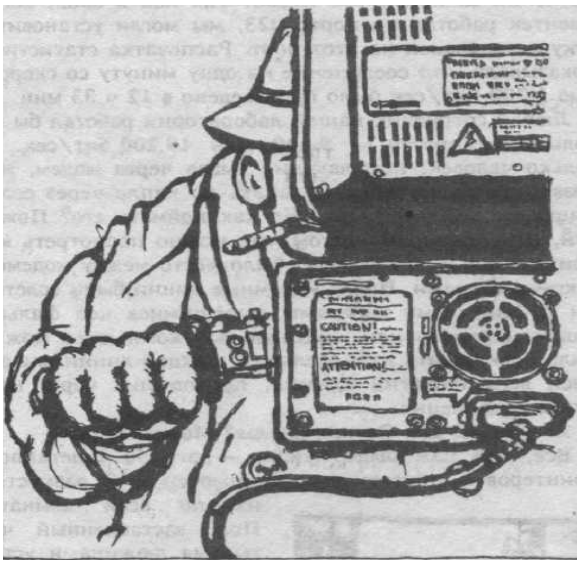
Некто незамеченным подключался к компьютерной сети военных для сбора сверхсекретной информации, но кто? В этой невыдуманной детективной истории астроном Клиффорд Стоулл рассказывает, как он проследил путь, которым таинственный хакер высокого класса осуществлял свою шпионскую деятельность. Отрывок перепечатан из сентябрьского номера журнала PC/Computing за 1989 год.



Кукушкино яйцо

Пора начинать разговоры. А то Алиса считает, что книжка без картинок или хотя бы без разговоров — книжка неинтересная.

Л.Кэролл

Я — ас системного программирования?

Еще неделю тому назад я был астрономом, с удовольствием конструирующим оптику для телескопов. Но я нашел себя, перейдя из обсерватории Кек Берклиевской лаборатории в компьютерный центр на цокольном этаже того же здания.

С обеих сторон от моей новой рабочей комнаты располагались конторы двух системных программистов — Вэйна Грэйвса и Дэйва Кливленда — опытнейших специалистов. Вэйн, Дэйв и я должны были обеспечивать работу компьютеров для общелабораторного пользования. Мы обслуживали дюжину главных компьютеров общей стоимостью около 6 миллионов долларов — огромных "рабочих лошадок" для решения физических задач. Предполагалось, что ученые - пользователи компьютеров, получат простую, но мощную компьютерную систему, надежную, как электрическая компания. Это означало, что машины работают непрерывно в течение суток. Мы, как компания, оказывающая услуги по использованию компьютеров, брали плату за использование машинного времени.

На второй день моей работы Дэйв тихо ворчал о каком-то непорядке в бухгалтерской системе UNIX. Кто-то, должно быть, использовал несколько секунд машинного времени, не заплатив за них. Компьютерные счета не совсем сходились: за последний месяц они показывали недостачу в 75 центов при общей сумме 2.387 долларов.

Надо сказать, что ошибка в несколько тысяч долларов тривиальна и легко может быть найдена. А ошибки в колонке цифр, соответствующих пенни, возникают от глубоко спрятанных проблем. Таким образом, поиск этих ошибок — подходящий тест для начинающего системного программиста.

Около 7 часов утра мой взгляд остановился на имени одного пользователя — Хантера. Парень не имел реального адреса для расчетов. Ха! Да это Хантер использовал на 75 центов времени в прошлом месяце, но никто не заплатил за него. Здесь и был источник нашего дисбаланса. Кто-то "зацепился*4 за нашу систему, когда к ней добавляли нового пользователя. Тривиальная проблема, вызванная тривиальной ошибкой.

На следующий день малоизвестный пользователь по имени Докмастер прислал нам электронную почту. Менеджер его системы заявил, что кто-то из нашей лаборатории пытался подключиться к его компьютеру
в конце недели (в выходные дни). Я заинтересовался, не связан ли Докмастер со строительством военных кораблей, на что указывал его пароль. Это было неважно, но стоило потратить несколько минут, чтобы выяснить этот вопрос.

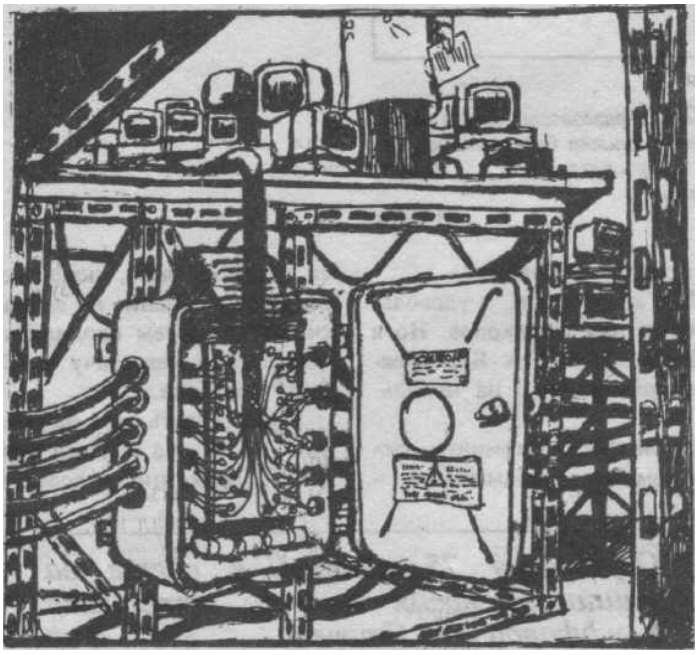
Почта указывала дату и время, когда кто-то с нашего UNIX-компьютера пытался подключиться к компьютеру Докмастера. Бухгалтерский файл указывал пользователя Свентека, подключившегося к нашей системе в 8 ч 25 мин, ничего не делавшего в течение получаса и затем отключившегося. В это время не было зарегистрировано никакой работы. Наша примитивная система также зарегистрировала деятельность Свентека, но указала время использования сети с 8 ч 31 мин до 9 ч 01 мин утра.

Ого! Еще одна проблема счета. Временные отметки не совпадают. Одна — показывает активность, когда другая — что все спокойно.

Почему две счетные системы показывают разное время? И почему некоторая активность была отмечена в одном файле без индикации ее в другом? Связано ли это с предыдущей проблемой оплаты? Исказил ли я показания файлов, когда искал ошибку?

Или есть другое объяснение — в недостаче виновен хакер?

Итак, как найти хакера, если он действительно существует? Я представил себе, что сделать это просто: надо только следить за каждым, кто использует счета Свентека и постараться проследить эти вызовы. Весь вторник я изучал журнал работы пользователей. Я написал программу, по которой мой терминал издавал звуковой сигнал, когда кто-либо подключался к сети.



В четвергв 12 ч 33 мин подключился Свентек. Я почувствовал прилив адреналина в крови и полное падение его уровня, когда Свентек через минуту исчез. Где он? Единственным указателем был идентификатор его терминала: использовался терминальный порт tt23. Я подозревал, что это было телефонное включение, но не сбрасывал со счетов возможности работы кого-то из лаборатории.

По счастливой случайности, соединение оставило следы. Техник по скрытому оборудованию, которого было трудно разглядеть в дебрях телефонных проводов, собирал статистику о том, сколько людей используют наш коммуникационный пункт включения. Совершенно случайно он записал номера портов всех соединений за последний месяц. Так как я знал, когда Свентек работал на порте tt23, мы могли установить, откуда он вышел на этот порт. Распечатка статистики показывала, что соединение на одну минуту со скоростью 1.200 бит/сек было произведено в 12 ч 33 мин.

Любой сотрудник нашей лаборатории работал бы на большой скорости — 9.600 или 19.200 бит/сек. И только человек, посылающий вызов через модем, мог позволить своим данным капать по капле через соломинку по 1.200 бит/сек. Но как поймать его? Пожалуй, единственным местом, где можно посмотреть все приходящие к нам вызовы, было место между модемом и компьютерами. Наши модемные линии были толстыми 25-жильными кабелями, змеящимися под фальшполом. Принтер или персональный компьютер можно было подключить параллельно к каждой линии для записи всех нажатий клавиш, проходящих через наш пункт соединения.

Авантюра? Да. Осуществимая? Может быть.

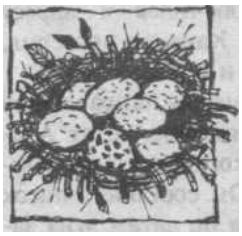
Все, что нам было нужно — это 50 телетайпов, принтеров и портативных компьютеров. Я разместил их по всей комнате. Пол, заставленный четырьмя дюжинами устаревших телетайпов и портативных компьютеров, выглядел как кошмарный сон инженера- электронщика. Я спал в центре этого сооружения, ухаживая за принтерами и компьютерами. Каждый из них собирал данные с какой-либо линии, и я просыпался от шума принтера, как только кто-нибудь подключался к нашей системе. Каждые полчаса в принтере кончалась бумага или заполнялась дискета в компьютере, и я должен был проматывать бумагу и менять дискеты. В субботу утром меня разбудил мой коллега. "Ну, где же твой хакер?"

Первые 49 принтеров и мониторов не показывали ничего интересного. Но из пятидесятого вышла распечатка длиной в 80 футов (-25 м). Ночью кто-то проскользнул как уж в нашу операционную систему.

Три часа хакер прогуливался по моей системе, читая все, что ему захочется. И не знал о том, что мой принтер DECwriter фиксирует все его действия. Там была каждая команда, введенная в компьютер, каждая опечатка и каждый ответ компьютера.

Этот принтер контролировал линию из Тимнета от компании, которая связывает компьютеры со всего света. Наш хакер мог быть где угодно.

Хакер стал привилегированным пользователем. Он был очень похожим на кукушку. Кукушка — это птица-паразит гнезд, которая откладывает яйца в чужие гнезда, и кукушкины птенцы выживают, если хозяйка гнезда игнорирует своих собственных птенцов. Наш загадочный визитер положил свою программу-яйцо в наш компьютер, заставил систему "высиживать" его и "кормить" привилегиями.



В это утро хакер написал короткую программу для захвата привилегий. Обычно система UNIX не допускает выполнения такой программы, так как никогда не дает привилегий выше установленных для пользователя. Но если хакер запускает свою программу из области с привилегированным денежным счетом, он становится привилегированным пользователем. Его задача состоит только в том, чтобы замаскировать эту программу — "кукушкино яйцо" — так, чтобы система "высиживала" его.

Каждые пять минут система UNIX выполняет собственную программу atrun. В свою очередь, atrun составляет график выполнения других задач и выполняет рутинные уборочные работы. Она идет в привилегированном режиме с

использованием всех возможностей и доверия операционной системы. Если заменить ее фальшивой программой, последняя будет выполняться каждые пять минут со всеми системными привилегиями. По этой причине программа atrun помещена в защищенную область системы, доступную только администратору системы. Никто другой не имеет прав доступа к atrun.

Здесь было "гнездо" для "кукушки": за пять минут она должна была заменить системную программу atrun своим "яйцом". Для этого нападения нужно было найти способ подбросить программу-яйцо в гнездо защищенной области системы. Барьеры операционной системы специально устроены так, чтобы не допустить этого. Но в системе была необдуманная часть, на которую мы никогда не обращали внимания.

Мы использовали мощную программу редактирования Gnu-Emaks. Но Gnu обладала большими возможностями, нежели просто редактор текстов. Это был фундамент, на котором могли строиться другие программы. Она даже имела встроенные средства для почты. Но вот незадача: в ее программном обеспечении была ошибка.

Из-за того, что программа Gnu была установлена в нашем компьютере с UNIX именно таким способом, редактор программы давал пользователю возможность посылать файл с почтой со своего на любой другой компьютер. Gnu-Emaks не проверяла, кто получает почту и хочет ли он ее получать. Никаких проблем в пересылке файла из вашей области машинной памяти в мою. Но лучше бы у вас не было возможности переписать файл в защищенную область системы: только администратор системы имеет право работать в ней.

Gnu не проверяла этого. Она позволяла кому угодно перенести файл в защищенное пространство системы, Хакер знал это, мы — нет. Он использовал ошибку в почтовой системе Gnu-Emaks, чтобы добраться до защищенной системной области. Попав в нее, он подбросил свой вариант специального файла atrun вместо его законной системной версии. Через пять минут система уже "высидела" его "яйцо". Программа atrun проверила и изменила статус пользователя Свентека и, вместе с ним, хакера, пользующегося паролем, и дала ему все привилегии администратора системы. Теперь он держал в руках ключи от моего компьютера. Затем, пользуясь своим новым системным статусом, хакер заменил ложную программу atrun на реальную и создал еще несколько программ мониторинга системы с целью легального внедрения в систему и сбора паролей законных пользователей.

На первых нескольких футах распечатки я увидел, как "кукушка" готовила "гнездо", откладывала "яйцо" и ждала, когда его "высидят". Следующие 70 футов (-21 м) показывали, как "кукушонок" расправляет крылья.

Как супер-пользователь, хакер имел возможность управлять нашей системой и читать чью угодно работу. Изучив несколько чужих командных и управляющих файлов, он открыл себе дорогу к компьютерам других лабораторий. Каждый вечер наш компьютер автоматически вызывал 20 других для обмена электронной почтой и новостями, пришедшими по сети. Когда хакер знакомился с информацией от этих телефонных номеров, он изучал 20 новых объектов, интересующих его. Мне пришлось сплести сеть достаточно мелкую, чтобы хакер попался в нее, но достаточно крупную, чтобы наши ученые свободно проходили через нее. Я должен был засечь хакера, как только он выйдет на линию, и попросить техников из Тимнета проследить его до места вызова. Так как я знал названия украденных денежных счетов, было нетрудно написать программу, которая следила бы за появлением на линии этого паршивца. Не проверяя каждого пользователя нашего компьютера, программа подавала звуковой сигнал, когда использовался украденный счет. Но я должен был оставаться невидимым для хакера и поэтому написал программу для новой системы UNIX-8, которую мы только что установили. Я мог подключить свою программу к нашей локальной сети, чтобы защитить ее от всех возможных нападений и иметь возможность следить за другими компьютерами, записывая на принтеры информацию, проходящую через сеть. В среду 3 сентября 1986 года исполнилась неделя с тех пор, как мы впервые обнаружили хакера. Неожиданно раздался сигнал о соединении: стал активным счет Свентека. Я побежал на станцию включений; начало распечатки свидетельствовало, что хакер подключился в 2 ч 26 мин и все еще работает. Выйдя на линию как Свентек, он первым делом просмотрел список имен всех работающих в сети в это время. К счастью, там не было никого кроме обычной бригады физиков и астрономов; моя программа, работающая как сторожевая собака, была надежно спрятана в компьютере с UNIX-8. Он не стал супер-пользователем; вместо этого он проверил Gnu-Emaks и убедился, что она не изменилась, В 2 ч 37 мин, через 11 мин после соединения, он неожиданно вышел из сети. Но мы уже начали прослеживать его соединение. Рон Вайвер проверил сеть Тимнета по всей Северной Америке. За пару минут он вышел на подключение с Тимнетского порта LBL до отдела Тимнета в Окленде, где кто-то подключился с телефона. Намного легче послать вызов прямо в нашу Беркли- евскую лабораторию, чем делать это через Оклендское отделение Тимнета. Вызывать нас через местный Тимнетский номер доступа все равно, что выезжать в соседний штат, чтобы проехать три квартала. Но вызов через Тимнет добавлял еще один уровень для прослеживания. Этот "кто-то" на другом конце линии знал, как прятаться. На следующее утро после очередного вторжения хакера в нашу систему мой начальник встретился с юристом лаборатории Элетой Овенс. Она, не тратя попусту времени, связалась с ФБР.

Наш местный отдел ФБР и глазом не повел. Фрэд Виникен — особый агент Оклендского агентства ФБР — спросил с недоверием: "Вы вызываете нас потому, что потеряли на 75 центов машинного времени?" Овенс пыталась объяснить, что информация требует обеспечения безопасности, и что наши данные ценны. Виййкён перебил ее: "Вот если вы сможете показать потер]©, превышающую миллион долларов, или что кто-то выведывал засекреченные данные, тогда мы начнем расследование. А до тех пор оставьте нас в покое."

В среду 10 сентября в 7 ч 51 мин хакер вышел в нашу систему на шесть минут. Меня не было в лаборатории в это время, но принтер сохранил три страницы его следов. Он подключился к нашему компьютеру из Тимнета как Свентек,

затем перепрыгнул на другую сеть. Используя сеть Милнет, соединяющую компьютеры военного ведомства, он подключился к адресу 26.0.0.113. Хакер вышел туда как Хантер, проверил, есть ли на этом адресе Gnu-Emaks, и исчез.

Он оставил четкие следы, ведущие по направлению к военному лагерю Редстоун в Аннистоне, штат Алабама, место размещения Редстоунского ракетного комплекса в 2.000 милях от Беркли. Он составил список файлов аннистонской системы. Судя по датам этих записей, он работал в аннистонских компьютерах с начала июня. В течение четырех месяцев незаконный "владелец" системы пользовался компьютером военных. Однако его обнаружили случайно, а не через какой-то логический источник или утечку информации.

Просмотрев внимательно утреннюю распечатку, я увидел, что в аннис- тонском компьютере хакер сменил пароль Хантера на Хэдджес. Наконец-то появился ключ к разгадке: из великого множества возможных паролей он выбрал Хэдцжес. Хэдджес Хантер? Хантер Хэдджес? (Что значит в переводе "искатель препятствий".)

Время шло. Если бы я не поймал хакера быстро, лаборато-[1] рия прекратила бы мою слежку за ним и перевела на другую работу. В 2 ч 30 мин заработал принтер, и хакер подключился с нового краденого счета — счета Горона. Через минуту после соединения я позвонил в компанию и Рону Вайверу в Тимнет. Я записывал, пока Рон диктовал. "Он вышел на ваш порт № 14, вызвав Тимнет из Окленда. Это наш порт 322, который находится... О, дай-ка посмотрю..." Я слышал, как он стучит по клавиатуре. "Так, это 2902.430-2902. Вот номер для слежения."

Телефонная компания по закону не может передать мне информацию о прослеживании сети, но мои принтеры показывали каждый его шаг. Пока я разговаривал с Тимнетом и телефонными техниками, хакер прокрался через мой компьютер. Его не удовлетворило чтение системной электронной почты и он сунул свой нос в почту нескольких физиков-ядерщиков.

Почитав нашу почту 15 минут, он "прыгнул" обратно на счет Горона, используя новый пароль — Бенсон. Он запустил программу, которая искала файлы наших пользователей для выявления их паролей, а пока она работала, обратился в Милнетский центр информации по сетям и запросил проход в ЦРУ.

Однако, вместо их компьютера, он нашел четырех человек, работающих в ЦРУ. Позднее я позвонил одному из них.

Я не знал, с чего начать. Как бы вы представились агенту разведки?

"Вы не знаете меня, но я администратор компьютера, и мы сейчас следим за хакером."

"Угу."

"Так, он искал путь для выхода на компьютеры ЦРУ. И нашел ваше имя и номер телефона."

"Кто вы?"

Нервничая, я представился, ожидая, что он пришлет отряд бравых парней в шинелях. Я описал нашу лабораторию, чтобы он понял: наша Народная Республика Беркли не имеет никаких официальных дипломатических связей с его организацией.

Через несколько дней он прислал делегацию. О'кей, на них не было шинелей и даже темных очков. Просто обычные костюмы и галстуки. Вэйн видел, как четверо из них прошли по коридору и передали послание на мой терминал: "Свистать всех наверх. Делегаты флота прибывают в портал по правому борту. Самый малый ход, чтобы избежать столкновения с кораблем IBM". Если бы он знал...

Четыре разведчика представились. Один парень лет пятидесяти-шестидесяти сказал, что он находится здесь как навигатор и не назвал своего имени, он просто молча просидел у нас все время визита. Второго шпиона звали Грэг Финнел, и я думаю, он был компьютерщиком, потому что чувствовалось, что костюм доставляет ему неудобство. Третий агент по имени Тиджей был сложен, как полузащитник. А четвертый был, по-видимому, "шишкой": все замолкали, когда он говорил. Они были больше похожи на бюрократов, чем на разведчиков.

Все четверо сидели тихо, пока мы рассказывали им обо всем, что видели. Мистер "Большой" кивнул и спросил: "Какие ключевые слова он просматривал?"

"Он искал слова типа "пароль", "ядерный", SDI (стратегическая оборонная инициатива — СОИ) и Norad (объединенная американо-канадская система раннего оповещения о ракетном нападении). Он выбрал несколько странных паролей: 1Ы hack (палубные части 1Ы), hedges (препятствия), jaeger (меткий стрелок), hunter (охотник) и benson. Счета, которые он украл, принадлежат Горону, Свентеку, Витбергу и Марку и почти ничего не говорят о нем, потому что это имена сотрудников нашей лаборатории."

Мистер "Большой" кивнул и спросил: "Скажите мне, что он делал в Аннистоне?"

"У меня есть небольшая распечатка об этом", — сказал я. — "Он был в их системе несколько месяцев, возможно, и год. Теперь, когда он знает, что засечен, он включается на очень короткое время."

Мистер "Большой" заерзал на стуле, давая понять, что визит окончен. Грэг задал еще один вопрос: "Какие военные объекты подверглись его нападению?"

"Наши, конечно, и военная база в Аннистоне. Он пытался проникнуть на ядерный военный полигон в Войт Сэндз (White Sonds Missole Ronge) и на военный судостроительный завод в Мэриленде. Думаю, он называется Докмастер."

"Дерьмо!", — одновременно воскликнули Грэг и Тиджей. Грэг сказал: "Как вы узнали, что он добрался до Докмастера?"

"Почти в то же время, когда хакер подпортил нашу счетную ведомость, с Докмастера прислали почту о том, что кто-то пытается вклиниться в их работу."

"И это ему удалось?"

"Я так не думаю. А, кстати, что такое этот Докмастер? Это военный судостроительный завод?"

Они пошептались, и мистер "Большой" кивнул. Грэг объяснил: "Нет, это не судостроительный завод. Докмастер работает на Агентство национальной безопасности (NSA)."

"Хакер пробрался в NSA? Странно. Этот парень хотел выйти в ЦРУ, NSA, военные ракетные базы и в штаб обороны северо-американских ВВС."

"Докмастер — единственный несекретный компьютер в NSA", — сказал Грэг. — "Он принадлежит их компьютерной группе безопасности, которая является открытой."

Мистер "Большой" медленно заговорил. "Мы можем немногое сделать в этой ситуации. Думаю, нет достаточных свидетельств иностранного шпионажа."

"Хорошо, а кто же должен работать с такими делами?"

"ФБР. Сожадею, но это не наша сфера компетентности. Все, что мы можем сделать в этом случае — представить четыре имени, которые, должен сказать, уже давно известны в этой области науки (эти имена использовал хакер)."

Разведчики удалились.

Разведчики не стали мне помогать, и я опять остался один. Я нашел в лабораторной телефонной книге номера всех Джигеров и Бенсонов и прикинул, что должен сделать £о же самое в Стенфорде. Поэтому я пошел в библиотеку. Мэгги Морлей, наш 45-летний документатор, играла в "настойчивый копатель" (rough-and-tumble Scrable): на ее двери был приколот список всех допустимых трехбуквенных слов в Scrable.

"Мне нужна телефонная книга Стенфорда," — сказал я. — "Я ищу в Силиконовой долине всех по имени Джигер или Бенсон."

"Джигер. Это слово хорошо послужило мне," — улыбнулась Мэгги. — "Стоит 16 очков, но однажды я уже выиграла с ним игру, когда J было выбрано для трехбуквенного счета. Тогда оно дало мне 75 очков общего счета."

"Эх, но мне оно нужно сейчас, потому что это пароль хакера. И я не знал, что фамилии можно исполь- . зовать в Scrable."

"Джигср — это не фамилия. Ну, это слово может быть фамилией — Элсворф Джигер, например, — известный орнитолог. Но, вообще, джигер — это название семейства птиц. Получило свое имя от немецкого слова "охотник[11].

"Что? Вы сказали "охотник"?"

"Да. Джигеры — это хищные птицы, которые заклевывают других птиц. Они мучают слабых птиц до тех пор, пока те не испустят дух."

"Это попадание в десятку! Вы ответили на мой вопрос. Мне не нужна телефонная книга."

"Могу ли я сделать еще что-нибудь для Вас?"

"Как насчет объяснения связи между словами hedges (преграды), jaeger (джигер), hunter (охотник) и benson?"

"Ну, связь между jaeger и hunter очевидна для каждого, знающего немецкий. А курильщикам хорошо известна компания "Benson & Hedgers".

О, мой бог, мой хакер курит сигареты "Benson '& Hedgers". Мэгги выиграла этот тур игры.

Во время одного телефонного слежения я выписал все номера и цифры, которые передал мне техник. Я вызвал номера со всеми их комбинациями и остановился <на компьютерном модеме в Майте — оборонном подрядчике рядом со штабом ЦРУ в Маклине, штат Вирджиния. Интересно, как далеко внедрился в нее хакер? Пролистав каталоги их файлов, я увидел, что 17 июня хакер создал здесь "троянского коня": В течение полугода некто бесшумно "минировал*1'компьютеры в Майте. По всей вероятности, Майте служило перевалочным пунктом, средством для перехода в другие компьютеры. Кто-то подключался к Майте, оглядывался там и отключался. Таким образом, станция Майте служила местом, где можно спрятаться, дырой в стене, которую трудно обнаружить.

В понедельник утром я вызвал на связь Билла Чандлера из Майте и сообщил ему эту новость. Билл хотел успокоить меня. Да, конечно, но как быть спокойным, когда кто-то тратит чужие деньги.

"Слушай, Билл, не мог бы ты прислать мне копии ваших компьютерных счетов?"

"Зачем?[41]

"Наверное, будет занятно посмотреть, куда еще добрался этот хакер."

Через две недели пришел толстый конверт, заполненный счетами из Чесапика и Потомака. Счета за полгода. Даты, время, телефонные номера и города. Наверное, их было... тысяч пять. Так много, что я не мог анализировать их вручную. Прекрасный материал для анализа на компьютере — у нас была масса программных средств для поиска корреляций. Все, что я должен был сделать, это ввести их в мой компьютер Macintosh и выполнить несколько программ.

Вы когда-нибудь печатали 5.000 телефонных номеров? Это так же занудно, как это звучит. А я должен был сделать это дважды, чтобы убедиться в отсутствии ошибок. Эта работа заняла два дня.

После проведенного анализа я обнаружил, что хакер еще не пробрался в мой компьютер. Но побывал он более, чем в шести, а, может быть, и в дюжине компьютеров.

Из Майте хакер соединился с Норфолком, Окрид- жем, Омахой, Сан-Диего, Пасадиной, Ливемором и Атлантой.

Очень интересно: он делал сотни одноминутных запросов по всей стране. Запросов на военные базы, кораблестроительные заводы ВМС, авиастроительные заводы и оборонным подрядчикам. Что вы можете узнать за одну минуту связи с абонентом?

В течение полугода хакер заглядывал на базы и в компьютеры по всей стране. И никто не знал об этом. Он был везде. Одинокий, молчаливый, анонимный, на-- стойчивый и, по-видимому, удачливый — но почему? Чем он интересовался? Что уже знает? И что он делает со своей информацией?

В пятницу 5 декабря в 13 ч 21 мин хакер появился снова. Через девять минут он исчез. Достаточно времени, чтобы я проследил подключение до Тимнета. Но специалист по источникам вызовов Рон Вайвер задержался на,обеде, и Тимнет не смог проследить подключение. Еще один шанс был потерян.

Рон ответил на мой вызов через час.

"Эй, Клифф, как это получается, что ты меня никогда не вызываешь по ночам?"

"Действительно, хакер не показывался ночью. Интересно, почему?" Рон заставил меня задуматься. В моей книге соединений записаны все появления хакера. Когда же, в среднем, он работает?

Я помню его вызов в 6 часов утра и в 7 часов вечера. Но никогда в полночь. Но ведь ночь должна быть самым подходящим временем для работы хакера.

Обычно хакер появлялся в полдень. Спокойное время. Итак, что это значит? Допустим, он живет в Калифорнии. Тогда он работает в течение дня. Если он на Восточном побережье, он на три часа опережает нас, тогда он работает около 15-16

часов.

Это не имеет смысла. Он должен бы работать ночью, сократить плату за дальние вызовы, не попасть в пробку в сети и не быть замеченым. А он бесстыдно врывается в нашу сеть днем. Почему?

Интересно, где бывает вечер, когда в Калифорнии полдень? Время обеда в Беркли — это время отхода ко сну в Европе. Неужели хакер приходит из Европы?

В субботу после обеда хакер опять пошел в атаку на нашу сеть. Я вызвал по телефону Рона Вайвера из Тимнета.

“У меня сейчас его соединение,“ — прошептал я. — “Проследи мой порт 14.“

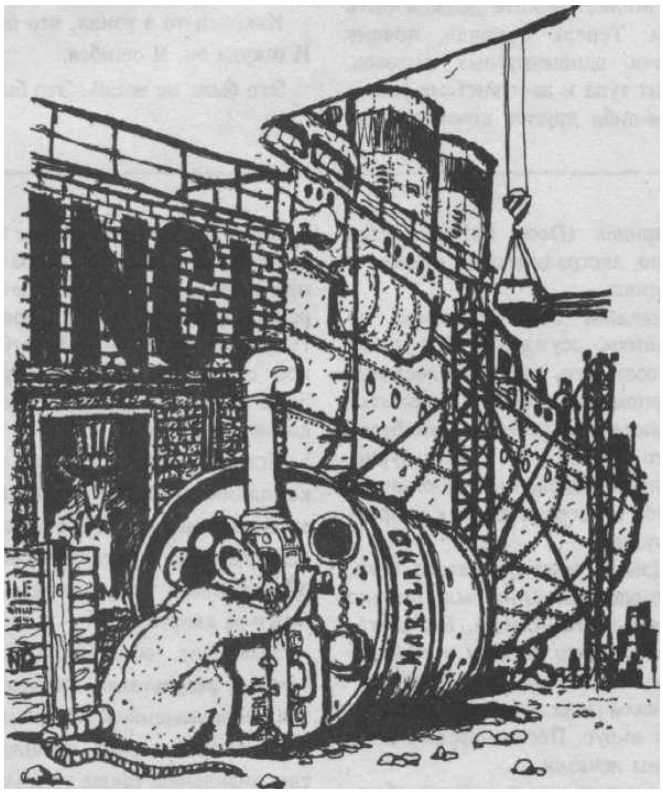
“Хорошо. Это займет одну минуту.“

Прошла целая вечность, пока Рон опять вышел на линию. “Эй, Клифф, ты уверен, что это тот самый парень?"

Я увидел, как хакер ищет слово SDI на нашем компьютере. “Да, это он.“

“Он пришел из входа, о котором я никогда не слышал. Я подключен к его сетевому адресу, теперь не страшно,, если он повесит трубку. Но парень пришел из какого-то странного места."

“Где оно?“



“Я не знаю. Это тимнетский узел 3513, который дает такую странную картину. Я должен просмотреть наш каталог файлов." В трубке появился фон — Рон работал на клавиатуре. “Вот оно. Твой хакер пришел в тимнетскую систему откуда-то еще. Он вышел в Тим- нет по линиям связи, обслуживаемым Международной телефонотелеграфной компанией <1TT).“

“Что это значит?"

“ITT принимает восточные вызовы через спутник связи над Атлантикой. Он передает от десяти до двадцати тысяч вызовов одновременно."

“Итак, мой хакер приходит из Европы?"

“Точно.'*

“Откуда?"

“Это то, чего я не знаю и вряд ли смогу разузнать. Но не отключайся, и я посмотрю, что еще могу найти здесь."

Опять заработала клавиатура.

Рон вернулся к телефону. “Так, в ITT эта линия называется DSEA 744031. Это ее номер. По ней можно соединиться с Испанией, Францией, Германией или Англией."

“Ну, а с чем же я соединен сейчас?"

“Увы, я не знаю. Через три дня нам пришлют информацию о плате за вызовы, тогда я смогу выяснить это. А пока я больше ничего не могу тебе сказать."

Рон дал отбой, но хакер по-прежнему висел на моем компьютере, пытаясь найти “отмычку" к лаборатории военно-морских исследований. В это время позвонил Стив Вайт — один из тимнетских специалистов по международным сетям.

“Рон не может вести слежение дальше," — сказал Стив. — “Я сделаю это сам."

Я продолжал наблюдать действия хакера, надеясь, что он не отключится, пока Стив не проследит соединение.

Стив опять вышел на линию. Со своим певучим, почти театральным, английским акцентом он сказал: “Твой хакер шлет вызов с адреса DNIC-2624- 542104214."

“Так откуда же приходит хакер?"

“Из Западной Германии. Сеть German Datex в ФРГ."

“Что это такое?"

“Это их государственная компьютерная сеть. Мы должны будем вызвать Бундеспост, чтобы узнать больше."

“Что это такое — Бундеспост?"

“Это государственная почтовая служба ФРГ. Монополия правительственных связей."

Стив, казалось, не верил в завершение удачного слежения. “Мы знаем, где он подключается к системе. Но существует два возможных способа сделать это. Может быть компьютер хакера находится в Германии и он просто выходит на линию German Datex. Если это так, мы спокойно обнаружим его. Мы знаем адрес, адрес укажет компьютер, а компьютер — на него".

“Это, скорее всего, не так," — сказал я, подумав о своем слежении в Майте.

“Да, похоже на это. Более вероятно, что он выходит в сеть German Datex через телефон".

“Также как и Тимнет, Datex дает возможность кому угодно подключиться к компьютерам в сети. Замечательно для бизнесменов и ученых. И хакеров".

“Настоящей трудностью будет немецкий закон," — сказал Стив.— “Я не знаю, считают ли они хакирова- ние преступлением."

“Ты, конечно, шутишь."

“Нет,“ — ответил он. “Во многих странах эти законы еще не приняты. А, например, в Канаде хакер, внедрившийся в компьютер, признается виновным скорее в краже электроэнергии, чем в нарушении чужого права владения. Он будет осужден только потому, что его соединение привело к трате микроватта мощности на компьютере".

Пессимизм Стива был заразительным. И его слежение

испортило мне настроение. Что, если мы не сможем схватить хакера, хотя наш круг замыкается вокруг него.

Германия. Я вспомнил, как узнал в библиотеке, что такое пароль хакера. “Джигер — это немецкое слово, значащее “охотник". Ответ был прямо передо мной, а я был слепым.

Некоторые детали были еще неясны, но я уже понял, как он работает. Где-то в Европе хакер вызывает сеть German Datex. Он просит соединить его с Тим- нетом, и Бундеспост делает это. Как только он достигает Штатов, он соединяется с моей лабораторией и расчищает себе дорогу в Милнет. Майте должен быть его транзитным пунктом. Теперь я понял, почему Майте оплачивает тысячи одноминутных вызовов. Должно быть, хакер звонит туда и дает системе указание соединиться с каким-либо другим компьютером.

Когда он отвечает, хакер подключается к нему с несуществующим именем и паролем. Он сканирует компьютеры, а Майте берет плату за услуги.

Но он избежит суда. По телефонным законам Майте.

Дорожка ведет в Германию, но она может и не окончится там. Возможно, кто-то и в Беркли может вызывать Берлин, соединяться с сетью Datex, затем через Тимнет вернуться в Беркли. Может быть начало пути лежит в Монголии. Или в Москве. Я не могу сказать. На текущий момент моя рабочая гипотеза — это Германия.

А он ищет военные секреты. Может быть, я преследую шпиона? Настоящего шпиона, работающего для “них", но кто такие — “они"?

Три месяца назад я увидел мышку, сделавшую небольшую дырку в моих платежных файлах. Мы спокойно наблюдали, как эта мышь через эту дырку прокралась сквозь наш компьютер, а затем в военные сети и компьютеры.

Наконец-то я узнал, что было нужно этому грызуну. И откуда он. Я ошибся.

Это была не мышь. Это была крыса.