Гайка Митич, Бойко Двачич

Вирьё моё!

Хроники невидимых хакерских войн от Сыктывкара до Сингапура

УДК 004.7
ББК 32.973.202
М66

Митич, Гайка.

М66 Вирьё моё! Хроники невидимых хакерских войн от Сыктывкара до Сингапура / Гайка Митич, Бойко Двачич. — Москва, 2025. — 320 с.

ISBN 978-5-6054442-9-9

Как остановить мировую эпидемию компьютерного червя, расследовать ограбление банка на миллиард долларов, поймать космических хакеров и обнаружить шпионские импланты спецслужб в айфонах топ-менеджеров. Первый производственный роман о жизни и работе российских специалистов по кибербезопасности.

УДК 004.7
ББК 32.973.202

ISBN 978-5-6054442-9-9

ОГЛАВЛЕНИЕ

ИНТРОДУКЦИЯ

Книги подобного рода принято начинать с пафосного эпиграфа. Что-нибудь глубокомысленное, французское. Но сколько мы ни бились, найти общую цитату для предисловия очень трудно. В голову лезет только всякая ерунда вроде: «Так много песен про баню спето, а мы споём ещё одну!»

Впрочем, для начала достаточно и этого. Ведь основная идея, сподвигнувшая нас на этот текст, очень проста — мы решили спеть песню, которую ещё никто не спел.

Один из авторов этой книги много лет занимался расследованием хитрых, масштабных, местами даже невероятных компьютерных преступлений, о которых вы наверняка ничего не знаете. Беспроводной червь заражает целый стадион зрительских мобильников со скоростью, превышающей скорость бегунов на этом стадионе. Злоумышленник выводит миллиард долларов из банка за несколько секунд, а потом теряет все деньги из-за нелепой грамматической ошибки. Отдыхающий в лесу на свадьбе аналитик находит вирус,

который вырубает заводы по обогащению урана. Агент самой мощной спецслужбы мира сливает в Интернет её шпионские секреты, поскольку ему дали некрасивый стол в офисе. Космические аппараты теряют связь из-за пацана, качавшего порнуху.

А вы, дорогие читатели, в это время видите на своём экране новость с заголовком «Сын известной певицы высказал своё мнение о дочери популярного актёра». Ну скучно же, правда?

Хотя нет, иногда вы видите новости о русских хакерах. О них есть множество публикаций и даже сериалов. Именно о русских. Это всегда удивляло второго автора данной книги. Как профессиональный журналист он много лет исследовал различные медийные феномены. Ему доводилось видеть, как мировая шумиха разворачивается вокруг полностью выдуманного события. Или наоборот — как огромное «слепое пятно» накрывает всё медиапространство, скрывая информацию об очень важных вещах.

Мем о русских хакерах — хороший предмет для подобного исследования, поскольку абсурдность этого мема сильно напоминает скетчи «Монти Пайтона» про вездесущую испанскую инквизицию. Судите сами: вокруг нас множество других стран, где не меньше компьютеров и айтишников, где бюджеты военных ведомств сильно превышают российский аналог, а количество спецслужб такое, что средний гражданин подобной страны даже не сможет перечислить их названия… Однако хакеры в новостях почему-то только русские. Ну может, ещё чуток китайских да северокорейских. И всё?

В общем, мы решили рассказать вам несколько историй о преступлениях и наказаниях, о шпионах и сыщиках, о королях и капусте невидимого кибермира. Для начала мы потренировались в более лёгком разговорном жанре — в подкасте. Но там многое приходилось упрощать. В итоге наш подкаст стал популярен у школьников и домохозяек и даже однажды попал на первое место в рейтинге Apple Podcasts в разделе «Технологии». Однако более продвинутые слушатели не раз намекали нам, что им «не хватает мяса». Так вот, в этой книге будет вам и белка, будет и свисток.

И самое главное: рассказывать об этом киберпанковском мире мы будем со стороны тех, кто занимается безопасностью, то есть защитой. Как ни парадоксально, эта сторона сетевого мира остаётся малоизвестной для большинства людей. Можно понять, почему флёр таинственности окружает другую сторону — преступникам надо скрываться. Это даёт отличную фору тем, кто о них пишет: тут всегда легко создать детективное напряжение, эдакую загадочность. Даже приврать можно, никто не будет особо опровергать. Именно так устроены почти все книги о хакерах.

Сторона защиты, по идее, должна быть более открытой. Но не тут-то было! На этой стороне полно своих недомолвок или просто забытых фактов, из-за чего возникает множество смешных (а иногда печальных или попросту вредных) стереотипов. И мы надеемся, что наш «репортаж с передовой» порвёт некоторые шаблоны представлений о работе ибэшников. Эти совы не то, чем кажутся. Это вообще не совы, а совсем другие дятлы.

Стоит сразу предупредить, что эта книга — не про бизнес. Об айтишном бизнесе написана уже куча книг. Но все эти коммерческие «истории успеха» очень похожи и в первую очередь заставляют задуматься о явлении под названием «ошибка выжившего». Множество компаний, строивших бизнес по сходным принципам, не превратились в Apple и Microsoft. А потому сложно поверить, что победителям помогли именно те факторы, которые задним числом описывает сам победитель. Может, там вообще случайность помогла гораздо больше?

Но мы не будем лезть в такие дебри. Эта книга — не о бренде, а о профессии. Мы просто покажем вам, как эволюционируют цифровые угрозы, как работают с ними аналитики и создатели защитных решений и что получается в итоге.

В прошлом такой жанр называли «производственным романом». Их часто писали в те времена, когда наша страна умела всё производить самостоятельно. Сейчас кибербезопасность — одна из немногих сфер, где у нас осталось собственное производство продуктов и сервисов мирового уровня. Вот про эту работу мы и расскажем. А о том, как продавать библии и пылесосы, вам расскажет кто-нибудь другой.

И конечно, придётся сразу разочаровать тех, кто ожидает увидеть в этой книге скандальный компромат. Нет, истории про безопасность всё-таки предполагают аккуратное обращение с информацией. Поэтому некоторые герои здесь останутся вообще без имён. Можно было бы ещё добавить стандартную фразу «все персонажи и события вымышлены», хотя это звучит нелепо даже в художественных

фильмах. Ну представьте, идёт такая молодая Анджелина Джоли по Нью-Йорку. Сама она, конечно, играет вымышленного персонажа из фильма «Хакеры» — но город Нью-Йорк вокруг вполне настоящий, его дожди и его автомобили не вымышлены!

Короче, наших героев мы слегка загримировали, но оставили максимум реальных исторических и технических деталей. Некоторые факты даже можно проверить: пруфные ссылочки собраны в конце книги. Главное, чтобы за деталями вы не потеряли общую картину. Надеемся, что мы и сами её не потеряли в этом хаосе, который называется «цифровая жизнь».

И большое спасибо всем, кто помогал нам с подготовкой текста и публикацией этой книги. Называть их поимённо не будем, поскольку мы и сами здесь — под псевдонимами. В общем, всем спасибо, и поехали!

ГЛАВА 1

ОПЕРАТОР ТАРЕЛКИ

Хмурым ноябрьским утром 2002 года худощавый молодой человек вышел из прокуренного тамбура поезда «Сыктывкар — Москва», купил на вокзале пару пирожков с котятами, а потом спустился в метро и поехал на станцию «Сходненская».

Целью его поездки было здание на улице Героев Панфиловцев, напоминающее большой старинный дисплей — вроде тех вокзальных табло, на которых показывают расписание прибытия поездов. В советское время в этом доме-дисплее располагался Научно-исследовательский институт радиофизики имени академика А. А. Расплетина, а занимались там разработкой «воздушно-космических средств ведения разведки СССР», то есть различных секретных антенн, локаторов и радаров.

Приехавший туда молодой человек (назовём его Сашей) тоже был не чужд радиофизики. У себя в Сыктывкаре он уже

четыре года работал «оператором спутниковой станции связи», через которую Сыктывкар был подключён к мировому Интернету. Оптоволоконные кабели в то время ещё не дотянули свои светящиеся щупальца до Крайнего Севера, и первый частный интернет-провайдер в Республике Коми раздавал доступ, полученный через спутник.

А это означало, что Саше как администратору узла связи нужно было не только подключать непонятливых клиентов, но и заниматься настройкой пятиметровой тарелки. Хотя тарелка умела автоматически поворачиваться за спутником, но иногда косячила. Такое бывало, когда солнце заходило за спутник и солнечная «засветка» обманывала тарелку — антенна начинала двигаться вслед за солнцем, а не за спутником.

В других случаях мешали иные явления природы: поскольку зима в Сыктывкаре длится девять месяцев, тарелку частенько заносило снегом и замораживало. Тогда оператору приходилось надевать тулуп и валенки и, выходя на 30-градусный мороз, орудовать метлой и ломом, добиваясь связи с космосом. Шапку-ушанку мы не упоминаем здесь только потому, что это слишком напоминало бы американские фильмы про русских космонавтов. Про это тоже будет, но позже.

В общем, можно было бы предположить, что худощавый молодой человек приехал в институт радиофизики ради обмена опытом. Скажем, чтобы с помощью коллег-специалистов по антеннам научить свою спутниковую тарелку не бегать за солнцем или даже самоочищаться от снега и льда.

Но нет, дорогой читатель, ты не угадал. Саша приехал в Москву не ради космической связи, а из-за своего странного хобби.

Он коллекционировал компьютерные вирусы.

# # #

На этом месте в художественном фильме, скорее всего, последовала бы серия флешбэков. Так киношники пытаются показать зрителю поворотный момент из прошлого, когда герой якобы осознаёт своё призвание.

В нашем случае можно было бы показать, как в 1988 году Саша, будучи учеником пятого класса, впервые видит в игровом салоне персональный компьютер (клон ZX Spectrum) с компьютерными играми. Затем действие перескакивает в восьмой класс, когда в школе начинается профориентация. Раз в неделю ученикам нужно ездить в общегородской УПК, чтобы научиться чему-то более полезному, чем спряжения глаголов. Все нормальные одноклассники Саши, конечно же, увлекаются перспективной профессией водителя грузовика. А Саша вместо этого замечает, что в УПК есть компьютерный класс, единственный на весь город.

К тому времени он уже является жадным читателем журналов «Техника — молодёжи» и «Наука и жизнь», где пишут про компьютеры и программирование. Плюс у него за спиной, как мы помним, незабываемая встреча с компьютерными играми в пятом классе. Поэтому он идёт изучать язык программирования MSX Basic на персоналках Yamaha MSX

с чёрно-зелёными дисплеями (цветной только у преподавателя). Когда короткое занятие заканчивается, Саша не успокаивается и пишет дома программы в тетрадке, чтобы на следующем занятии погонять их на «Ямахе». В итоге он создаёт свою первую игру, где на экране изображена карта Средиземного моря античных времён, а по ней передвигаются корабли пиратов.

Античность тут неслучайна. Чтобы адепты компьютерных игр не присваивали себе все заслуги просвещения, а сценаристы будущего не облегчали себе задачу слишком банальным флешбэком, нужно сообщить, что Саша в этот период гораздо больше увлекается историей и географией. (На этом месте в фильме должна зазвучать песня Виктора Цоя со словами: «Саша очень любит книги про героев и про месть».) В общем, парень действительно много думает про Древний Рим. И по окончании школы идёт поступать на исторический факультет местного университета. Но для поступления ему не хватает одного балла.

Может, здесь и произошёл основной поворот судьбы? Дело в том, что в старших классах школы, вслед за появлением предмета «Информатика», ученики должны были пройти производственную практику-стажировку. А у Саши к тому времени уже было четыре года опыта в программировании. Поэтому двоюродный брат Саши, начальник литейного цеха на Сыктывкарском машиностроительном заводе, предложил ему пройти стажировку в литейном цеху, где уже началась компьютеризация: там поставили три персоналки. В основном их использовали как дополнение к принтеру, то есть вели на них небольшой документооборот и печатали приказы.

Итак, после неудачи с историческим факультетом Саша отправляется работать в литейный цех, где до этого проходил стажировку. Но теперь он идёт туда с настоящей должностью «оператора ЭВМ второго разряда» (как получить первый, никто на заводе не знал). Компьютерный парк постепенно растёт и апгрейдится, появляется новый софт для бухгалтеров и проектировщиков. Вместе с одним из коллег Саша пишет скрипты для создания чертежей в AutoCAD и даже придумывает навороченную защиту от копирования для своего первого продукта — это библиотека полезных расширений AutoCAD для машиностроения.

Тем временем, то есть в 1995 году, в Сыктывкаре появляется тот самый Интернет, который через спутниковую тарелку. Появляется он, что характерно, не у телеком-операторов, а на местной фабрике нетканых материалов «Комитекс». Зародившийся в нетканых материалах провайдер в свою очередь начинает подключать местные учебные заведения. Среди них — и тот университет, в который Саша так и не поступил. Но теперь он попадает туда другим путём: это его вторая работа, администрирование узла связи. Здесь он и сам знакомится с Интернетом, летающим через спутник.

Но где же тут поворот? Вроде пока ничего особенного: тысячи людей в это время становятся админами-эникейщиками первых компьютерных сетей, читают сетевые конференции провайдера «Релком», бродят по первым русским сайтам и даже начинают делать свои.

Что ж, добавим ещё один флешбэк. В конце 1995 года в литейном цехе, где Саша продолжает работать параллельно с университетом, ставят новые компьютеры — и новые

программы. Не будем долго рассказывать, где в те времена брали софт, сократим до самой сути: где попало. И Саша решает проверить установленные программы антивирусом.

Раньше эта рутинная процедура не вызывала никакой реакции. Видимо, потому, что антивирус тоже был какой попало. Но на этот раз Саша использует новый Dr.Web и получает бесконечный экран красных строчек: все компы заражены. Вирус называется Natas.4744.

Надо представить себе шок нашего героя. До этого он читал про вирусы только в журналах, но то были просто переводные страшилки про другие страны вроде историй о гигантских крысах в сточных коллекторах Нью-Йорка. А здесь вирус прямо перед глазами — и пришёл он с дискеты, которую принесли из головного офиса завода!

Последовавшая за этим прогулка Саши через 16 цехов кончается аналогичным шоком у коллег-айтишников в головном офисе. Оказывается, там тоже всё заражено, и не одним только «Натасом».

К чести айтишников, надо признать, что их раздолбайство в те времена имело свои оправдания. Большинство первых вирусов были просто экспериментами, зачастую они не делали ничего серьёзного. Тот же Natas (перевёрнутое слово Satan), написанный в 1992 году 18-летним парнем из Калифорнии, в принципе умел форматировать диск заражаемого компа. Но делал он это не всегда, а только с вероятностью 1/512. Так что у жертв было время, чтобы этот вирус найти и вычистить. Да и чистить было несложно: вирусную дописку в заражённом файле можно было легко увидеть в редакторе кода.