

Документальный триллер

КЛИФФОРД
СТОЛЛ

ЯЙЦО КУКУШКИ

ИСТОРИЯ
РАЗОБЛАЧЕНИЯ
ЛЕГЕНДАРНОГО
ХАКЕРА

Москва

издательство

РОДИНА

2022

УДК 323
ББК 66.4
С 81

Clifford Stoll
The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer
Espionage — New York: Doubleday. 1989

Столл К.

С 81 Яйцо кукушки. История разоблачения легендарного хакера / К. Столл. — М.: Родина, 2022. — 384 с. — (Документальный триллер).

ISBN 978-5-00180-800-8

В отличие от плохого танцора, хорошему сисадмину мешают только кукушкины яйца. Их откладывают в его компьютер злобные хакеры, чтобы из них вылупились программы, делающие своего папу-кукушку суперпользователем.

Сисадмин Клиффорд Столл случайно обнаружил, что кто-то посторонний входил в систему, используя данные уволившегося полгода назад сотрудника. Началась охота на хакеров, которая закончилась задержанием в 1987 году жителей ФРГ — легендарного хакера Маркуса Гесса и трех его подельников Ганса Хьюбнера, Дирк-Отто Бжезинского и Карла Коха, которые успешно атаковали 400 компьютеров Министерства обороны США и его подрядчиков и продавали добытые секреты КГБ.

Автор подробно и честно рассказал о том, как смог разоблачить советских кибершпионов. В отличие от посвященных этой же проблеме американских фильмов, изрядно нашпигованных техническими ляпами, этот документальный детектив без ошибок описывает работу охотников за хакерами.

**УДК 323
ББК 66.4**

© Столл К., 2022
ISBN 978-5-00180-800-8 © ООО «Издательство Родина», 2022

Глава 1

Волшебник, я? Еще неделю назад я был астрономом и в свое удовольствие орудовал телескопами. Сейчас, оглядываясь на это времечко, я вижу, что подремывал годами, пока не уплыли последние денежки по моему гранту.

К счастью, в обсерватории Кек при Лаборатории Лоуренса в Беркли астрономов принимали на вторичную переработку — и вместо биржи труда я оказался в компьютерном центре, в подвале Лаборатории. Могу показать парочку компьютерных фокусов, чтобы потрясти астрономов. Гораздо быстрее коллег разбираюсь во всяких головоломных ситуациях. Выходит, я — компьютерный волшебник? Не знаю, все-таки главное для меня — астрономия...

А что теперь-то? Уныло глядя на терминал, я продолжал думать об орбитах планет и астрофизических явлениях. Как новичку, мне довелось выбирать между застекленным отсеком с единственным окном, выходящим на мост Золотые Ворота, и душным кабинетом, заставленным книжными полками. Наплевав на свою клаустрофобию, я остановился на последнем в надежде незаметно дремать за письменным столом. Рядом располагались кабинеты Вэйна Грэйвса и Дэйва Клэвланда — «зубров»-системщиков. Они громко и постоянно цапались между собой, поэтому я разузнал много любопытного. Вэйн находился в натянутых отношениях с остальными работниками — по его мнению, некомпетентными лентяями. Сам-то он систему знал назубок, начиная с программ-драйверов и кончая СВЧ-антеннами. Единственной приличной вычислительной машиной он считал ВАКС, выпускаемый фирмой ДЭК. Других компьютеров для него просто не существовало — он не признавал ни ИБМ, ни ЮНИКС, ни Макинтош.

Дэйв Клэвлэнд — безмятежный Будда ЮНИКСа — терпеливо выслушивал бурные речи Вэйна, который безуспешно пытался его подначить: «Ученые всего мира выбирают ВАКСы. Эти машины позволяют создавать надежные программы дюжиной способов!» Дэйв парировал: «Вы ошастливьте „фанатов“ ВАКСа, а я позабочусь об остальных». Увы, Клэвлэнд не раздражался, поэтому неудовлетворенный Вэйн угасал и погружался в ворчанье.

Прекрасно. В первый же рабочий день я оказался маслом на бутерброде, который регулярно падал мною вниз и тем самым прерывал мой дневной сон. Зато мой внешний вид вполне соответствовал стандартному облику сотрудника лаборатории Беркли: поношенная рубашка, потертые джинсы, длинные волосы и дешевые кроссовки. На управленце можно было иногда увидеть и галстук, но при этом заметно снижалась производительность труда.

В обязанности нашей тройки (Вэйна, Дэйва и мои) входило обслуживание компьютеров лаборатории. Мы ведали дюжиной больших машин — громадных «тяжеловозов», решающих физические задачи. Стоили эти «рабочие лошадки» примерно шесть миллионов долларов. Надо полагать, что ученые, использующие эти компьютеры, рассматривали их как простых производителей, надежных не меньше, чем взаправдашние кони: работать они должны круглые сутки, а мы — старшие конюхи — несли ответственность за каждый цикл вычислений. Из четырех тысяч сотрудников лаборатории услугами главных компьютеров пользовалась примерно четверть. Для каждого из этой тысячи ежедневно велся учет машинного времени, при этом «гроссбухи» хранились в компьютере. Час вычислений стоит триста долларов, поэтому учет надо было вести страшно скрупулезно, и нам приходилось гоняться за каждой выводимой на печать страницей, за каждым блоком дискового пространства и за каждой минутой процессорного времени. Для сбора такой информации имелся отдельный ком-

пьютер. Раз в месяц на нем распечатывались отчеты и рассылались по отделам.

Однажды ко мне ввалился Дэйв и невнятно забормotal о неприличном поведении системы учета ЮНИКСа. Кто-то использовал несколько секунд машинного времени, не заплатив за них. Баланс не сходился; по счетам за прошлый месяц на сумму 2387 долларов была обнаружена недостача в 75 центов. Докопаться до источника ошибки в несколько тысяч долларов — пара пустяков. Но причины недостач в несколько центов обычно зарыты глубоко, и такие раскопки — стоящая проверочка для начинающего компьютерного волшебника.

— Чисто сработано, а? — наивно сказал я.

— Разберись с этим — и ты удивишь мир, — ответил Дэйв.

Детская забава! Я погрузился в программу учета. Она была похожа на кастрюлю со смесью всего на свете, куда начинающий кулинар закладывал любимые продукты, мешал, пробовал, а в результате дал дуба. Однако это рагу все же насыщало нашу лабораторию и просто вылить его было нельзя. В нем я нашел куски, написанные на Ассемблере, Фортране и Коболе — древнейших языках программирования. Я бы не удивился, встретив процедуры на древнегреческом, латыни или санскрите. Конечно же, никакой документации в помине не существовало. Только самый наивный поваренок мог отважиться сунуться со своей ложкой, не зная броду.

Худо-бедно, но все же было чем заняться после обеда. Кроме того, оставался шанс выловить из этого компота ягодку покрупней. Дэйв показал мне системную процедуру учета подключений к компьютеру, занесения в журнал имен пользователя и терминала. Система фиксирует каждое подключение, регистрирует идентификатор задачи пользователя, расходуемое пользователем процессорное время и время отключения. Дэйв объяснил, что есть две системы

учета. Обычная программа учета ЮНИКСа просто заносит в отдельный файл записи событий. Но Дэйв создал вторую программу, которая обеспечивает хранение более подробных сведений о том, кто пользовался компьютером.

Сменявшие друг друга группы скучающих студентов годами писали, писали и, наконец, написали программы анализа всей учетной информации. Одна программа производит сбор данных и «засовывает» их в файл. Вторая — считывает этот файл и вычисляет стоимость сеанса работы с компьютером. Помимо всего прочего существует третья программа, которая обеспечивает подведение итогов и распечатку счетов, рассылаемых по отделам. Итоговая сумма из этой третьей программы сравнивается с результатом, получаемым от внутренней программы учета. Два учетных файла, созданных одновременно различными программами, должны давать один и тот же ответ. В течение года все работало как часы, но на этой неделе что-то сломалось. Первое подозрение — ошибка округления. Похоже, что каждый элемент файла учета сам по себе правилен, но при суммировании разности в десятые доли цента накапливаются, что в конечном итоге и приводит к ошибке в 75 центов. Доказать это можно либо углубившись в анализ процесса работы программ, либо путем тестирования, подавая на вход различные наборы данных. Чтобы зазря не размахивать мачете в зарослях тростника, я написал свою коротенькую программу проверки файлов и убедился, что с первой программой проблем нет. Со сбором информации все в порядке.

Вторая программа отняла у меня больше времени. За час я слепил «заплату» и понял: все работает. Программа суммирует длительности промежутков времени и затем умножает их на стоимость. Потеря 75 центов — не на ее совести.

И третья программа ведет себя хорошо: рыщет по списку пользователей, имеющих право доступа, находит их

регистрационные записи и распечатывает счета. Ошибка округления? Нет, ни в одной из программ не может пропасть и сотой доли цента. Странно. Откуда же взялись эти дурацкие 75 центов?

Ну что ж, пусть я гоняюсь за призраком, но упрямства мне не занимать: из принципа проторчу здесь до полуночи!

Еще пару-тройку раз все проверив, я сильно зауважал это доморощенное чудо света — программу учета. Факт, что баланс не сходился, но программы не виноваты. К этому времени я нашел список пользователей, имеющих право доступа, и понял, каким образом происходит составление счетов для отделов. Около 7 вечера мне на глаза попалось имя Хантер. У этого парня оказался неправильный адрес счета. Ага! В прошлый месяц он задарма попользовался компьютером ровно на 75 центов.

Вот оно что! Кто-то добавил подпольного пользователя. Элементарно! Победа! Когда я упивался сознанием своей гениальности, заглянула Марта, моя подружка, и мы отпраздновали мой маленький триумф в кафе «Рим» ночным капучино.

Настоящий волшебник справился бы за несколько минут. Зато я утешал себя тем, что изучил систему учета и немного набил руку в древних языках программирования. На другой день я отправил Дэйву весточку по электронной почте, раскрывая суть трюка.

Дэйв появился у меня около полудня и, шлепнув на стол стопку инструкций, мимоходом буркнул, что никогда не вводил пользователя по имени Хантер — это, скорее всего, сделал другой менеджер системы. Вэйн отрезал: «Это не я. ЧЧИ». Он частенько завершал свои сентенции аббревиатурами. Эта означала: «Читай Чертову Инструкцию».

Я читал инструкцию. Операторам не полагалось вводить нового пользователя без занесения данных в систему учета. В других вычислительных центрах могли попросту

нацарапать имя пользователя в журнале, поставить его на учет и дать команду компьютеру. Нам же нужно было следить за всем и всеми, поэтому наша система была поумней. Она содержала ряд специальных программ, позволяющих автоматически проделывать всякие там системные штучки и выполнять нудную бумажную работу. Никакому недотепа в голову не пришло бы вручную вводить нового пользователя. Сама же система такую плюху никогда не сделает.

И все же такой недотепа поработал. Правда, я не мог выяснить, кто он. Никто не знал Хантера. Не было на него и учетной документации. Поэтому я удалил это имя из системы — если начнет вопить, все вернем обратно.

Спустя день компьютер по имени Докмастер прислал нам сообщение по электронной почте: якобы некто из нашей лаборатории нагло пытался вломиться в его компьютер в прошлый уикенд.

Докмастер мог находиться где угодно, но все указывало на Мэриленд. Пересылаемое по электронной почте сообщение проходит через десяток компьютеров и каждый оставил на нем свою отметку.

Дэйв ответил на послание неизменным: «Разберемся». Жди, когда перестанет болеть голова от своих проблем. Однако что-то привлекло внимание Дэйва в полученном от Докмастера сообщении и он передал его Вэйну, сопроводив вопросом: «Что это еще за Докмастер?» Вэйн отдал послание мне и предположил: «Наверное, какой-нибудь банк». Я полагал, что Докмастер это одна из верфей военно-морского флота. Сообщение не выглядело документом особой важности, хотя может быть и стоило потратить пару минут и повнимательней присмотреться к нему. В послании указывались дата и время попытки ворваться в Докмастерский компьютер с нашего ЮНИКСа. Поэтому я проштудировал файлы, в особенности записи, сделанные в субботу утром, и опять наткнулся на расхождения в двух системах учета. По файлу, созданному «родной» сис-