Гайка Митич, Бойко Двачич

Вирьё моё!

Хроники невидимых хакерских войн от Сыктывкара до Сингапура

Гайка Митич Бойко Двачич

Вирьё моё! Хроники невидимых хакерских войн от Сыктывкара до Сингапура

«Автор»
2026

Бойко Двачич Г.

Вирьё моё! Хроники невидимых хакерских войн от Сыктывкара до Сингапура / Г. Бойко Двачич — «Автор», 2026

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.«Иронично и грамотно авторы вовлекают нас в темные глубины цифрового леса, где переплетаются высокие технологии и низкие замыслы, и только взгляд опытного специалиста по безопасности дает шанс разобраться — как на самом деле начинались и развивались самые значимые атаки». — Андрей «КиберДед» Масалович.«Книги о хакерах выходят каждый год. Гораздо реже пишут о тех, кто защищает нас от хакеров. Кажется, это первая книга, авторы которой решили раскрыть профессию вирусного аналитика со всех сторон, включая многие малоизвестные детали. Получилось весело, ностальгично и хочется снова реверсить!» — Евгений Касперский, путешественник и блогер.

Содержание

Гайка Митич Бойко Двачич
Вирьё моё! Хроники невидимых хакерских войн от Сыктывкара до Сингапура

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. Там же, в конце, мы добавили небольшой словарь с разъяснением профессиональных терминов, которые используются в тексте.

Ну и последнее, что осталось сказать в предисловии: 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.

А вот когда Саше встретился OneHalf, это было похуже. При каждой загрузке заражённой машины этот вирус шифровал две дорожки на жёстком диске, но затем временно расшифровывал их, когда к ним обращались какие-то процессы. Таким образом, деятельность вируса оставалась незамеченной, и он продолжал шифровать диск с каждым запуском. И раскрывал своё присутствие только тогда, когда была зашифрована половина диска — тогда вирус выводил сообщение: «Dis is one half. Press any key to continue …»

Как лечить от такой заразы? Если просто удалить вирус и почистить главную загрузочную запись, диск останется зашифрованным! Имевшийся у Саши антивирус Dr.Web с этим не справлялся. В поисках средства борьбы Саша нашёл в Интернете ещё один отечественный антивирус, который назывался всего тремя буквами. Этот лечил корректно.

Теперь у «оператора ЭВМ» было уже две дискеты с антивирусами. Посещая другие организации с компьютерами, он и там проводил свои исследования. Коллекция вирусов росла. Одновременно собиралась статистика и аналитика — где какой заразы больше, как она распространяется и чем лечится.

Стало ясно, что в компьютерных сетях кипит своя жизнь, которая мало кому видна. И наш герой не на шутку увлёкся этой жизнью.

# # #

В современной российской системе образования есть модная болезнь, которая называется soft skills. На самом деле болезнь гораздо более общая, и состоит она в том, что популярные западные концепции перетаскиваются к нам совершенно бездумно. И даже без вменяемого перевода на русский язык, что и выдаёт бездумных копировщиков.

На многих мероприятиях, где обсуждаются перспективные профессии будущего, вы обязательно услышите про важность навыков коммуникации: умение проводить публичные выступления, вести переговоры, организовывать командную работу. Всё это и называют soft skills. В результате моды на эти навыки многие IT-компании сейчас страдают от переизбытка эффективных менеджеров, которые умеют красиво болтать — и не умеют ничего другого.

Однако в 90-е годы в России наблюдался сильный перекос в другую сторону: зарождающийся бизнес и вправду не умел общаться. Особенно это было заметно в IT-сфере, поскольку люди технического склада, мягко говоря, не отличаются повышенной коммуникабельностью.

Как это связано с нашим героем? В доморощенных исследованиях Саши часто попадались вирусы, которые не детектировались. Иногда антивирус отмечал файл как «подозрительный» на основе некоторых эвристик (набора признаков, характерных для вирусов), однако не мог точно опознать эту заразу. А бывало и так, что антивирус не видел ничего подозрительного, зато сам Саша видел что-то странное в коде. Логично было отослать такой файл (сэмпл) в

какую-нибудь вирусную лабораторию, чтобы там его разобрали и классифицировали как следует.

Здесь и обнаружилась заметная разница в коммуникативных скилах у тех, кто сидел в вирлабах. Создатель Dr.Web не отвечал на Сашины письма. Вообще никогда. А вот автор антивируса со второй дискеты отвечал на каждое сообщение очень обстоятельно.

Из такого общения в сетевой конференции relcom.comp.virus выросло сообщество NF (Network Friends), состоявшее из таких же региональных активистов, которые собирали вирусы у себя в глубинке и обменивались информацией. В 1998 году они даже стали выпускать собственный электронный журнал «Земский Фершал», где публиковали свои вирусные находки, статистику и странный фольклор, понятный только посвящённым [1]:

— Удивляюсь я всё-таки тому, как много жёсткого диска жрёт отец Вындоуз! — говорил за завтраком командир Нортон.

— Чему удивляться, когда у него солитёр, — в тон ему отвечал товарищ Комманд Ком.

Товарищ Комманд Ком жил на системной дискете и вёл беспорядочную жизнь, отчего и страдал. Заразившись, он шёл к доктору Аидстесту. Посадил доктор Аидстест товарища Кома в высокое кресло, взял его за нижнюю челюсть:

— А теперь, — говорит, — скажи: «Формат а-а-а-а:».

В том же сетевом сообществе обитали и представители компании, выпустившей антивирус с названием из трёх букв. Сначала они предложили Саше стать российским представителем в проекте Wild List. В этой международной рассылке собирали статистику по вирусным эпидемиям из разных стран, а у сетевого сообщества NF таких данных по России было даже больше, чем у антивирусной компании. Ведь компания знала только то, что им присылали на анализ. А региональные энтузиасты отслеживали подпольную компьютерную жизнь во всём её диком многообразии на местах.

Через некоторое время Сашу, как и многих других парней из этого сетевого сообщества, позвали на работу в Москву. Так он и оказался в здании института радиофизики — но совсем не из-за спутниковой тарелки.

На входе его встретили суровые бабушки-охранницы, свора бездомных собак и турникеты со старинными металлическими пропусками. Но внутри, в высоких цехах бывшего советского НИИ, шло уже другое кино, с евроремонтом и пальмами в кадушках.

Впрочем, зубры из вирлаба, встретившие Сашу на собеседовании, тоже были суровы. «Имел дело с дизассемблером? А в кернелах сидел?» Они задавали много странных вопросов, на которые он не знал ответа.

А потом пришёл Главный. Спросил:

— Сколько лет?

— Двадцать шесть.

— Женат?

— Да.

— Сколько лет?

— Женат или жене?

— Ха-ха! Годится!

Вечером ему позвонили в гостиницу и сказали, что он принят. Оставалось только съездить в Сыктывкар и сдать там все дела. И последний раз почистить спутниковую тарелку от снега.

Глава 2. ПИЦЦА С ЧЕРВЯМИ

«В будущем каждый станет всемирно известным на 15 минут». Эту цитату приписывают Энди Уорхолу — но кажется, он никогда такого не говорил.

Согласно одной из версий, осенью 1967 года Понтус Хультен, директор шведского музея Moderna Museet, попросил журналиста Олле Граната помочь с подготовкой выставки Уорхола. Используя переданные ему тексты Уорхола, Гранат должен был написать программу выставки. Директор музея также просил использовать в программе ту самую цитату про 15 минут славы. Гранат возразил, что в материалах Уорхола таких слов нет. На что Хультен ответил: «Даже если он этого не говорил, он вполне мог бы так сказать. Давай так и напишем».

А по версии фотографа Ната Финкельштейна, эту фразу помог закончить Уорхолу сам Финкельштейн в 1966 году, когда снимал художника на улице. Собралась толпа, все пытались попасть в кадр со знаменитостью, и Уорхол якобы заметил тогда, что все хотят прославиться. А фотограф якобы добавил: «Да, примерно на пятнадцать минут, Энди».

Так или иначе, в 2002 году американский эксперт по безопасности Николас Уивер в своём выступлении на конференции Usenix использовал цитату «In the future, everyone will be world-famous for 15 minutes» для описания гипотетического компьютерного червя, который способен распространяться с максимально возможной скоростью, и за 15 минут заразить все уязвимые системы в Интернете. Концепция основывалась на примерах червей CodeRed и Nimda, которые уже в 2001 году вызвали заметные эпидемии, хотя и не мирового масштаба.

Мрачное предсказание Уивера про 15-минутное заражение всей планеты назвали «червём Уорхола» (Warhol worm). И кое-кто решил воплотить эту идею в жизнь. Попутно этот человек опроверг концепцию другого художника, Бэнкси: «В будущем каждый получит 15 минут анонимности». Нет, этот человек получил гораздо больше анонимности — он до сих пор не найден.

# # #

В 2002 году вирлаб, куда попал Саша, состоит из четырёх вирусных аналитиков и Главного. Эти пятеро — первая линия обороны. Их задача — «долбить вирьё». Из-за постоянного стука по клавиатурам Главный окрестил их «дятлами». Прозвище прижилось и даже полюбилось, кто-то наклеил на дверь вирлаба картинку с дятлом Вуди, а сегмент сети так и назвали — woodpeckers.

Работа вирусной лаборатории заключается в ручном разборе тысяч писем, приходящих от пользователей со всего мира. Письма попадают на первоначальный анализ либо к Главному, либо к дежурному аналитику.

Часть писем сразу отсеивается как ложные срабатывания или как уже известные вредоносы. А вот остальные сообщения дежурный должен проанализировать сразу либо перенаправить другому аналитику согласно специализации. Кто-то лучше разбирается в бэкдорах (средства для скрытого дистанционного доступа), кто-то в кейлогерах (клавиатурные шпионы), а кто-то в макровирусах (используют для размножения макроязык документов MS Office).

По-английски работа такого аналитика называется reverse engineering, что часто переводится корявым выражением «обратная разработка». С переводами у наших айтишников вообще туго. Ну что делать, не филологи. Просто берут подстрочник каждого слова и склеивают вместе. Получаются такие удивительные франкенштейны, как «лужи данных» или «наводнение греха». Или вот совсем парадоксальное выражение: «Вредоносная полезная нагрузка». С другой стороны, если все свои понимают — какая разница?

Суть реверса — прогнать бинарный файл через дизассемблер, восстанавливая команды на языке ассемблера. А затем по этим кодам разобраться в логике работы вредоносной проги. Ну и заодно понять, по каким признакам можно автоматически детектировать эту заразу и как от неё лечить.

А вирусописатели, конечно же, стараются зашифровать эту логику, используя специальные упаковщики-протекторы. Если аналитик видит, что код подвергся такой маскировке, он передаёт заразу в специальный отдел, где работают криптографы. Они умеют снимать протекторы и распаковывать архивы. Они же разбирают различные форматы файлов. Например, Microsoft Office работает с файлами формата OLE. Если в такой файл встроен вредоносный макрос, нужно найти в файле соответствующий блок с этим макросом и вернуть его на обработку аналитику.

Самая жесть — работа по выходным, когда на дежурство заступает один аналитик. Задача дежурного в выходной: по возможности разобрать весь поступающий поток самостоятельно, без перебрасывания писем на других экспертов, ведь они смогут начать работу только с понедельника. И хотя Главный почти всегда работает в эти дни, у него бывают командировки. В такую смену прикрыть тебя некому.

Полтора месяца обучения Саши пролетели очень быстро, пришёл и его черёд заступать на смену в субботу. Это случилось 25 января 2003 года. В те дни вирлаб добавлял в антивирусные базы около 500 новых угроз за неделю. Примерно по сотне на аналитика, хотя Главный иногда работал за троих. Выходило так, что за субботнюю смену Саше надо обработать штук 50. Примерно по десятку в час, 5–6 минут на один вирус. Нормальный график для опытного аналитика, но для первого раза очень стрёмно.

Саша начал с того, на чём специализировался: с макровирусов и скриптовых вирусов. К 2003 году их популярность уже падала, но они до сих пор составляли до половины входящего потока в вирлабе. На слуху была ещё история про почтового червя «Анна Курникова», который предлагал пользователям посмотреть эротические фотки известной теннисистки, но вместо фоток запускал скрипт на Visual Basic, пересылая себя по всем контактам в адресной книге жертвы. Похожий вирус Love Letter использовал более универсальную заманuху: в заголовке письма было написано просто «I love you». Мало кто мог устоять против такого признания.

Ещё веселее работал почтовый червь SirCam, разлетевшийся по миру летом 2001 года. Если человек открывал вложение письма, вредоносный скрипт брал какой-нибудь файл из папки «Мои документы» на компьютере этого человека, заражал файл своей копией и рассылал дальше по всем контактам почты.

Поэтому эпидемия SirCam сопровождалась утечкой многих интересных документов — их можно было безопасно читать, вырезав вирус редактором типа Hiew. Достоянием масс стали различные финансовые отчёты, секретные файлы ФБР и даже планы украинского президента Кучмы: оказалось, что украинская администрация ведёт документооборот на русском языке, а вовсе не на украинском, который они в это время навязывали остальному народу. А разоблачительный червяк между тем продолжал способствовать просвещению масс: даже спустя несколько месяцев после начала эпидемии британский IT-журнал The Register выходил с заголовками типа «Тысячи идиотов до сих пор заражены вирусом SirCam».

Но и эти пятнадцатиминутки славы, растянутые на месяцы, уже остались в прошлом. А Саше нужно было разгребать свежий субботний поток. К полудню пришёл Главный и тоже погрузился в разбор почты. Он постоянно вёл переписку с экспертами из других компаний, у них были свои приватные списки рассылок для небожителей с многолетним стажем.

Сначала работа шла спокойно. Саша попробовал разобрать несколько больших бинарных файлов, время от времени дёргая Главного вопросами для подтверждения своих выводов: вирьё или не вирьё?

Через пару часов дверь распахнулась, на пороге появился Денис, пресс-секретарь компании.

— Ребзя! — сказал он, встав в центре комнаты. — А вы новости вообще слышали?

Аналитики переглянулись. Какие новости, мы тут мир спасаем, некогда нам…

— Там по телеку говорят, что Южная Корея без Интернета осталась, уже пять часов сидят!

Это сейчас смешно, когда новости получаешь из телеграм-каналов, спустя всего пару минут после любого события, а по телевизору про них рассказывают в лучшем случае через несколько часов. Но в 2003 году традиционные СМИ были главным источником новостей. А телевизора-то в вирлабе не было!

Новостные сайты помогли узнать, в чём дело: по всему миру падали интернет-сервисы. Помимо Южной Кореи, которая из-за перегрузки сети уже как будто вернулась в XIX век, пугающие новости поступали из Европы, США, Австралии. Тут и сами аналитики заметили, что Интернет работает слишком медленно, а число сообщений от почтовых серверов о недоставленных письмах резко выросло.

Можно было предположить, что это эпидемия червя, как та самая «Анна Курникова». А если так, задача понятна — надо срочно добыть файл, разобрать и задетектить!

Но файла не было. Саша проверил все свежие поступления в почте. Кто-то уже присылал ссылки на новости с вопросами, что это такое и как защититься. Но не было ничего похожего на файл с неизвестным червём.

Главный погрузился в пучины переписки с другими компаниями. Минуты шли.

— Слушай, тут кое-что прислали… — сказал вдруг Главный. — Похоже, просто кусок кода, непонятно откуда и какой-то мелкий… Я тебе кину тоже, посмотри.

Саша посмотрел. В коде не было ни начала, ни конца. Просто какие-то байты, среди которых виднелись текстовые строки:

h.dllhel32hkernQhounthickChGet
Qh32.dhws2_f
etQhsockf
toQhsend

Пресс-секретарь Денис убежал за пиццей. Главный с азартом долбил клавиатуру — он зарылся в дизассемблер, разбирая машинный код и добавляя к нему комментарии, подбирая нужные операции.

— Да вот же оно, вот! — Он откинулся в кресле и по-детски захлопал в ладоши.

Бессмысленный набор байтов превращался в стройные строчки машинного языка с операторами функций и системных вызовов.

— Смотри, тут он вот это берёт, вот сюда прибавляет, потом генерирует вызов, снова прибавляет… — Главный вслух проговаривал то, что творилось на экране. Но Саша всё равно ничего не понимал.

— А вот тут он собирает адрес и пуляет себя дальше. Всё! — Гигант реверса хлопнул себя по коленям. — Я сейчас ещё доразберу остатки, но уже всё ясно. А ты бери и детектируй, дятел!

— Но где же сам файл?

— А это и есть он, больше ничего нет. Сколько тут? Так, 376 байт. Вот оно целиком всё тут. Детектируй.

Сев на своё место, Саша открыл редактор антивирусных баз и начал заполнять поля. Первым шло «название». Что тут у нас? Червь. Значит, пишем Worm. Дальше платформа — Win32. Теперь название надо.

Принципы придумывания названий для новых вредоносов — отдельная большая история, которую мы ещё расскажем. Но в тот момент право на название было у Главного.

— А как назовём-то?

— Ой, ну возьми там из кода что-нибудь… Что там есть?

— Тут только «h.dllhel32hkernQhounthickChGet».

— Отлично. Берём hel, добавляем к нему kern. Так и назовём: Helkern!

Каждая антивирусная компания могла придумать своё название заразы либо взять уже известное от других. На тот момент других известных ещё не было. Однако в то же самое время червя исследовали в других лабах и там давали ему свои имена. Поэтому в истории этот червь остался не только как Helkern, но и как Slammer, он же Sapphire.

Итак, Саша дописал строку названия «Worm.Win32.Helkern» и указал тип файла. Теперь нужно «наложить маски», то есть выбрать куски кода, из которых получилась бы хорошая сигнатура — опознавательный признак для детектирования вируса. Для этого идеально подошла функция по собиранию IP-адреса из кусочков.

Дальше — запустить процедуру срочного выпуска антивирусных баз. Обычно этот процесс занимает несколько часов: новый апдейт проходит тщательное тестирование на коллекции чистых файлов, чтобы выявить ложные срабатывания и проверить работоспособность антивируса. Но в экстренной ситуации можно сократить время тестирования до часа, проверив апдейт только на ограниченной выборке. В надежде, что всё сделано правильно и потенциальный ущерб от ошибки меньше, чем ущерб от запоздалой реакции.

Главный сел писать письма коллегам-конкурентам, рассказывая о новой заразе. Да, они были конкурентами в бизнесе, но как эксперты по безопасности делали общее дело, поэтому обмен информацией шёл постоянно.

А Саше ещё предстояло выяснить, как эта зараза распространялась. Главная хитрость состояла в том, что червь не записывал себя в виде файла на диск — он был «бестелесным». Точно так же, как CodeRed в 2001 году. Достучавшись до следующего сервера, червь попадал прямиком в оперативную память, генерировал там произвольные IP-адреса и отправлял свои копии на серверы с этими адресами.

Но как же он заражал произвольно выбранный сервер? Ему помогала уязвимость, ошибка в реализации программы для базы данных. Оказалось, что атаке подвержены сервера, где работает программа MS SQL.

Но это совсем не новая дыра! О ней знали за полгода до эпидемии, с июля 2002 года. Тогда же компания Microsoft выпустила заплатку для исправления ошибки. Однако в те годы мало кто занимался оперативной установкой обновлений. Не парилась с этим даже в Microsoft: как стало известно позже, несколько их серверов тоже подкосил червь.

Простейший функционал, но потрясающая реализация и эффективность. Чтобы защититься, нужно либо установить заплатку для MS SQL, либо настроить систему контроля трафика (firewall) на отсекание вредоносных пакетов, пока они летят по сети. Ещё от червя можно избавиться перезагрузкой сервера, ведь зараза живёт только в оперативной памяти. Но как только сервер снова подключается к Интернету, он тут же может получить очередной вредоносный пакет. Традиционные антивирусы в лечении не помогают, ведь удалять с диска нечего, а лечить оперативную память в эти годы почти никто не умеет.

Пиарщик Денис вернулся с пиццей, и коллеги сели писать статью о том, как работает только что разобранный червь.

Пресс-релиз без ложной скромности назвали «376 байт, которые потрясли мир».

# # #

Мир действительно трясло. За первые 15 минут атаки червь умудрился поразить несколько десятков тысяч серверов. За следующие полчаса — несколько сотен тысяч. А за час заразились практически все сервера, которые могли быть заражены. То есть включённые и непропатченные.

А дальше все они генерировали в памяти новые адреса для атаки и слали туда пакеты с червём, те самые 376 байт. Рассылались они тысячами в минуту, так что Интернет оказался забит этими вредоносными пакетами, летающими туда-сюда. Один из российских банков сообщил, что за три часа они зафиксировали более 20 тысяч попыток червя пробиться на их сервер.

И даже спустя десять лет в Интернете продолжали летать пакеты Helkern. Достаточно было кому-нибудь установить новый сервер с непропатченным MS SQL — и он заражался, превращаясь в пулемёт, выстреливающий тысячи новых копий червя каждую минуту.

К счастью, для обычных пользователей прямого риска не было. Мало кто из них имел собственный SQL-сервер. Для них червь создавал проблемы только с загруженностью каналов и зависанием интернет-сервисов. Именно тогда Саша осознал: если бы подобный червь заражал ещё и устройства всех простых пользователей, от такой эпидемии Интернет едва ли смог бы оправиться.

И хотя пицца уже была съедена, а червь разобран и описан, до спасения мира было ещё далеко. Эпоха глобальных эпидемий сетевых червей только началась. Во время выступления на конференции в Ганновере через три месяца Главный скажет, что Интернет уже сидит на таблетках, а вскоре ему понадобятся капельница и морг. Вот к какому хаосу ведёт сетевая анонимность.

И кстати, да, личность создателя Helkern до сих пор не установлена. Уязвимость в MS SQL была известна за полгода до эпидемии. И код эксплойта (программы, которая использует эту уязвимость для атаки) уже был доступен многим хакерам.

Впоследствии кто-то нашёл куски кода, похожие на Helkern, среди файлов китайской хакерской группы Honker Union. Возможно, за этой эпидемией действительно стояли китайцы. Другой бестелесный червь, CodeRed, появившийся на полтора года раньше, при заражении веб-сервера подменял главную страницу на текст с таким признанием:

HELLO! Welcome to http://www.worm.com! Hacked By Chinese!

В пользу азиатской версии говорит и главная жертва эпидемии — Южная Корея. Она пострадала сильнее всего, в первые же минуты после запуска червя.

И хотя ни одна из азиатских хакерских групп не призналась в авторстве Helkern, желающие получить свои 15 минут славы всё равно нашлись. Спустя пару недель после начала эпидемии радикальная исламская группировка «Харакат уль-Муджахидин» взяла на себя ответственность за произошедшее. Террористы заявили, что они «начали киберджихад» и использовали Интернет, чтобы посеять хаос и смятение среди неверных.

В качестве доказательства своего авторства исламисты указали на число 42, которое содержалось в одной из первых инструкций кода вируса. Оно обозначает сокращённое название их группировки — HUM. В латинском алфавите буква H имеет порядковый номер 8, U — 21, а M — 13, что в сумме даёт 42.

Многие аналитики весьма удивились такой вольной трактовке символов и инструкций на ассемблере. А ФБР заявило, что группировка «Харакат уль-Муджахидин» не входит в число подозреваемых, однако деятельность экстремистов и их возможное отношение к эпидемии тщательно изучаются.

Зато вирлаб, разобравший червя, получил свои 15 минут славы прямо на следующий день после начала эпидемии, в воскресенье. Столь грандиозное событие вызвало массовый интерес, тем более что с наступлением рабочего понедельника количество заражённых систем обещало

вырасти. Телеканалы прислали свои съёмочные группы, дабы прямо с передовой линии электронного фронта провести разъяснительную работу в вечерних выпусках новостей.

Сашу до интервью не допустили: «Первый канал» снимал Главного. Однако Саша смотрел на всё это с таким интересом, что Главный заметил. И подойдя к нему, прищурился:

— А ты в следующий раз пойдёшь!

Ждать следующего раза пришлось не так уж и долго.

Глава 3. РАЗНЫЕ ЛЮДИ

«За спиной каждого успешного мужчины стоит женщина», — сказала однажды Грета Гарбо, стоя за спиной какого-то бомжа. «А за спиной каждого неуспешного стоят две», — ответил Марк Твен.

В наши дни делать такие неполиткорректные заявления опасно, даже если вы приписали эти цитаты очень известным людям. Но мы возьмём на себя смелость сказать, что за каждой вредоносной программой стоит человек.

Если ты знаешь, чего хотел автор вируса, ты быстрее поймёшь логику его программы и потенциал развития идеи. А это крайне важно для предсказания будущих угроз.

Сейчас добыча таких знаний превратилась в полноценное направление исследований — Threat Intel. Поисковые боты-разведчики прочёсывают тёмные глубины Даркнета и светлые облака социальных сетей, выявляя атаки ещё на стадии подготовки. Нейросети ищут сходство в кодах различных вредоносов и определяют почерк хакерских групп по коллекциям «цифровых генов». Психологи выявляют потенциальных хакеров ещё в детском саду и вшивают им специальные чипы… Хотя нет, тут мы слишком забежали в будущее.

Начиналось всё с методов попроще. Да и общая картина, в плане человеческих мотивов, двадцать лет назад радикально отличалась от сегодняшней — большинство вирусов создавались без какой-либо коммерческой цели. Хотя киберпреступники уже существовали, но они ещё не использовали вредоносные программы на полную мощь, в основном занимаясь простым фишингом или столь же простыми взломами вроде подбора пароля 11111.

Основным же источником массовых угроз служили любители. Создавали они свои вирусы чаще всего из хулиганских побуждений — навредить соседу, школе. Либо для самовыражения: о, про мою выходку напишут в новостях!

Однако уже существовала небольшая прослойка «идейных». Вот они-то и были серьёзной проблемой. Эти люди проводили настоящие исследования технологий, пытаясь выйти за рамки обычного программирования: найти недокументированные возможности в софте или обойти защитные механизмы, крайне слабые на тот момент. Занимались они этим чисто из любопытства и для удовольствия и преступниками как будто и не считались: «Мы просто ведём теоретическую работу». Основным противником идейных стали именно антивирусные лабы, а не соседи по школьной парте.

Встречались, кстати, и совсем идейные, которые считали вирусы олицетворением компьютерной жизни и относились к своим созданиям как к живым организмам. В общем, играли в эволюцию. В хакерских журналах того времени в отношении вирусов часто употреблялся термин «зверушка». Кто-то даже создал «двуполый» вирус, который был способен распространяться, только если в памяти одного компьютера одновременно оказались «мужская» и «женская» версии.

Более заметная эволюция происходила в это время в человеческих коллективах. Возникшая в 90-е вирусная сцена делится на группы: к началу XXI века на этой сцене практически не осталось вирусописателей-одиночек, хотя некоторые люди переходили из группы в группу. Почти каждый коллектив выпускал электронный журнал с описаниями своих инноваций, некоторые уже делали веб-сайты.

В конце 90-х этот подпольный мир переживает сильнейший кризис из-за глобального перехода от операционной системы MS-DOS к Windows. Старые трюки уже не работают, а кодить под Windows гораздо сложнее. Многие выходят из игры, но с 1998 года появляется новое поколение «идейных», которое выступает на вирусной сцене примерно до 2006 года.

Самая легендарная группа того времени называлась 29A (число 666 в шестнадцатеричной системе). Группа активно поддерживала свой демонический имидж, выпуская журналы по пятницам 13-го. Возникла эта тусовка в середине 90-х в испанском сегменте сети FIDO. С появлением собственного сайта группа стала международной — в неё вступали хакеры со всего мира, включая и российских. Но всегда присутствовало испано-бразильское ядро.

Именно 29A ответственна за создание множества эпохальных вредоносных программ конца 90-х — начала 2000-х. Вот только часть из них:

Happy99 — считается первым червём, который умел распространяться через почту.

Hybris — один из первых почтовых червей, использовавших загрузку дополнительных модулей из центра управления.

Cabir — первый червь для Symbian OS, летающий через Bluetooth.

Duts — первый вирус для Windows CE.

Esperanto — первый кроссплатформенный и мультипроцессорный вирус. Мог работать под DOS, Windows и MacOS, на процессорах Intel x86, Motorola и PowerPC.

Stream — первый вредоносный код, прятавший себя в «потоки» файловой системы NTFS.

Lindose — вирус, способный заражать файлы Windows и Linux.

Donut — первый вирус на платформе .NET.

Cap — один из первых макровирусов для MS Word.

Заметьте: все эти творения были концептуальными! Их первые версии практически никогда не несли серьёзных деструктивных функций и не представляли угрозы для широкого круга пользователей. Один из членов группы, известный под ником Mr. Sandman, в интервью сравнивал себя с поэтами и художниками, а свои вирусы считал произведениями искусства.

Проблема была в другом. Избрав антивирусную индустрию в качестве оппонента и постоянно подкидывая ей новые вызовы, эти теневые исследователи отвлекали внимание и ресурсы на противодействие. Антивирусникам приходилось реагировать на все инновации — даже если такие находки не несли особого вреда.

Вот, скажем, компания Microsoft придумала «потоки»: это такой способ хранения дополнительной информации в файловой системе. Тут же выходит зверушка под названием Stream, которая умеет прятаться в «потоках». А на момент появления этого концепта ни один антивирус в мире не проверяет «потоки». Значит, нужно реализовать эту проверку, потратив месяцы на анализ, разработку и тестирование.

Но сколько после этого было создано боевых вредоносных программ, использующих технологию «жизни в потоке»? Да не больше десятка.

Поэтому едва ли можно утверждать, что деятельность группы 29A двигала эволюцию антивирусных продуктов. Очень уж много энергии уходило на борьбу с фантомами. Когда на анализ поступает новый неизвестный образец, долго рассуждать нельзя. Ведь авторы этих концептов публикуют исходные коды в открытом доступе. А значит, любой хулиган или преступник может модифицировать описанную технологию под свои задачи — и выпустить по-настоящему опасный код.

В те же годы эволюция человеческих отношений создавала свою особую этику в антивирусной индустрии. Но чтобы рассказать о ней, вытащим на свет ещё одну любопытную зверушку.

# # #

В январе 2004 года по Интернету разлетелся червь MyDoom, который до сих пор, даже спустя 20 лет, остаётся рекордсменом по целому ряду параметров. Это был самый быстрорас-

пространяющийся почтовый червь в истории, он заразил полмиллиона компов по всему миру, вызвал общее замедление трафика Интернета на 10%, а суммарный ущерб от эпидемии оценили в 38 миллиардов долларов (тоже непобитый рекорд). За голову автора объявили награду в 250 тысяч долларов, но его так и не нашли.

Разлетаясь по почте, червь превращал заражённые компы в гигантскую зомби-сеть для DDoS-атак: все они начинали посылать множество запросов на сервера компаний SCO и Microsoft, тогдашних лидеров на рынке проприетарного программного обеспечения. Неудивительно, что в создании червя обвиняли сторонников операционной системы GNU/ Linux с открытым кодом. И конечно же, русских обвиняли в первую очередь: ведь, как известно, это русские придумали любовь и открытые коды, чтобы не платить капиталистам.

Но для нашей истории интересна другая деталь. В коде некоторых штаммов червя MyDoom содержалось зашифрованное сообщение, которое гласило: «Мы ищем работу в AV-индустрии».

Это могло бы стать зачином для типичного голливудского фильма категории B. Представим себе крутого вирусописателя (пусть его играет Джуд Лоу), который только что уложил своим червём весь Интернет. После этого он идёт прямиком в антивирусную компанию, где его принимают с распростёртыми объятиями. И назначают гонорар, явно превышающий те несчастные 250 тысяч долларов, что обещаны за его голову. И вот теперь он — вирусный аналитик, который за неделю должен разобрать 500 новых вирусов. Только в воскресенье он наконец может отдохнуть, то есть заняться своим любимым хобби: снова сесть на целый день за комп и написать ещё одного несчастного червячка. Прямо как в анекдоте: «Пришёл на пляж — а там станки, станки…»

Нет, в реальности такое кино не прокатит. Одно из первых правил антивирусной индустрии — запрет принимать на работу человека, когда-либо создававшего малвару. Какой компании будет приятно, если её сотрудника вдруг арестуют за его прошлые делишки? Или ещё хуже, он окажется агентом «тёмной стороны», который нанесёт вред бизнесу изнутри или раскроет секреты противнику? Да и вообще, чтобы создавать технологии защиты, нужен совсем другой склад ума. Ломать — не строить.

В качестве примера можно привести историю вирусописателя Benny, члена той самой группы 29A, в составе которой он создал несколько десятков вредоносных программ. В начале 2003 года, в очередном номере журнала группы, он сообщил о своём уходе — и как будто стал вести жизнь приличного человека.

Настоящее его имя было Марек Стрихавка, а жил он в городе Брно. Марек устроился на работу в чешскую компанию Zoner, которая писала софт. Пополнив свою команду крутым специалистом, компания разработала антивирусную утилиту и решила выйти с ней на рынок. Продукт назвали ZAV — Zoner Antivirus.

25 ноября 2004 года в дом Марека вломилась чешская полиция: все его компьютеры изъяли, а его задержали. Полицию интересовала его прошлая жизнь в составе 29A и возможная причастность к созданию червя Helkern/Slammer, который поразил Интернет за полтора года до этих событий — примерно в то время, когда Марек объявил об уходе с вирусной сцены.

Доказательств причастности Марека к червю не нашли, уголовное дело не возбудили, руководство компании Zoner выразило полное доверие своему сотруднику. И всё же в индустрии их антивирус стал «недоверенным». Сам Марек в итоге ушёл в другую чешскую компанию, Safetica, где занимаются защитой от утечек. Тоже неплохо для бывшего члена банды, стоявшей за технологиями, которые впоследствии использовались для кражи данных.

Показательна и история 18-летнего немца Свена Яшана, автора червей Netsky и Sasser. В первой половине 2004 года эти черви были в ответе за 70% мировых заражений. А червь Netsky оставался самым массовым почтовым червём на протяжении ещё двух лет.

Нанесённый урон тоже был немалым. Червь Sasser вырубил рентгеновские аппараты в одной из шведских клиник, авиакомпания Delta Air Lines отменила несколько полётов из-за сбоя компьютеров в аэропортах, агентство France-Presse несколько часов оставалось без спутниковой связи, а британская береговая охрана на целый день лишилась доступа к своим камерам слежения. Среди пострадавших также числились офисы Еврокомиссии и банк Goldman Sachs.

Неудивительно, что компания Microsoft назначила награду в 250 тысяч долларов за информацию об авторе этой заразы. Так его и нашли: Свена сдал одноклассник, узнавший о награде. Вирусописателя арестовали в мае 2004 года.

Поскольку на момент выпуска своих червей Яшан ещё считался несовершеннолетним, он отделался лёгким условным сроком, штрафом и исправительными работами. Осенью того же года его наняла в качестве консультанта по инфобезу немецкая компания Securepoint.

Такое решение вызвало множество негативных откликов в индустрии, а крупная немецкая антивирусная компания Avira и вовсе прекратила сотрудничество с Securepoint. «Мне бы не хотелось, чтобы к нашим разработкам приложил руку создатель вирусов», — заявил основатель Avira [2].

На российской, а точнее постсоветской вирусной сцене начала 2000-х обитало лишь несколько вирусописателей мирового уровня, таких как z0mbie и zhengxi. Однако коды, созданные ими, заставляли аналитиков поломать голову.

Среди групп выделялась Stealth Group WorldWide (SGWW), которая сформировалась в 90-е в Киеве, а затем открыла филиал в Москве. Члены группы создавали уже не только концептуальные вещи — там было много настоящих вредоносов, которые среди прочего заразили посольство США в Киеве и вызвали ещё ряд локальных эпидемий. А их электронный журнал Infected Voice, предтеча популярного журнала «Хакер», в 90-е годы был единственным журналом, который писал о компьютерном андеграунде на русском языке.

Со временем руководство SGWW стало всё больше склоняться к идеологии антисоциального толка. Причиной, очевидно, была безнаказанность. Хотя за 10 лет в составе группы побывало более 100 человек, никого из них не привлекли к ответственности за киберпреступления — в то время ещё не было нужных статей Уголовного кодекса. Как только они появились, активность группы стала сходить на нет. К тому же люди повзрослели, обзавелись семьями и стали интересоваться другими вещами. Сейчас многие из них вполне устроены, некоторые даже работают руководителями в известных компаниях.

Однако значительная часть членов SGWW влилась в ряды русскоязычной киберпреступности. Здесь, пожалуй, и возникает отличие от зарубежных хакерских групп того времени. На Западе большинство таких «исследователей» легко находили себе легальную высокооплачиваемую работу. Не в антивирусной индустрии, конечно, но программисты они были хорошие.

На территориях развалившегося СССР получить такую работу было сложней. Зато преступный мир привлекал высокими доходами, а милиция ещё не умела расследовать такие хитрые дела. Неслучайно писатель Брюс Стерлинг, посетивший Россию в середине 90-х, назвал её «страной победившего киберпанка».

И ещё одно отличие отечественной киберпреступности, связанное с деньгами. В начале 2000-х западная IT-индустрия стала назначать крупные денежные награды за информацию о хакерах. И как показал пример Свена Яшана, метод зачастую помогал… но не в случае русских хакеров.

До сих пор на сайте ФБР висит предложение заплатить три миллиона долларов за «Славика» из Анапы, который считается автором банковского трояна Zeus. Долгое время это была максимальная награда, которую когда-либо обещали за голову киберпреступника. Но никто не позарился на этот приз.

Недавно рекорд побило новое объявление: 10 миллионов предлагают за информацию, которая поможет арестовать Руслана Перетятько и Андрея Коринца, обвиняемых в атаках на американскую оборонку в составе группировки Callisto / Coldriver. И специально для увеличения числа забавных совпадений в нашей книге Минюст США уточняет, что оба хакера — из Сыктывкара. Как и наш герой Саша.

# # #

Чем же отвечала антивирусная индустрия? Разумеется, все компании были конкурентами. Все боролись за клиентов, контракты, партнёров. Но на экспертном уровне индустрия дружила.

Создатели первых антивирусных утилит начали обмениваться информацией ещё через сеть FIDO. В 1990 году они создали CARO — Computer Antivirus Research Organization. В ней зародились общие правила и стандарты безопасности. Например, Virus Naming Convention — соглашение о том, как называть новые вирусы. Членство в CARO стало синонимом признания среди спецов мирового уровня.

Другое заметное явление — Virus Bulletin. Этот журнал выходил ещё в 1989 году и сначала в бумажном виде. Со временем проект превратился в лабораторию по тестированию антивирусных продуктов: лучшим присуждали премии. Конференция VB на многие годы стала главным мероприятием индустрии, а выступление на ней — мечтой каждого ИБ-эксперта.

Обмениваются эксперты не только информацией, но и самими вирусами. Раз в неделю вирлаб, где работает Саша, отправляет множество своих находок коллегам из Norton Antivirus, а те в ответ присылают свой зоопарк. Со временем в таком обмене будут участвовать все антивирусные компании: европейские, американские, азиатские.

Мешает ли это развивать собственный бизнес? Нет, поскольку каждая компания создаёт свои технологии детектирования и удаления заразы. Кроме того, признание профессионального сообщества помогает продвижению на рынке. А чтобы завоевать доверие коллег, надо участвовать в конференциях, публиковать статьи, выступать с исследованиями. Скрытные же вызывают подозрение.

И чем сложнее угрозы, тем активнее кооперация. Из сообщества на пару десятков человек вырастает индустрия с сотнями тысяч сотрудников и десятками миллиардов долларов оборота. Но на уровне технических специалистов принципы сотрудничества много лет остаются прежними.

Появляются даже проекты типа VirusTotal.com. Запущенный в 2004 году испанской компанией Hispasec Sistemas, этот сайт позволяет загрузить подозрительный файл и проверить его большинством известных антивирусов. А создатели антивирусов, которые предоставили проекту свои движки, получают образцы новой малвары для улучшения качества своих детектов. Вот такая коллективная милота.

# # #

Ну что, дорогой читатель, ты уже поверил в этот простой чёрно-белый мир, где вирусописатели живут совершенно отдельно от антивирусной индустрии, никогда не берущей их на работу, а в самой индустрии царит мир, дружба и жвачка?

Нет, это была лишь присказка. Наш детективный роман только начинается. И в нём, конечно же, всё будет «не так однозначно».

С годами геополитика активнее вмешивается в дружественный мир экспертов по безопасности. Медийная паранойя про вездесущих русских хакеров начинает портить отношение даже к тем, кто вовсе не преступник.

В 2012 году на московской конференции по безопасности PHDays выступал известный американский криптограф Брюс Шнайер. После конференции он очень хвалил её: «Она вдохновляет, она практична и весьма контркультурна». Да что Шнайер! — на той же конференции выступал крепкий мужик из Пентагона, рассказывал про отличие арабских хакеров от китайских.

Но вскоре ветер переменился. И в 2018 году тот же Брюс Шнайер в интервью журналу The Daily Beast уже не может позволить себе позитивные высказывания о московских коллегах. Ту же самую конференцию он теперь описывает как базу для тренировки и найма русских хакеров и всячески дистанцируется от организаторов мероприятия: «Они подарили мне красивый жёсткий диск, отделанный кожей, с ручками и циферблатами в духе стимпанка. Но я никогда не подключал его ни к чему!» [3]

Изменились и многие ИБ-проекты, славившиеся международным сотрудничеством. В 2012 году корпорация Google купила тот самый VirusTotal, где любой желающий мог проверить подозрительный файл. А ещё через три года этот сервис, как и прочие сервисы Google, стал недоступен для жителей Крыма. Словно бы люди на этом полуострове заслужили больше вирусных атак, чем жители других регионов.

Впрочем, об этом позже. А пока вернёмся в начало 2000-х. Не столь однозначен был и полный отказ антивирусной индустрии от контактов с «тёмной стороной». Вылавливать заразу только тогда, когда она уже распространяется — слишком пассивная стратегия. Всё-таки это война, и реакция должна быть максимально оперативной. А ещё лучше — проактивной.

Смотрите, вот вирмейкерская группа собирается опубликовать очередной выпуск электронного журнала с описаниями своих новых концептуальных творений, из которых преступники тут же начнут клепать разные версии боевой заразы. Но если аналитикам удастся получить эти концепты заранее, можно научиться детектировать вирус ещё до того, как зараза пойдёт атаковать широкие массы.

Сейчас уже можно рассказать, какая социальная технология помогала решить эту задачу: антивирусная индустрия активно использовала агентов на стороне противника. Эти люди, внедряясь в вирмейкерские группы, получали доступ к опасным разработкам ещё до публикации. А значит, могли переслать такие данные в вирлаб для анализа. Формально они не были сотрудниками компании. Просто сознательные добровольцы. Но именно такой человек помог оперативно создать лекарство для борьбы со следующей, уже беспроводной эпидемией.

Глава 4. КЛЕТКА ФАРАДЕЯ

В августе 2005 года, на 10-м чемпионате по лёгкой атлетике в Хельсинки, российская прыгунья с шестом, к тому времени уже олимпийская чемпионка Елена Исинбаева установила очередной мировой рекорд. Она взяла высоту в 5,01 метра.

В то же самое время, пока спортсмены показывали чудеса бега, прыга и метания на олимпийском стадионе финской столицы, первый в истории мобильный червь незаметно захватывал смартфоны болельщиков на трибунах того же стадиона.

Червь быстро перепрыгивал с одного мобильника на другой, преодолевая расстояния до десяти метров. Безо всякого шеста, поскольку распространялся он по радиопротоколу Bluetooth.

Чтобы сдержать эпидемию, представителям финской антивирусной компании F-Secure пришлось на следующий день установить на входах стадиона специальные сканнеры. С помощью этих устройств отлавливали пользователей с заражёнными устройствами и не пускали их на чемпионат.

До этого беспроводной червь заразил уже тысячи смартфонов Nokia по всему миру, будучи первым червём для операционной системы Simbian. По подсчётам аналитиков, для заражения всех таких смартфонов в Москве ему понадобилось бы лишь четыре часа.

Однако в Москве эту заразу научились детектировать на год раньше, в июне 2004-го. Червя назвали Cabir. Ну или в полной версии, вместе с профессией и местом проживания — Worm.SymbOS.Cabir.

Более того, в Москве даже предсказали его появление: ещё на полгода раньше. В декабре 2003-го нашему герою Саше, который уже целый год проработал вирусным аналитиком, наконец-то разрешили выступить на публике. Вирлаб проводил пресс-конференцию, посвящённую итогам года в сфере кибербеза. И кто-то из журналистов спросил: а как насчёт мобильных вирусов, когда же они появятся и порадуют общественность?

Саша ответил: «Через год, когда мы снова соберёмся на такое же итоговое мероприятие, они, скорее всего, уже будут».

Это был его первый прогноз, в который он и сам не очень верил. Вокруг были только классические вредоносы для операционки Windows, а она не спешила стать мобильной. Не особенно взлетела и зараза для карманных компьютеров Palm: файловые вирусы для него появились ещё в 2000-м, но они не летали без проводов. Казалось бы, ничто не предвещало…

# # #

Итак, на дворе горячий июнь 2004-го. В вирлабе уже появились ночные смены — благодаря ещё четырём аналитикам, присоединившимся к команде, разбор вредоносного потока стал круглосуточным. А один из агентов с доступом к материалам вирмейкерской группы 29A только что прислал очередную инновацию, которая разработана этой группой и вскоре будет опубликована.

Обычно у дежурного аналитика уходит не более получаса на обработку сэмпла. Но в этот раз дежурный задумался надолго. Зараза создавалась не для Windows, не для процессоров на архитектуре x86. Какой-то совсем другой ассемблер — раньше с таким никто в лабе не сталкивался.

Дежурный передал проблему ночному сменщику. Сменщик Роман оказался проворнее. Он выяснил, что малвара написана для мобильной операционки Symbian. Ещё за пару часов он разобрался с ARM-ассемблером и понял, что делает этот код.

Зараза попадает на смартфон через Bluetooth, сканирует окружающие устройства с таким же беспроводным доступом и пересылает свои копии на них. При этом никакой вредоносной нагрузки, чисто концептуальная игрушка — заразить как можно больше окружающих. Но есть минус для пользователя: постоянные попытки червя раздать свои копии сажают батарею смартфона.

Дальше аналитикам нужно было воспроизвести заражение. Долго искали по офису, у кого из коллег есть подходящая Nokia. Нашли пару устройств, вежливо попросили «дать поиграть». Загрузили червя на один из них и стали ходить рядом, включив Bluetooth на втором устройстве. Сработало: на второй смартфон прилетел файл, выводящий надпись «Caribe».

А что с названием, кстати? Наверное, было бы проще всего называть вирусы именно так, как называются их файлы. В данном случае — Caribe. Но в антивирусной индустрии не принято использовать «авторские» имена вредоносов, чтобы не создавать тем авторам лишнюю рекламу.

Однако название должно быть связано с заразой. Главный покрутил слово «Карибы» так и эдак, после чего вспомнил сотрудницу с созвучной фамилией. Позвонил ей:

— Слушай, хотим в твою честь новый вирус назвать: «Кабир».

— Ха-ха. Ну можно…

На следующий день утром она позвонила Главному сама:

— Ты что мне устроил! Мог бы сказать, что это первый вирус для мобилок! Мне друзья весь телефон оборвали!

Кстати, эту главу мы неслучайно начали с женских рекордов. Не то чтобы нам очень хотелось порадовать феминистов, просто тем жарким летом 2004 года в вирлабе случилась сразу пара достижений, связанных с женщинами.

Буквально через месяц после поимки первого Symbian-червя Cabir, названного в честь сотрудницы, был пойман и первый вирус для другой мобильной платформы — Windows CE. Назвали его Duts. Это тоже была ночная смена. А дежурного аналитика, который во всём разобрался, звали Алиса.

# # #

На примере «Кабира» можно хорошо увидеть, что происходит дальше с концептами, которые появились как достаточно безвредные. Когда группа 29A открыла фрагменты исходного кода в очередном номере своего электронного журнала, новые модификации Cabir стали появляться каждую неделю.

Заражению подверглись даже сотрудники компании, в которой работал Саша. Это был, как говорят военные, friendly fire. Дело вот в чём. Бродя по городу, Саша и его коллеги-аналитики продолжали отлавливать варианты «Кабира» в дикой природе типа московского метро. А затем тестировали их у себя на работе. Через некоторое время сотрудники с других этажей стали жаловаться, что к ним через Bluetooth стучатся какие-то подозрительные файлы.

Стало ясно, что проводить эксперименты с беспроводной заразой нужно в изолированной среде. Так в компании появилась специальная комната, над устройством которой поработали радиофизики. Наконец-то знания соседей по зданию, создававших в советское время секретные радары, пригодились мирному населению. Помимо экранирования мобильных вирусов, специальная комната позволяла экспертам отдохнуть от навязчивых звонков.

Появление этой «клетки Фарадея» предвещало кардинальную смену парадигмы. На пороге стояло будущее, в котором вредоносное ПО уже не ограничивается привычными компьютерами. А значит, вирлабу понадобится исследовать и тестировать телевизоры, холодильники… автомобили?

С автомобилями их опередили коллеги из финской компании F-Secure, благо они обитали гораздо ближе к финской «Нокии», производящей операционку Symbian. А на этой операционке уже работали медиасистемы нескольких моделей автомобиля Toyota. Когда в «Нокии» узнали про «Кабир», то сразу призвали соотечественников из F-Secure для тестирования. «Тойоту» загнали в экранированный подземный гараж и атаковали «Кабиром» с заражённого мобильника.

Компьютерная система автомобиля отказалась принимать вирус через Bluetooth. Однако выявилась другая проблема: после интенсивных тестов у машины сел аккумулятор, а бортовой компьютер вырубился. Машина буквально «умерла» — даже дверные замки перестали открываться. Позже какие-то немецкие исследователи-экстремалы проводили аналогичные тесты и на улице: ставили над автобаном Bluetooth-пушки, бьющие на 50 метров, и сканировали автомобили на ходу.

Испуганные разработчики операционки стали спешно закручивать гайки. Например, ограничили функционал для сторонних разработчиков. Кроме того, Bluetooth теперь включался не по умолчанию, а только по команде пользователя.

Что до вирлаба, где работал Саша, то там, конечно же, выпустили антивирус для Symbian. Отдельный движок, отдельные базы и инфраструктура обновлений. Однако многие люди на тот момент вообще не понимали, зачем нужен антивирус, и не спешили его ставить. Так что клоны «Кабира» успешно распространялись по миру, это и привело к эпидемии на стадионе в Хельсинки спустя год после первого обнаружения этого червя.

С другой стороны, в начале 2000-х смартфоны с полноценными операционками типа Symbian или Windows CE были ещё не особо распространены: 90% пользователей имели простые мобильники с программами на Java. Трояны, нацеленные на такие устройства, стали серьёзной мобильной угрозой — они буквально крали деньги. Пользователь скачивал с какого-нибудь форума Java-приложение, которое маскировалось, например, под игру «Змейка». Заразив телефон, вредонос начинал отсылать SMS на платные номера.

Для молодёжи надо пояснить, что существовал в то время такой удивительный сервис у телеком-операторов: посылаешь SMS на короткий номер, и у тебя автоматически списывается сотня-другая рублей. Сервис использовали для различных викторин, телефонного секса и прочих вариантов «относительно честного отъёма денег у населения». Но ведь гораздо удобнее, когда самому пользователю вообще ничего делать не надо — мобильный вирус может автоматически посылать SMS, опустошая твой мобильный счёт.

Следующим прорывом в сфере мобильной заразы стал червь Comwar, появившийся в 2005 году. Он использовал два способа распространения: через Bluetooth и в виде MMS-сообщений, которые червь рассылал по всему контакт-листу заражённого устройства. Сообщения маскировались под всё то, что пользователь с удовольствием загрузит: игры, порно, антивирусы. В городе Валенсия этот червь заразил сотни тысяч смартфонов, нанеся ущерб на несколько миллионов евро.

Разнообразие мобильной заразы быстро росло. Уже через пару лет после выхода довольно безвредного «Кабира» антивирусная индустрия имела дело с полным спектром угроз на мобильных платформах. Поэтому в компании, где работал Саша, создали специальное подразделение анализа мобильных угроз, которое он же и возглавил.

Этому отделу пришлось не только изучать совершенно новый набор устройств, но и придумывать новые способы защиты. К примеру, как распространяются MMS-сообщения? По сути, это электронная почта в сети мобильного оператора. Саша и его коллеги договорились с рядом телекомов, чтобы включить на почтовых шлюзах проверку на мобильные вирусы. Статистика впечатляла: счёт заражённых сообщений шёл на сотни тысяч. Но на почтовом шлюзе заразу можно вырезать сразу, не дожидаясь, пока она достигнет адресатов.

Забегая вперёд, отметим, что дальнейшая эволюция мобильных угроз принесла ещё много сюрпризов — а вот технология Bluetooth спустя десять лет была практически забыта вирусописателями. Редким примером её использования стал многофункциональный троян Flame, атаковавший страны Ближнего Востока в 2012 году. Он умел многое, в том числе распространяться по Bluetooth. А основной его задачей был шпионаж, включая прослушку через микрофоны заражённых устройств. Но о таких крутых шпионах мы расскажем в отдельных главах.

Глава 5. ПРИНЦИП ЛУКОВИЦЫ

Доводилось ли вам видеть на двери своего подъезда бумажное объявление, предлагающее услуги «компьютерного мастера»? Мастер обещает вылечить ваш комп от любых вирусов и поставить все нужные программы. Ниже написан телефон или ещё какой контакт.

Не советуем пользоваться этими контактами: известно много мошеннических схем вокруг таких объявлений. Ради навязывания дополнительных услуг подобный мастер может нарочно «залечить» ваш комп до состояния полной тыквы. Обращайтесь лучше к проверенным людям.

Профессиональные сервисы такого рода называются по-разному. Но в самых крутых случаях звучит слово «форензика». Вообще это раздел криминалистики: эксперты выезжают к клиенту, у которого что-то произошло в компьютерной сети, изучают детали инцидента и собирают цифровые доказательства для расследований и судов.

«Но мне-то зачем такой мастер? — спросит иной читатель. — Могу же сам поставить антивирус, он и поймает всю заразу. А в суды я вообще не люблю ходить…»

И действительно, в начале 2000-х годов таких сервисов с выезжающими экспертами практически не было. Саша и его коллеги просто анализировали новые образцы малвары и добавляли детектирующие записи в базу антивируса. Но так работало не всегда.

Весной 2005 года служба безопасности крупного банка обратилась в вирлаб с необычной просьбой: приехать и посмотреть кое-что. Аналитики в ответ попросили прислать подозрительные файлы для исследования. «Никаких файлов нет», — сказали в банке.

Делать нечего — Саша и ещё один аналитик, Алексей, отправились в московское отделение пострадавшего банка, захватив с собой некоторые программки-утилиты, которые использовали на работе.

В банке они услышали такую историю. На компьютерах в одном из отделений сформирована проводка на перевод денег со счёта на счёт. Сейчас такие операции автоматизированы, но в начале 2000-х они ещё требовали участия людей. Перевод оформляет операционист банка, затем подтверждает контролёр — и транзакция проходит. Но в этот раз перевод произошёл ночью, когда в банке никто не работал.

Это и насторожило безопасников, проверявших ночные логи. Однако на жёстких дисках компьютеров, с которых совершалась операция, они ничего не нашли. Антивирус тоже молчал. Компы привезли в центральное московское отделение банка и оставили Сашу и Алексея в одной комнате с этими машинами.

Вносить свои изменения в жёсткий диск банка нельзя — вдруг он ещё будет фигурировать как вещдок в суде. Поэтому парни копируют его содержимое на свой диск и исследуют привезёнными с собой утилитами. Смотрят логи запуска и остановки системных процессов, пытаются найти свежесозданные файлы.

Но логи не показывают никаких необычных процессов, либо они просто подчищены. И новых файлов нет: все системные файлы как будто созданы в одно время, когда установили операционную систему.

Следующая идея — взять весь список файлов и сравнить со стандартным списком того, что должно быть установлено в чистой системе. Эта проверка занимает целый день… и всё же удаётся найти подозрительный драйвер, с которым что-то не то. Файл отправляют электронной почтой в вирлаб, чтобы там посмотрели на него повнимательнее.

Когда Саша и Алексей возвращаются на работу, дежурный аналитик Алиса сообщает им результаты — это руткит. Программа, которая умеет скрывать свою работу от операционной

системы. Запустив подозрительный драйвер, коллеги видят это воочию через файловый менеджер FAR: файл исчез из каталога.

# # #

Чтобы пояснить, как работает такая зараза, придётся немного углубиться в общую архитектуру программного обеспечения на популярных в то время персоналках. Сильно усложнять не будем. Лишь вспомним, как в известном мультфильме Шрек сообщил Ослу, что тролли — парни непростые. «Тролль как луковица, у него есть слои!» — говорил тогда Шрек.

Примерно так и с программами на компе. Самый глубинный, самый низкий уровень — прошивка. Это встроенное программное обеспечение, которое обычно записывается в постоянную память устройства при изготовлении. Самый простой машинный язык, управляющий «железом».

Дальше идёт BIOS, базовая система ввода-вывода. Это набор более продвинутых микропрограмм, которые процессор достаёт из постоянной памяти и записывает в оперативную, после чего передаёт управление этой системе.

Получив управление, BIOS проделывает ряд процедур начальной загрузки: тестирует подсистемы компьютера, применяет всякие настройки, а затем загружает в оперативную память код загрузчика операционной системы и передаёт управление ему.

Дальше загружается более высокий слой: собственно операционная система, куда входит множество разнообразных программ для управления устройствами — драйверы. Операционка даёт вам понятный интерфейс, то есть абстрактный язык, позволяющий работать с файлами и прикладными программами. Вы всего лишь двигаете иконку файла на экране, а операционка переводит это на более конкретный язык своего драйвера, типа «возьми данные по такому-то адресу на диске и запиши их по другому адресу на другом диске». Ну а этот машинный язык переводится в самые низкоуровневые команды для процессора. Как-то так в общих чертах устроена многослойная душа нашего Шрека.

После загрузки в память руткит работает на уровне ядра операционной системы (kernel level). Он маскируется под легальный драйвер Windows и имеет такие же высокие привилегии, то есть может перехватывать управление программами, которые работают в более высоких слоях луковицы.

Это и даёт руткиту возможность «подчистить» файловую систему, скрывая определённые файлы. По той же причине увидеть работу руткита не позволяли инструменты, которыми пользовались Саша и Алексей. Ведь эти утилиты работали на достаточно высоком уровне.

О методе руткита знали ещё с 80-х годов. Уже тогда архитектура программного обеспечения позволяла проводить эксперименты с запуском «нестандартных» программ, имеющих слишком большие права. Такие утилиты вначале появились в UNIX-системах, откуда и пошло их название (root — администратор UNIX-системы, kit — набор инструментов).

Но той весной 2005-го вирусные аналитики столкнулись с первым боевым применением этой техники под Windows. И тут же выяснилось, что такая малвара попала в вирлаб не впервые.

— Я такое уже видела, — говорит Алиса, глядя на код.

Парни с удивлением смотрят на неё — ну, примерно как смотрел тот парень, которого Анджелина Джоли доводила в сами-знаете-каком фильме. Алиса и выглядит соответствующе: коротко стриженная, в джинсах и кожанке, в крепких мужских ботинках, с микросхемами на рюкзаке и татуировкой-иероглифом на руке. Она выучила ассемблер в 15 лет и бросила учёбу в двух технических вузах.

— Когда, где ты это видела?

— Кажется, месяцев семь назад присылали…

Как можно вспомнить подобную вещь, разглядывая массив бинарного кода? На самом деле, это и есть главная профессиональная фича вирусных аналитиков. После нескольких месяцев работы намётанный глаз начинает распознавать паттерны в том, что кажется другим людям просто хаосом символов и цифр на экране.

В вирлабе даже устраивают конкурсы на скорость распознавания вредоносов по коду. Победитель получает право выбрать пиццу, а это очень серьёзный приз. Ведь обычно решение о выборе пиццы принимает Главный. Его любимая — неизменно гавайская, с ананасами. Все остальные уже терпеть не могут эти ананасы.

Поэтому борьба за право выбрать пиццу идёт нешуточная. По команде каждый аналитик берёт файл из потока — и кто быстрей разберётся. Рекорд на вынесение вердикта — девять секунд, а на создание детектирующей записи — 43 секунды.

Так что после слов Алисы о том, что код руткита ей уже знаком, коллеги бросаются его искать. И находят в архивах прошлого года раннюю версию той же программы. Кажется, на тот момент никто полностью не осознал, что это такое.

Этот образец прислал не агент вирлаба, как предположили вначале. Письмо пришло с анонимного адреса. Скорее всего, это сделал сам автор заразы — хотел проверить, выйдет ли обновление антивируса, после которого руткит будет детектироваться. Ведь если бы такое случилось, попытку скрытных банковских переводов сразу бы пресекли.

Но именно это и выдало автора. Аналитики передали в банк результаты своей экспертизы, включая то самое письмо с первой версией руткита. А служба безопасности банка выяснила, что письмо пришло с IP-адреса в том же городке, где случилась электронная кража денег. Автор руткита явно имел доступ в местное отделение банка. И не просто доступ, а должность сотрудника, плотно работавшего с компьютерами: ведь загрузить на них руткит мог только человек с правами админа. В общем, круг подозреваемых сильно сузился.

# # #

В тот год осенняя погода стояла долго на дворе: новые руткиты плодились как грибы после дождя. И это были уже не отдельные утилиты, а целые конструкторы для создания различных вредоносных программ (кража данных, рассылка спама и т. д.). Но среди прочих возможностей они теперь включали и функции руткита — сокрытие своих действий и файлов в операционной системе.

Таким был, например, популярный бэкдор Haxdoor. Осенью 2005 года аналитики из вирлаба ежедневно выявляли новые версии этой заразы. Ежедневно!

Скрытность руткитов стала серьёзным вызовом для всей антивирусной индустрии. Ведь если антивирус тоже работает на уровне ядра операционки, он либо вообще не видит руткит, либо, даже если видит, ничего не может сделать, потому что у руткита тоже высокие привилегии в системе.

Тем не менее индустрия начинает отвечать на вызов. Некоторые компании и отдельные энтузиасты выпускают утилиты для выявления руткитов, такие как RootkitRevealer. Другие добавляют новые хитрые модули к антивирусу, чтобы он мог «заморозить» некоторые системные процессы и проверить их.

Совершенно неожиданный удар в спину получает эта индустрия (а с ней и миллионы пользователей) на праздник Хэллоуин 2005 года. Эксперт по кибербезопасности Марк Руссинович, один из авторов программы RootkitRevealer, во время тестирования новой версии этого инструмента обнаруживает неизвестный руткит на одном из своих компов. К удивлению эксперта, источником очень скрытной шпионской программы оказался компакт-диск с песнями группы Van Zant.

И это не пиратский диск, а легальная продукция корпорации Sony. Просто они решили применить технологию руткита для защиты авторских прав (Extended Copy Protection) на миллионах своих CD. Скрытная программа, невидимая даже для антивирусов, должна была предотвращать попытки копирования дисков. А заодно информировать корпорацию о тех компьютерах, где происходят такие попытки. И всё это без ведома покупателей тех самых дисков [4].

Скандальное разоблачение шпионской технологии выявило ещё один интересный факт: этот «легальный руткит» встречали и другие исследователи, но юристы советовали им не обнародовать находку и не предлагать инструменты для удаления шпиона. Ведь таким образом они нарушили бы американский закон DMCA, запрещающий вскрывать копирайтную защиту.

Зато антивирусная компания, где работал Саша и его коллеги, сразу же опубликовала предупреждение о возможных последствиях этой сомнительной инновации. Руткит, забравшийся на уровень ядра операционки, не только вносит нестабильность и тормоза в работу компьютера (вплоть до «синего экрана смерти»), но и может использоваться для создания новых вредоносов.

Реакция Sony на такие предупреждения поразила мир не меньше, чем их технология защиты от копирования. «Большинство людей вообще не знают, что такое руткит, так зачем им беспокоиться?» — заявил один из топ-менеджеров корпорации.

Однако прогноз аналитиков сбылся буквально через неделю. Сразу несколько антивирусных компаний рапортовали о появлении троянов Breplibot, Stinx-E и Ryknos, работающих на основе технологии Sony. Пользователи получали письмо с вредоносным вложением, после его открытия на компьютер проникала зараза, которая пряталась в файле с именем sysdrv.exe. Если на компе был установлен руткит от Sony, он скрывал присутствие и активность всех файлов с префиксом sys — включая и новый вредонос. И такое происходило у всех, кто слушал диски Sony с соответствующей защитой от копирования.

В конце концов корпорация одумалась, отозвала диски с руткитом и урегулировала несколько судебных разбирательств. Однако, по мнению некоторых экспертов, этот случай положил начало «большой народной нелюбви» к Sony, что позже вылилось в масштабные хакерские атаки на корпорацию.

# # #

В конце 2006 года на форумах киберпреступников появляются слухи о неуловимом рутките Rustock. Он и вправду кажется невероятно скрытным: в течение следующих полутора лет антивирусная индустрия не может его поймать. Некоторые даже говорят, что это выдумка. Другие утверждают, что с помощью этой программы-невидимки создана самая мощная сеть зомби-компьютеров для рассылки спама.

Прорыв происходит только весной 2008-го. Российская антивирусная компания Dr.Web добывает образец файла с руткитом: это поддельный драйвер операционной системы Windows. Код руткита зашифрован неизвестным способом, и аналитикам требуется больше месяца, чтобы разобраться в коде и создать средства для детектирования и лечения. Затем Dr.Web извещает о находке остальную антивирусную индустрию.

Однако в истории остаётся много белых пятен. Непонятно, каким способом и когда распространился этот руткит и почему его так долго не могли обнаружить. Исследователи из Dr.Web так и не нашли дроппер — файл, который устанавливает руткит в систему.

С этого места эстафету подхватывает тот самый вирлаб, где работают Саша и его коллеги. В своих ловушках, созданных для сбора вредоносных файлов, они находят около шестисот образцов руткита. Так они восстанавливают картину эпидемии.

Оказалось, что Rustock распространялся по каналам группировки IFrameBiz. Её уже знали по таким творениям, как Harnig, Tibs, Femad, LoadAdv, и различным модификациям Trojan-Downloader.Agent. Следы группы ведут в Петербург, к известному провайдеру хакерских сервисов Russian Business Network (RBN).

Питерские вообще лидировали в среде отечественного сетевого криминала с середины 90-х. Вспомнить хоть Владимира Левина — он считается первым в мире хакером, которого посадили за кражу денег из банка другой страны через Интернет. Такая аура северной столицы неудивительна. Именно здесь в «лихие девяностые» высокая концентрация лучших естественно-научных вузов страны сочеталась с настоящей нищетой среди студентов тех самых вузов. Даже обыкновенный сахар стал дефицитом, который продавали только по карточкам. И добывать его приходилось другими способами.

Некоторые студенты, отложив конспекты и компьютеры, просто шли работать грузчиками в порт Ораниенбаума. Но были и такие, кто научился добывать свой альтернативный сахар, не отходя от компа. Именно эти выходцы из ЛЭТИ и других питерских вузов создали легендарный хостинг RBN, дававший крышу всевозможным видам киберпреступности, включая спам, фишинг и кражу банковских карт. Этому же провайдеру хакерских услуг приписывали организацию DDoS-атак на государственные сайты Эстонии после того, как эстонские националисты добились сноса «Бронзового солдата» — памятника советским воинам в Таллине.

За несколько лет существования RBN создала одну из мощнейших систем распространения вредоносов на основе ботнетов. Так называются сети, состоящие из тысяч, а порой и миллионов заражённых компьютеров, на которые можно быстро загрузить новую вредоносную программу. Ботнет как способ распространения заразы стал самой эффективной альтернативой почтовым рассылкам, с которыми антивирусная индустрия уже научилась бороться.

Именно к этому сервису, работавшему под витриной IFrameBiz, обратились летом 2007 года авторы руткита Rustock, чтобы распространить своё творение. Но либо троянцы IframeBiz не могли незаметно активировать Rustock в системах, либо авторы руткита не хотели давать в руки распространителей сам код руткита, опасаясь кражи технологий. Так что для «заливки» по каналам IFrameBiz создали совершенно отдельный троянский модуль.

Этот загрузчик был обнаружен вирлабом ещё осенью 2007 года. Он детектировался как Agent.ddl и содержал в себе драйвер-руткит. Сняв защиту с зашифрованного драйвера, аналитики поняли, что перед ними — тот самый «разносчик эпидемии», блокировка которого помогает остановить распространение Rustock.

# # #

Очередная история успеха? Как бы не так! В ответ на выявление руткитов создатели вредоносов открывают новые способы стать невидимками. Помните луковицу Шрека? Можно ведь скрыться в более глубоких слоях луковицы.

В конце 2007 года через ботнет той же хакерской группы IFrameBiz распространяется троянец-шпион Sinowal. Позже его можно будет подцепить и на взломанных сайтах, и на порноресурсах, и на сайтах с пиратским софтом. Шпионская программа мониторит весь трафик жертвы, вылавливает обращения к банковским сайтам и пересылает украденные банковские реквизиты на сервер злоумышленников.

Sinowal становится большой болью для антивирусных компаний на весь следующий год. Повторяется та же история: заразу никто не видит. Даже в конце 2008-го детектировать и лечить угрозу умеют только 4 из 15 популярных антивирусов.

Этот тип малвары называется «буткит», поскольку заражает загрузочный сектор диска: MBR, Master Boot Record, главную загрузочную запись. Из этого сектора BIOS берёт код, кото-

рый будет управлять дальнейшей загрузкой операционной системы. Но если зараза записала себя в загрузочный сектор, она может стартовать раньше операционки — и иметь более высокие привилегии.

Загруженная после этого операционка попадает под контроль буткита. И даже если антивирусная программа получает низкоуровневый доступ к физическому диску для проведения там своих проверок, буткит перехватывает эти вызовы и может выдать ложный результат.

А значит, коллегам Саши (теперь это аналитики Серёжа и Слава) нужно тоже забраться в этот слой луковицы, исследовать установленные буткитом перехватчики и научиться лечить заражённый MBR.

И одновременно, как в случае Rustock, нужно выявить сеть распространения буткита — чтобы антивирус мог блокировать заразу, когда она ещё только пытается перебраться на компьютер пользователя с заражённого сайта. Почти все серверы, участвующие в процессе заражения, показывают русскоязычный след: они работают в рамках известных российских и украинских «партнёрок» (схемы взаимодействия между владельцами серых сайтов и авторами вредоносов).

К 2012 году бум руткитов и буткитов как будто затихает. Конечно, работает над этим не только антивирусная индустрия, но и сама корпорация Microsoft, которая тоже реагирует на угрозы. Разработчики Windows запрещают запуск неподписанных драйверов, вводят дополнительные проверки при загрузке, меняют способы работы с памятью.

Одно из самых заметных новшеств — на смену BIOS приходит UEFI (Unified Extensible Firmware Interface). Как и в случае BIOS, это набор программного обеспечения, которое работает на промежуточном уровне. То есть непосредственно над прошивкой «железа», но ниже операционки Windows, которая загружается после. UEFI работает быстрее, чем старушка BIOS, имеет графический интерфейс и считается более безопасной…

Вы уже догадались, что будет дальше? Ещё один слой луковицы можно обойти, забравшись ещё глубже. Непосредственно в прошивку.

Как это часто бывает, концепт появляется за несколько лет до боевого применения. Буткит, способный модифицировать UEFI, найден в 2015 году в утечке исходных кодов итальянской компании HackingTeam, которая делает шпионский софт для госорганов и спецслужб. Какое-то время никаких серьёзных последствий как будто не видно, но…

В 2020 году аналитики вирлаба будут расследовать целевую атаку, направленную на дипломатические учреждения Африки, Азии и Европы. Шпионский набор софта, используемый для атаки, назовут MosaicRegressor. В некоторых случаях это вредоносное ПО попадает на компьютеры жертв через модифицированный код UEFI. Даже при обнаружении заразы избавиться от неё антивирусными средствами невозможно. Единственный способ — перепрошивка материнской платы.

Вдумчивый читатель, следящий за нашими разоблачениями луковой шелухи, конечно же, понимает, что дальше мы должны занырнуть в самую глубь. На физический уровень, где испуганно жужжат кремниевые чипы, заражённые нехорошими электронами.

Но погоди, вдумчивый читатель, ты у нас не один! Есть и такие, кто хочет почитать про что-нибудь более близкое, человеческое.

Например, про деньги.

Глава 6. КРИПТА, ДА НЕ ТА

Появление криптовалют имело много интересных последствий. Некоторые были очевидными и часто обыгрывались в новостях и сериалах. Для тех, кто всё проспал, напомним основные сюжеты.

Вот человек, купивший первые биткоины по цене куска пиццы в 2010-м. Через несколько лет он становится миллионером — жизнь удалась. Но это слишком простенькая короткометражка.

А вот другой человек, который в 2013 году выбрасывает на помойку старый жёсткий диск с кодами своих кошельков, где хранится 7500 биткоинов.

За 10 лет стоимость выброшенного вырастает до 250 миллионов долларов. Бывший владелец диска организует раскопки мусорной свалки с использованием рентгеновских сканнеров и искусственного интеллекта [5]. Отличный материал для комедии в духе «Кремниевой долины»! Кстати, они и вправду сделали такую серию с горе-миллионером на свалке.

Или вот ещё один человек, потративший кучу денег на суперкомпьютерную ферму для майнинга… В деталях он не разбирался, усвоил только одно: если у тебя есть большие вычислительные мощности, ты можешь участвовать в создании того шифрованного блокчейна, который и обеспечивает криптовалютам их криповую валютность. А самым активным участникам этого процесса периодически выдают новые монетки-биткоины. Короче, накупи побольше процессоров — и начинай добывать электронное золото!

Вот только цена хвалёной крипты почему-то перестала расти именно тогда, когда ты вложился в этот самый майнинг. Кажется, тебя просто развели продавцы процессоров. Что же делать с ненужными вычислительными мощностями? Поверить в следующий бум, заняться искусственным интеллектом? А может, лучше просто застрелиться? Это уже заявка на «Оскар» по разделу «Лучший драматический актёр».

В той индустрии, о которой наша книга, сюжеты бывают и позаковыристей. Вот какой-то хитрец решил, что нет смысла вкладываться в покупку новых компов, когда есть множество доступных старых. И запустил скрытный майнинг криптовалюты на серверах телеком-оператора, где ему довелось работать администратором. Ну а что, пусть простаивающие компы приносят пользу! Хотя всем известно, что бесплатного сыра не бывает: нагруженные такой задачей компы потребляют больше электроэнергии, за которую будет платить работодатель того самого администратора. С юридической точки зрения это не что иное, как кража электроэнергии с переводом её в криптовалюту.

Но кто, как не криминал, заинтересован в разных вариантах кражи? Идею скрытной добычи крипты на чужих мощностях подхватывают вирусописатели — и вот уже вирусы-майнеры заражают сотни тысяч машин, обсчитывая заветные блокчейны без ведома владельцев. Чем же ответит индустрия безопасности? Неужели просто заблокирует заразу?

Нет, это слишком банально, а мы любим погорячее. Самый удивительный ответ дают разработчики антивирусов Norton 360 и Avira: они встраивают криптомайнер прямо в свои антивирусы, которые вообще-то должны защищать пользователя от паразитной нагрузки. Но кому интересны мелкие проблемы пользователя — по сравнению с грандиозной идеей запустить сразу 500 миллионов клиентских компьютеров на добычу цифрового золота! [6]

К сожалению, все эти голливудистые истории золотодобычи затмили в общественном сознании другую важную особенность криптовалют. Хотя и эта фича не особенно новая. Вы можете сами получить удовольствие от её использования, когда расплачиваетесь в магазине наличными — на монетках и купюрах не написано ваше имя, и его никто не спрашивает!

Для наших предков это было нормой. Зато наш молодой читатель наверняка испытывает сейчас приступ удивления: «А что, так можно было? Все платежи — анонимные?!» Ведь он

всегда платит картой, а это означает не только предъявление паспорта, но и сбор всех данных о его покупках, доходах, предпочтениях, перемещениях, любимых позах…

Да, современная банковская система превратилась в мощнейший инструмент слежки. Для этого, конечно, есть рациональное объяснение. Переходя на безналичные расчёты, люди доверяют банку проверку участников сделки.

Кроме того, банковская система гарантирует и защиту самой транзакции. Ведь электронные деньги на вашем счету — это просто числа в файле. Число можно исправить, просто дописав парочку нулей (как многократно делали хакеры). А в защищённых денежных сделках должен работать закон сохранения. Если у одного участника сделки электронная монетка добавилась к счёту, то у другого такую же монетку нужно списать. Никаких случайных удвоений или исчезновений монеток. И кто-то должен за этим следить.

Почти сразу после появления Интернета начались разработки альтернативных систем дистанционных платежей. По задумке они должны были работать в недоверенной сетевой среде без централизованного посредника — банка и избыточной идентификации участников сделки. Но при этом в них должен был соблюдаться «закон сохранения».

В 2009 году такой механизм реализовали в сети Bitcoin благодаря криптографической технологии blockchain. Если говорить совсем просто — гарантом сделок здесь выступает не один администратор (банк), а вся децентрализованная сеть, распределённая база, где хранятся все транзакции. Причём они закодированы таким образом, что их нельзя подделать. А суть майнинга — включение своих вычислительных ресурсов в работу этой криптосети и получение вознаграждения в виде новых биткоинов. Но даже эти счастливчики остаются анонимными, их отличает только номер кошелька.

Вот так и получилось, что, помимо новой золотой лихорадки, криптовалюта привела к развитию мощной альтернативной экономики. Экономики вымогательства на основе платежей, в которых невозможно вычислить получателя.

# # #

Вымогатели начинают доставать пользователей персоналок где-то с 2004 года. Первые ласточки ничего не шифруют, просто блокируют.

Таков троянец Krotten. Вы получаете файл, в котором якобы содержится генератор кодов для нелегального пополнения счёта мобильника. После запуска троянец регистрирует себя в ключах автозапуска системного реестра на вашей персоналке. И при каждой следующей загрузке Windows вместо классического интерфейса на экране появляется предложение заплатить за восстановление доступа. А именно: прислать вымогателю по электронной почте «код пополнения счёта “Киевстар” на 25 гривен».

Однако эта малвара не портит пользовательские файлы, и вирлаб без проблем выпускает средство для лечения.

А вот вымогатель Gpcode похитрее. Спам с этой программой рассылается по электронным адресам, собранным на сайте job.ru. Люди, которые искали работу и разместили там свои резюме, получают письмо с предложением — якобы от представителя солидной западной компании. В письме «соискателю» предлагают заполнить приложенную анкету для приёма на перспективную работу.

Когда человек открывает присланный ему троянский файл (документ MS Word), запущенный вредонос обходит все каталоги, шифрует файлы и почтовые базы данных. Для расшифровки нужно писать автору заразы на почту в домене yahoo.com.

В декабре 2004 года вирлаб, где работает Саша, получил первые образцы файлов, зашифрованных с помощью Gpcode. Судя по множеству признаков, шифрующая программа россий-

ского происхождения. От этого трояна уже пострадали несколько банков, рекламных агентств и других организаций с крупным документооборотом.

Но самопальный алгоритм шифрования, используемый автором трояна, пока ещё достаточно прост. Ключ — общий для всех зашифрованных пользователей — хранится прямо в коде вредоноса. Аналитики вирлаба быстро находят ключ и добавляют в свой антивирус нужную функцию расшифровки.

А потом в течение полутора лет они наблюдают, как растёт автор. Он выпускает несколько десятков модификаций шифровальщика, пробуя другие алгоритмы.

В январе 2006-го вирлаб добывает версию Gpcode.ac, где используется один из наиболее стойких публичных шифров — RSA. И если в первых зимних версиях длина ключа шифрования Gpcode составляет 56 бит, то весной это уже 330 бит, а летом все 660 бит. Даже если задействовать все компьютеры мира, на подбор ключа такой длины потребуются сотни лет.

И это ещё не последняя версия Gpcode. Но с этого места уже понятно, что игра в «лобовой» взлом шифра перебором уже проиграна. Однако есть надежда, что создатель малвары облажался в практической реализации своих криптоалгоритмов.

Одна из первых его ошибок — слишком короткая длина ключа шифрования. Когда взлом Gpcode путём полного перебора стал бессмысленным, один из аналитиков собрал все ранние взломанные ключи и разложил их на компоненты. Вот в чём фишка — ключи в RSA-шифровании состоят из комбинации очень длинных чисел. Как оказалось, при генерации ключей автор изменял лишь часть компонент. А значит, перебирать нужно лишь часть ключа. Так вирусные аналитики сделали то, что вызвало так много вопросов — невозможный на то время подбор RSA-ключа в 660 бит за очень короткое время.

Этот успешный взлом шифра как будто «остудил» вирусописателя. Автору вредоноса понадобилось почти два года, чтобы создать усовершенствованный вариант.

Новая версия, Gpcode.ak, использует для шифрования файлов симметричный алгоритм RC4. А вот ключ для этого шифрования уже зашифрован алгоритмом RSA с 1024-битным ключом, где все старые компоненты заменили новыми. И старый трюк со взломом RSA уже не проходит. Кстати, именно такая комбинация RSA + RC4 с аналогичной длиной ключей используется в популярной программе шифрования данных PGP (Pretty Good Privacy). А ещё она применяется для защиты сетевых соединений — например, в HTTPS для шифрования ваших данных при обращении к веб-страницам интернет-банкинга.

Над взломом RSA + RC4 работало много великих умов, но задача казалась нерешаемой. Однако и тут аналитики вирлаба продолжили «работу над ошибками».

Во-первых, они заметили, что после создания зашифрованной копии файла вредонос удаляет оригинал файла с диска простой операцией DeleteFile. Но на деле эта операция не уничтожает данные. Просто в таблице файлов меняется параметр, указывающий, что данная область диска свободна и туда можно записать что-то другое. И пока новых записей не сделано, там по-прежнему лежит «удалённый» файл, который можно восстановить. Например, с помощью бесплатной утилиты PhotoRec, которая изначально создавалась для спасения самого важного, что хранится на компьютерах всего мира — бесконечных пользовательских фоток из отпуска.

Но такой подход требует большого везения: зачастую удалённые файлы оказываются уже перезаписаны чем-то новым и не восстанавливаются. Значит, надо снова думать, что делать с зашифрованными копиями.

Если RSA взломать не получается, можно попробовать взломать ключ RC4, ведь именно им шифровали данные. Правда, анализ кода показывает, что длина ключа RC4 слишком велика для полного перебора. Кроме того, у каждой жертвы шифровальщика этот ключ отличается: он выбирается случайно во время работы вируса.

И здесь автор Gpcode совершил очередную ошибку. Ведь по-настоящему случайных вещей в цифровом мире почти не бывает. Круче всего было бы использовать для получения случайных чисел какой-нибудь физический процесс вроде колебаний температуры материнской платы. Но добраться до таких данных сложно.

Поэтому на практике используются генераторы псевдослучайных чисел. Это некая математическая функция, которая выдаёт последовательность более-менее разнообразных цифр. Здесь слабое звено — самое первое число (seed), от которого начинается вычисление функции. Если узнать или угадать его, то можно воспроизвести псевдослучайную последовательность и восстановить ключ шифрования.

Как выяснилось, автор Gpcode использовал в качестве «сида» значение процессорного регистра TSC (Timestamp Counter) — он содержит количество тактов процессора с момента включения компьютера. А это относительно небольшое число для перебора!

Почему автор совершил такую банальную ошибку? Скорее всего, он использовал виртуальную машину. Этот софт позволяет имитировать виртуальный компьютер внутри физического — получается эдакая «Матрица». В ранних версиях виртуальных машин значение регистра TSC рандомизировалось специально и не было связано с настоящим процессором и его тактовым счётчиком. Разрабатывая и тестируя Gpcode на виртуальной машине, автор зловреда оказался обманут «Матрицей». Он верил, что у него есть по-настоящему аппаратный генератор случайных чисел.

Но универсального способа расшифровки всё равно нет. И борьба с новыми версиями шифровальщика становится всё сложнее. Остаётся последний и самый эффективный вариант — найти самого автора.

Вообще, злоумышленники часто выдают себя сами, на этот счёт есть много народных мудростей типа «жадность фраера сгубила». В 2008 году автор шифровальщика Gpcode сам написал письмо в антивирусную компанию, где работает Саша, и предложил им выкупить программу для дешифровки. Возможно, вирусописателю просто надоело заниматься мелким вымогательством, так что он захотел получить одну большую награду сразу. Для доказательства своего авторства он даже прислал аналитикам утилиту, которая позволяла расшифровать один зашифрованный компьютер.

Платить ему, конечно, не стали. Но письмо дало несколько зацепок. Правда, компания Yahoo отказалась деанонимизировать почтовый ящик, с которого писал злоумышленник. Да и IP-адрес в заголовке письма позволил лишь выяснить, что автор шифровальщика ведёт переписку через зомби-компьютер, который входит в ботнет для рассылки спама с трояном-шифровальщиком. Заражённые машины находились в США. Все эти данные передали в правоохранительные органы.

# # #

В истории Gpcode существовала ещё одна ниточка, основанная на известном принципе «следуй за деньгами». Своим зарубежным жертвам злоумышленник предлагал переводить выкуп на кошелёк в платёжной системе Liberty Reserve. Эта финансовая компания, зарегистрированная в Коста-Рике гражданином украинского происхождения, часто использовалась для отмывки денег. По этой причине в 2013 году её разгромили американские правоохранители, а её основателя приговорили к 20 годам тюрьмы.

Расследование, проводившееся несколько лет в 17 странах мира, и последующее закрытие Liberty Reserve вполне могли стать причиной исчезновения автора Gpcode. Многие мошенники лишились денег после разгрома этой платёжной системы. А кого-то, возможно, даже поймали и посадили на основе данных, полученных после анализа арестованных активов.

Эта же история показала главное слабое место в схемах работы вымогателей — платёжные системы. С 2012 года именно эту слабость начали закрывать криптовалюты: появилась возможность по-настоящему анонимных платежей.

Бизнес сразу начал приносить огромные доходы. Их легко оценить, поскольку информация о транзакциях Bitcoin вполне доступна, разве что без имён. В декабре 2013 года журнал ZDNet посчитал, что жертвы шифровальщика CryptoLocker за два месяца перевели авторам малвары около 27 миллионов долларов, по цене биткоина на тот момент [7]. Сейчас, спустя десять лет, обороты вымогателей составляют миллиарды, а жертвы платят до 50 миллионов долларов за один выкуп.

Но если файлы зашифрованы так хорошо, что никакой антивирус не справляется — почему бы не заплатить? В конце концов, современная IT-индустрия точно так же продаёт нам свой софт! Мы уже давно не являемся полноправными владельцами программ, которые покупаем. Нет, это всего лишь временные лицензии. По окончании срока лицензии нужно платить снова, иначе ваш софт грозит превратиться в тыкву.

И верно, модель схожая. Разница совсем небольшая: с легального IT-бизнеса мы всё-таки можем требовать качественной работы, раз уж заплатили. Многочисленные «истории успеха» шифровальщиков быстро привели к тому, что делать их стала всякая школота с кривыми кодами. В итоге даже получение ключа после отправки выкупа отнюдь не гарантировало, что дешифратор сработает.

Бывали и такие ошибки, в результате которых шифровальщик вообще не мог корректно отправить ключ. Таков был червь WannaCry, атаковавший мир в 2017 году. В этом случае криптолокер превращается в вайпер, то есть «стиратель»: зашифрованные данные пропадают безвозвратно.

Или такой вариант: компания выплачивает несколько миллионов выкупа, получает ключ… а процесс расшифровки занимает несколько месяцев. Ущерб для бизнеса получается почти такой же, как если бы данные просто стёрли.

И если первые вымогатели просили немного, но у многих (простых пользователей), то с годами они стали переключаться на крупных клиентов. Конечно, атаковать банк или больницу посложнее. Зато выкуп сразу такой, что вполне оправдывает затраты на подготовку атаки.

Одно из последних новшеств в этой криптоэкономике — система оценки выкупа на основе доходности компаний-жертв. Почти как оборотные штрафы: «Будьте так добры, заплатите два процента с вашего оборота!» Появились и разнообразные компании-посредники, которые за определённый процент от «спасённых» активов берут на себя переговоры с вымогателями.

Конечно, лучший вариант борьбы — это когда полиции удаётся захватить центр управления шифровальщиком. В этом случае можно получить ключи для спасения всех жертв без выкупа. Так случилось в мае 2014-го, когда был захвачен центр управления ботнетом Gameover ZeuS. В ходе операции полиция получила и базу закрытых ключей, используемых шифровальщиком CryptoLocker.

Однако для такого решения требуется активное международное сотрудничество правоохранителей и антивирусной индустрии. Наиболее известным проектом подобного рода стал сайт NoMoreRansom.org, где публикуются ключи расшифровки и утилиты для удаления различных шифровальщиков.

Конец ознакомительного фрагмента.