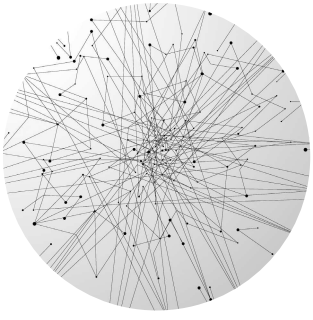

АЛЕКСЕЙ САБУРОВ

Москва
2023

УДК 821.161.1-312.4
ББК 84(2Рос=Рус)6-44
С12

Все совпадения в произведении
носят случайный характер

Сабуров, Алексей Владимирович.
С12 Антихакер / Алексей Сабуров. — Москва : Эксмо, 2023. — 352 с.

ISBN 978-5-04-188233-4

Талантливый специалист IT Марк Озеров занимается проверкой систем защиты компаний от хакерских атак. После выполнения одного из заданий он получает электронное письмо с просьбой помочь разобраться в деле самоубийства некой Марины Зайцевой. Якобы с ее почты конкурентам были переданы очень ценные сведения, после чего девушка была уволена с работы, впала в депрессию и в результате свела счеты с жизнью.

Марк соглашается помочь. В ходе расследования у него возникает ощущение, что некоторые трагические события последних дней жизни Марины были специально подстроены. В то же время Марк понимает, что его втягивают в чужие грязные дела, и решает выйти из игры, как ему кажется, навсегда.

Но эта история только начинается. Через несколько дней в дом Марка врывается киллер...

УДК 821.161.1-312.4
ББК 84(2Рос=Рус)6-44

ISBN 978-5-04-188233-4

ЧАСТЬ ПЕРВАЯ

Марк

ГЛАВА 1

Марк Озеров предпочитал работать ночью. Даже глубокой ночью, после трех. Он подкатился к рабочему столу. Два безрамочных двадцатичетырехдюймовых монитора Alienware уже светились мягким приглушенным светом, геймерские клавиатура и мышь отвечали им своей подсветкой, словно дразня. Выглядело это в темноте комнаты как рубка межзвездного корабля из фантастики девяностых. Справа от стола на расстоянии вытянутой руки высились башни-близнецы компьютерных корпусов, напичканные самыми современными платами, скоростными видеокартами и объемными дисками памяти. Их мощные вентиляторы равномерно гудели, точно двигатели, прогреваемые перед запуском. В общем, так и было, Марк собирался снова улететь из этой обустроенной комнаты в коттедже под Екатеринбургом в опасный сетевой мир. Стоило только ввести правильный приказ в командной строке. Слева в качестве резерва на алюминиевой подставке со встроенным охлаждением был приготовлен ноутбук с изображением головы инопланетянина на закрытой крышке — тоже Alienware. Иногда его помощь была ох как нужна.

Вся техника была черного цвета: Озерову нравился этот простой и надежный цвет, без хайтековских загонов

под металлик или еще хуже — хипстерских цветных ярких пятен. Дополняли стол стильные треугольники колонок Bang & Olufsen, конечно, того же беспроигрышного цвета. Хорошая музыка в идеальном звучании действовала как банка Red Bull — не давала заснуть и выдохнуться. Марк нажал на Random play, и из архива размером с Марианскую впадину нехитрый алгоритм выбрал «Smack my bitch up» от Prodigy. «Одно из лучших вступлений в истории музыки», — с радостным удовлетворением подумал Марк и ввел сетевой адрес сервера «Кузбасской угольной компании» в поисковую строку. В этот момент мощные ударные ворвались в гипнотизирующий ритм начала песни. Понеслась.

Разница во времени с Кемерово — два часа. Он мог сегодня начать раньше, немного за полночь: в Сибири уже наступало мертвое время. Даже если система, которую он взламывал, заметит это и отправит тревожный сигнал своему администратору, тот вряд ли вылезет из пригретой постели, чтобы проверить, что же там случилось. После трех ночи мозг, который уже уснул, всегда отговорит от подъема даже самого добросовестного работника. В это время любая дебильная задача уж точно может подождать до утра, пусть даже за это и заплачены деньги, может, даже и большие, но всегда недостаточные, чтобы прерывать самый лучший и глубокий предутренний сон.

Сетевой адрес Марк получил от заказчика. Этот заказ был немного странный, впрочем, любая операция всегда имела собственные заморочки. Ему требовалось проскользнуть на сервер компании, затем сломать управленческую программу и скачать годовой финансовый отчет. Но на этом миссия не заканчивалась. Зачем-то нужно было еще пробиться на внутренний почтовый сервер жертвы и отправить добытые документы с одного из почтовых ящиков. Ну, и наконец стереть цифровые отпечатки своего вторжения с электронных каталогов компьютера.

Сканирование портов всегда было первым шагом при любой атаке, это как осмотр стены в поиске дверей, калиток и других проходов, которыми пользуются люди, чтобы сообщаться с внешним миром. Нет ни одной крепости без ворот и ни одного замка без потаенного хода — в этом и заключена главная возможность для разведчика. Конечно, можно вскарабкаться на стену, но лучше сначала подергать за ручки дверей и форточек. Да, порты еще говорят, с кем ты имеешь дело, как язык тут же отличает русского от француза, немца или испанца, особенно если ты полиглот. «Кузбасская угольная» использовала сервер на Windows, и Марк прекрасно знал, на каком языке нужно разговаривать, чтобы вскружить его электронную голову. Быстрым нажатием клавиши он открыл папку «Для Винды» и начал запускать заготовленные программы. Его прокачанные боевые машины и оптическая выделенная интернет-линия позволяли наносить противнику миллион уколов в секунду, пока слабое место не будет найдено.

Первая запущенная программа проверяла код на существующие лазы от старых взломов. Если хакер уже проделал дырку в системе, то обычно он старался зашить в ней команду для своего использования или последующих вскрытий. На своем языке называя ее бэкдор. Этим всегда можно воспользоваться знающему человеку, как плохо прибитой доской в заборе, о которой известно только своим. Но результатов поиск пока не дал: или сервер еще девственен, или администратор внимательно следил за своими угодьями и закопал вражеские ходы.

Вторая программа исследовала ошибки самого кода. Любое программное обеспечение всегда имеет слабые места, ведь пишут ее люди, а людям свойственна лень, безалаберность и просто некомпетентность. Поэтому рабочая и проверенная временем программа вдруг начинает вести себя неадекватно при получении совершенно неожиданного для нее приказа. Какая-то строка программного кода

становится неуправляемой, вернее, ее тащит в другом, нужном взломщику направлении. Разработчики борются с этими «уязвимостями», как они сглажено называют свое разгильдяйство, и выпускают одно обновление за другим, в которых зачищают обнаруженные ошибки. Но администраторы компаний за бесконечной очередью текущей работы или в связи с абсолютно теми же человеческими недостатками, что и у программистов, постоянно забывают их устанавливать. Да и орды хакеров всего мира ищут новые способы проникнуть за цифровые стены, и усилия тем настырнее, чем популярнее приложение и богаче разработчик. Microsoft у них в особом почете. Он даже удостоился нескольких кличек и аббревиатур: Мелко-мягкие, Мелкософт. Марку нравилась аббревиатура M$. Деньги Гейтс греб ковшом самого большого в мире бульдозера.

Озеров, не останавливаясь, запустил третью программу. Ее сущностью было выявить имена пользователей сервера. Накануне вечером он посерфил корпоративный веб-сайт кузбасской компании и создал список возможных английских вариантов написания фамилий всех работников, которых нашел. Администраторы не выдумывали ничего нового, раз за разом называя учетки тремя-четырьмя способами: Ivanov, alexeyivanov, aivanov, a.ivanov. Кроме фамилий он добавил еще и несколько простых юзернеймов, таких как admin, user123, director, test. Зачастую созданные при настройке или тестировании эти имена не имели пароля совсем или тот был просто бутафорией.

Оставив программы копать и ломать, Марк вернулся к информации, полученной от открытых портов (там очень часто прятались ключики от квеста), и в сертификате службы шифрования он обнаружил новое для себя имя пользователя. Если повезет, то это мог быть логин администратора, который устанавливал сервер. Найти администратора — это всегда важно, потому что у него, как

правило, полный доступ ко всему. Марк тут же добавил имя в список проверки.

Программы начали отчитываться о проделанной работе. Скрытых тропинок от былых проникновений не обнаружилось. Марк не особо переживал по этому поводу, хотя по статистике, которую он читал, больше двадцати процентов всех серверов вскрыты и их владельцы даже не догадываются об этом. Зато проверка по пользователям дала отличные результаты: он теперь знал четыре логина, в том числе подтвердился и пользователь из сертификата службы шифрования. Теперь можно было выпускать «Дурачка». Программа, конечно, называлась по-другому, но Марк относился к ней с особой нежностью и называл по-своему. Она с бешеной скоростью пыталась вскрыть уже рассекреченные логины, подбирая отмычки в виде незамысловатых наборов букв и цифр из базы «Самые популярные пароли». Алгоритм был простой, но именно программы-дурачки приносят самые высокие цифры взлома в мире. Люди все-таки очень похожи друг на друга по глупости и самоуверенности. И когда Озеров в очередной раз читал в новостях, что обнародованы данные пользователей популярного интернет-ресурса, он явственно представлял, как по каждому из этих миллионов учетных данных уже настойчиво, как стрелки часов, работают эти неутомимые электронные черви. И пару жертв «на дурака» они точно накопают.

Загрузив в «Дурачка» раскрытые имена, Марк отправил его в экспедицию за паролем. Этот поход мог затянуться, хотя программа и подставляла несколько десятков тысяч паролей в секунду от классических P@sw0rd до вариаций на тему фамилии, именно поэтому логин типа Ivanov1985! — это ключ, который лежит под грязезащитным ковриком с говорящей надписью WELCOME!

Марк представил, что происходит в этот момент в прохладном темном помещении с табличкой «Сервер-

ная» на входной двери. Именно сейчас сервер почувствует, что в его дверь начали ломиться незваные гости. Как он отреагирует? Сообщит администратору о нездоровой активности? Это было не страшно: с учетом позднего времени вряд ли тот на ночном дежурстве. Если бы Марк пытался проникнуть в банк или маркетплейс, то его бы раздавили со скоростью «Формулы-1», несмотря на часть суток: там с этим строго. Но менее зацикленные на интернете компании, пусть даже и крупные, беспечно считают, что их электронная собственность в безопасности. Они очень часто вкладывают большие деньги в сигнализацию в помещениях, видеонаблюдение, нанимают охранников, но самый популярный для преступлений — интернет-канал защищает неумелый администратор, да и то лишь в рабочее время. А администратор неумелый, потому что всех, кто по-настоящему смыслит в программировании, хищнически разобрали те же банки, маркетплейсы и другие IT-разработчики.

Ничего не происходило. Соединение работало. Марк ожидал, что кемеровский сервер отключит его неожиданно активный IP-адрес, но тот благосклонно позволял себя мутузить. Честно говоря, отключение бы не помогло, потому что Марк всегда работал через симулятор IP-адреса, и при бане одного адреса тут же подключался другой, затем следующий и следующий... А их число где-то близко к бесконечности. Это позволило бы только немного притормозить процесс.

Можно было подождать, возможно, активированные программы выполнят свои задачи. Дисплеи показывали загружаемые команды и ответы атакуемого сервера на них. Строки английских слов, цифр, знаков заполняли синий фон экрана, сдвигались вниз новыми строками, скрывались за нижней кромкой мониторов. Компьютеры справа издавали мышиные писки и звуки скребущихся когтей, точно десятки крыс своим шебуршением обеспе-

чивали их работу. Озеров наслаждался этим звучанием нагруженных видеокарт и раскрученных до максимальных скоростей жестких дисков, ему нравился особенный голос его машин, точно они были живыми. Точно он был не один. The Offspring из черных колонок весело вещал, что «дети не в порядке». Но у Марка все было как надо.

Он снова вернулся к открытым портам. Современные тенденции на удаленную работу, доступность данных из любой точки мира сделали прорыв в производительности, но порядком изрешетили защиту. Марк нашел еще один сертификат с новым сетевым адресом. При вводе его загрузилась страница входа в CREATIO. Что за неведома зверюшка? Быстрый поиск «creatio» в Google выдал, что это CRM-система. Вот это уже была несомненная удача. Если пароли для сервера обычно раздает администратор и старается сделать их сложными и надежными, то CRM-кой пользуются обычные сотрудники, и им надо как-то запомнить очередной пароль, а для этого он должен быть удобный и очевидный для них. Марк снова запустил проверку пользователей из списка, добытого на сайте компании. И совпадений оказалось целых пять. «Дурачок» принялся за новый вызов, как проголодавшаяся крыса, мелко стуча острыми цифровыми зубками. Теперь ко взлому был подключен и ноутбук, чтобы не тормозить уже запущенные процессы.

Именно инопланетянин и вытащил первый выигрышный билет. Пользователь с именем test сдал положительный тест с популярным паролем разработчиков 1qazxsw@. Возможно, отладчики системы забыли удалить пользователя после запуска, возможно, посчитали, что пароль получше, чем qwerty123, и можно не заморачиваться. И скорее всего сисадмин даже и не знал об этом. Но Марк уже был внутри CRM и думал, как это можно использовать. Этот прорыв не вел его автоматически к цели. Ему нужно было взломать финансовую программу.

Естественно, test имел самые широкие права администратора, иначе ничего не испытаешь и не отладишь, поэтому в программе CRM Озеров мог найти что угодно. Главное — было понять, что искать. Его все так же интересовали данные пользователей. С его-то полными правами они были как в кружке оптического прицела. Марк скопировал всех пользователей, включая администратора, с их паролями и начал вводить по очереди в форму входа на сервер. Конечно, Озеров рассчитывал, что подойдет именно пароль админа, тогда бы он получил на сервере максимальные права, чтобы ничто не мешало ему расправиться с финансовой системой, но тот грамотно вводил разные пароли для каждого из ресурсов. Сработал один из новых пользователей z.koltsov, имени которого не было на сайте, но, видимо, обладавший высокой властью, чтобы иметь допуск и в CRM, и на сервер. Его пароль был надежен, и его нельзя было подобрать с помощью «Дурачка», но он оказался слишком самоуверен, используя его несколько раз. Было бы идеально, если бы его данные подошли и дальше.

Суперправ у некого Кольцова не оказалось, и сервер все еще не был захвачен. Но тот, безмятежно сопя сейчас под теплым одеялом, послушно открыл следующую дверь, которая вела на финансовую кухню компании, с помощью того же логина и пароля Озерову удалось зайти в 1С. Марк остановил всех своих взломщиков. То, что они не дали результата, можно было признать как крепкую работу защитников. Пароли выдержали его натиск, а системные болячки программного обеспечения были пролечены. Чаще всего информационные крепости быстро сдавались, но Марк ведь и не пытался штурмовать настоящие цитадели банков и интернет-компаний: против них работают только командами, а осады тянутся неделями.

Разобравшись в структуре 1С, Марк сформировал требуемый заказчиком отчет и скопировал его себе. Первая

часть задания была выполнена. Он глянул на часы. С начала атаки прошло шестьдесят семь минут. По ощущениям Озерова прошло не более десяти минут, настолько его захватило действие, впрочем, как всегда.

Компьютерная программа корпоративной электронной почты, которую нужно было сломать, крутилась на этом же сервере, что облегчало работу. Будь это отдельный сервер или, еще хуже, федеральный почтовик, это могло бы весьма затянуть или вообще поставить выполнение задания под угрозу.

Почтовому ящику редко достаются простые пароли. Именно в электронной почте у человека лежит самое ценное: мысли, слова, дела — в целом взаимоотношения с другими людьми. Сейчас туда еще приходят счета, банковские выписки, коды доступа для всех остальных ресурсов. Долгая история существования почт изобиловала взломами, потерями паролей и скандалами, случившимися после этого. И так уж сложилось: пароль на почте самый матерый из всех существующих. А почтовый сервер — это вообще как подземное банковское хранилище. Только наличие мощных инструментов и достаточного времени позволит распечатать его. Поэтому не тратя время на подбор пароля, Марк сразу перешел к другому набору оборудования.

Он мог продвигать атаку двумя способами. Первый из них — установить снифер — программу, которая отслеживает весь сетевой трафик, проходящий через сетевой интерфейс, и перехватывает пакеты данных, в которых будут и имена пользователей, и пароли. Но этот обмен начнется только утром, а по условиям задания он должен получить результат до начала рабочего дня. Кроме того, опытный системный администратор может увидеть сбои в системе и отследить как саму атаку, так и направление, откуда она ведется. Во втором варианте, находясь внутри сервера, он мог запускать патчи, направленные на изме-

нение конфигурации системы, и подменить администратора системы собой, получив полные права. А с высоты этих прав уже накинуться на почтовый сервер и заставить его поделиться ключами от своих замков.

Последний вариант Марк признал предпочтительным и включился в рутинную работу. Пальцы летали по клавиатуре, рассылая приказы компьютерным войскам: кому какой редут следует штурмовать. Для начала он вывел из строя антивирус, применив несложную программу, разрешающую любые действия пользователя. Спящий господин Кольцов, ведомый руками Марка, начал проверять одну возможность за другой: получение пин-кода для аутентификации смарт-карт с помощью запуска NT-хеша, дискредитация тикет-системы, чтобы изготовить себе «золотой билет», который дает полный доступ, атака на файлы групповой политики с целью выдачи пароля для ее смены. Марк без устали вводил свои алгоритмы, точно средневековый алхимик заклинания. Синий экран мельтешил командами и ответами на них, отображая схватку техники и человека. Борьба вовлекала, заставляла думать, ругаться, кидать все новые силы, как будто это и не искусственный интеллект противостоял Марку, а настоящий противник из плоти и крови. В один момент зазвучал сигнал телефона. «Черт! Уже четыре часа», — подумал Марк, а значит, в Кемерово пробуждался новый день, и пора было сворачивать удочки и заметать следы. Ничья.

Марк сегодня не смог обыграть компьютер. Тот был качественно настроен, и владелец внимательно ухаживал за его состоянием. Если бы не забытый пользователь в клиентской программе, то исход поединка мог быть совсем не в пользу взломщика. Впрочем, еще не все методы проникновения были использованы. Если задаться целью и запастись временем, то результат поединка будет совсем другим. Впрочем, на том часто и строится защита: что нападающий охренеет от преград и пойдет искать другого

лоха. Позволить себе идеальную защиту, как у банка, не может себе почти никто. Марк снес память сервера о выполненных командах, стер свои изменения в исходном коде и, не удержавшись в гранях заказа, все-таки установил снифер и замаскировал его среди груды приложений Мелкософта. В крайнем случае это будет очередной проверкой для IT-персонала кузбассцев.

Оборвав песню Нелли Фуртадо, Марк выключил свой обуглившийся в боях межгалактический истребитель. Турбины вентиляторов стихли, и диски, крутанув несколько оборотов, удивленно замолчали. Наступила абсолютная тишина. Раздражающий свет раннего летнего солнца уже проникал в комнату. Лесной коттеджный поселок, и так хранивший спокойствие и молчание тайги, в этот час светлой ночи словно вымер. Даже птицы, даже насекомые еще не решались проснуться.

Марк откинул голову на спинку кресла. Постепенно напряжение работы стало отпускать его, уступать место усталости, удовлетворенной выполненным делом, и, наконец, сну. Сейчас он доберется до кровати и заснет на пять-шесть часов. После, позавтракав, ему нужно будет написать отчет для «Кузбасской угольной компании» о выявленных уязвимостях их системы защиты данных, показать свой путь взлома, чтобы исправить эту ошибку, а также рассказать о неудаче взлома их почтового сервера. Еще от него ждут письменные рекомендации о защите от хакерских атак. Все согласно официально подписанному договору.

ГЛАВА 2

Проснулся Марк поздно, уже почти в одиннадцать. Солнце свысока палило в окна его спальни, насмехаясь над недостаточно плотными шторами. Но у него свободный график — может себе позволить! Марк умылся,