ГЛАВА 1

История защиты программного обеспечения

Прежде чем мы начнем рассматривать приемы атак ПО и техники защиты от них, хотелось бы дать вам представление о долгой и интересной истории безопасности программного обеспечения. Краткий обзор главных событий в этой области за последние 100 лет позволяет более или менее ясно представить технологию, на которой основываются современные веб-приложения. Попутно вы увидите, что разработка механизмов безопасности всегда тесно связана с находчивостью и дальновидностью хакеров, которые все время ищут способы взломать или обойти эти механизмы.

Истоки хакерства

За последние два десятилетия хакеры не только приобрели известность, но и стали пользоваться дурной славой. В результате не знакомому с этой областью человеку может показаться, что хакерство связано исключительно с Интернетом и что массовым это явление стало в последние 20 лет.

Это так лишь отчасти. Разумеется, число хакеров резко возросло с возникновением Всемирной паутины, но первые из них появились в середине XX века, а возможно, и раньше. Все упирается в определение самого понятия «взлом». Эксперты спорят, в каком же именно десятилетии появились хакеры, потому что некоторые примечательные события, случившиеся в начале прошлого века, очень напоминают современные хакерские атаки.

К примеру, в 1910-х и 1920-х годах наблюдались отдельные характерные случаи, которые можно квалифицировать как взлом. Большинство из них связано с вмешательством в работу передатчиков и приемников кода Морзе или радиоволн. Но эти события случались редко, и я не могу вспомнить ни одной крупномасштабной операции, которая была сорвана в результате злоупотребления этими технологиями.

Впрочем, я не историк. Я специалист по безопасности с опытом поиска и устранения глубоких архитектурных проблем и уязвимостей на уровне кода в корпо-

ративном ПО. До этого много лет работал инженером-программистом, создавая веб-приложения на разных языках и в различных средах. Я до сих пор продолжаю писать программы автоматизации безопасности, а в свободное время участвую в проектах. Поэтому не буду углубляться в исторические детали, а просто упомяну, что этот раздел основывается на многолетних независимых исследованиях и ключевое значение тут имеют уроки, которые можно извлечь из событий давно ушедших дней и применить сегодня.

Я не ставил перед собой цели сделать исчерпывающий обзор, поэтому в данной главе лишь кратко опишу основные исторические события, а отсчет мы начнем с 1930-х. Давайте же посмотрим, какие события привели к современной расстановке сил между хакерами и инженерами.

«Энигма», 1930-е

Показанная на рис. 1.1 электромеханическая роторная машина *«Энигма»* использовалась для шифрования и расшифровки текстовых сообщений, отправляемых по радио. Это устройство немецкого производства приобрело особую важность во время Второй мировой войны.

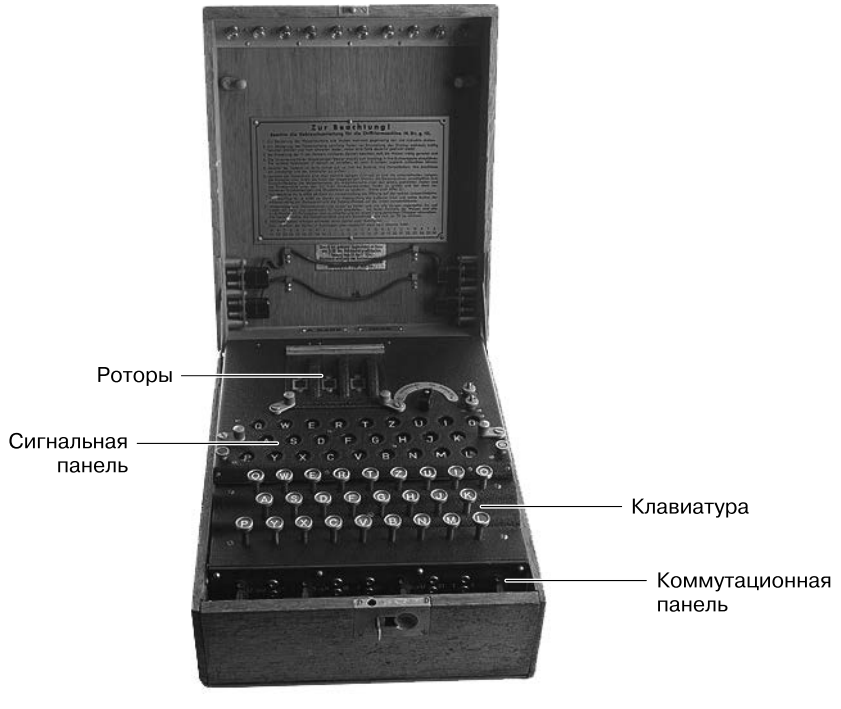

Рис. 1.1. Шифровальная машина «Энигма»

Устройство напоминало большую механическую пишущую машинку. При каждом нажатии клавиши роторы перемещались и записывали на первый взгляд случайный символ, который передавался на все ближайшие «Энигмы». На самом деле символы не были случайными, а определялись вращением ротора и параметрами конфигурации, которые можно было изменить в любой момент. Читать или расшифровывать отправленные сообщения могла только «Энигма» с идентичной конфигурацией. Именно это ценное свойство позволяло избежать перехвата важных сообщений.

Сейчас уже невозможно сказать, кто конкретно изобрел механизм шифрования на основе роторов, но популяризовала эту технологию немецкая компания Chiffriermaschinen AG, которой управляли два человека. В 1920-х годах представители этой компании путешествовали по Германии, демонстрируя технологию, в результате чего в 1928 году ее взяли на вооружение немецкие военные для обеспечения безопасности передачи сверхсекретных сообщений.

Предотвращение перехвата передаваемых на дальние расстояния сообщений стало достижением, которое раньше невозможно было даже представить. Перехват сообщений до сих пор остается популярной у хакеров техникой, которую называют *атакой посредника* (man-in-the-middle attack). И для защиты от таких атак современное ПО применяет методы, аналогичные (правда, гораздо более мощные) тем, которые использовались 100 лет назад машинами «Энигма».

Для своего времени эта машина была впечатляющим технологическим достижением, хотя и не лишенным недостатков. Для перехвата и дешифровки сообщений требовалась «Энигма» с такой же конфигурацией, как и у отправителя. Поэтому один раскрытый журнал конфигурации, или в современных терминах *закрытый ключ* (private key), мог вывести из строя всю сеть этих машин.

Для борьбы с этим все группы, отправляющие сообщения через «Энигму», регулярно меняли конфигурацию машин. Перенастройка занимала много времени. Во-первых, обмен журналами конфигурации происходил только лично, поскольку безопасных способов удаленного обмена данными еще не существовало. Для пары машин с двумя операторами это сделать нетрудно. Но для более крупной сети требовалось несколько курьеров, что увеличивало вероятность кражи журнала конфигурации или, например, его продажи.

Вторая проблема с передачей записей конфигурации заключалась в том, что перенастройка «Энигмы» проводилась вручную. И для этого требовался специально обученный сотрудник. Программного обеспечения в те времена еще не было, и корректировка конфигурации означала вмешательство в аппаратную часть, сводясь к изменению физической компоновки и проводки коммутационной панели. Настройщик должен был разбираться в электронике, а таких специалистов в начале 1900-х годов было крайне мало.

Сложность и длительность процесса перенастройки привела к тому, что обновления обычно производились раз в месяц. И только для особо важных линий связи это делалось ежедневно. Это означало, что перехват или утечка журнала конфигурации давали злоумышленникам — хакерам прошлого — доступ ко всем передачам до конца месяца.

Для машин «Энигма» использовался алгоритм, известный как симметричное шифрование. В этом случае для шифрования и дешифровки служит один и тот же криптографический ключ. Такая схема шифрования до сих пор применяется в ПО для защиты данных при передаче (между отправителем и получателем), но в классическую схему, ставшую популярной благодаря машинам «Энигма», уже внесено множество улучшений.

ПО позволяет создавать намного более сложные ключи. Современные алгоритмы генерации создают ключи, подбор которых методом перебора всех возможных комбинаций *(атака грубой силой)* на самом мощном современном оборудовании может занять более 1 млн лет. Кроме того, в отличие от перенастройки конфигурации машин «Энигма», программные ключи можно быстро менять.

Ключи могут пересоздаваться при каждом входе пользователя в систему, при каждом сетевом запросе или через определенный интервал времени. В результате при использовании такого типа шифрования в ПО утечка ключа дает доступ к одному сетевому запросу, в худшем случае, если ключ заново генерируется при входе в систему, доступ к сеансу появляется на несколько часов.

Если углубиться в историю современной криптографии, мы в итоге дойдем до 1930-х годов и Второй мировой войны. Можно с уверенностью утверждать, что машина «Энигма» стала важной вехой в обеспечении безопасности удаленной связи. Соответственно, именно ее можно считать отправной точкой для развития такой дисциплины, как защита программного обеспечения.

Это технологическое достижение породило и тех, кого сейчас называют хакерами. Ведь именно появление у стран гитлеровской коалиции машины «Энигма» заставило силы союзников разрабатывать методы взлома шифров. Генерал армии Дуайт Дэвид Эйзенхауэр говорил, что это необходимо для победы над нацистами.

В сентябре 1932 года польскому математику Мариану Реевскому (Marian Rejewski) предоставили украденную «Энигму». В октябре 1932 года французский шпион Ганс-Тило Шмидт (Hans-Thilo Schmidt) смог передать ему действующие конфигурации, что дало Реевскому возможность перехватывать сообщения и позволило начать анализ принципов шифрования, на которых основывалась работа машины. Мариан пытался определить как механический, так и математический принципы. Он хотел понять, как конкретная конфигурация аппаратного обеспечения приводит к выводу зашифрованного сообщения.

Попытки дешифровки базировались на ряде теорий относительно того, как определенная конфигурация машины влияет на результат вывода. Анализируя закономерности в зашифрованных сообщениях и выдвигая теории, основывающиеся на механическом устройстве «Энигмы», Реевский и его коллеги Ежи Ружицкий (Jerzy Różycki) и Генрих Зыгальский (Henryk Zygalski) в конечном счете смогли разобраться в принципе ее работы. Поняв порядок и положение роторов, а также схему соединений на коммутационной панели, команда смогла эмпирически определить соответствие между конфигурациями и шаблонами шифрования. У них получилось с приемлемой точностью перенастроить плату и после нескольких попыток приступить к считыванию зашифрованной радиопередачи. К 1933 году команда ежедневно перехватывала и расшифровывала сообщения, передаваемые «Энигмами».

Подобно современным хакерам, команда Реевского перехватывала поток данных и путем перестраивания схемы шифрования получала доступ к чужим ценным данным. Именно поэтому я считаю Мариана Реевского и его команду одними из первых хакеров.

Со временем Германия начала наращивать сложность шифрования для машин «Энигма». Для этого постепенно увеличивали число роторов, осуществляющих шифрование. В конце концов процесс перестраивания конфигурации стал слишком трудоемким, и команда Реевского не могла осуществить его за разумное время. Эта противомера отлично демонстрирует отношения, которые складываются между хакерами и теми, кто пытается им помешать.

Такие отношения существуют и сегодня, потому что изобретательные хакеры постоянно совершенствуют методы взлома программных систем. А по другую сторону хорошо подготовленные инженеры постоянно разрабатывают новые методы защиты.

Автоматизированный взлом шифра «Энигмы», 1940-е

Английский математик Алан Тьюринг (Alan Turing) наиболее известен благодаря разработке теста, известного сегодня как тест Тьюринга. Он предназначался для оценки сложности машинных диалогов и установления их отличий от разговоров с реальными людьми. В сфере искусственного интеллекта (ИИ) этот тест часто считается одним из ключевых принципов.

Наибольшую известность Алану Тьюрингу принесли работы, связанные с ИИ, но при этом он также был пионером в области криптографии и автоматизации. Перед

Второй мировой войной и во время нее исследования Тьюринга были сосредоточены в первую очередь на криптографии. С сентября 1938 года он по совместительству работал в Правительственной школе кодирования и шифрования (Government Code and Cypher School). Это одновременно научно-исследовательский институт и разведывательное управление, которое финансировалось британской армией и располагалось в особняке Блетчли-парк в Англии.

Исследования Тьюринга в основном были связаны с анализом машин «Энигма». В Блетчли-парке он занимался этим под руководством Дилли Нокса (Dilly Knox), который в то время уже был опытным криптографом.

Как и польские математики до них, Тьюринг и Нокс хотели найти способ взломать ставший значительно более мощным шифр немецких «Энигм». Благодаря сотрудничеству с Польским бюро шифров (Polish Cipher Bureau) они получили доступ ко всем проведенным десятью годами ранее исследованиям группы Реевского. Это означает, что к тому моменту британцы хорошо разобрались в том, как работала «Энигма». Они понимали взаимосвязь между роторами и электрической схемой и знали, как конфигурация устройства связана с шифрованием передаваемых сообщений (рис. 1.2).

Рис. 1.2. Пара роторов, использовавшаяся для калибровки конфигурации передачи машин «Энигма», — аналоговый эквивалент изменения первичного ключа цифрового шифра

Группа Реевского смогла обнаружить в шифровании закономерности, позволившие логически определять конфигурацию «Энигм». Но это решение было невозможно масштабировать на увеличившееся в десять раз количество роторов. За время перебора всех возможных комбинаций успевала выйти новая версия конфигурации. Поэтому перед Тьюрингом и Ноксом стояла задача найти решение, допускающее масштабирование. Фактически им требовался универсальный, а не узкоспециализированный метод.

Криптологическая «бомба» (рис. 1.3) представляла собой механическое устройство с электрическим приводом, которое пыталось автоматически реконструировать положение роторов в «Энигме», анализируя отправленные машиной сообщения.

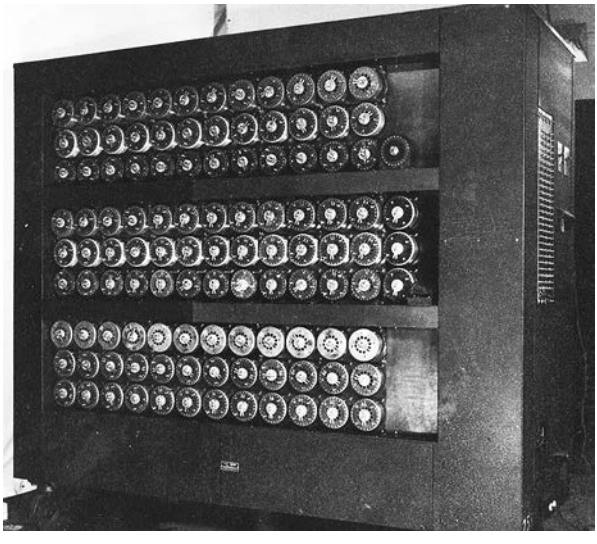

Рис. 1.3. Одна из первых «бомб» из Блетчли-парка, использовавшаяся во время Второй мировой войны (обратите внимание на то, сколько рядов роторов применялось для быстрого определения конфигурации «Энигм»)

Первая криптологическая «бомба» была создана поляками в попытках автоматизировать разработки Реевского. К сожалению, эти устройства определяли конфигурации не всех «Энигм»: например, они были неэффективны против машин с более чем тремя роторами. Масштабировать «бомбы» на «Энигмы» с более сложной конструкцией не получилось, и в военное время поляки вернулись к ручным методам расшифровки перехватываемых сообщений.

По мнению Алана Тьюринга, оригинальные машины не справились с задачей, потому что не были универсальными. Создание машины, способной определить конфигурацию «Энигмы» при любом количестве роторов, он начал с простого допущения: чтобы правильно разработать алгоритм дешифровки, нужно знать слово или фразу из зашифрованного сообщения и его позицию внутри сообщения.

К счастью, немецкие военные общались между собой, у них были приняты очень строгие правила коммуникации. В частности, каждый день машины «Энигма»

рассылали подробный региональный прогноз погоды. Благодаря этому все подразделения были в курсе погодных условий. Немцы не догадывались, что группа Тьюринга использует эти прогнозы как отправную точку для обратного проектирования.

Знание входных данных (прогноза погоды), отправляемых с помощью «Энигмы», значительно упростило алгоритмическое определение актуальных настроек этой машины. Полученную таким способом информацию Тьюринг использовал для разработки дешифровальной машины, работа которой не зависела от количества роторов в «Энигме».

Тьюринг попросил выделить средства на создание «бомбы», позволяющей точно определять конфигурацию «Энигмы», необходимую для перехвата и чтения зашифрованных сообщений. Как только бюджет был утвержден, Тьюринг сконструировал «бомбу», 108 барабанов которой вращались со скоростью 120 оборотов в минуту и позволяли проверить почти 20 000 конфигураций «Энигмы» всего за 20 минут. Это дало возможность быстро узнавать любую новую конфигурацию. Шифровальная машина «Энигма» перестала быть безопасным средством связи.

Сегодня такая стратегия обратного проектирования известна *как атака на основе открытых текстов* (known plaintext attack, KPA). Знание фрагмента зашифрованного текста значительно увеличивает эффективность алгоритма дешифровки. Подобные методы используются и современными хакерами для получения доступа к зашифрованным данным, хранящимся или применяемым в программном обеспечении. Созданная Тьюрингом машина стала важной исторической вехой, ведь это был один из первых автоматизированных инструментов взлома.

Фрикинг, 1950-е

После «Энигмы» и криптографической битвы между крупными мировыми державами следующим важным событием стало широкое внедрение телефонной связи. Телефон дал обычным людям возможность быстро связываться друг с другом, несмотря на расстояния. Но растущим телефонным сетям требовалась автоматизация.

В конце 1950-х годов телекоммуникационные компании, такие как AT&T, начали внедрять новые телефоны, звонок с которых автоматически направлялся на номер назначения на основе исходящих аудиосигналов. Нажатие клавиши на панели телефона вызывало звук определенной частоты, который интерпретировался на коммутаторе. Набор таких звуков преобразовывался в числа, и вызов направлялся соответствующему абоненту.

Тональный набор (tone dialing) стал важным усовершенствованием, без которого было бы невозможным функционирование крупных телефонных сетей. Он резко снизил расходы компаний, поскольку позволил обойтись без операторов, которые раньше осуществляли коммутацию вручную. Теперь хватало одного оператора, следящего за сетью на случай возникновения проблем. За время, которое раньше занимало обслуживание одного вызова, он мог управлять сотнями.

Но быстро нашлись люди, сообразившие, что системой, построенной на интерпретации звуковых сигналов, можно легко манипулировать. Воспроизводя звуки нужной частоты рядом с телефонной трубкой, можно менять функциональность устройства. Энтузиастов, экспериментировавших с этой технологией, в конечном счете стали называть *фрикерами* (phreakers). Фактически это предшественники современных хакеров, специализировавшиеся на взломе телефонных сетей. Точное происхождение термина не установлено, но чаще всего считается, что это комбинация слов freaking («проклятый», «чертов») и phone («телефон»).

Мне более осмысленным кажется другой вариант, согласно которому основой термина послужило словосочетание audio frequency («частота звуковых колебаний»), ведь телефоны того времени использовали язык звуковых сигналов. Тем более что хронологически возникновение термина «фрикинг» практически совпадает с появлением оригинальной системы тонального набора от AT&T. До этого момента вмешаться в работу телефонной линии было гораздо труднее, потому что при каждом звонке оператор на телефонной станции вручную соединял абонентов.

Наиболее примечательным событием, связанным с фрикингом, стало открытие того, что звук частотой 2600 Гц использовался AT&T как сигнал завершения вызова. По сути, это была управляющая команда, встроенная в систему тонального набора. Если издать звук такой частоты, система коммутации зарегистрирует вызов как завершенный, хотя на самом деле он остается открытым. Это позволяет бесплатно совершать междугородные и международные звонки.

Открытие частоты 2600 Гц часто связывают с именем подростка Джо Энгрессиа (Joe Engressia), который умел точно воспроизводить звуковые сигналы телефонной линии с помощью свиста и хвастался друзьям, демонстрируя тональный сигнал, мешающий набору номера. Некоторые считают Джо одним из первых фрикеров, хотя он сделал это открытие случайно.

Позже его друг Джон Дрейпер (John Draper) обнаружил, что игрушечные свистки, которые в качестве подарка клали в коробки с хлопьями Cap'n Crunch, издавали звук частотой 2600 Гц и, правильно применяя такой свисток, можно совершать бесплатные звонки в любую точку мира. Эта информация быстро распространилась, и в конечном счете появилось оборудование, позволяющее нажатием кнопки издавать звук определенной частоты.

Первое из этих устройств было известно под названием *«синий ящик»* (blue box). Оно почти идеально воспроизводило сигнал 2600 Гц, что позволяло воспользоваться уязвимостью телекоммуникационных систем для совершения бесплатных звонков. И это было только начало. Более поздние поколения фрикеров вмешивались в работу таксофонов, предотвращали выставление счетов за телефонную связь, имитировали сигналы военной связи и даже умели подделывать идентификатор вызывающего абонента.

Фактически архитекторы первых телефонных сетей учитывали только поведение обычных, законопослушных людей и их намерения общаться. В современном программном обеспечении такой подход называется проектированием по оптимистичному сценарию. Это привело к фатальной уязвимости, но послужило важным уроком, который актуален и сегодня: при проектировании сложных систем следует всегда исходить из наихудшего сценария.

В конце концов знание слабых мест системы тонального набора привело к выделению бюджетов на разработку мер противодействия фрикерам, направленных на защиту доходов телекоммуникационных компаний и увеличение надежности телефонной связи.

Метод борьбы с фрикингом, 1960-е

В 1960-х годах появилась новая технология набора телефонных номеров, известная как двухтональный многочастотный аналоговый сигнал (dual-tone multifrequency signaling, DTMF). Это была разработка компании Bell Systems, запатентованная и ставшая известной как Touch Tones. Она привязана к расположению кнопок телефона в виде трех столбцов и четырех рядов. Нажатие каждой кнопки приводит к подаче двух сигналов с разными частотами, а не одного, как в оригинальных системах тонального набора.

В табл. 1.1 приведены двухтональные сигналы с указанием используемых частот, соответствующие клавишам телефона.

Таблица 1.1. Частоты, используемые в двухтональных сигналах

1	2	3	**(697 Гц)**
4	5	6	**(770 Гц)**
7	8	9	**(852 Гц)**
*	0	#	**(941 Гц)**
(1209 Гц)	**(1336 Гц)**	**(1477 Гц)**	

Развитие технологии DTMF в значительной степени было связано с легкостью обратного проектирования систем тонального набора, чем и пользовались фрикеры. Разработчики из Bell Systems полагали, что благодаря системе DTMF, использующей два тона одновременно, злоумышленникам будет намного сложнее получить к ней доступ.

Двухтональный сигнал уже нельзя было легко воспроизвести человеческим голосом или свистком, что делало новую технологию более надежной. Это яркий пример успешной разработки средства обеспечения безопасности и противодействия фрикерам — хакерам той эпохи.

Механика генерации звуков DTMF проста. За каждой клавишей находится переключатель, заставляющий встроенный динамик испустить два сигнала: частота первого зависит от строки, в которой находится клавиша, а частота второго — от столбца. Именно поэтому сигнал и называется *двухтональным*.

Международный союз электросвязи (International Telecommunication Union, ITU) принял DTMF в качестве стандарта, а позже эту технологию начали применять не только в телефонии, но и в кабельном телевидении (для определения времени перерыва на рекламу).

Технология DTMF наглядно демонстрирует, что при правильном планировании на этапе разработки систему можно построить таким образом, что ее взлом будет затруднен. Разумеется, сигналы DTMF также поддаются декодированию, но для этого нужно приложить значительно больше усилий. Со временем коммутационные центры перешли с аналогового на цифровой ввод, что практически уничтожило фрикинг.

Начало компьютерного взлома, 1980-е

В 1976 году компания Apple выпустила персональный компьютер Apple 1. По сути, это была укомплектованная системная плата, к которой нужно было докупать и подключать корпус, источник питания, клавиатуру и монитор. Было произведено и продано всего несколько сотен таких устройств.

В 1982 году компания Commodore International выпустила Commodore 64 — персональный компьютер, которым сразу можно было пользоваться. Он поставлялся с собственной клавиатурой, имел встроенную поддержку звука и даже умел работать с многоцветными дисплеями.

До начала 1990-х продажи компьютера Commodore 64 доходили до 500 000 штук в месяц. Позже эта цифра начала ежегодно расти, и вскоре компьютеры стали обычным инструментом как в бизнесе, так и в быту, взяв на себя множество

рутинных задач, в том числе управление финансами, бухгалтерский учет и продажи.

В 1983 году американский специалист в области информатики Фред Коэн (Fred Cohen) создал первый компьютерный вирус. Этот вирус умел копировать сам себя и легко передавался с одного ПК на другой через дискеты. Он был встроен в обычную программу и замаскирован от всех, у кого не было доступа к ее исходному коду. Позже Коэн стал одним из первых специалистов по безопасности программного обеспечения, показав, что не существует алгоритма, способного обнаружить все возможные компьютерные вирусы.

В 1988 году аспирант факультета вычислительной техники Корнельского университета Роберт Моррис (Robert Morris) создал вирус, заразивший множество компьютеров по всей стране. Вирус приобрел известность как *червь Морриса* (Morris Worm), а сам термин «червь» стали использовать для обозначения самовоспроизводящегося компьютерного вируса. Уже в день своего выпуска червь Морриса заразил примерно 15 000 подключенных к сети компьютеров.

Впервые в истории правительство США задумалось о необходимости официальных предписаний для подобных случаев. Счетная палата оценила ущерб от червя в 10 млн долларов. Морриса приговорили к трем годам условно, 400 часам общественных работ и штрафу в 10 050 долларов. Он стал первым хакером, осужденным в Соединенных Штатах.

В наши дни большинство хакеров вместо вирусов, заражающих операционные системы, создают вирусы, нацеленные на браузеры. Современные браузеры предоставляют чрезвычайно надежный механизм обеспечения безопасности программ. Веб-сайт не может запустить исполняемый код, направленный против операционной системы хоста, вне браузера без явного разрешения пользователя.

Хотя атаки современных хакеров в первую очередь нацелены на пользовательские данные, к которым можно получить доступ через браузер, у них есть много общего с атаками, нацеленными на операционные системы. Это такие вещи, как масштабируемость (возможность переходить от одного пользователя к другому) и маскировка (сокрытие вредоносного кода внутри обычной программы).

В современных условиях масштабирование атак происходит через электронную почту, социальные сети или мессенджеры. Некоторые хакеры даже создают законные сети для продвижения одного вредоносного сайта.

За безобидно выглядящим интерфейсом может скрываться вредоносный код. Для фишинга (кражи конфиденциальных данных пользователей) создаются страницы, которые выглядят как реальные социальные сети или сайты банков. Подключаемые модули для браузера (плагины) часто ловят на краже данных, а иногда хакеры находят способы запустить свой код на чужих сайтах.