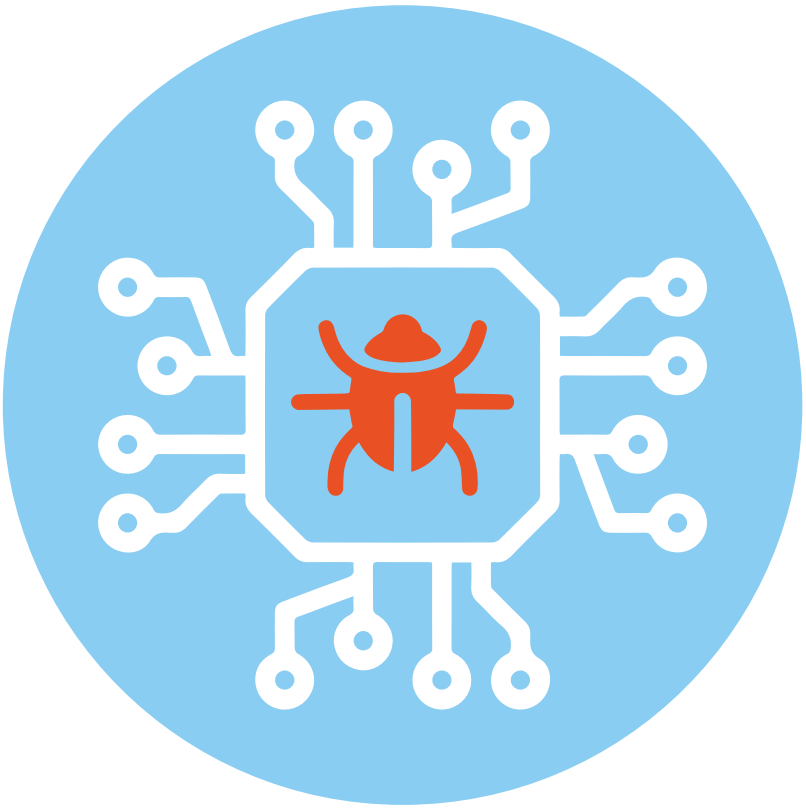

Глава 4

Арсенал киберпреступников

В главе 2 мы провели инвентаризацию нашего цифрового хозяйства и увидели, что нам есть, что терять. А сейчас поговорим об инструментах, с помощью которых киберпреступники творят свои темные дела.

Чтобы успешно противостоять преступникам, необходимо понимать, как они нас атакуют, в какие наши слабые места бьют, и, исходя из этого, выстраивать линию обороны.

Можно во все это не вникать? Есть же специально обученные люди: вот пусть они все как следует настроят, а мы будем просто пользоваться.

Увы, так не получится. В сфере цифровых технологий к сегодняшнему дню сложилась примерно такая же ситуация, какая наблюдалась в среде автолюбителей лет пятьдесят назад: чтобы «железный конь» исправно бегал, каждый водитель должен был стать немножко автомехаником. Помните, как было в старых фильмах? Машина внезапно останавливается, из нее, чертыхаясь, выходит водитель и, только поковырявшись какое-то время под капотом, едет дальше.

Знаете, почему таких сцен нет в современном кино? Потому что техника существенно изменилась. Если на приборной панели замигала лампочка, это означает, что нужно не лезть под капот, а ехать в сервис.

Если на приборной панели замигала лампочка, это означает, что нужно не лезть под капот, а ехать в сервис.

Но в том, что касается обеспечения кибербезопасности компьютеров и смартфонов, ситуация с сервисом на сегодняшний день еще далека от идеала. Например, просто за установку антивируса (пиратской копии или бесплатного) в Москве попросят от 500 до 2000 рублей, а настройка wi-fi-роутера обойдется в 300-1500 рублей. При этом комплексной услуги по обеспечению безопасности всей цифровой жизни человека никто не предлагает, так что спасение утопающих продолжает оставаться делом рук самих утопающих: пользователям волей-неволей придется беспокоиться о своей кибербезопасности самостоятельно.

Темпы роста киберпреступности в нашей стране значительно опережают все другие виды криминальной деятельности. Так, по данным Генпрокуратуры, за первые восемь месяцев 2019 года количество зарегистрированных преступлений в России выросло почти на 67%. А в 2018 году киберпреступность показала двукратный рост.

Краткая история вирусов: начало

Давным-давно, когда компьютеры были большими, а данные — маленькими, никаких вирусов не существовало вовсе. Писать программы тогда было делом трудным и хлопотным, поэтому программисты по большей части занимались чем-то важным и полезным, а не созданием вредоносного ПО.

Но в один прекрасный день каким-то умникам пришла в голову мысль, что можно написать программу, которая будет самовоспроизводиться до тех пор, пока не займет всю свободную память. Сказано — сделано! В 1961 году математики фирмы Bell Labs изобрели необычную игру «Дарвин», в которой несколько программ, названных «организмами», сражались за память компьютера. Это были еще не вирусы, но их предвестники — киберобъекты, наделенные свойством размножения по подобию живых организмов. И до начала эпохи персональных компьютеров эти протовирусы служили лишь забавой программистам, не представляя никакой опасности.

В сегодняшнем виде компьютерные вирусы появились в начале 1980-х, когда «персоналки» попали в руки школьников и студентов.

В том виде, в каком мы их знаем сегодня, компьютерные вирусы появились в начале 1980-х, когда «персоналки» попали в руки школьников и студентов. Поначалу вирусы были вполне безобидны, ведь их создавали не для того, чтобы кому или чему-либо причинить вред, а из пустого тщеславия. Первым получил распространение вирус ElkCloner, написанный пятнадцатилетним школьником из Питтсбурга по имени Ричард Скрента.

Возможно, это несколько удивит молодых поклонников Стива Джобса, но «Лось-клонировщик» (так можно перевести название вируса), передаваясь через дискеты, заражал операционную систему компьютеров Apple II. Это сейчас продукты компании из Купертино считаются эталоном безопасности, а в то время они работали под управлением одной из версий DOS — со всеми вытекающими для безопасности последствиями. Вирус питтсбургского школьника не вредил преднамеренно — лишь иногда случайно ломал систему, а в «нормальном режиме» после каждой 50-й загрузки выводил на экран стишок.

Elk Cloner:	«Лось-клонировщик»:
The program with a personality It will get on all your disks It will infiltrate your chips Yes it's Cloner! It will stick to you like glue It will modify RAM too Send in the Cloner!	Программа с индивидуальностью. Он проникнет во все ваши диски, Он внедрится в ваши чипы. Да, это — Клонировщик! Он прилипнет к вам, как клей, Он даже изменит оперативную память. Отправь Клонировщика!

Появление ElkCloner прошло практически незамеченным, поскольку владельцев техники Apple тогда было немного. Зато вирус Brain («Мозг»), который инфицировал компьютеры IBM PC, наделал много шума и вошел в историю как вызвавший первую эпидемию (или даже пандемию).

Brain («Мозг») инфицировал компьютеры IBM PC и вошел в историю как вирус, вызвавший первую эпидемию (или даже пандемию).

Его создали в 1986 году братья-студенты Базит и Амджад Фарух Алви из Пакистана. По своей природе Brain тоже был достаточно мирным — он всего-навсего замедлял работу флоппи-дисков. Более того, братья даже оставили свой адрес и телефоны, чтобы пользователи зараженных компьютеров могли с ними связаться:

> *WelcometotheDungeon © 1986 Basit&Amjads (pvt). BRAIN COMPUTER SERVICES 730 NIZAM BLOCK ALLAMA IQBAL TOWN LAHORE-PAKISTAN PHONE: 430791,443248,280530. Beware of this VIRUS.... Contact us for vaccination...*

«Зачем вы это сделали?» — спросил их Микко Хиппонен (Mikko Hyponen), эксперт по кибербезопасности компании F-Secure. В 2011 году, спустя четверть века после эпидемии Brain, он специально приехал в Лахор по указанному адресу, где и нашел авторов «Мозга». Для Хиппонена эта поездка была сродни паломничеству. Ведь он, потративший большую часть своей жизни на борьбу с вредоносными программами, встретился с авторами первого вируса, с которым ему пришлось столкнуться.

В интервью Хиппонену братья рассказали, что были молоды, горячи и очень хотели наказать пиратов, которые нелегально копировали их

медицинскую программу для мониторинга работы сердца. Но что-то пошло не так — и вирус начал бесконтрольно распространяться, в результате чего добрался до Великобритании, США и ряда других стран. Первый звонок от инфицированного поступил из Университета Майами, а вслед за ним на братьев обрушился целый шквал звонков, так что телефоны им пришлось отключить. Но в целом история с Brain закончилась если и не удачно, то без особых потерь: зараженные компьютеры вылечили, а законов, предусматривающих наказание за создание вирусов, в Пакистане не существовало. И сейчас братья Фарух Алви руководят одной из крупнейших в стране телекоммуникационных компаний — Brain Telecommunications, расположенной все по тому же адресу. Вирусов они больше не писали.

А вот создателю первого компьютерного червя (программы, которая самостоятельно распространяется по сети) — Роберту Моррису (Robert Morris), аспиранту Корнеллского университета — повезло меньше. Он стал первым осужденным по закону о компьютерном мошенничестве и злоупотреблениях (Computer Fraud and Abuse Act), принятому в США в 1986 году.

> *Червь Морриса, или «Великий червь» (Great Worm), запущенный 2 ноября 1988 года, парализовал весь тогдашний интернет, заразив около 6000 серверов — 10% от общего количества (по другим данным — 2000 серверов). И снова эпидемия возникла из-за ошибки в механизме распространения!*

По задумке Морриса, его программа должна была записать себя на каждый доступный компьютер в сети, что могло произойти практически незаметно. Но так уж случилось, что вирус начал заражать каждую систему многократно и в итоге съедать все вычислительные мощности. Естественно, на это обратили внимание.

В результате из безвредного, как считал автор, интеллектуального упражнения червь превратился в опасную атаку типа «отказ в обслуживании» (DoS)[1]. В принципе, Роберта Морриса могли и не найти — он достаточно хорошо замаскировался. Однако его отец, работавший в АНБ, убедил сына сдаться добровольно. И, судя по всему, правильно сделал. Моррис-младший отделался условным сроком и штрафом в 10 тысяч долларов — при том, что ущерб от его «эксперимента» оценивался в 96,5 миллиона. Правда, согласно распространенному мнению, оценка ущерба была сильно завышена.

Моррис отделался условным сроком и штрафом в 10 тысяч долларов, хотя ущерб от «эксперимента» оценивался в 96,5 миллиона.

Чего только не вытворяли вирусы 1980-1990-х годов рождения! На мониторах зараженных ими компьютеров возникали самые разные и не всегда приличные надписи и расхаживавшие взад-вперед мультяшные персонажи; демонстрировались чудные визуальные и звуковые эффекты и др. Иногда вирусы даже играли с пользователями, как, например, вирус Casino. При инфицировании компьютера он предлагал пять раз сделать ставку на примитивной слот-машине. Если вам выпадал выигрыш, вирус честно оставлял ваши файлы в покое, если нет — безжалостно удалял.

---

1 *DoS (Denial of Service, «отказ в обслуживании») — хакерская атака на вычислительную систему с целью доведения ее до отказа. В результате атаки пользователи системы могут лишиться доступа к предоставляемым системным ресурсам (серверам) или этот доступ будет затруднен.*
Чаще употребляется термин DDoS (от англ. Distributed Denial of Service, «распределенный отказ в обслуживании»), означающий, что запросы на атакуемый сервер поступают с множества адресов.

Еще один вирус-пакостник — Laroux, один из первых вирусов для Excel. Он не только заражал все электронные таблицы, но при каждом открытии файла случайным образом округлял числовые значения в ячейках на 0,001% вверх или вниз. Постепенно ошибка накапливалась, что могло привести к неприятным последствиям.

> *А 2 июня 1997 года студент Датунского университета (Тайбэй, Тайвань; КНР) Чэнь Инхао (Chen Yinghao) создал первую версию вируса Chernobyl («Чернобыль» или CIH — по первым слогам имени автора). Вирус заражал компьютеры с операционными системами Windows 95 и ежегодно срабатывал 26 апреля — в годовщину катастрофы на Чернобыльской АЭС. CIH стирал загрузочную область жесткого диска, реже — данные BIOS. В последнем случае требовалось менять чип на материнской плате или даже приобретать новый компьютер, поскольку старый полностью выходил из строя. По оценкам, CIH заразил более 60 миллионов ПК по всему миру и причинил ущерб в размере свыше 1 миллиарда долларов. Но что примечательно — непосредственно к Чэнь Инхао не было подано ни одного иска, и к ответственности его никто не привлек.*

Такого рода «вирусотворчество» можно считать проявлением обычного вандализма — наряду с битьем окон, порчей общественного транспорта или созданием граффити, ведь финансовых интересов авторы вирусов прошлого века не преследовали. И не потому, что были бескорыстными. Дело в том, что получить деньги с жертвы и при этом остаться незамеченным было сложно, а получить срок в цивилизованной стране — легко.

В наши дни вирусы ведут себя тихо. Они больше не показывают нам забавные картинки, не проигрывают мелодии и даже не пишут

никаких сообщений, кроме требований выкупа. Они максимально скрытно проникают в компьютер или телефон, маскируют свое присутствие и ждут подходящего момента, чтобы ограбить владельца. Теперь главная цель вирусописателей — не потешить свое самолюбие, а получить деньги.

Теперь главная цель вирусописателей — не потешить свое самолюбие, а получить деньги.

От интеллектуальных забав к извлечению денег

Преступный мир не сразу распознал, какие возможности открывает наступление компьютерной эры. Вероятно, для обычных бандитов это было слишком сложно, поэтому пальма первенства в сомнительном, с точки зрения этики, соревновании по монетизации компьютерных угроз принадлежит ученым. Но если ученые могут выдвигать блестящие идеи, это еще не означает, что они способны блестяще воплощать их в жизнь. Нередко и незаурядные умы допускают нелепые ошибки, оборачивающиеся крахом.

Весьма поучительный пример, а вместе с тем и сюжет для комедии — история первого вируса-вымогателя AIDS («СПИД»), известного также как Aids Info Disk и PC Cyborg Trojan[1].

В 1989 году д-р Джозеф Л. Попп (Dr. Joseph L. Popp), эволюционный биолог из Гарварда, разослал почтой (обычной, а не элек-

1 *Virus Bulletin, January 1992.*

тронной!) 20 тысяч дискет по обширному списку адресатов, включая подписчиков журнала PC Business World и делегатов конференции по СПИДу, проходившей под эгидой Всемирной организации здравоохранения. Где он взял эти списки? Купил под вымышленным именем у некоего кенийского бизнесмена.

Письма адресатам поступили от компании PC Cyborg Corporation, зарегистрированной в Панаме (ох уж эти панамские оффшоры!), а в приложенной к дискете лицензии на использование ПО значилось, что дискета содержит интерактивную анкету для оценки риска заражения СПИДом.

Однако кроме анкеты на дискете был еще записан и вирус-шифровальщик, который активировался после 90-й загрузки компьютера и зашифровывал все имена файлов на жестком диске, а после шифровки на экране появлялся текст с требованием заплатить от 189 до 378 долларов якобы за «аренду программного обеспечения». Таким нехитрым образом вымогатель пытался придать своим действиям законный вид. Забавно, но все это было изложено и на бумаге — в приложенном лицензионном соглашении. Но кто их читает! Отправить деньги нужно было на анонимный счет в Панаме. Взамен же вымогатель обещал прислать пароль для расшифровки файлов.

Впервые вирус AIDS проявил себя в Англии, причем под удар попали именно медицинские учреждения. Скотланд-Ярд немедленно начал расследование.

В канун Рождества главный герой этой истории возвращался с семинара ВОЗ из Найроби через Амстердам в США. Внимание

сотрудников аэропорта Схипхол привлекла тревожная надпись на его чемодане "DR. POPP HAS BEEN POISONED", что можно было перевести как «Д-р Попп отравлен» или, если учесть, что рейс прибыл из Африки, подумать, что доктор инфицирован ВИЧ. Разумеется, нидерландские полицейские решили его досмотреть, а во время досмотра обнаружили среди вещей печать PC Cyborg Corp, о чем и сообщили своим британским коллегам. Доктору позволили добраться до Огайо, а там арестовали и экстрадировали в Великобританию, где он должен был предстать перед судом по обвинению в 11 эпизодах вымогательства. Очевидно, что пострадавших было больше, просто далеко не все обратились в полицию. Но и выявленных эпизодов оказалось вполне достаточно для возбуждения дела.

Никогда не используйте в качестве пароля свое имя! Не будьте как д-р Попп!

Среди изъятых у подозреваемого дискет был найден его дневник, в котором обнаружили ключ шифра от вируса — «Dr. Joseph Lewis Andrew Popp Jr». Банально, не правда ли? Никогда не используйте в качестве пароля свое имя! Не будьте как д-р Попп! Также среди его файлов нашли и полный исходный код программы-вымогателя. В общем, доказательств для суда набралось предостаточно.

> *Как установило следствие, стоимость дупликации носителей и почтовые расходы доктора превысили 10 тысяч фунтов. К этому сыщики прибавили затраты на регистрацию компании в Панаме, аренду помещения в Лондоне и в итоге обнаружили, что у этой авантюрной затеи складывается вполне внушительный бюджет. Это дало повод усомниться в рациональности действий Поппа. Однако, как вскоре было подсчитано, заплати все получатели дискет полную стоимость «лицензии» — 378*

долларов, доктор собрал бы в сумме 7,5 миллионов. И даже если бы его шантажу поддался всего один процент получателей дискет, и все они заплатили бы минимальный выкуп — 189 долларов, итоговые 38 тысяч покрывали все издержки. К тому же американский поверенный Поппа подтвердил, что доктор собирался вести бизнес с размахом и в дальнейшем планировал разослать не менее двух миллионов дискет.

К чести адресатов Поппа, только 5% из них вставили инфицированные дискеты в свои компьютеры. Люди оказались не такими беспечными, какими, видимо, их считал доктор.

Во время суда Попп вел себя странно: надевал на голову картонную коробку, накручивал на бороду бигуди, а на нос надевал презерватив, который, по его словам, защищал «от радиации и микробов». Адвокаты настаивали, что их подзащитный планировал жертвовать полученные от аферы деньги на альтернативные образовательные программы по СПИДу. И это, по данным следствия, было чистой правдой. В итоге многие пришли к выводу, что доктор на самом деле никто иной, как криптоанархист, своего рода Робин Гуд, который пытается инициировать реформы в просвещении по вопросам СПИДа. Хотя, согласно The Guardian, Поппом могли двигать и куда менее благородные мотивы — например, месть за то, что ему было отказано в работе в ВОЗ. Но, в конце концов, суд, невзирая на многочисленные сомнения и подозрения, решил, что доктор все-таки сошел с ума, и отправил его домой.

Забавный факт: после высылки из Англии крестный отец кибервымогателей Джозеф Попп основал в городе Онионта на севере штата Нью-Йорк оранжерею бабочек, назвав ее своим именем. Эта оранжерея существует по сей день.

Эксперты, изучавшие вирус AIDS, признали концепцию Поппа гениальной, а ее техническую реализацию — весьма слабой, ведь доктор использовал симметричное шифрование, а это довольно ненадежный метод. Он предусматривает, что для шифровки и расшифровки применяется один и тот же ключ, который хранится в теле вируса. То есть жертва, имея определенную квалификацию, может сама обнаружить этот ключ и спасти свои данные без какого-либо выкупа. Тем не менее, AIDS впервые показал действенную схему монетизации вирусов, которую в дальнейшем многократно использовали преступники. Особую популярность эта схема приобрела с появлением биткойна.

Однако эпизод непосредственно с вирусом AIDS остался в памяти лишь как экстравагантная выходка чудака-ученого. Последователей у него не нашлось, что, в общем-то, понятно — кто возьмет на себя труд по рассылке тысяч дискет? А вот когда все компьютеры подключились к электронной почте, и доставка вирусов значительно упростилась, преступники оценили его изобретение по достоинству.

> *По мнению упоминавшегося выше Микко Хиппонена[1], рубежом, когда создание вирусов окончательно превратилось в преступную деятельность с целью извлечения выгоды, стал 2003 год. Тогда появился вирус Fizzer — сложный почтовый червь, созданный исключительно в коммерческих целях. Его авторы открыли еще один способ монетизации. Их червь заражал компьютеры, из которых был сформирован ботнет — сеть компьютеров-зомби, тайно управляемых злоумышленниками.*

1 *Mikko Hypponen. The History and the Evolution of Computer Viruses. // Privacy-pc.com, 19 марта 2012.*

Затем создатели Fizzer стали продавать услуги по рассылке спама с зараженных машин другим злоумышленникам.

Если вы станете рассылать спам со своего адреса, провайдер его быстро заблокирует. Поэтому организаторы рассылок постоянно нуждаются в новых, еще не скомпрометированных адресах. Новые почтовые ящики теоретически можно регистрировать вручную, но это слишком неэффективный процесс, и активность такого рода тоже легко пресекается. А вот запустить рассылку с тысячью случайных адресов реальных пользователей — это эффективно!

Очень быстро многие любители вирусов поняли, что могут использовать свои навыки для заработка, если будут сотрудничать со спамерами, красть пароли и данные кредитных карт, когда люди совершают онлайн-покупки.

Вскоре очаги вирусных инфекций сменили локацию. В старые добрые времена — до того, как вирусы превратились в «машины по производству денег» — они создавались главным образом в странах Западной Европы, США, Канаде, Японии, Австралии. Но самые горячие точки сегодняшнего дня — это Россия, Украина, Казахстан, Румыния, Молдова, Китай, Бразилия и Иран.

Киберпреступность сегодня выгоднее торговли наркотиками. По данным Cybersecurity Ventures, ежегодная прибыль от наркобизнеса составляет около 400 миллиардов долларов, а киберпреступники в 2018 году заработали в общей сложности около 600 миллиардов.

За время, прошедшее с появления первых вирусов, мир коренным образом изменился. Эпоха хакеров-одиночек давно канула

в Лету, и теперь нам приходится иметь дело с организованной преступностью. Хуже того, образовалась целая преступная индустрия: одни злоумышленники разрабатывают вредоносное ПО и продают его, другие организуют атаки, третьи обналичивают добытые деньги.

Цифровой бестиарий: знай своего врага

Существует широкое разнообразие видов вредоносных программ, в том числе вирусов, червей, троянов, вымогателей, шпионских программ и прочее, объединяемых термином malicious software — вредоносная программа. Собирательно их еще называют malware (по-русски — «вредоносные программы», а на сленге — «зловреды»).

> *Зловреды тайно действуют против интересов пользователя, в чем бы это ни выражалось. Это может быть кража паролей и учетных данных, личной информации, номеров банковских карт, кодов доступа и денежных средств, шантаж и вымогательство, навязчивая реклама, звонки и SMS на платные номера, уничтожение данных, захват аккаунтов и тому подобное.*

При всем разнообразии методов киберпреступники действуют примерно по одной и той же схеме. Сначала необходимо незаметно проникнуть в устройство пользователя и замаскироваться. Затем нужно доставить и распаковать «полезную нагрузку» — собственно, инструмент для совершения диверсии, — и в подходящий момент нанести удар. Поэтому названия типов зловредов чаще

всего происходят либо от способа проникновения, либо от вида совершаемого действия.

Вообще говоря, деление зловредов на типы весьма условно. Это не систематика млекопитающих, когда только на основе строения зубов вы можете отнести животное к отряду грызунов и предположить, как оно выглядит. Зловреды же практически невозможно четко структурировать по типам, ведь здесь возможны любые химеры, обладающие качествами разных типов. Это в живой природе невозможно скрестить ужа и ежа, а в киберпространстве — запросто! Но пусть нам и трудно точно классифицировать всех наших врагов, с основными категориями вредоносного ПО все-таки стоит познакомиться.

Вирусы
Viruses

В обыденной жизни и в СМИ вирусом называют любую вредоносную программу — все, чем «болеет» компьютер. Технически это не вполне корректно.

Вирус отличает от других зловредов его способность к самораспространению и свойство внедряться в код других программ или системные области на устройстве. То есть он ведет себя подобно биологическому вирусу, который проникает в живые клетки и там размножается, а затем передается дальше. (Кстати, честь открытия вирусов принадлежит русскому ученому Дмитрию Ивановскому.)

Эпидемии компьютерных вирусов вспыхивают подобно эпидемиям гриппа и также лечатся «противовирусными препаратами» — специальными программами, иногда уникальными для каждого вируса.

Ваш антивирус может оказаться неэффективен против нового вируса — как прошлогодняя вакцина не может справиться с новым вирусом гриппа. Поэтому нужно регулярно обновлять базы вирусных сигнатур, но и это не гарантия. Всегда есть временной промежуток между появлением яда и противоядия. Так что антивирус — не панацея, а лишь средство гигиены. С его помощью перекрываются известные каналы заражения и определяется набор «таблеток» от известных вирусов, если ваш компьютер или телефон подцепили кого-то из них.

То есть у каждого есть риск оказаться «нулевым пациентом» — быть первым, у кого обнаружат неведомый ранее вирус. Поэтому не стоит слишком расслабляться, даже если у вас стоит самый новый и навороченный антивирус. Враг не дремлет!

Черви
Worms

Червь — совершенно другой зверь. Если вирусу нужен переносчик в виде дискеты (в старое время), флешки или зараженного файла, то червь

распространяет себя сам. Существует несколько разновидностей червей.

Интернет-червь — первый червь в истории. Будучи однажды запущенным, он стремится заполонить собой всю сеть. Ему вообще не нужен никакой «транспорт». Этот червь сканирует подряд IP-адреса, и, если находит незащищенное подключенное устройство, проникает в него. Теоретически червь такого типа может заразить весь интернет менее чем за 15 минут. Его назвали «червь Уорхола» — в честь Энди Уорхола, автора изречения «В будущем каждый получит шанс на 15 минут славы». Эпидемия червя SQL Slammer, заразившего в 2003 году более 75 тысяч серверов за 10 минут, была близка к этой модели распространения.

Обычно скорость распространения червей меньше, так как они используют более сложные техники. Например, находят в компьютере список пользователей и пытаются взломать их пароли, чтобы атаковать и эти системы. В 2001 году во время эпидемии червя CodeRed II за 28 часов заразились около 350 тысяч узлов сети.

Почтовый червь действует несколько иначе. Попав в компьютер, он начинает рассылать сообщения всем контактам из адресной книги пользователя якобы от его имени. При этом червь для убедительности прикрепляет к сообщению

какой-либо файл с диска, предварительно заразив его. В результате адресат получит зловреда, а файлом-переносчиком может послужить любой документ: любовное письмо, конфиденциальный контракт, очень личная фотография или копия паспорта. Здесь мы уже видим и черты вируса: есть переносчик «болезни», а для заражения требуется опрометчивое действие человека. Хотя некоторые почтовые черви — например, Nimda — могут активироваться даже в режиме предварительного просмотра сообщений. Вы еще ни разу не кликнули на опасное письмо, а уже заразились.

Встречаются и другие типы червей, использующие уязвимости разных протоколов. Мы не собираемся изучать их во всех подробностях, но у нас есть вопрос: зачем их создатели это делают? Вариантов множество: от банального вредительства до скрытного майнинга криптовалют. Главное, что червь дает преступнику контроль над вашим устройством, и тот в результате может делать что угодно. Допустим, рассылать детскую порнографию. И когда в вашу дверь постучат сотрудники правоохранительных органов, вам придется доказывать, что вы были не в курсе, что конкретно делает ваш компьютер.

Трояны
Trojans

Это старый добрый троянский конь в декорациях компьютерной эры. Доверчивый пользователь

видит что-то полезное, загружает себе, открывает — а оттуда толпа разных зловредов.

Подобно древнегреческим воинам, вышедшим из деревянного коня, программа-троян открывает ворота вашей крепости, а дальше все происходит по уже известному сценарию: вредительство, кража данных, незаконное использование техники и прочее.

Например, получаете письмо от своего знакомого с приложенной картинкой — а это почтовый червь сам себя рассылает. Или скачиваете полезную программу с какого-то сайта, установили — и заразились. В отличие от обычных вирусов и червей, трояны не обладают механизмом репликации, но поскольку они хорошо замаскированы — спрятаны внутри «коня» — люди загружают их себе сами, часто — с удовольствием.

Специально для поклонников фирмы Apple: трояны уже стали обычным делом для маков и айфонов, тогда как обычные вирусы на этих устройствах встречаются редко. Все дело в том, что вы сами открываете дверь этому зловреду, и хваленая безопасность вендора здесь не имеет значения.

Вымогатели
Ransomware

Самый популярный на сегодняшний день тип зловреда — вымогатели. И своей популярностью

вымогатели обязаны предельно простой схеме монетизации: проникаешь в компьютер, шифруешь файлы (что чаще) или блокируешь систему — и вперед, требуешь выкуп. Обычно указываются сравнительно небольшие суммы — порядка 500 долларов, поэтому многие пострадавшие предпочитают заплатить. Иногда преступники выполняют свое обещание — присылают ключи дешифровки, иногда — нет.

Вымогателем может оказаться и вирус, и червь, и троян. Название происходит от слова 'ransom' — «выкуп». Оно отражает не механизм заражения, а суть действия зловреда. Этот способ криминального заработка зацвел буйным цветом с появлением криптовалют, когда стало практически невозможно отследить получателя выкупа.

Если вы стали жертвой вымогателей, не спешите им платить — сначала разберитесь, что за «зверь» на вас напал. Есть простые зловреды, которые только блокируют доступ к функциям системы, и от них, как правило, можно избавиться без выкупа.

С шифровальщиками дело обстоит хуже. Если зловред написан грамотно, то шансов взломать его шифр практически не существует. Тогда жертва встает перед выбором: платить или не платить. Отказ означает утерю всех своих данных. Но перед таким выбором может встать лишь тот пользователь, который не делает резервное копирование важ-

ных файлов. А кто регулярно их копирует, может с легким сердцем послать преступников в любом удобном направлении и восстановить данные.

Показательный случай произошел в ноябре 2016 года, когда троян HDDCryptor, известный также под именем Mamba, зашифровал более двух тысяч серверов Агентства муниципального транспорта Сан-Франциско (SFMTA) и потребовал выкуп в размере 100 биткойнов (на тот момент — 73 тысячи долларов). Система управления транспортом поездов от этой атаки не пострадала, но билетные автоматы и многие внутренние системы были выведены из строя.

Агентство блестяще справилось с ситуацией — просто выключило турникеты и открыло метро для бесплатного проезда. Горожане даже подумали, что это рекламная акция. Тем временем инженеры агентства восстановили данные из резервных копий, и уже на следующий день городской транспорт заработал в обычном режиме. Злоумышленник остался с носом[1].

Вы еще не озаботились резервным копированием ваших файлов? Это самый простой и надежный способ защиты от кибервымогателей, а заодно и от таких несчастий, как кража ноутбука или неожиданный потоп, устроенный соседями сверху.

---

1 *San Francisco Rail System Hacker Hacked. // Krebsonsecurity.com, 16 ноября 2016.*

Шпионы
Spyware

В отличие от вымогателей, программа-шпион ничем себя не выдает. Сидит себе тихо, собирает ваши данные и передает своему хозяину. Зачем? Как правило, жуликов интересуют только деньги. И чтобы украсть их у пользователя ПК, шпион охотится за номерами его счетов и банковских карт, логинами и паролями к интернет-банкам или даже к криптокошельку.

Но случается, что шпионским софтом пользуются правоохранительные органы или спецслужбы. Во многих странах это разрешено законодательством. К сожалению, трудно провести четкую грань, когда эти средства применяются для поимки настоящих преступников, а когда — для слежки за гражданами.

Что может делать шпион? Грубо говоря, все: подслушивать, подглядывать, читать вашу переписку, фиксировать местонахождение. Ну а дальше все зависит от планов владельца шпионской программы. Например, шпион может не размениваться по мелочам, а долго и упорно ждать поступления крупной суммы на счет, — и как только она поступит, в один момент ее похитить.

Наверное, вам уже захотелось установить защиту от программ-шпионов, правда? Но не спешите! Здесь, как и в шпионских фильмах, полно двойных агентов.

Интернет кишит поддельными антишпионскими программами, разумеется, бесплатными. Но вместо того, чтобы защитить вас, они запустят в ваш компьютер стаю новых зловредов. Чтобы не попасться на эту удочку, предварительно изучите «досье» защитника, посмотрите отзывы об этом ПО в авторитетных источниках.

Рекламное ПО
Adware

Adware — зверек назойливый, но не слишком опасный. Как можно догадаться, его название происходит от слова 'advertisement' — «реклама». Его миссия состоит в том, чтобы показывать вам рекламные объявления, когда вы этого не хотите. Его излюбленное место обитания — браузер, ведь именно через браузер вы «смотрите» на мир.

Разработчики этого ПО получают доход от показов рекламы и кликов. Но если бы они показывали что-то стоящее! Чаще всего с помощью adware рекламируют такую ерунду, что кликнуть можно только случайно. И вы обязательно кликните, если весь экран будет завален всплывающими окнами, которые никак не получается закрыть! В этот момент автор зловреда и получит свою трудовую копеечку. Стоит ли объяснять, что он заинтересован, чтобы вы как можно дольше терпели все это рекламное безобразие на своем компьютере.

Поэтому создатели рекламного ПО стараются делать свои продукты приставучими как репей. И преуспевают в этом. Чаще всего пользователю не удается самостоятельно удалить adware, и приходится прибегать к помощи антивирусов с соответствующим функционалом.

Но и рекламщики не дремлют. В 2015 году выяснилось, что рекламное ПО Vonteera отключает многие антивирусы, чтобы те его не удалили. А это уже за гранью! Если раньше еще можно было относиться к adware снисходительно, поскольку серьезной угрозы для пользователя это ПО не представляло, то теперь — нет. Отключение антивируса означает, что ваш компьютер остается беззащитным перед другими атаками, чего нельзя допускать ни в коем случае.

Таким образом, можно констатировать, что рекламное ПО окончательно перешло на темную сторону и является полноценным зловредом.

Фейковое ПО
Scareware

Строго говоря, scarware — не вполне зловред. Скорее, это — безобидная бабочка — стеклянница, притворяющаяся грозной осой. Scarware пытается напугать пользователя, чтобы тот сделал необдуманную покупку. Например,

фейковое ПО может сообщить, что ваш ПК вдруг заразился страшным вирусом, и если вы прямо сейчас не купите «противоядие», то рискуете остаться без компьютера.

Происходит имитация угрозы и навязывание покупки совершенно бесполезного товара. И хорошо, если просто бесполезного, а не зловредного. Правда, тогда это не scarware, а троян.

Казалось бы, банальный «развод», но это работает. Многие покупают навязываемые пустышки. Чтобы не оказаться в их числе, выберите доверенного поставщика средств антивирусной защиты, установите их и пользуйтесь. Как увидите всплывающее окно с информацией об инфекции, проверьте с помощью антивируса, насколько эта информация правдива. Если новоявленный спаситель предлагает отключить установленные средства защиты, это — стопроцентный зловред.

Различные «чистильщики реестра», «оптимизаторы Windows», «ускорители» и тому подобное часто оказываются фейками, имитирующими бурную деятельность. Они пытаются заманить пользователей яркими картинками, щедрыми скидками (до 90%!) и фантастическими обещаниями. Безусловно, среди них есть и полезные программы. И уход за ком-

пьютером действительно необходим. Но будьте бдительны, проверяйте репутацию продуктов и поставщиков.

К настоящему моменту проблема фейкового ПО достигла такого масштаба, что Microsoft объявил ему войну. С 1 марта 2018 года Windows Defender и другие продукты Microsoft начали классифицировать программы, отображающие принудительные сообщения как нежелательные и подлежащие удалению при обнаружении.

Руткиты
Rootkits

Руткит представляет собой набор программ, предназначенных для доступа к компьютеру в обход стандартных путей. Кроме того, он часто маскирует другое ПО, чтобы его не обнаружили ни пользователь, ни антивирус.

Название происходит от слова «root» — так во многих системах называлась учетная запись самого привилегированного пользователя. То есть руткит дает злоумышленнику администраторские полномочия, и тот может делать с вашим компьютером все, что ему заблагорассудится.

Классно, не правда ли? Одна проблема: как руткит незаметно установить на вашем ПК? Здесь

на помощь преступникам приходят наши старые знакомцы — трояны и социальная инженерия. Обнаружить руткит сложно, а удалить, случается, и вовсе невозможно. Иногда для этого требуется переустановка операционной системы или даже замена оборудования.

Известность руткиты получили после скандала с защитой от копирования компакт-дисков компании Sony BMG. Если бы в 2005 году вы купили один из 22 миллионов CD с записями поп-музыки и прослушали его на своем плеере, никаких проблем не случилось бы. А вот если бы вы решили прослушать этот диск на компьютере, то на нем без вашего согласия и без каких-либо предупреждений автоматически установилась бы DRM-система (Digital Rights Management — управление цифровыми правами).

Чтобы скрыть следы своей диверсии, Sony BMG добавила в пакет установки руткит, который изменял поведение Windows. В результате операционная система переставала видеть все файлы и папки с названиями, начинавшимися с символов «sys». Именно в такой папке и пряталась DRM-система звукозаписывающей компании.

Скандал разразился 31 октября 2005 года, когда исследователь компьютерных угроз Марк Руссинович (ныне технический директор Microsoft Azure) опубликовал в своем блоге подробный анализ программного обеспечения, установлен-

ного на его компьютер при проигрывании музыкального диска. Кроме блокировки копирования, этот секретный софт еще шпионил за пользователями, отправляя отчеты об их музыкальных привычках производителю.

В ответ на упреки в нарушении прав граждан один из руководителей Sony BMG Томас Хессе раздраженно заявил в интервью: «Большинство людей даже не знают, что такое руткит, так почему они должны волноваться об этом?» Да потому, что этот руткит, делая файлы и папки невидимыми для системы, включая антивирус, тем самым пробивал огромную брешь в безопасности компьютеров. И этим молниеносно воспользовались хакеры. Прошло всего девять дней, и появился вариант зловреда Breplibot, который использовал этот «подарок» от борцов с пиратством.

Бэкдоры
Backdoors

Буквально "backdoor" — «задняя дверь», или, как мы чаще называем, «черный ход». Это специально или случайно оставленная разработчиками лазейка, позволяющая получить доступ к данным или к удаленному управлению всей операционной системой в обход стандартных мер безопасности.

Зачем оставляются такие лазейки? Например, чтобы восстановить забытый вами пароль

и спасти ваши данные. Но некоторые вендоры утверждают, что никаких бэкдоров у них нет в принципе, и помочь они не в состоянии. В частности, Apple по этой причине отказалась вскрывать айфон террориста, несмотря на давление полиции.

Бэкдор — любой метод, с помощью которого авторизованные и неавторизованные пользователи могут обойти обычные меры безопасности и получить высокий уровень доступа пользователя (он же root-доступ) в компьютерной системе, сети или программном приложении.

Снифферы
Sniffers

Сниффер, или анализатор пакетов, — программа для перехвата сетевого трафика. Полезная вещь, которую администраторы используют для диагностики сети, в том числе для выявления вирусной активности, а хакеры применяют этот инструмент, чтобы украсть логины и пароли пользователей, особенно бесплатных wi-fi сетей.

Сам по себе сниффер — вполне легальная и нужная в хозяйстве штука, примерно как отвертка в доме. Представляете, сколько на свете продается разных отверток? Вот и снифферы предлагаются в избытке. А это означает высокую вероятность того, что кто-то может использовать их в корыстных целях.

Известны случаи установки сниффера на компьютер жертвы при помощи трояна, а, установив сниффер, преступник может удаленно анализировать ваш сетевой трафик — со всеми вытекающими неприятными последствиями.

Ботнет
Botnet

Ботнеты — сети из зараженных компьютеров «зомби», которые могут использоваться для DDoS-атак, рассылки спама, распространения вирусов и других деструктивных действий. На каждом из «зомби» установлен специальный агент — бот, находящийся в «спячке», пока не поступит команда от хозяина сети.

Некоторые ботнеты достигают огромных размеров. Например, Necrus, появившийся в 2012 году и здравствующий до сих пор, содержит 6 миллионов зараженных устройств. В ноябре 2017 года с его помощью преступники осуществили рассылку нового штамма вируса-шифровальщика Scarab. В результате массовой компании было отправлено около 12,5 миллионов инфицированных электронных писем. Скорость рассылки превысила 2 миллиона писем в час.

В «зомби» могут превратиться не только компьютеры, но и любые умные устройства, подключенные к сети: веб-камеры, телевизоры,

пылесосы, кофеварки и даже лампочки. Ведь для участия в DDoS-атаке много ума не требуется, достаточно постоянно посылать один и тот же запрос на указанный адрес.

Например, летом 2016 года — во время Олимпийских игр в Рио-де-Жанейро — один из ботнетов, основу которого составляли около 10 тысяч зараженных веб-камер, проводил многочисленные и продолжительные DDoS-атаки. Но, несмотря на участившиеся подобные случаи, производители IoT-устройств пока не слишком задумываются об их безопасности.

Майнеры
Miners

Когда стоимость биткойна резко взлетела вверх, киберперступники тут же придумали новый способ заработка: на компьютер жертвы тайно устанавливается майнер криптовалюты, который работает на благо своего владельца, но за счет хозяина оборудования. Таким образом, преступник получает свои монеты практически задаром, а вы платите за электричество и недоумеваете, почему ваш ПК так медленно работает.

Майнер не крадет ваши деньги и данные, он просто использует ваши ресурсы. По сравнению с прочими видами угроз эта, надо признать, не самая страшная. Но все равно обидно!

Мобильные зловреды
Mobile malware

Смартфон, младший брат компьютера, болеет теми же болезнями, что и старший братишка. Есть мобильные вирусы, трояны, кейлоггеры, шпионы, вымогатели, ботнеты и даже майнеры криптовалют. Предсказуемо, что на Android их больше, но и на iOS зловреды тоже достаточно частые гости. Считать, что устройства Apple на 100% безопасны, было бы весьма наивно.

Встречаются на мобильных устройствах и специфические вредоносы. Например, одним из первых способов заработка, придуманных мошенниками, была отправка SMS на платные короткие номера.

Также весьма востребован в преступном мире перехват звонков и особенно SMS. Это не только позволяет ревнивым мужьям и женам удовлетворить свое любопытство (к слову, с нарушением Уголовного кодекса РФ), но еще и помогает воровать деньги со счетов.

Даже если вы устанавливаете приложения только из официальных магазинов, это еще не гарантия от рисков. Зловреды проникают и в продукты из официальных магазинов — под видом нормальных приложений. Еще одна уловка жуликов — chargeware. Это ПО совершает покупки через приложения без вашего ведома. Никаких оповещений на экране вы не увидите, а деньги уплывут в неизвестном направлении.

Разумеется, это не исчерпывающий перечень угроз, к тому же их число постоянно растет. Чтобы оценить, какое вредоносное ПО наиболее популярно на подпольных форумах, исследователи Insikt Group проанализировали около 4 миллионов сообщений на русском, английском, китайском и других языках. В период с мая 2018 по май 2019 года они выявили более 100 тысяч вариантов вредоносных программ в 61 категории[1].

Перед любым продавцом вредоносного ПО стоит серьезная проблема: как бороться с конкуренцией, особенно с альтернативными продуктами? В ход идут известные маркетинговые приемы. Продавцы троянов и спам-сервисов предоставляют праздничные скидки, а надежные анонимные хостеры выплачивают реферальные бонусы существующим клиентам, отправляющим к ним новых заказчиков, — прямо как в акциях «приведи друга».

Но преступник и честность — понятия несовместимые. На этом подпольном рынке процветает обман и надувательство. Например, был случай, когда продавец программы-вымогателя встроил в свой продукт еще и майнер биткойнов, который работал на компьютере покупателя. Но покупатели не остаются в долгу — malware взламывают также, как и обычный коммерческий софт, а разработчики жалуются на пиратов, использующих их продукты без лицензии. Вот уж воистину «вор у вора дубинку украл».

---

1 *Bestsellers in the Underground Economy: Measuring Malware Popularity by Forum, 2019.*

Кибероружие

Правительства многих стран берут на вооружение хакерские методы и разрабатывают кибероружие. Перед этим оружием ставятся самые разные задачи: от обычного шпионажа до выведения из строя промышленных объектов или даже провоцирования катастроф.

Впервые о кибероружии заговорили в 2010 году, когда был обнаружен червь Stuxnet. Существует предположение, что этот червь — специализированная разработка спецслужб Израиля и США, направленная против завода по обогащению урана в Иране. Естественно, этого никто не признал.

> *Stuxnet — непростой червь. Он поражал не все компьютеры, а только определенной модели Siemens S7-417, применяемой на химических заводах. И не все подряд, а лишь те, которые использовались для настройки программируемых логических контроллеров — устройств, непосредственно управляющих работой оборудования. Для этого червь проверял наличие в компьютере специального софта Step 7. Но это еще не все. Червь активировался только в тот момент, когда к зараженному компьютеру подключали для настройки высокочастотные преобразователи энергии. И, опять же, не абы какие преобразователи, а произведенные компанией VaCom. Как раз такие использовались на иранском заводе.*

В итоге Stuxnet нарушил работу почти 1000 центрифуг для обогащения урана. При этом авторы червя сумели настолько ловко замести следы, что иранские специалисты списали инцидент на ме-

ханические проблемы с оборудованием. Очень может быть, что этот эпизод стал первым случаем успешного применения кибероружия.

Наши домашние устройства вряд ли станут целями столь мощных и изощренных атак. Но эта история интересна нам тем, что червя Stuxnet не заметил ни один антивирус. Его обнаружили лишь годом позже, когда он уже успел выполнить свою задачу. Отсюда неутешительный вывод: в киберпространстве нападающая сторона имеет преимущество, а, следовательно, наши средства защиты, увы, не всегда смогут защитить наши ПК.

В киберпространстве нападающая сторона имеет преимущество, а, следовательно, наши средства защиты не всегда смогут защитить наши ПК.

Так что же делать? Неужели сдаваться?

Нет. Просто нужно научиться осмотрительности, ведь основная причина подавляющего большинства случаев заражения и других неприятных инцидентов — человеческий фактор, то есть мы с вами, беспечные пользователи.

Берегите свои данные!

Контрольные вопросы

1. Что такое вирусы? Когда они появились?

2. Какие разновидности зловредов вы знаете?

3. Как трояны попадают в компьютер?
4. Что значит DDoS?
5. Что такое ботнеты и зачем они нужны?
6. Что такое вирус-шифровальщик и в чем его опасность?
7. Какой лучший способ защиты от вируса-вымогателя?
8. Чем плохо рекламное ПО (adware)?
9. Зачем создается фейковое ПО?
10. Что такое руткит и в чем его опасность?
11. Как избежать заражения своего компьютера?
12. Насколько безопасны айфоны?
13. Какие особые типы вирусов поражают смартфоны?