что один крупный поставщик программного обеспечения особенно активно взялся за партнёрские программы, продававшие его продукты. Партнёрские программы, торгующие пиратскими программами «OEM», то есть программным обеспечением «производителя оригинального оборудования», в основном продают дорогостоящие продукты, включая Microsoft Windows и продукты Adobe. Судя по реакции на форумах OEM-партнёрок, весьма вероятно, что речь шла об Adobe.

«Этот поставщик взялся за всё. Они сделали это так быстро - и не только ради собственных продуктов, - что почти полностью закрыли всю экосистему OEM, - сказал Сэвидж. - Несколько [OEM-партнёрских программ] выжили, отказавшись от бренда этой компании, но вначале, когда никто не понимал, что происходит, это остановило весь бизнес для всех».

Договоры между банками и Visa и MasterCard предусматривают запрет продавцам торговать товарами и услугами, которые незаконны в стране, где эти товары или услуги приобретаются либо используются, или и то и другое. У ассоциаций кредитных карт есть стандартный порядок приёма жалоб на такие транзакции: они предупреждают банк интернет-продавца, в том числе уведомляют о возможных штрафах за несоблюдение требований. После жалобы на такую деятельность банк продавца проводит расследование и может оспорить вопрос, если считает жалобу ошибочной. Но если банк решит не оспаривать жалобу, ему потребуется принять меры для предотвращения подобных транзакций в будущем, иначе ассоциации карт наложат на него последовательность всё более крупных штрафов.

Исследователи заметили: случай за случаем торговые счета, долго использовавшиеся в мошеннической деятельности до подачи исследователями жалобы в IACC, как правило, прекращали использоваться в течение месяца после подачи жалобы.

По словам Сэвиджа, данные позволяют предположить, что частный сектор может оказать значительное влияние на киберпреступность, просто взявшись за финансирование таких операций.

«Для этого не нужны ни судья, ни сотрудник правоохранительных органов, ни даже сколько-нибудь сложные средства безопасности. Если вы можете купить товар, значит, остаётся запись, и эта запись указывает на торговый счёт, получающий деньги, - сказал Сэвидж. - Visa и MasterCard неодобрительно относятся к продажам незаконных товаров через свои сети и надлежащим образом реагируют на жалобы правообладателей брендов, основанные на контрольных покупках».

Примерно в то же время, когда исследователи передавали свои выводы IACC, Visa вводила ряд изменений в правила работы, которые, по всей видимости, были специально направлены против интернет-аптек и продавцов контрафактных товаров. Во-первых, продажи товаров, отнесённых к фармацевтическим, впервые были прямо классифицированы как «высокорисковые» наряду с азартными играми и различными видами услуг прямого маркетинга, а от эквайеров, заключавших новые договоры с высокорисковыми интернет-продавцами, потребовали значительно более тщательной проверки, включая $100 миллионов собственного капитала и хорошую репутацию в программах управления рисками.

Кроме того, новые документы прямо называли среди примеров незаконных транзакций «незаконную продажу рецептурных лекарств» и «продажу контрафактных либо нарушающих права на товарные знаки товаров или услуг». Наконец, изменения включали более жёсткие шкалы штрафов за несоблюдение требований.

Одно из лучших доказательств успеха стратегии контрольных покупок поступает непосредственно от людей, управлявших партнёрскими программами, которые вознаграждают спамеров и злоумышленников за продвижение поддельных антивирусов, пиратских программ и сомнительных сайтов с таблетками. В июне 2012 года руководитель одной популярной аптечной партнёрской программы опубликовал длинное сообщение на gofuckbiz.com, русскоязычном форуме, обслуживающем различные подобные партнёрские программы. В той ветке обсуждения, которая теперь занимает более 250 страниц, руководитель партнёрской программы объясняет нескольким озадаченным участникам форума, почему аптечным программам было так трудно поддерживать надёжную обработку кредитных карт.

> В мае 2011 года Visa запустила новую программу, так называемую «Глобальную программу защиты брендов». Как это обернётся для банков и продавцов, тогда никто не знал, поэтому в тот момент почти ничего не изменилось - всё продолжало работать как прежде. Через несколько месяцев Visa начинает действовать, и начиная с ноября 2011 года на продавцов посыпались штрафы в размере $25 000 за каждый домен, содержащий бренды Viagra, Cialis и/или Levitra либо другие защищённые авторским правом лекарства.

Руководитель продолжал:

> Под удар попали все партнёрские программы. Сегодня все крупные партнёрские программы выплатили по этой программе штрафы, превышающие сотни тысяч. Под удар попадают и банки, и, хотя в большинстве случаев они могут покрыть финансовые потери за счёт продавцов - при условии достаточного оборота, - проверки Visa, репутационные риски и прочие неприятности осложняют их работу. Поэтому некоторые банки полностью отказались от этого бизнеса, некоторые сильно сократили объём «фармацевтических» платежей, [а] некоторые тем или иным способом «перестраховались», что привело к практически нулевому уровню одобрения. Некоторые (банки) продолжают работать, но сегодня их число очень ограничено.

Другой партнёр программы мошеннических аптек выразил положение дел куда менее деликатно, заметив:

> Сейчас у большинства партнёрских программ масса отказов, отмен и зависших платежей, и, ИМХО, это мало зависит от программы; общая картина печальная: грёбаная Visa выжигает нас напалмом.

По словам Сэвиджа, после того как процессоры сайтов с таблетками обожглись на штрафах Visa, многие начали намеренно «неверно кодировать» аптечные транзакции. Компании кредитных карт требуют, чтобы каждая транзакция помечалась кодом, определяющим вид приобретаемого товара или услуги. Таких кодов тысячи (например, код фармацевтики - 5192), а договоры, которые

продавцы обязаны подписывать с ассоциациями карт, дают последним право налагать огромные штрафы на продавцов, кодирующих высокорисковые транзакции как деятельность с более низким риском.

«К этому моменту большинство оставшихся аптечных партнёрок начали отчаиваться и делать безумные вещи, например отмывать свои транзакции через парковки и случайные банки в Соединённых Штатах, - сказал Сэвидж. - Неверное кодирование было замечательным, потому что [поначалу] в отношении большинства контрафактных товаров мы, исследователи, не могли пожаловаться на них в Visa, поскольку у нас не было правового основания в отношениях с Visa. Мы не могли просто сказать: „Эй, вот подделывают продукт Pfizer. Visa, тебе следует что-то с этим сделать“. Действительно принять меры может только правообладатель бренда».

«Но о неверном кодировании кто угодно может сообщить что угодно. Если мы обнаруживаем, что одна из этих фармацевтических лавок пользуется американским банком и неверно кодирует транзакции, то часто можем просто позвонить в банк и сказать: „Эй, вы знаете, что это происходит?“ И чаще всего они говорят: „Большое спасибо“, потому что за обработку неверно закодированных транзакций им могут выписать крупные штрафы. Поэтому, если вы им сообщите, они смогут всё закрыть прежде, чем Visa узнает и оштрафует их».

Деймон Маккой, доцент факультета компьютерных наук Университета Джорджа Мейсона, сказал, что многие партнёрские программы аптек, запугивающих программ и OEM-программного обеспечения ответили на наступление платёжных систем введением обременительных мер безопасности для отсеивания контрольных покупок. Например, некоторые программы мошеннических аптек, такие как RxPayouts, начали требовать от покупателей отправлять сканы или факсы водительских удостоверений и физических кредитных карт. Другие решили обрабатывать платежи только существующих клиентов.

Но обе меры безопасности могут причинить вред как клиентам, так и партнёрам. Исследователи отмечают, что введённое в январе 2012 года требование RxPayouts о предоставлении новыми клиентами удостоверения личности с фотографией вызвало возмущение среди партнёров. По словам исследователей, один партнёр написал в ответ: «Это новое правило убивает меня, мой коэффициент конверсии новых клиентов упал до [нуля]. Как только новые клиенты узнают, что им нужно отправить в клиентскую службу по факсу удостоверение личности с фотографией, они отменяют заказ».

Маккой сказал, что новые требования также защищают партнёрские программы ещё от одного потенциального источника головной боли и неприятностей: мошеннических партнёров, которые присоединяются к программе только ради комиссионных за заказы, размещённые с помощью украденных кредитных карт.

«Первоначально партнёрские программы делали это для защиты от кардеров, и раньше, если по покупке происходил возврат платежа, расходы на него несла партнёрская программа, - сказал Маккой. - Теперь, если поступает возврат платежа, они вычитают эту сумму из последующих заработков партнёра».

Исследователи заметили, что аптечные партнёрские программы в последнее время также заменяют фирменные лекарства их непатентованными аналогами, например цитратом силденафила вместо Viagra, тадалафилом вместо Cialis и так далее. Операторы этих программ убеждают партнёров, что такие действия устранят проблемы брендов и товарных знаков и тем самым подорвут способность правообладателей закрывать как отдельные сайты, так и связанные с ними торговые счета.

Позволит ли этот последний шаг банкам, обслуживающим подобные предприятия, и дальше беспрепятственно это делать вопреки сетям кредитных карт, ещё предстоит выяснить, по словам процитированного выше руководителя партнёрской программы, который опубликовал на

gofuckbiz.com следующее.

«К чему это в итоге приведёт, покажет время. Либо все перестанут использовать известные бренды, которые так хорошо знакомы покупателям, и начнут пользоваться индийскими названиями дженериков или названиями действующих веществ, либо все продолжат соревноваться в этой безумной гонке: кто кого перехитрит».

Глава 12. Эндшпиль

В июне 2011 года Врублевский совершил вторую за тот год незапланированную поездку на Мальдивы. На этот раз он бежал из Москвы, поскольку получил сведения, что прокуратура готовится предъявить ему уголовные обвинения в связи с кибератакой на билетные системы Аэрофлота в июле 2010 года.

Следователи уже арестовали братьев Игоря и Дмитрия Артимовичей, предположительно совместно создавших ботнет Festi и управлявших им. Оба брата отрицают, что управляли ботнетом или рассылали спам, и утверждают, что российская полиция подбросила доказательства на их компьютеры. Российские прокуроры получили подписанное Игорем признание, где говорилось, что Врублевский нанял его для атаки на Assist, платёжного процессора Аэрофлота. Во время атаки ChronoPay входила в число нескольких компаний, претендовавших на выгодный контракт по обработке платежей Аэрофлота, и прокуроры утверждали, что атака должна была помешать Assist сохранить контракт. По иронии судьбы, через месяц после атаки Аэрофлот передал контракт не одной из этих компаний, а Альфа-банку, крупнейшему частному банку России.

Российские власти напомнили Павлу, что на Мальдивах его также могут задержать американские либо иные иностранные власти, и потому он добровольно вернулся в Москву.

По прибытии Врублевского арестовали и отправили в Лефортово, похожую на крепость тюрьму строгого режима, построенную в Москве в 1881 году. Тюрьма приобрела дурную славу во время холодной войны, когда советский КГБ использовал её для изоляции и допросов политических заключённых. В 1994 году контроль над Лефортово передали российской милиции, а позднее - ФСБ, службе-преемнице КГБ.

В тюрьме Врублевский признался, что распорядился атаковать Assist, но позднее отказался от этого заявления. Тем не менее его адвокат, сотрудник ChronoPay Станислав Мальцев, тот самый бывший российский милиционер, который некогда отвечал за расследование обвинений Врублевского в незаконной предпринимательской деятельности, утверждал, что его клиент должен оставаться на свободе до суда. Суд отклонил ходатайство и распорядился держать Врублевского в Лефортово шесть месяцев - максимальный предусмотренный законом срок предварительного заключения по предъявленным ему обвинениям.

«Главный риск его освобождения заключается не в том, что он убежит, а в том, что он сделает что-нибудь плохое свидетелям и попытается убедить их не сообщать и не давать показаний с какой-либо информацией о нём», - сказал Гусев в телефонном интервью.

Это смелое заявление для человека, чьи утёкшие журналы чатов показывают, что он и Ступин заплатили $1,5 миллиона за возбуждение уголовного дела против Врублевского и $50 000 за начало дела против Игоря и Дмитрия Артимовичей - братьев, которые под общим псевдонимом Engel предположительно использовали свой ботнет Festi для рассылки спама в интересах Rx-Promotion и периодических разрушительных атак на интернет-сайты, включая DDoS против Аэрофлота, из-за которого Врублевский оказался в тюрьме.

Ниже приведён фрагмент утёкшего чата, предположительно между Гусевым и Ступиным, датированного 26 сентября 2010 года. Двое мужчин уже решили закрыть SpamIt и размышляли, не сделать ли то же самое с GlavMed. Врублевский здесь назван Paul, западным эквивалентом имени Павел.

> **ГУСЕВ:** По-моему, ты не до конца понимаешь, что происходило в последний год. У Пола есть план: либо посадить меня в тюрьму, либо прикончить. Его намерения совершенно ясны. Есть только два варианта: 1 - ничего не делать и никому ничего не платить, а в итоге либо сесть в тюрьму, либо продолжать скрываться, пока не исчерпаются все ресурсы; 2 -

делать то же, что и он, с той же целью.

Гусев говорит Ступину, что «любая война стоит денег, ресурсов и нервных клеток. Нельзя воевать понемногу: либо сражаешься до конца, либо вообще не начинаешь. Engel будет постоянно нам вредить... Если существует хоть какая-то потенциальная возможность вывести его из игры, мы должны ею воспользоваться. $50 тысяч - очень мало по сравнению с убытками, которые мы понесли из-за его DDoS-атак, и по сравнению с будущими убытками, если он снова будет нас DDoS-ить».

Гусев говорит Ступину: если тот не внесёт свою долю взятки в $50 000 за возбуждение уголовного дела против братьев Артимовичей, Гусев будет вынужден получить больший контроль над аптечной партнёркой. Ступин в конце концов соглашается, но заявляет для протокола, что считает это плохой идеей.

Чаты также показывают, что примерно в то же время Гусев посетил российскую ФСБ, где его склонили к сотрудничеству и передаче сведений о крупных игроках отрасли мошеннических аптек.

«У них тонны информации и очень хорошее понимание того, как всё работает, куда входят и откуда выходят деньги, - сказал Гусев Ступину в январе 2010 года. - У ФСБ определённо есть информация о движении денег по кошелькам. Подводя итог: если они захотят посадить меня в тюрьму, они это сделают. Они также спрашивали о тебе. Пока они хотели, чтобы я работал на них и давал информацию о других. Они обещали всевозможные выгоды от сотрудничества с ними».

Любопытно, что утёкшие журналы чатов между Гусевым и Ступиным были получены следователями ФСБ, задержавшими Ступина и сделавшими криминалистическую копию его жёсткого диска. Каким-то образом Engel - возможно, с помощью взяток, уплаченных Врублевским, - получил копию этих журналов и передал их нескольким источникам, включая автора этой книги.

Разговоры из этих журналов чатов занимали заметное место на протяжении всей книги, но один из самых показательных и честных разговоров содержится в ветке обсуждения на российском форуме веб-мастеров сайтов для взрослых master-x.com. Эта ветка полна комментариев спамеров, которых вытеснили из бизнеса или которые потеряли деньги из-за фармацевтических войн между Гусевым и Врублевским. Сейчас она занимает более ста страниц.

Эпическое обсуждение на master-x.com начинается с того, что почти все используют псевдонимы и вообще пытаются скрывать свои настоящие личности, но примерно в середине ветки Гусев начинает ссылаться на себя так, что это явно выдаёт в нём автора. В этом разговоре Гусев становится непривычно эмоциональным и разражается серией всё более враждебных тирад в адрес Артимовича.

Гусев говорит, что российские веб-мастера понимали: фармацевтические войны между ним и Врублевским были лишь состязанием в том, у кого больше денег и связей. Гусев также предупреждает Артимовича, что Врублевский, вероятно, обратит свой гнев на него, когда выйдет из тюрьмы. (Признав, что Врублевский нанял его для DDoS-атаки на Assist, Артимович, по существу, решил судьбу Павла.)

Имей в виду, что Паша очень подлый человек. И какая у него долгая память! Видишь ли, то, что после ухода из ChronoPay мои дела шли лучше, чем у него, причиняло ему жесточайшую боль в заднице 7 лет!!! Он не мог спать, страшно из-за этого страдал! Вот что такое зависть. Она медленно, но верно разрушает человека. А теперь представь его психологическое состояние после окончания тюремного срока. Голодный, злой, брошенный всеми подхалимами, без бизнеса и, хуже всего, с ясным осознанием, что в конце концов он так и не смог посадить меня в тюрьму. Думаю, психика Паши не выдержит такого давления. А поскольку до меня он добраться не сможет, то сосредоточится на тебе и твоём брате.

А затем Гусев говорит, что, возможно, сам отомстит Артимовичу раньше Врублевского.

> Но всё это рассуждения о возможном будущем. Что касается настоящего, думаю, я всё равно доберусь до тебя первым. Я раньше предупреждал тебя: если ты попытаешься втянуть мою семью в этот конфликт, последствия будут очень суровыми. Я лично найду тебя, оторву голову и поменяю её местами с твоей задницей - скорее всего, никто не заметит разницы.

• * *

23 декабря 2012 года российские прокуроры освободили Врублевского из Лефортовской тюрьмы, всего за три дня до его дня рождения. Его освобождение едва ли было проявлением милосердия. По российскому законодательству шесть месяцев были максимальным сроком, в течение которого прокуроры могли держать его под стражей до суда.

Через несколько часов после возвращения в московский дом Врублевский уже писал в Twitter и блоге о своём триумфальном освобождении. Он также не стал терять времени и позвонил автору этой книги главным образом для того, чтобы пожаловаться на обращение и бытовые условия в знаменитой тюрьме. В долгом телефонном разговоре Врублевский сетовал на присутствие множества заключённых-мусульман, содержавшихся в его части Лефортово, и на их постоянные возгласы.

«У меня не было даже горячей воды или грёбаного окна, а свет горел двадцать четыре часа в сутки, - вспоминал Врублевский. - Это самая строгая тюрьма в России, и половина заключённых сидит там за какой-то мусульманский терроризм. На три месяца мне перекрыли общение с семьёй... ни телефонных звонков, ни посещений, ничего. Только эта хрень „Аллах акбар!“ пять раз в день!»

Адвокат запретил Врублевскому обсуждать дело, но, как всегда, у него нашлась забавная история о своём положении. Когда заключённого Лефортово собираются освободить, старшие арестанты торжественно сообщают ему о серьёзной традиции, согласно которой освобождённый узник должен позднее сжечь одежду, в которой вышел на свободу. Опасаясь навлечь на себя новые несчастья несоблюдением традиции, на следующий день после освобождения Врублевский пригласил домой друзей, чтобы предать огню одежду, которая была на нём при заключении в Лефортово и освобождении оттуда.

«Представьте картину: серая, мерзкая погода, мы стоим за домом с одеждой, в которой я вышел из тюрьмы, - вспоминал Павел, едва сдерживая смех. - Стоим, курим перед костром, устраиваем похороны одежды. Как в настоящем голливудском фильме, только без драматической музыки в этот момент. Говорят серьёзные вещи вроде: „Чувак, больше туда не попадай, бла-бла“. И вдруг жена выбегает из дома с криком: „Павел, ты сжигаешь не те туфли!“ Оказалось, я сжёг свои дорогие туфли Yamamoto, а не те, в которых вернулся из тюрьмы!»

Во время заключения Врублевский подписал полное признание, где говорилось, что именно он организовал атаку на Assist, процессора кредитных карт Аэрофлота. В признании Врублевского утверждалось, что он поручил сотруднику ChronoPay Максиму Пермякову, специалисту компании по информационной безопасности, перечислить $20 000 платежами WebMoney в кошелёк Игоря А. Артимовича, предполагаемого ботмастера спамерского ботнета Festi и бывшего сотрудника Sun Microsystems в России. И действительно, длинная цепочка писем в массиве сообщений, утёкших из ChronoPay, подробно и точно описывает эту операцию.

Артимович, арестованный следователями российской Федеральной службы безопасности (ФСБ), подписал аналогичное признание, где утверждал, что ChronoPay наняла его использовать Festi для атаки на Assist. ФСБ также арестовала брата Артимовича Дмитрия, внештатного программиста.

Всем четверым мужчинам - Врублевскому, Пермякову и братьям Артимовичам - предъявили обвинения в нарушении двух статей российского Уголовного кодекса: статьи 272 о «неправомерном доступе к компьютерной информации» и статьи 273, запрещающей использование и распространение вредоносных компьютерных программ. Обе статьи предусматривают лишение свободы на срок от трёх до семи лет.

Но в сентябре 2012 года суд, рассматривавший дело, отказался рассматривать обвинения по второй статье, заявив, что срок давности для обвинения подсудимых в использовании и распространении вредоносных компьютерных программ истёк.

До начала суда все обвиняемые, кроме одного - Пермякова, - отказались от признаний, сделанных в заключении, заявив, что в тот момент подвергались сильному психологическому давлению со стороны следователей. Артимович говорит, что полиция его даже избила.

Пермяков, однако, в конце концов признал свою роль в схеме и согласился помогать прокурорам в расследовании. Для многих, внимательно следивших за судом, это не стало большим сюрпризом. До прихода в ChronoPay Пермяков сам был сотрудником российской ФСБ.

Пермяков вполне мог быть и источником утёкших писем и документов ChronoPay. В своих многочисленных тирадах и рассуждениях об источнике утечки Врублевский твёрдо стоял на том, что компромат ChronoPay был не украден хакерами, а передан кем-то из отдела информационных технологий компании. Любопытно, что, хотя вследствие утечки в Сети оказалась многолетняя служебная переписка почти всех ведущих сотрудников ChronoPay, почтовый ящик Пермякова заметно отсутствовал в этом архиве.

В любом случае, возможно, вполне уместно, что процесс над Врублевским и его сообщниками разворачивался как выдающийся пример той самой коррупции, которую бывший генеральный директор ChronoPay так долго замышлял использовать в своих коммерческих интересах.

Аэрофлот утверждал, что DDoS-атака Festi почти на неделю вывела из строя возможность принимать бронирования авиабилетов через сайт и средства обработки кредитных карт и что атака причинила компании ущерб как минимум в 146 миллионов российских рублей (примерно $5 миллионов). Но, как отмечала российская «Новая газета», которая освещала дело Врублевского, возможно, внимательнее и скептичнее любой другой новостной организации, судья сослалась в решении на денежный ущерб, хотя арбитражный суд отказался признать эти цифры и отклонил иск Аэрофлота о возмещении имущественного ущерба в связи с атакой. Арбитраж указал, что большинство клиентов, которые не могли купить авиабилеты в Интернете, просто бронировали их через сторонние службы либо приобретали в кассах Аэрофлота.

Ближе к концу суда, в июне 2013 года, Врублевского снова арестовали и заключили под стражу, предположительно за попытку запугать свидетеля обвинения. Прокуроры утверждали, что Врублевский позвонил одному из свидетелей, мужчине по имени Никита Евсеев, и предложил деньги в обмен на молчание. Адвокаты Врублевского отрицали это обвинение и заявляли, что подпись другой свидетельницы, Анастасии Курочкиной, была подделана обвинением и что на самом деле она никогда не осматривала и не подтверждала неприкосновенность доказательств, которые обвинение намеревалось представить в суде.

Адвокаты Врублевского утверждали, что обнаружили: Курочкина в действительности была подругой или девушкой сотрудника правоохранительных органов, расследовавшего DDoS-атаку для обвинения.

По словам Алексея Михайлова, эксперта по информационной безопасности, уроженца Москвы, ныне живущего в Нью-Йорке, который неотступно следил за делом с самого начала, прочёл все доступные интернет-публикации российской прессы и отдельные сообщения западных изданий, адвокаты Врублевского почти наверняка были правы, утверждая, что подпись подделали. Он объясняет значение поддельной подписи и роль свидетельницы в этом деле.

«По сути, следователи ФСБ сфальсифицировали часть доказательств, и, к сожалению, в России это не редкость, - сказал Михайлов. - В российских уголовных процессах есть понятие „понятой“: это должен быть посторонний человек, не имеющий заинтересованности в деле или связи с ним, примерно как в Америке, где случайных людей вызывают для исполнения обязанностей присяжных. Его приводят в помещение, где работают с доказательствами, и он должен засвидетельствовать, что обвинение обращается с доказательствами надлежащим образом. В данном случае свидетельница должна была подтвердить, что определённые доказательства, полученные от Артимовича, не были скомпрометированы. Это должен быть совершенно случайный человек, но тот факт, что свидетельница в данном деле была хорошей подругой, если не девушкой, следователя по делу, вызывает большие подозрения».

Тем не менее суд проигнорировал доказательства, представленные защитой, и оставил в силе решение заключить Врублевского под стражу за воздействие на свидетеля.

Игорь Артимович, со своей стороны, до заключения дал интервью *The New York Times*, где заявил, что не отвечал за Festi, а его связь с ChronoPay возникла из-за проекта внутри компании, целью которого была разработка антивирусного продукта под брендом ChronoPay.

Такое заявление может показаться нелепым и диковинным для компании, которая сыграла столь важную роль в развитии и процветании отрасли мошеннических антивирусов - бизнеса, вымогавшего у жертв деньги: на системы пользователей устанавливали вредоносную программу, а затем предлагали купить бесполезный защитный продукт, якобы предназначенный для удаления вызванного ею заражения.

Но в утверждениях Артимовича, похоже, есть доля правды. Когда в феврале 2011 года я посетил Врублевского в Москве, он рассказал мне о планах выпустить средство борьбы с вредоносными программами под брендом ChronoPay и кодовым названием ChronoPay Antivirus. Помню, в тот момент мы оба неловко посмеялись, однако среди множества утёкших из ChronoPay документов есть технические материалы, где упоминается разработка различных антивирусных модулей. Документы позволяют предположить, что компания наняла программистов для обратной разработки бесплатной версии коммерческого средства защиты от вредоносных программ Malwarebytes.

К концу июля 2013 года суд вынес приговор. Всех четверых обвиняемых признали виновными. Врублевского и братьев Артимовичей приговорили каждого к двум с половиной годам колонии. Пермяков получил немного меньший срок - два года, поскольку помогал прокурорам в расследовании.

Михайлов сказал, что твёрдо убеждён: почти всё случившееся с Врублевским в связи с уголовным делом - его возбуждение, расследование, обвинение, суд и окончательный приговор - имело очень мало общего с отправлением правосудия в западном понимании, зато напрямую связано с его бывшим деловым партнёром Гусевым и, конкретнее, со взятками, которые Гусев заплатил российской ФСБ.

Он отмечает, что российский Уголовный кодекс и правовая система не особенно хорошо приспособлены к преследованию за многие высокотехнологичные преступления.

«Много лет назад, когда впервые возникла проблема взломов и киберпреступности, государство приняло закон, по которому незаконно получать несанкционированный доступ к компьютерной системе. А в этом деле обвинение утверждало, что, атаковав Assist [процессора кредитных карт Аэрофлота], хакеры фактически получили несанкционированный доступ к Аэрофлоту, поскольку смогли отключить обработку кредитных карт и его сайт», - сказал Михайлов.

«Нельзя посмотреть на это и сказать, что с правовой точки зрения здесь есть логика или смысл. Обвинению пришлось работать с тем, что у него было. Поэтому ему и предъявили это обвинение, хотя любой нормальный суд сразу отклонил бы его по целому ряду причин. Обвинение

действительно представило некоторые доказательства его связи с братьями Артимовичами. Но, похоже, значительная часть этих доказательств либо была сфальсифицирована, либо в деле не соблюдалась надлежащая правовая процедура».

Михайлов отметил, что 51 процент Аэрофлота принадлежит российскому государству и что нападение на этот государственный актив стало источником стыда и раздражения для многих представителей политической власти страны.

«Практика, когда компании в России используют коррумпированные правоохранительные органы, чтобы бороться друг с другом и отнимать долю рынка, очень распространена, - сказал он. - Но когда одна сторона готова платить крупные суммы или в деле участвуют политики, вся надлежащая процедура немедленно выбрасывается в окно. В таких обстоятельствах исход дела определяют политические связи и финансовые вопросы».

Михайлов сказал, что, по его мнению, Врублевский сильно недооценил серьёзность и силу дела, которое выстроили против него враги.

«Когда его первоначально выпустили из тюрьмы до суда, он попытался выиграть дело по существу, и это было большой ошибкой и с его стороны очень наивно, - сказал Михайлов. - Возможно, он чувствовал за кулисами финансовую поддержку благодаря своим прежним взяткам коррумпированным правоохранительным органам. К несчастью для него, Гусев в конце концов нашёл куда более мощное оружие для этого конфликта и получил преимущество. [Предоставить] $1,5 миллиона одним платежом - серьёзное усилие с его стороны даже по меркам российской коррупции. Я сильно сомневаюсь, что Врублевский потратил столько же, даже если учесть его прежние попытки разрешить проблему Fethard и последующий найм Мальцева начальником службы безопасности. Гусев выиграл войну или по крайней мере битву, значительно подняв ставки. Уверен, сейчас Врублевский с радостью заплатил бы вдвое больше за освобождение, но из его нынешнего положения договариваться намного труднее».

Михайлов предсказал, что Врублевский не проведёт в колонии так много времени, а если и отбудет полный срок, широкая известность заключённого может защитить его там.

«Паша богатый человек, или по крайней мере раньше был богатым. У него был дом в самом богатом районе за пределами Москвы. Ему по-прежнему принадлежит крупная доля ChronoPay. На его месте я бы продал всё, чтобы выйти. В России это относительно осуществимо, если только против тебя не работает ФСБ. Они управляют страной. Если кто-то в ФСБ взял $1,5 миллиона у Гусева, вероятно, деньги Паши они уже не примут. Но в пользу Врублевского работает другое обстоятельство. Его дело привлекло большое внимание, а значит, возможно, тюремная администрация будет за ним присматривать. О нём и об этом деле написаны сотни статей. Полагаю, тюрьма и российское правительство не хотят, чтобы такую публичную фигуру, как он, изнасиловали и порезали в тюрьме. Это плохая реклама».

Михайлов поспешил отметить, что он не апологет Врублевского, которого считает неизбежной мишенью кармического правосудия.

«По крайней мере это принесло кое-что положительное. Павел понёс ответственность за крошечную долю своих преступлений, - сказал Михайлов. - Его суд явно был мошенничеством, и надлежащая правовая процедура не соблюдалась. Но Паша выйдет из тюрьмы очень злым, вероятно, примерно через год. Он будет жаждать крови, и кто знает? Может быть, через несколько лет Гусев разделит ту же судьбу».

Многие предсказания Михайлова сбылись сразу на нескольких уровнях. Неясно, заплатил ли Врублевский за эту привилегию, но в июне 2014 года, отбыв менее года из назначенных двух с половиной лет, он был освобождён без каких-либо публичных объяснений, насколько мне удалось установить путём обширного исследования, и получил разрешение вернуться домой к семье в Москву.

Местные российские газеты предположили, что его выпустили из тюрьмы, потому что он понадобился государству. В ответ на американские санкции против России за финансирование и организацию пророссийских сепаратистов, вызывавших беспорядки и вооружённый конфликт на Украине, Visa и MasterCard в марте 2014 года прекратили обслуживать платежи клиентов как минимум двух ведущих российских банков. Президент России Владимир Путин ответил подписанием закона, требовавшего создать отечественную безналичную национальную платёжную систему в обход компаний кредитных карт. Закон также ввёл строгие новые требования для международных платёжных провайдеров, работавших в России.

В телефонном интервью вскоре после освобождения Врублевский сказал мне, что адвокаты строго запретили ему обсуждать дело. Он утверждал, что не знает, почему его освободили досрочно, но не думает, что это как-то связано с национальной платёжной системой.

«Наверное, потому, что я был хорошим пожарным», - сказал Врублевский, объяснив, что последние пять месяцев заключения добровольно работал пожарным в отдалённом посёлке вокруг колонии - бывшем угледобывающем районе Рязанской области России примерно в 200 километрах к юго-востоку от Москвы.

«Я видел вещи и места, которых люди видеть не должны, но видел и кое-что забавное, - сказал Врублевский в ответ на вопросы о тюремном сроке. - Я выхожу, а люди спрашивают меня о национальной платёжной системе, и я сижу и говорю: „Мужик, ты шутишь? Я могу довольно подробно рассказать, как поить коров водой из пожарной машины, но ничего не знаю о последних изменениях в федеральном законе!“»

Врублевский остаётся главным акционером ChronoPay, компании, которую он хочет продать как можно скорее. Когда я спросил, не опасается ли он, что недавний скандал и заключение помешают этим усилиям, Врублевский дал понять: всё, что не убило его и его компанию, лишь сделает их обоих сильнее.

«Вы считаете BMW хорошей машиной? Эта компания производила двигатели для немецких самолётов во Вторую мировую войну. Вот вам и ответ. Когда кто-то делает хороший продукт - а ChronoPay хороший продукт, - всё остальное вторично».

Гусев остаётся в изгнании за пределами России, где его сейчас разыскивают по уголовным обвинениям в ведении незаконного бизнеса в GlavMed и SpamIt. По словам Врублевского, он считает, что Гусев скрывается с семьёй где-то в Испании или Турции, но независимо подтвердить это не удалось. В любом случае, где бы Гусев ни находился сегодня, вряд ли в ближайшее время он будет путешествовать. В интервью 2011 года он сказал, что опасается: международная организация полицейских ведомств Интерпол может опубликовать уведомление о его аресте, если он решит пересечь европейские границы.

«Я ожидаю, что очень скоро могу оказаться в базе данных Интерпола, - сказал Гусев. - Я уже нахожусь в базе российской полиции, поэтому, к сожалению, не могу приехать в Россию. Уверен, Павел делает всё возможное, чтобы моё имя внесли в список Интерпола, и для меня может быть очень опасно лететь самолётом или пользоваться каким-нибудь транспортом через границу».

Кимберли Зенц, специалист по киберпреступности из компании Verisign iDefense в Рестоне, штат Вирджиния, годами следила за враждой. Она сказала, что считает Врублевского агрессором, которого погубили огромное эго и избыток необоснованной уверенности.

«Он любит внимание, а киберпреступники не должны любить внимание, - сказала Зенц. - Но так он может очень публично быть большим начальником и получать уважение за свою роль в подпольном сообществе».

Но, по словам Зенц, подорвать империю спама и мошеннических антивирусов Врублевского помогли и другие факторы.

«Он действительно оказался на неправильной стороне истории, - сказала Зенц. - Когда-то люди жаловались, что России нет дела до киберпреступности. И думаю, Павел неправильно понял, как далеко может зайти и что может атаковать. Та часть его личности, которая позволила ему вырастить ChronoPay именно так, как он это сделал, была той же частью, которая заставила его перейти границы, атаковать Assist и думать, что он может взяться за Гусева и ни с тем, ни с другим не возникнет никаких проблем».

Профессор UCSD Стефан Сэвидж сказал, что Врублевский казался одержимым постоянным изобретением всё новых и более грандиозных схем чёрных шляп.

«Чтобы понять, как он мог иметь эту законную компанию и всё равно хотеть накачать её фармой, поддельными антивирусами и всем прочим, нужно смотреть на него именно в таком свете, - сказал Сэвидж. - Он явно чувствовал потребность быть большим человеком. И несомненно, если посмотреть на его взаимодействие с другими людьми в ChronoPay - и на то, что он постоянно появлялся на европейских конференциях Visa по безопасности и мошенничеству, - ясно, что он видит себя фигурой больше жизни. Ему не нужно было делать всё это, чтобы иметь хороший уровень жизни. Он мог работать совершенно законно, хотя, возможно, делал то, что делал, ради поддержания определённого образа жизни. Но я также подозреваю, что отчасти дело было в его определённом круге общения среди киберпреступников, на которых он пытался произвести впечатление».

Но хотя фармацевтические войны, возможно, временно окончены, глобальная угроза спама сильнее, чем когда-либо. Гибель многих крупных спамерских партнёрских программ вроде SpamIt и Rx-Promotion совпала с заметным и более зловещим изменением способов монетизации киберпреступности. Начнём с того, что работа Сэвиджа, Microsoft и правообладателей брендов, сотрудничавших с Международной коалицией по борьбе с контрафактом (IACC), которая сильно повысила стоимость получения партнёрками услуг процессинга кредитных карт, фактически уничтожила значительную часть отрасли мошеннических антивирусов, или запугивающих программ, которую так заботливо взращивала ChronoPay. Но её место заняла куда более коварная угроза: программы-вымогатели.

Подобно запугивающим программам, программы-вымогатели чаще всего распространяются через взломанные или вредоносные сайты, эксплуатирующие уязвимости браузеров. Обычно эти мошеннические схемы выдают себя за Министерство внутренней безопасности или ФБР либо соответствующий федеральный следственный орган в стране жертвы и пытаются запугать людей, заставляя их платить штрафы, чтобы избежать преследования за якобы скачанные детскую порнографию и пиратские материалы.

Программа-вымогатель блокирует компьютер жертвы, пока та не заплатит выкуп или не найдёт способ удалить вредоносную программу. Всё чаще программы-вымогатели шифруют все файлы на компьютере жертвы и удерживают их ради выкупа, пока жертва не заплатит. Жертвам велят оплатить выкуп, купив предоплаченную дебетовую карту или денежный ваучер, которые продаются в магазинах у дома и торговых точках по всему миру. Затем жертве велят отправить нападавшим код ваучера или номер карты, позволяющий преступникам обменять эти сведения на наличные.

«Не думаю, что случайно мы наблюдаем подъём программ-вымогателей по мере того, как этим партнёрским программам становится труднее находить непрерывный поток банков, готовых помогать им обрабатывать карточные платежи за запугивающие программы, - сказал Сэвидж. - Есть множество людей, привыкших хорошо зарабатывать, для которых поддельные антивирусы и запугивающие программы стали проблематичными, а фарма в действительности не является вариантом. В экосистеме образовалась пустота, где люди могут зарабатывать. Совершенно не случайно эти схемы с программами-вымогателями, по существу, обходят традиционные платёжные системы».

За последние несколько лет также произошло заметное изменение в том, как ботмастеры используют имеющиеся ресурсы. По данным российской компании Kaspersky Lab, занимающейся антивирусами и безопасностью, к первому кварталу 2014 года доля спама в электронной почте упала до 66,3 процента, на 6,42 процентного пункта ниже предыдущего квартала. Но, чтобы компенсировать сокращение доходов от коммерческих почтовых посланий, многие злоумышленники всё чаще сдают ботнеты в аренду для рассылки вредоносных программ, представляющих гораздо более серьёзную угрозу для потребителей, особенно для тех из нас, кто никогда не открывает спам или нежелательные письма, не говоря уже о покупках через них.

Отличный пример - ботнет Rustock, который начал в 2007 году с продвижения схем накачки и сброса акций. Много лет он входил в число ведущих мировых рекламодателей аптечных сайтов, но за последние годы преступники во главе Rustock направили больше спамерских ресурсов на массовую рассылку вредоносных программ в тысяче обличий - от поддельных сообщений FedEx и UPS до фальшивых уведомлений об аудите от Налоговой службы США. В большинстве случаев эта крадущая пароли вредоносная программа нацелена на малые и средние предприятия Соединённых Штатов и Европы и стремится заразить компьютер человека, отвечающего за финансы организации. Получив его имя пользователя и пароль от банковского счёта организации, мошенники проводят поддельные банковские переводы со счёта жертвы на контролируемые ими счета.

По словам Гэри Уорнера из Алабамского университета в Бирмингеме, вредоносные программы, рассылаемые через спам Cutwail, действительно входят в число ведущих причин захвата корпоративных счетов. Эта всё более распространённая напасть киберпреступности ежегодно поражает тысячи малых предприятий и часто приводит к убыткам отдельных пострадавших организаций в сотни тысяч долларов.

Другое заметное изменение заключается в том, что киберпреступные предприниматели, управляющие собственными ботнетами, всё чаще стараются извлечь больше ценности из каждой заражённой системы, тщательно собирая скомпрометированные системы ничего не подозревающих пользователей и выискивая в них каждую крупицу личных данных, например пароли, лицензионные ключи программ и учётные записи социальных сетей, которые можно перепродать в киберподполье, сказал Сэвидж. Более того, теперь существует больше киберпреступных базаров, чем когда-либо, помогающих ботмастерам сбывать эти данные. Иными словами, вполне возможно, что прямо сейчас киберпреступник продаёт кому-то вашу личную информацию и получает за неё круглую сумму.

«Подобно тому как эскимосы-иннуиты старались использовать каждую часть кита, теперь мы наблюдаем эволюцию, в ходе которой ботмастеры тщательно разрабатывают заражённые системы и монетизируют найденные данные, - сказал Сэвидж. - Похоже, сегодняшняя мантра звучит так: „Зачем оставлять неиспользованные ресурсы на столе?“»

Пока одни используют программы-вымогатели и сбор данных, сказал Сэвидж, многие другие бывшие партнёры и руководители провалившихся партнёрок запугивающих программ, фармы и пиратского программного обеспечения ищут следующую большую возможность.

«Это период инноваций, и люди явно осматриваются в поисках другой золотой жилы, не хуже фармы, которая приносила больше денег и надёжнее всего остального, - сказал он. - Несколько партнёрских программ пытаются торговать пиратскими электронными книгами и фильмами; другие занялись [рекламой] займов до зарплаты. Теперь существует множество программ, которые пишут курсовые работы для студентов. Похоже, сейчас это большое дело».

Другой фактор, давящий на спамерскую отрасль, говорит Сэвидж, состоит в том, что многие партнёры добились большего успеха в рекламе сайтов с помощью так называемых методов «чёрного SEO», манипулирующих позициями их сайтов в поисковых системах. Он отмечает, что самым высокооплачиваемым участником среди тысяч аптечных партнёров GlavMed с огромным

отрывом был специалист по чёрному SEO под псевдонимом Webplanet. Похоже, этот предприимчивый молодой хакер заработал все свои деньги на манипулировании поисковыми системами.

«Сейчас ведётся много игр с [рекламным мошенничеством] или чёрным SEO, - сказал Сэвидж. - Пока многие из этих ребят становятся более разносторонними и переживают своего рода период перегруппировки. А та часть людей, которая успешно занимается аптечным спамом, либо отступает, либо говорит: „Да, придётся согласиться на меньшую прибыль или найти другую нишу“».

По прогнозу Сэвиджа, через два-три года интернет-фарма как отрасль умрёт.

«Останется несколько небольших партнёрских программ, но я сомневаюсь, что будут крупные программы вроде Rx-Promotion или GlavMed, - сказал Сэвидж. - Они просто привлекают слишком много внимания и давления со стороны карточных систем вроде Visa и MasterCard».

Комментарии Сэвиджа пугающе повторяют слова, которые я услышал от Игоря Гусева в нашем последнем интервью в середине 2011 года.

«Очень странно, что некоторым людям понадобилось провести столько дорогостоящих исследований, чтобы понять, что [самая] слабая часть этого бизнеса - обработка карт, - сказал Гусев. - Им нужно давить на карточных процессоров, этих чудовищ, которые регулируют [лишь] под очень сильным общественным давлением. Думаю, это был бы очень мощный удар, и интернет-фарма умерла бы за два года, если бы им как-то удалось отключить продавцов, связанных с интернет-фармой».

Гусев тоже размышлял, какой станет следующая большая партнёрка после гибели аптечных программ.

«Думаю, следующая большая возможность будет связана с видео, аудио и, возможно, социальными сетями, - сказал он. - Это будет какой-то сервис вроде того, что Google и Apple сейчас пытаются сделать с совместным доступом и загрузкой всех ваших MP3 и видео в веб-службу, чтобы вы могли обращаться к ним откуда угодно. Единственный вопрос - какую модель они будут использовать для выставления счетов и как люди станут за это платить».

Гусев сказал, что думает заняться консалтингом и консультировать интернет-партнёрские программы о том, как ориентироваться в бурных водах, населённых сомнительными процессорами кредитных карт и подозрительными банками, поддерживающими эти отрасли.

«Честно говоря, я присматриваюсь к этому бизнесу, - сказал Гусев. - С одной стороны, это довольно рискованно, потому что я хочу держаться как можно дальше от дел, способных привести к новому уголовному делу. Но, с другой стороны, я могу заработать немного денег, просто консультируя таких продавцов, если они согласятся платить какой-то процент за мой опыт, потому что банки жизненно важны для всего этого».

Большинство читателей этой книги, вероятно, никогда ничего не заказывали из рекламы в незапрошенной нежелательной почте и не принимали рецептурных лекарств неизвестного происхождения, заказанных в Интернете. Но существует бессчётное множество способов, которыми даже самые осторожные интернет-пользователи всё равно в конечном счёте поддерживают спамеров, мошенников и организованных киберворов. И почти все эти способы неизменно происходят из одной причины: безразличия.

Каким бы устройством мы ни пользовались для выхода в Интернет - работающим под управлением Microsoft Windows, Mac OS X, Linux или Android, - каждый из нас играет роль в противодействии интернет-мошенничеству или содействии ему. Поэтому все мы являемся либо частью проблемы, либо частью решения. Середины больше нет. Современные интернет-угрозы в полной мере используют людей, отстающих с обновлениями безопасности, а также тех, кто бездумно открывает незапрошенные вложения электронной почты и нажимает случайные ссылки в письмах или в

Facebook и Twitter, которые кажутся законными. Подробнее о том, что каждый из нас может сделать для борьбы со спамом и вредоносными программами и для лучшей защиты в Интернете, читайте в эпилоге, который следует сразу за этой главой.

Эпилог. Мир без спама: как защитить себя от киберпреступности

Многие из нас получали спамерское письмо от друга или близкого человека, а через несколько минут - его паническое сообщение о том, что учётную запись электронной почты взломали, с предупреждением не открывать и не отвечать ни на одно из писем злоумышленника. Безусловно, для многих пользователей это тревожная ситуация. Но куда страшнее другая истина: если современные киберворы захватят ваш почтовый ящик (или телефон, планшет, учётную запись Twitter или Instagram - вообще что угодно), извержение спама будет едва ли не самым безобидным из возможных последствий.

Настоящая ценность вашей учётной записи электронной почты для преступников заключается не только в способности качать спам или даже пересылать вредоносные программы и вирусы всему списку контактов. В зависимости от того, что вы делаете с учётной записью и как давно ею пользуетесь, ваш почтовый ящик может стоить намного больше, чем вы воображаете.

Например, зарегистрируйтесь в любой интернет-службе, и она почти наверняка потребует указать адрес электронной почты. Почти во всех случаях человек, контролирующий этот адрес, может сбросить пароль любой связанной службы или учётной записи - просто запросив письмо для сброса пароля. Ваш пенсионный фонд, банковский счёт или страховой план связан с этим почтовым ящиком? Получивший контроль над электронной почтой злоумышленник - с помощью фишинга или установки вредоносной программы на вашу систему - может просто зайти на сайты, управляющие этими счетами, запросить сброс пароля, нажать ссылку в письме и изменить ваши пароли (и начнёт он с пароля электронной почты)!

Даже если у захватившего ваш почтовый ящик человека нет времени или желания перехватить управление всеми связанными учётными записями, он, вероятно, знает, что эти записи имеют стоимость при перепродаже в киберпреступном подполье. Сколько стоят такие связанные учётные записи? Централизованной биржи взломанных учётных записей в подполье, конечно, нет, но некоторые представления дают недавние прейскуранты, опубликованные несколькими негодяями, торгующими скомпрометированными нефинансовыми учётными записями.

Например, несколько преступников в подполье продают украденные имена пользователей и пароли от работающих учётных записей на overstock.com, dell.com и walmart.com по два доллара за каждую. Другие продавцы торгуют учётными записями fedex.com и ups.com по пять долларов за штуку, а записи Apple iTunes - от восьми долларов. Учётные записи, к которым прилагаются данные доступа к связанным с каждым сайтом адресам электронной почты, могут стоить на доллар-два дороже.

Некоторые преступные магазины устанавливают ещё более низкие цены на взломанные учётные записи, беря всего по три доллара за активные записи на dell.com, overstock.com, walmart.com, tesco.com, bestbuy.com и target.com, если назвать лишь несколько. Это может показаться мелочью, едва ли стоящей усилий, но помните: преступники, занимающиеся такой деятельностью, очень часто управляют крупными ботнетами, а значит, могут одновременно собирать сведения с сотен и тысяч взломанных компьютеров.

Даже если ваша электронная почта не связана с интернет-магазинами, она, вероятно, подключена к другим важным для вас учётным записям. Взломанные почтовые записи используют не только для массовой рассылки мусора. Из них извлекают адреса ваших контактов, которых затем могут затопить вредоносными программами, спамом и фишинговыми атаками. Эти же контакты могут даже получить сообщение, где утверждается, что вы застряли без денег в чужой стране, и содержится просьба перевести куда-то деньги. Поверьте, бессчётное множество людей действительно откликаются на такие поддельные просьбы о помощи и переводят деньги прямо в

карманы киберворов.

Если вы покупали программы, вероятно, лицензионные ключи к ним хранятся где-то среди ваших электронных писем. Пользуетесь интернет-службами, или «облачными» хранилищами файлов, например Dropbox, Google Drive или Microsoft SkyDrive, для резервного копирования или хранения фотографий, файлов и музыки? Ключ, открывающий доступ к этим файлам, тоже лежит в вашем почтовом ящике.

И что хуже всего: если взломанную учётную запись веб-почты использовали как резервную для получения писем о сбросе пароля одной из других ваших учётных записей, угадайте, что произойдёт? Теперь нападавшие могут захватить обе записи.

Надеюсь, теперь ясно, что ради защиты почтового ящика от воров стоит принять некоторые меры предосторожности. К счастью, несколько простых советов и действий помогут сохранить контроль над учётной записью электронной почты, а также надёжно защитить систему, через которую вы к ней обращаетесь.

До недавнего времени некоторые крупнейшие поставщики интернет-услуг не предлагали почти никакой защиты, кроме требования ввести имя пользователя и пароль. Однако всё больше крупных поставщиков переходят к включению многофакторной аутентификации, чтобы помочь пользователям избегать захвата учётных записей. Gmail.com, Hotmail/Live.com и Yahoo.com теперь предлагают многоэтапную аутентификацию, которой пользователи могут и должны пользоваться для дополнительной защиты записей. Обычно она предполагает отправку числового кода в текстовом сообщении или приложении смартфона: этот код необходимо ввести вместе с именем пользователя и паролем. Код отправляется и запрашивается каждый раз при обнаружении подозрительного входа, например попытки войти с компьютера или интернет-адреса, обычно не связанного с вашей учётной записью.

Dropbox, Facebook и Twitter предлагают дополнительные варианты защиты учётной записи, не ограничиваясь советом выбирать надёжные пароли. Чтобы проверить, позволяет ли поставщик электронной почты, социальной сети или другой службы связи дополнить защиту учётной записи двухфакторной аутентификацией, посетите сайт twofactorauth.org. Если рядом с вашим поставщиком стоит галочка, нажмите значок в столбце «Docs» рядом с ним, чтобы открыть ссылку на инструкции по настройке и включению этой функции.

Парольное безумие

Включение двухфакторной аутентификации - хороший способ повысить безопасность учётной записи, но, если изначально вы полагаетесь на никудышные пароли, вы по-прежнему находитесь в опасности. Кроме того, двухфакторную защиту пока предлагает не каждая важная служба или сайт. Почти никто не любит пароли - иногда их так мучительно запоминать, - но, к сожалению, мы вынуждены пользоваться ими, пока не придумаем более надёжные и устойчивые ко взлому способы защиты информации.[1]

Вот несколько советов по созданию надёжных паролей. Уделите минуту изучению этих рекомендаций и инструментов и подумайте, не стоит ли усилить некоторые пароли, если они им не соответствуют.

Если вы похожи на меня - действительно ненавидите пароли, но понимаете, что жизнь слишком коротка, чтобы пытаться запомнить их сотни, - возможно, стоит подумать о менеджере паролей. Это компьютерные программы или интернет-службы, которые помогают пользователям не только выбирать и применять гораздо более надёжные пароли, но и лучше их защищать. Для хранения паролей они используют стойкое шифрование.

Если вам нужна помощь в выборе надёжных паролей, но вы не верите, что сможете запомнить столь загадочные и длинные варианты, как «#$DG3dcLqzil%&*wp», есть хорошая новость: менеджеры паролей созданы именно для этого. Почти все они встраиваются в браузер и получают и подставляют пароли при посещении сайта, для которого вы ранее попросили программу запомнить пароль. Вам потребуется лишь создать и запомнить один надёжный «мастер-пароль», который программа будет запрашивать при посещении одного из таких сайтов.

Среди наиболее популярных инструментов управления паролями - KeyPass, Password Safe и RoboForm. Ещё один отличный вариант - LastPass, который полностью работает в Интернете. (Он не требует установки специальной программы на компьютер, поэтому вы можете обращаться к паролям с любой машины, включая смартфон.)

Если вы предпочитаете самостоятельно выбирать пароли и управлять ими либо вам просто нужен действительно хороший мастер-пароль для менеджера паролей, вот несколько советов, позволяющих избежать никудышных паролей:

• Создавайте уникальные пароли, сочетающие слова, цифры, символы, прописные и строчные буквы.

• Не используйте имя пользователя сети в качестве пароля.

• Не используйте легко угадываемые пароли вроде «password» или «user».

• Не выбирайте пароли на основе сведений, которые могут быть не настолько конфиденциальны, как вы думаете: даты рождения, номера социального страхования или телефона, имён членов семьи или домашних животных либо чего-нибудь ещё, о чём вы пишете в социальных сетях. (Преступники тоже пользуются Facebook, Twitter и Instagram!)

• Не используйте слова, которые можно найти в словаре. Свободно доступные в Интернете инструменты взлома паролей часто поставляются со словарными списками, перебирающими тысячи распространённых имён и паролей. Если вам необходимо использовать словарные слова, попробуйте добавить к ним цифру, а также знак препинания в начале или конце слова (или и там и там!).

• Избегайте простых сочетаний соседних клавиш. Например, «qwerty», «asdzxc» и «123456» - ужасные пароли, которые взламываются элементарно.

• Некоторые из самых легко запоминаемых паролей вообще не являются словами: это наборы слов, образующие фразу или предложение, например первое предложение вашего любимого романа или первая строка хорошей шутки. Сложность полезна, но главное - длина. Когда-то выбор буквенно-цифрового пароля длиной от восьми до десяти символов считался вполне хорошей практикой. Сегодня хакерам и спамерам всё доступнее создание чрезвычайно мощных и быстрых инструментов взлома паролей, способных перебирать десятки миллионов возможных комбинаций паролей в секунду. Просто помните: каждый добавленный к паролю или парольной фразе символ на порядок усложняет атаку методом полного перебора.

• Не используйте один пароль на нескольких сайтах. Как правило, можно безопасно повторно применять один пароль на сайтах, которые не хранят конфиденциальные сведения о вас, например новостном сайте или дискуссионном форуме, при условии, что вы не используете этот пароль на конфиденциальных сайтах.

• Никогда не используйте пароль, выбранный для электронной почты, на каком-либо другом интернет-сайте. Если вы так сделаете, а сайт электронной торговли, где вы зарегистрированы, взломают, велика вероятность, что вскоре кто-то будет читать вашу почту.

• Что бы вы ни делали, не храните список паролей на компьютере в виде простого текста. Если компьютер взломают, это всё равно что вручить свою личность киберпреступникам. Мои взгляды на разумность письменного списка паролей со временем изменились. Я склонен согласиться со

специалистом по безопасности Брюсом Шнайером, который советует пользователям не беспокоиться о том, что они записывают пароли и кто-то случайно увидит их в реальной жизни. Только не храните эти сведения на виду. Самый безопасный способ запоминать пароли - составить список всех сайтов, для которых у вас есть пароль, и рядом с каждым записать имя пользователя и подсказку, имеющую смысл только для вас. Если вы забудете пароль, большинство сайтов пришлют его по электронной почте, если вы помните, с каким адресом регистрировались.

Поддерживайте актуальность

Никакие инструменты защиты учётных записей в мире не помешают захватить ваш почтовый ящик или запись Facebook, если компьютер скомпрометирует крадущая пароли вредоносная программа. Хотя антивирус и брандмауэр в системе помогают отражать угрозы, они далеко не панацея, а современные киберугрозы создаются так, чтобы избегать их обнаружения, особенно в критические первые двенадцать-двадцать четыре часа после массовой рассылки вредоносной программы через спам и ссылки в социальных сетях.

Важно понимать, что ключевой принцип защиты любой системы - концепция «эшелонированной обороны»: необходимо иметь несколько уровней безопасности и не полагаться чрезмерно на единственный подход или технологию, которая должна заблокировать все атаки. И угадайте, какой уровень важнее всех? Вы!

Запомните и соблюдайте «Три правила безопасности в Интернете» Кребса, и вы резко снизите вероятность передать компьютер или мобильное устройство преступникам. Коротко говоря:

• Правило 1: «Если вы этого не искали, не устанавливайте». Очень многие интернет-угрозы зависят от обмана пользователя, которого заставляют что-то сделать: нажать ссылку или вложение в письме либо установить специальный браузерный плагин или приложение. Обычно такие атаки принимают форму запугивающих программ или всплывающих окон поддельных антивирусов, которые пытаются напугать людей и заставить установить защитный сканер. Другие популярные мошеннические схемы показывают вам видео, но затем настаивают, что для просмотра содержимого необходимо установить специальный «кодек», видеоплеер или приложение. Устанавливайте программы, обновления программ или дополнения браузера только в том случае, если вы сами изначально их искали. А прежде чем что-либо устанавливать, полезно получить программу непосредственно из источника. Сайты вроде MajorGeeks.com и Download.com утверждают, что проверяют программы, предлагаемые для скачивания. Но, подобно тому как вы не стали бы покупать товар в Интернете без элементарного изучения его качества и характеристик и проверки, что это именно нужный товар, потратьте несколько минут на поиск и чтение комментариев и отзывов других пользователей программы, чтобы убедиться, что не соглашаетесь на большее, чем ожидали. Кроме того, не отвечайте непосредственно на почтовые уведомления, которые (якобы) пришли от Facebook, LinkedIn, Twitter, вашего банка или другого сайта, хранящего личные сведения. Вместо этого заходите на такие сайты через закладку браузера и управляйте социальными сетями таким способом. Одна случайно неверно набранная буква веб-адреса может привести на враждебный сайт, созданный для использования опечаток.

• Правило 2: «Если установили, обновляйте!» Да, важно поддерживать операционную систему в актуальном состоянии с последними исправлениями, например от Microsoft, Apple или Google, но безопасность компьютера также требует заботы о приложениях, работающих поверх операционной системы. Преступники постоянно атакуют уязвимости широко установленных программных продуктов, таких как Java, Adobe PDF Reader, Flash и QuickTime. Производители этих продуктов несколько раз в год выпускают обновления, исправляющие ошибки безопасности, поэтому важно как можно скорее обновлять их до последних версий. Некоторые продукты могут уведомлять

пользователей о новых обновлениях, но такие сообщения часто приходят через несколько дней или недель после выпуска исправлений. Прекрасный ресурс для всех, кого утомляют обновления, - Personal Software Inspector от Secunia, бесплатный инструмент, который периодически выполняет сканирование и предупреждает пользователей об устаревших защитных программах. Последнюю версию также можно настроить на автоматическое обновление таких продуктов. У FileHippo тоже есть хороший бесплатный инструмент проверки обновлений.

• Правило 3: «Если оно вам больше не нужно, удалите!» Мусор - враг быстрого компьютера. К сожалению, многие производители компьютеров поставляют машины с кучей раздутых программ, которыми большинство покупателей ни разу не пользуется. В дополнение к мусорным программам от производителя обычный пользователь за месяцы и годы устанавливает десятки программ и дополнений. В совокупности они могут отрицательно сказаться на быстродействии компьютера. Многие программы добавляют себя в список элементов, запускаемых при каждой перезагрузке, из-за чего перезапуск компьютера становится похож на наблюдение за сохнущей краской. Он длится вечность. И помните: чем больше установлено программ, тем больше времени нужно тратить на их обновление последними исправлениями безопасности.

Надеюсь, эти советы окажутся для вас полезными и своевременными. Дополнительные сведения о безопасности в Интернете, включая новости о последних угрозах, преступных схемах и ошибках программ, которые используют интернет-спамеры и мошенники, ищите на моём сайте KrebsOnSecurity.com. А когда окажетесь там, напишите мне через контактную форму на krebsonsecurity.com и расскажите, что вы думаете об этой книге.

Сноски

[1] [назад] Важно отметить, что для некоторых цифровых технологий и устройств разрабатываются улучшенные методы защиты и идентификации. Например, многие европейские банки встраивают в кредитные карты чипы, которые делают мошенническое использование карт более трудным и дорогостоящим. Эта технология постепенно внедряется и в Соединённых Штатах. Ещё одна заслуживающая упоминания недавняя мера безопасности - добавление на некоторые телефоны и ноутбуки технологии идентификации по отпечатку пальца для их блокировки и разблокировки. И, несомненно, впереди ещё многое.

Беседа с Брайаном Кребсом

Не могли бы вы немного подробнее рассказать о предыстории этой книги?

Великая писательница Тони Моррисон однажды сказала: «Если есть книга, которую вы хотите прочитать, но она ещё не написана, значит, вы должны её написать». Это довольно точно описывает происхождение этой книги, хотя в своём случае я, вероятно, немного изменил бы изречение: «Если есть книга, которую необходимо написать, и вы единственный, кто может это сделать, значит, вы должны написать эту книгу!» Благодаря тому, что два враждующих короля киберпреступности решили взломать друг друга и передать главные тайны противника мне и правоохранительным органам, у меня появилась уникальная возможность пригласить обычного человека в странный и несколько пугающий мир, которого прежде не видели даже опытные специалисты по киберпреступности.

Поскольку по образованию и опыту вы прежде всего журналист, что привело вас к теме кибербезопасности?

Хотя программистом как таковым я никогда не был, значительную часть детства я возился с компьютерами и текстовыми электронными досками объявлений - интернет-сообществами, существовавшими до современной Всемирной паутины. Я всерьёз заинтересовался кибербезопасностью в 2001 году, после того как китайские хакеры полностью захватили мою домашнюю сеть. После этого я стал несколько одержим изучением темы, и эта одержимость до сих пор окончательно меня не отпустила.

Каковы главные мотивы киберпреступников, представленных в «Спамерской нации»?

Их главные мотивы - те же слабости, которые вызывают большинство раздоров в жизни, включая жадность, жажду власти, месть и, возможно, прежде всего гордыню. Меня поразило, что столь многие люди, глубоко вовлечённые в распространение спама и вредоносных программ, вообще согласились со мной разговаривать, не говоря уже о подробном описании своего бизнеса. Но, как мы видим в книге, многие из них очень гордились своей работой и «достижениями».

Представители правоохранительных органов любят повторять несколько прописных истин о киберпреступности; чаще всего звучит утверждение, что современных киберпреступников больше не интересует слава и они выбирают богатство вместо известности. Но с моей точки зрения, хотя деньги и правда являются главным предметом забот большинства современных киберзлодеев, у большинства всё ещё огромное эго, которое им трудно держать в узде.

Какой главный урок вы извлекли из этого опыта?

Написание книги стало самым трудным и полезным опытом в моей профессиональной карьере. Великому мастеру Леонардо да Винчи приписывают слова: «Произведение искусства никогда не заканчивают, его лишь оставляют», - и это же стало самым трудным аспектом написания книги: найти мужество и уверенность, чтобы перестать её переделывать и объявить готовой к публикации (даже если тайно, глубоко внутри, голос всё ещё говорит: «Да, но уверен, мы ещё могли бы передвинуть это и добавить то, и...»).

Что вы хотели бы дать читателям «Спамерской нации»? Какие советы или уроки они должны вынести в первую очередь?

Я хотел бы, чтобы читатели лучше поняли, насколько сильно в повседневной продуктивности и благополучии зависят от компьютеров и других сетевых устройств, а также лучше разобрались, как не позволить ворам захватить их данные, личности и устройства.

Я хотел бы, чтобы читатели поняли: спам по-прежнему остаётся самым популярным и эффективным способом совершения и распространения киберпреступлений. Люди склонны считать проблему спама решённой благодаря спам-фильтрам и папкам нежелательной почты. И всё же нам постоянно напоминают, что крупнейшие взломы - от Target до JP Morgan - обычно начинаются с того, что кто-то открывает незапрошенное письмо.

Важно также, чтобы пользователи осознали настоящую ценность собственных компьютеров или почтовых ящиков. Преступники прекрасно знают, сколько стоят эти активы, а такой разрыв в осведомлённости ставит обычного потребителя в крайне невыгодное положение по сравнению с современными интернет-противниками.

Вам и вашей семье угрожали, вас пытались подкупить и даже атаковали различными способами спамеры и киберпреступники, которых вы разоблачаете, стараясь вывести их преступления на свет. Заставляли ли их действия вас задуматься о прекращении работы? Или они делают вас ещё решительнее в стремлении добиться справедливости?

Я никогда не думал оставить эту тему. Напротив, личные атаки, с которыми мы с семьёй боролись последние несколько лет, лишь укрепили мою решимость и дальше проливать свет на эту область и подтвердили правильность моего неизменного внимания к теме.

Что в своей работе о киберпреступности и кибербезопасности вы сделали бы так же? Что сделали бы иначе?

В школе я усерднее занимался бы математикой и естественными науками. У меня никогда не было большой склонности ни к одной из этих областей, но в сорок два года мне пригодилось бы больше навыков программирования и написания сценариев. К счастью, когда мне нужны такие навыки, обычно можно положиться на сеть источников, которые чрезвычайно охотно помогают, но я искренне хотел бы, чтобы эти способности давались естественнее. Я также начал бы учить русский

в более раннем возрасте; это открыло в моей журналистской работе гораздо больше возможностей и направлений, которые иначе были бы просто недоступны.

Вы всегда хотели быть журналистом-расследователем или начинали с другой профессии?

Да, с тех самых пор, как работал в редакции школьной газеты. Но формального журналистского образования у меня нет. Большую часть опыта я приобрёл на работе. До прихода в *The Washington Post* я занимал совершенно бесперспективную должность, которую абсолютно ненавидел. Мой тогдашний лучший друг помог мне устроиться в Post отвечать на телефонные звонки в отделе подписки, где обычно звонил клиент, не получивший утреннюю газету. Оттуда я «выпустился» на работу в редакции, где делил время между сортировкой почты и записью под диктовку сообщений репортёров с мест событий. К счастью, между такими звонками оставалось достаточно времени, и я часто предлагал идеи статей разным редакторам различных отделов газеты. В итоге я написал десятки статей почти для половины отделов, прежде чем получил официальную должность репортёра - в 1999 году в информационном агентстве, принадлежавшем *The Washington Post*.

Что самое трудное в вашей работе? В написании этой книги? А что приносит наибольшее удовлетворение?

Я глубоко верю в идею, что тяжёлый труд сам по себе является наградой. Хотя одни лишь упорная работа и дисциплина никогда не гарантируют успеха, это лучшие и самые надёжные пути к успеху из известных мне. Некоторые из лучших моих статей и крупнейших сенсаций появляются после недель или месяцев журналистской работы - нередко над материалами, которые в какой-то момент я почти бросил из-за чистого разочарования или изнеможения. Но я бы сказал, что именно это приносит наибольшее удовлетворение в моей работе: видеть, как материалы проходят весь путь от крошечного зерна догадки, идеи или сенсации, а через недели или месяцы получить награду, когда эта догадка, идея или сенсация превращается в статью, которая в итоге становится международной новостью.

Мне очень повезло, поскольку сама природа работы позволяет довольно регулярно видеть и испытывать передовые изменения. Кроме того, как независимый репортёр я главным образом отвечаю лишь перед собой и совершенно свободен сосредоточиться на освещении новостей, которыми никто другой не занимается, вместо постоянной погони за материалами, за которыми следят другие издания. Поэтому репортёрская сторона моей работы обычно намного увлекательнее и интереснее собственно написания, которое для меня, безусловно, труднее всего.

Когда я только начал работать репортёром в Post, один из моих первых редакторов, журналист старой школы, довольно резкий и прямолинейный, рявкнул, что восхищается моими репортёрскими навыками, но пишу я дерьмово (он употребил гораздо более красочное слово). Он попытался смягчить удар, сказав, что журналист в начале карьеры редко бывает одновременно отличным репортёром и превосходным автором; большинство, по его словам, вначале хороши в одном из этих умений и осваивают другое лишь со временем благодаря практике и внимательному наблюдению.

И всё же я научился получать удовольствие от процесса и куда более тяжёлой работы по написанию и описанию своих расследований и по-настоящему оценил итеративную природу ремесла, обретя больше терпения и дисциплины. Для меня самое большое удовлетворение в

написании приносит сознательный, порой неровный процесс, когда начинаешь с пустой страницы и один за другим собираешь все компоненты истории. В конечном счёте всё сводится к поиску лучшего способа сшить эти фрагменты в историю, которая удерживает интерес читателя и, будем надеяться, побуждает его вступить в разговор о ней. Именно это я и намеревался сделать с помощью этой книги.

Благодарности

Писатели обычно народ одинокий, но им редко удаётся создать приятное для чтения произведение объёма и сложности книги без огромной помощи и терпения друзей и коллег.

«Спамерская нация» была бы невозможна без помощи нескольких носителей русского языка, которые провели со мной бесчисленные часы, распутывая разговоры и связи между различными реальными персонажами этой книги. В частности, я хотел бы поблагодарить Алека Гельденберга, Алексея Михайлова и Максима Суханова за неустанную работу над переводом документов, писем и журналов чатов и за помощь в сведении фактов воедино.

За знания о хакерском подполье и его обитателях выражаю искреннюю благодарность Лоуренсу Болдуину, Адаму Дрейку, Алексу Холдену, Лэнсу Джеймсу, Джону О и Кимберли Зенц.

За помощь в извлечении закономерностей и смысла из эпических грузовиков данных я особенно признателен Деймону Маккою, Стефану Сэвиджу, Бретту Стоун-Гроссу, Гэри Уорнеру (и их армиям аспирантов).

Джо Менн и Миша Гленни поддержали меня и дали мудрые советы именно тогда, когда это было нужно. Если бы не многочасовая беседа с Роландом Доббинсом во время Снежного Армагеддона 2009 года, возможно, мне не хватило бы смелости самостоятельно стать независимым журналистом. Благодарность неопределённого характера также полагается Дж. Б. Снайдеру, замечательному человеку, который всегда делает именно то, что обещает.

За то, что я до сих пор остаюсь в физической и сетевой безопасности, я обязан нескольким людям больше, чем готов признать. Крис Бартон сохранял меня и мой сайт в Сети и подальше от неприятностей даже перед лицом зачастую сокрушительных атак. Group-IB и Kaspersky Lab сыграли важнейшую роль, прикрывая меня в Москве. Здесь, в Штатах, мне помогали различные неназванные сотрудники правоохранительных органов; спасибо вам всем.

И последнее, но не менее важное: я хотел бы поблагодарить постоянных читателей моего сайта KrebsOnSecurity.com за их ободрение, поддержку и вдохновение в последние пять лет. Без вас я не смог бы этого сделать.

Источники

Глава 1. Паразит

При исследовании автогонки, в которой погиб Коля McColo, оказалась полезной запись в блоге ThreatExpert (ныне принадлежит Symantec) за ноябрь 2008 года, как и новостное сообщение о происшествии, опубликованное в тот же день российским изданием «Российская газета» (ng.ru). Я также опирался на публикации форума Crutop.nu и утёкшие чаты в системе мгновенных сообщений между Ступиным и Игорем Гусевым, где обсуждалось, кто собирался присутствовать или присутствовал на похоронах McColo. Для сведений о Дмитрии Gugle Нечволоде я использовал интервью с Игорем Вишневским в системе мгновенных сообщений.

Глава 2. Пуленепробиваемый

Значительная часть справочных сведений о RBN была получена из российских и белорусских новостных источников, включая compromat.ru и *Transitions Online*, а также из документального фильма Виктора Чамковского «Операция „Консорциум“», текст которого по-прежнему доступен по адресу web.archive.org. Связь Александра Рубацкого с RBN также подтверждалась письмом российскому правительству от депутата Государственной думы Ильи Пономарёва. Раздел о похищении Петровского опирался на новостные источники и сообщения, включая *Ecommerce Journal* (web.archive.org) и белорусскую электронную газету «Дневник». Раздел о роли российского провайдера связи Eltel в RBN подтверждался статьёй *Russian Newsweek* 2009 года. По всей видимости, с тех пор Eltel купила Beeline, одна из крупнейших российских компаний мобильной связи.

Глава 3. Фармацевтические войны

Данные, подтверждающие утверждения о предполагаемой связи Врублевского с Red & Partners, впервые были опубликованы 31 июля 2009 года в статье *The Washington Post* «Следуя за деньгами: мошеннические антивирусные программы» (voices.washingtonpost.com). Я вернулся к этой истории в публикации на KrebsOnSecurity.com в мае 2010 года под названием «Следуя за деньгами, часть II» (krebsonsecurity.com).

Полученные из Торговой палаты Нидерландов открытые документы, относящиеся к Red & Partners и показывающие, как Игорь Гусев (DPNet) и Павел Врублевский (Red & Partners) совместно основали ChronoPay в 2003 году и стали равными акционерами, можно посмотреть в Интернете здесь: krebsonsecurity.com. (Примечание: это нидерландский документ, который был опубликован.)

Некоторым сведениям, составляющим эту главу, трудно указать точный источник. Например, хотя предполагается, что Гусев или тесно связанные с ним хакеры получили и обнародовали электронные письма, таблицы и записи телефонных разговоров ChronoPay за несколько лет, я не смог этого подтвердить. Как говорилось в главе, сведения анонимно передал источник под псевдонимом Boris. Однако генеральный директор ChronoPay Врублевский подтвердил, что документы действительно были украдены у ChronoPay. Данные о GlavMed и SpamIt, включая записи ICQ-чатов администратора GlavMed-SpamIt Дмитрия Ступина с коллегами и сотрудниками

(спамерами) за четыре года, были оплачены Врублевским и переданы автору и властям США.

Глава 4. Знакомство с покупателями

Эта глава почти целиком опиралась на интервью с людьми, покупавшими лекарства у GlavMed-SpamIt и Rx-Promotion. В ней также приведены цитаты и точки зрения из интернет-интервью с Игорем Вишневским, называвшим себя спамером и признававшим, что финансировал и перепродавал спамерский ботнет Cutwail. Я также использовал сведения из государственных источников, включая FDA (fda.gov). Кроме того, глава ссылается на несколько новостных сообщений о ценах на рецептурные лекарства в Соединённых Штатах. Среди них статья *Bloomberg.com* от 1 мая 2014 года «Цены на лекарства бросают вызов гравитации, удваиваясь для десятков препаратов». Исследование Tufts было опубликовано 18 ноября 2014 года под названием «Стоимость разработки нового лекарства и получения разрешения на его продажу составляет $2,6 миллиарда». Цифры FTC взяты из опубликованного ведомством 22 декабря 2014 года отчёта «Сотрудники FTC выпускают отчёт за 2013 финансовый год о патентных соглашениях производителей фирменных лекарств с конкурентами-дженериками».

Глава 5. Русская рулетка

Для начальной истории о смерти Марсии Бержерон я опирался на материал *Vancouver Sun* 2007 года. В качестве дополнительных справочных сведений об истории Бержерон я получил у властей Британской Колумбии копию заключения коронера.

Несколько фактов в этой главе ссылаются на статьи *The New York Times* или цитируют их. В разделе, подробно рассказывающем, как противоугревой препарат Accutane попал под действие новых правил безопасности Управления по контролю качества пищевых продуктов и лекарственных средств, использованы сведения из статьи Гардинера Харриса от августа 2005 года. Статья Харриса и Кэти Томас в *The New York Times* от апреля 2013 года помогла исследовать роль индийских аптек, производивших противолейкозный препарат Gleevec по значительно более низкой цене, чем западные фармацевтические компании.

Источником сведений об урегулировании на $500 миллионов, которое Google заключила с Министерством юстиции США из-за незаконного разрешения канадским интернет-аптекам рекламировать лекарства американским потребителям, стала статья Дэвида Голдмана на CNN. При обсуждении соглашения Pfizer с Министерством юстиции на $2,3 миллиарда использовались сведения из статьи Рона Уинслоу в *The Wall Street Journal*.

В этой главе упоминается происшествие, о котором незадолго до моего посещения Алабамского университета в Бирмингеме сообщали новости: случай так называемого «каннибала с дамбы», который, как сообщалось, жевал лицо бездомного после предполагаемого употребления солей для ванн. В то время лаборатория UAB исследовала химический состав вещества, которое власти считали солями для ванн. Но, как позднее сообщили CNN и другие издания, последующие токсикологические анализы застреленного полицией подозреваемого обнаружили не соли для ванн, а марихуану.

Глава также ссылается на исследование Merck. Оно никогда официально не публиковалось; в действительности ссылки относятся к интернет-разведданным, которые Merck собрала в 2009-2010 годах и предоставила по просьбе автора.

В разделе, где упоминается письмо FDA предполагаемому партнёру Врублевского в Rx-Promotion, имеется в виду письмо от 8 октября 2010 года, адресованное некоему Jorge Smark по адресу hellmanh@gmail.com. См. fda.gov.

Глава 6. Партнёр(к)и в (дез)организованной преступности

Главным источником вдохновения для этой главы стала основополагающая статья Дмитрия Самосейко из SophosLabs Canada о партнёрских программах «Партнёрка: что это и почему вас это должно волновать». Глава также в значительной мере опирается на данные, собранные исследователями Калифорнийского университета в Сан-Диего, Международного института компьютерных наук и Университета Джорджа Мейсона.

Глава 7. Знакомство со спамерами

Раздел, подробно описывающий возвышение называвшего себя спамером Игоря Вишневского, ссылается на статью Бретта Форреста в *Wired* от августа 2006 года «Грязная жизнь и скверная смерть российского короля спама», где также взято интервью у самого Вишневского. Часть сведений о ботнете Вишневского Cutwail, также известном как «0bulk Psyche Evolution», взята из статьи, представленной в марте 2011 года на четвёртом симпозиуме USENIX исследователями безопасности Бреттом Стоун-Гроссом, Торстеном Хольцем, Джанлукой Стрингини и Джованни Виньей, под названием «Подпольная экономика спама: взгляд ботмастера на координацию крупномасштабных спамерских кампаний».

Часть сведений о связи печально известного спамера Питера Северы с осуждённым спамером Аланом Ралски взята из сорокастраничного обвинительного заключения, поданного Министерством юстиции при преследовании Ралски. Необработанные данные о рассылочной мощности крупнейших спамерских ботнетов преимущественно взяты из отчётов Dell SecureWorks и M86 Security.

Глава 8. Старые друзья, заклятые враги

Обсуждение рейдерских атак на российские компании ссылается на статью Брендена Карбонелла, Дмитрия Фукса, Веры Кримнус, Эда Ма и Лизы Сафьян из выпуска 2010 года Института Лаудера Уортонской школы Пенсильванского университета от 20 апреля 2009 года под названием «Враждебные поглощения: русский стиль» (см. knowledge.wharton.upenn.edu). Раздел о Сколково, технологическом парке за пределами Москвы, который российские руководители представляли восточной Кремниевой долиной, опирался на статью Ингрид Лунден в *TechCrunch* от марта 2012 года. Кроме того, в главе использована статья *The New York Times* от октября 2010 года «Почтовый спам сокращается после российских репрессий».

Глава 9. Встреча в Москве

Раздел, объясняющий вероятную причину полицейского рейда на вечеринку Rx-Promotion, ссылается на серию полицейских облав на московские игорные заведения, красочно описанную в

феврале 2011 года российскими изданиями Svobodanews, РИА Новости и «Российская газета» (rg.ru).

В начале моего интервью с Врублевским он косвенно упоминает Саида Амирова, четырежды избиравшегося мэром столицы Дагестана. Для справочных сведений об аресте Амирова и продолжавшемся суде по предполагаемой торговле оружием я использовал материалы *The Moscow Times* и *Business FM Radio*.

Глава 10. Борцы со спамом

Сведения о доле спама в электронной почте во второй половине 2013 года взяты из статистики, опубликованной Kaspersky Lab в ноябре 2013 года в её блоге securelist.com. История атаки на Blue Security опирается на мои материалы об этом происшествии в *The Washington Post*. Раздел об атаках на Spamhaus в марте 2013 года ссылается на мартовские и апрельские статьи *The New York Times* о Свене Олафе Камфёйсе.

Глава 11. Ликвидация

Источником сведений о соглашении с признанием вины осуждённого спамера Олега Николаенко стала статья *Milwaukee Journal Sentinel* от марта 2013 года. Другие упоминания ликвидаций ботнетов и спамеров в этой главе опираются на мои собственные материалы об этих событиях на KrebsOnSecurity.com.

Глава 12. Эндшпиль

В начале главы используются сведения из статьи *The New York Times* об Игоре А. Артимовиче от сентября 2013 года «Интернет-атака позволяет заглянуть в спамерское логово». Российские издания «Ведомости», «Новая газета» и РИА Новости были незаменимы благодаря их сообщениям о запутанном суде над Врублевским.

По данным многочисленных российских изданий, Максим Пермяков был единственным из четырёх обвиняемых по делу Врублевского, кто признал свою роль в схеме: по просьбе Врублевского он нанял братьев Артимовичей для DDoS-атаки на Assist, компанию, напрямую конкурировавшую с фирмой Врублевского за выгодный контракт по обработке кредитных карт с крупнейшей российской авиакомпанией.

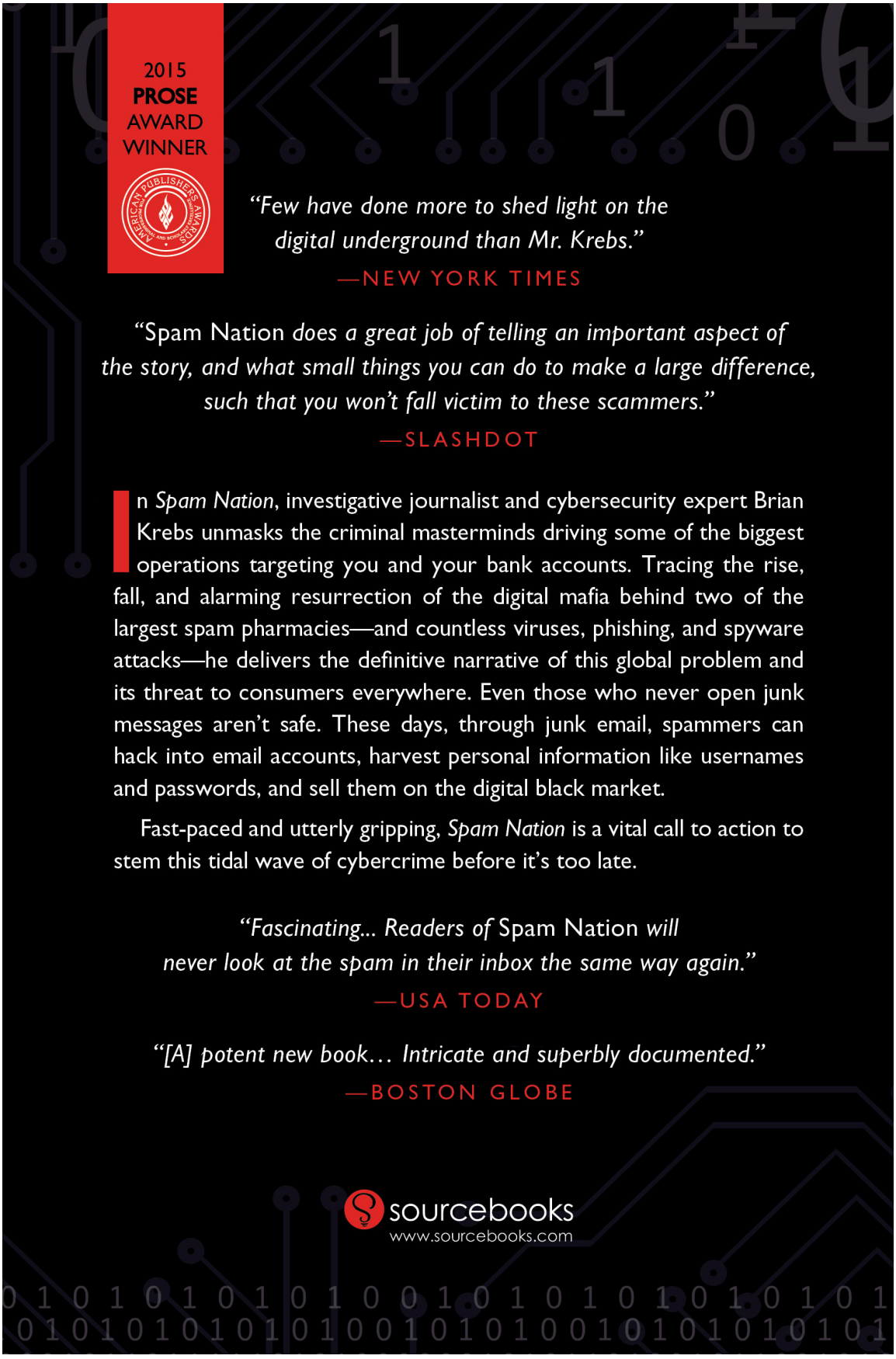
Об авторе

Фото: Кристоф Клерикс.

Брайан Кребс - редактор KrebsOnSecurity.com, ежедневного блога, посвящённого подробным новостям и расследованиям в области кибербезопасности. Третий год подряд судьи RSA Conference 2013 года, крупнейшего в мире собрания по компьютерной безопасности, называли KrebsOnSecurity.com блогом, лучше всего представляющим отрасль безопасности. KrebsOnSecurity также получил награду как самый образовательный блог о безопасности в 2013 и 2014 годах, а в 2013 году Кребс вместе со специалистом по безопасности Брюсом Шнайером был включён в Зал славы блогеров безопасности.

С 1995 по 2009 год Кребс работал репортёром *The Washington Post*, освещая для газеты и сайта безопасность в Интернете, технологическую политику, киберпреступность и вопросы конфиденциальности. Его статьи и расследования также публиковались в *Popular Mechanics*, *Wired.com*, *The Guardian*, *The Sydney Morning Herald* и многих других изданиях. Кребс окончил Университет Джорджа Мейсона в 1994 году со степенью бакалавра гуманитарных наук по международным отношениям.

Задняя обложка



Лауреат премии PROSE 2015 года

> «Мало кто сделал больше господина Кребса, чтобы пролить свет на цифровое подполье».
>
> - *The New York Times*

> «*„Спамерская нация“* великолепно рассказывает о важной стороне этой истории и о том, какие небольшие действия помогут вам добиться значительных перемен, чтобы не стать жертвой этих мошенников».
>
> - *Slashdot*

В «Спамерской нации» журналист-расследователь и специалист по кибербезопасности Брайан Кребс разоблачает преступных вдохновителей некоторых крупнейших операций, направленных против вас и ваших банковских счетов. Прослеживая возвышение, падение и тревожное возрождение цифровой мафии, стоящей за двумя крупнейшими спамерскими аптеками, а также за бесчисленными вирусами, фишинговыми атаками и атаками шпионских программ, он создаёт исчерпывающее повествование об этой глобальной проблеме и её угрозе потребителям повсюду. Даже те, кто никогда не открывает нежелательные сообщения, не находятся в безопасности. Сегодня с помощью нежелательной почты спамеры могут взламывать учётные записи электронной почты, собирать личные сведения, такие как имена пользователей и пароли, и продавать их на цифровом чёрном рынке.

Стремительная и невероятно захватывающая «Спамерская нация» - жизненно важный призыв к действию, чтобы остановить эту приливную волну киберпреступности, пока не стало слишком поздно.

> «Увлекательно... Читатели *„Спамерской нации“* больше никогда не будут смотреть на спам в своём почтовом ящике по-прежнему».
>
> - *USA Today*

> «Сильная новая книга... Сложная и великолепно документированная».
>
> - *The Boston Globe*

Sourcebooks
sourcebooks.com