Автор: Сергей Рублёв © Lenta.Ru КОМПЬЮТЕРЫ, МИР 2738 07.11.2005, 14:38 220

Дело Левина живет и побеждает. Как проходил один из крупнейших банковских взломов в истории.

Внимание общественности вновь приковано к событиям более чем десятилетней давности, когда организованной преступной группировкой с участием русского хакера Владимира Левина была предпринята крупнейшая на тот момент попытка "электронного ограбления". Возвращение интереса к данной теме было вызвано вновь открывшимися подробностями этого дела.

Сатурн" почти не виден

Вкратце сюжет выглядит следующим образом: в 1994 году петербургский компьютерщик Владимир Левин, взломав хитроумные системы защиты, внедрился в компьютерную сеть нью-йоркского "Ситибанка" и перевел более 12 миллионов долларов со счетов его клиентов на различные зарубежные счета. Когда банк среагировал на жалобы клиентов, у которых стали пропадать деньги, к делу подключилось ФБР. Часть переведенных средств была получена в разных странах наличными, и дальнейшая их судьба осталась неизвестной, однако большинство курьеров было арестовано в разных странах при попытках получить деньги на руки. При содействии МВД России удалось выяснить, что неизвестный хакер выходил в сеть из помещения компьютерной фирмы "Сатурн СПб", после чего оперативными методами была установлена его личность. Однако арестовать Левина на территории России было невозможно, поскольку в УК РФ на тот момент еще отсутствовали статьи о компьютерных преступлениях, и с точки зрения действовавшего тогда законодательства он был полностью невиновным. В результате, как утверждается, тонкой психологической игры, проведенной сыщиками двух стран (включая телефонные звонки арестованных подельников, угрозы со стороны имевших отношение к делу "братков" и т.п.), удалось добиться того, что Левин запаниковал и отправился в Великобританию, предположительно - к другу детства своей матери Леониду Глузману. Он был арестован, едва ступил на британскую землю, прямо в аэропорту "Стэнстед" 3 марта 1995 года, после чего был экстрадирован в США, где и был осужден на 3 года тюрьмы.

Вся эта история была реконструирована достаточно подробно и многократно описывалась в прессе - установлены имена большинства сообщников, которые также получили различные сроки, восстановлена хронология практически всех событий. Основная часть украденных денег была благополучным образом возвращена законным владельцам, - из более чем 12 миллионов не удалось найти только около 250 тысяч, да и то злые языки поговаривают, будто это "Ситибанк" под шумок решил списать собственную недостачу. И, тем не менее, в истории осталось одно темное место - всего одно, но зато какое.

Все до единого люди, которые знали Владимира Левина лично, оценивали его хакерские таланты достаточно невысоко. Он отнюдь не являлся гением в области программирования или математики, совершенно не производил впечатления суперинтеллектуала. В любительской сети ФИДО, которая в 1994 году была в России основным местом обитания передовой компьютерной молодежи (достаточно отметить, что генеральный директор ЗАО "Демос-Интернет" Василий Долматов или глава российского представительства Microsoft Ольга Дергунова были в то время сисопами ФИДО), Левин также ничем особо не прославился. Да и содержание его работы в пресловутой компании "Сатурн СПб" точнее всего может быть охарактеризовано словом "эникейщик", - так на компьютерном жаргоне называют низкоквалифицированных специалистов широкого профиля, занимающихся установкой программ, перетыканием кабелей и заменой картриджей в принтерах. В то, что Левин оказался гением конспирации и успешно маскировался многие годы, лелея коварные замыслы, никто из людей, знавших его лично, попросту не верит. Попытки ФБР использовать его в качестве консультанта или хотя бы источника информации также потерпели полное фиаско, - а ведь у этих ребят было и чем его припугнуть, и что посулить. Наконец, и сам Левин, в 2000 году, уже после своего освобождения давший показания в петербургском УВД, утверждал, что все необходимые действия производил по бумажке, тупо набирая команды, смысл которых был ему не очень понятен.

Эти обстоятельства породили массу всевозможных предположений и спекуляций, - например, будто Левин имел сообщников в самом "Ситибанке", благодаря чему и получил подробнейшие инструкции по обходу систем защиты. Банк, разумеется, провел внутреннее расследование инцидента; результаты этого расследования, разумеется, не публиковались, - однако не то что об арестах, а хотя бы об увольнениях, которые могли бы быть связаны с делом Левина, до сих пор не известно.

Итак, - похищенные средства практически полностью возвращены владельцам; участники преступной группировки получили и отбыли свои сроки; дело благополучно закрыто и передано в архив, - все довольны. Вопрос о том, кто же на самом деле взломал "Ситибанк", похоже, никого так и не заинтересовал.

Откровения старого хакера

2 ноября 2005 года на сайте "Независимого обзора провайдеров" появилась статья "Дело Левина: недостающее звено", подписанная псевдонимом ArkanoiD. Обращая внимание читателей на тот факт, что в 1994 году "компьютерных" статей УК РФ еще не существовало и что все возможные сроки давности как по российскому, так и по американскому законодательству уже истекли, автор делится воспоминаниями о том самом взломе "Ситибанка", одним из основных участников которого, он, по его словам, являлся.

По его словам, группе российских хакеров, занимавшихся исследованием сетей протокола X.25 (технология, и сегодня активно применяемая в банковском деле, телеграфии и в ряде других приложений, а в 1994 году куда более распространенная, чем IP-технология, на основе которой работает Интернет), удалось получить доступ к электронной доске объявлений "Ситибанка". Используя ее в качестве плацдарма, участникам группы удалось получить права доступа к некоторым серверам во внутренней сети. Дальнейшее же было, в первую очередь, прямым следствием безалаберности сотрудников банка. Так, получив доступ к корпоративной электронной почте, хакеры сумели перехватывать письма, в которых в явной форме пересылались пароли и инструкции по доступу к различным системам. В тех случаях, когда этой информации недоставало, пароли к серверам подбирались при помощи простейшей программы перебора, благо были для этого достаточно простыми, чтобы присутствовать в типовом словаре. Несмотря на то, что сеть банка была оснащена системой обнаружения вторжений, системные администраторы оказались настолько самонадеянными и невнимательными, что хакеры смогли разгуливать по их владениям практически не маскируясь - отчетов системы просто-напросто никто не читал.

Эта хакерская группа исповедовала идеологию white hats ("белых шляп"). В хакерской среде присутствует деление на "черные" и "белые шляпы", слегка напоминающее встречаемое в сказках подразделение волшебников на добрых и злых. "Черные шляпы" считают для себя возможным воспользоваться своими знаниями и обнаруженными в чужих системах уязвимостями для совершения деструктивных действий, хищения чужих денег и т.п. Для "белых шляп" это является этически неприемлемым - их основной целью является изучение сложных систем, выявление неочевидных особенностей их работы, получение и распространение информации. Возможно, далеко не все из участников группы были столь искренними идеалистами, - последовавшие события это подтверждают, - а отсутствие попыток воспользоваться доступом к счетам клиентов банка объясняется элементарной осторожностью и наличием головы на плечах. Тем не менее, сервера "Ситибанка" использовались участниками группы в качестве исследовательского полигона и даже игровой площадки - как вспоминает ArkanoiD, его любимым развлечением в то время была игра в "Star Trek", удаленно запущенная на одном из банковских серверов.

Совершенно неудивительно, что в обстановке полнейшей безалаберности системных администраторов русские хакеры в скором времени стали фактически хозяйничать в банковской сети, изучив ее намного лучше ее собственных владельцев. Они располагали поэтажными планами размещения оборудования, имели возможность доступа к счетам клиентов и даже решали мелкие технические проблемы, возникавшие у банковских работников. Эта вакханалия продолжалась несколько месяцев, в течение которых электронные системы одного из крупнейших банков мира находились под практически полным контролем группы российских хакеров, и никто этого даже не замечал, пока однажды один из участников группы не продал рецепт входа в банковскую сеть Владимиру Левину за 100 долларов наличными - в чем, собственно, тут же раскаялся, но было уже поздно. Левин еще только-только размышлял и планировал, как можно с выгодой воспользоваться полученной информацией, а участники группы замели следы и покинули сеть "Ситибанка", чтобы никогда больше туда не возвращаться.

Who is Mr. ArkanoiD?

Первые же закономерные вопросы, возникающие при ознакомлении с этой историей, смахивающей на сценарий голливудского фильма: насколько данная информация является достоверной, кто такой этот

таинственный ArkanoiD, рассказывает ли он правду или же совершенно сторонний человек по каким-то причинам решил сделать себе паблисити, поворошив историю давно минувших дней?

На обращение по электронному адресу, указанному в качестве контактного в статье, опубликованной на "Независимом обзоре провайдеров", был получен ответ, что контактировать с журналистами напрямую автор не намерен, а любые его контакты с прессой следует осуществлять через Александра Милицкого - совладельца и руководителя "Обзора", одного из ведущих российских экспертов в области Интернета и телекоммуникаций.

"Независимый обзор провайдеров" хорошо известен на телекоммуникационном рынке как ресурс, периодически публикующий острые и неоднозначные, но достоверные и качественные статьи, - достаточно отметить, что громкий скандал о пиринговых войнах магистральных интернет-операторов разразился в конце 2002 года именно после публикации на "Обзоре". Сам Александр Милицкий заявляет, что у него нет абсолютно никаких оснований сомневаться в достоверности сообщаемых в статье сведений. Раскрыть личность автора он, как утверждается, не смог бы при всем желании - их общение происходит через Интернет, и г-ну Милицкому неизвестны ни настоящее имя, ни адрес ArkanoiD`a. Впрочем, и те сведения, которые могли бы так или иначе привести к раскрытию псевдонима, он отказывается сообщить иначе, чем по решению суда (ссылаясь на Закон РФ "О средствах массовой информации"), хотя при этом он отдельно подчеркивает, что с точки зрения действовавшего на тот момент российского законодательства автор статьи не совершил никакого преступления, а сроки давности по американским законам уже истекли. Он сообщил лишь, что ArkanoiD живет в Санкт-Петербурге, работает экспертом по информационной безопасности в одной из IT-компаний и не занимается никакой незаконной деятельностью.

На заданный нашим изданием при посредничестве г-на Милицкого вопрос, является ли он главным действующим лицом в истории со взломом "Ситибанка", или есть и другие лица, внесшие серьезный вклад в осуществление этой операции, ArkanoiD ответил дословно следующее: "Да, являюсь - не только как координатор, но и как исследователь. Кроме упомянутых в этой истории, было еще несколько человек, принимавших активное участие, но сейчас контакта с ними у меня нет. Если кто-то из участников считает, что я недостаточно внимания уделил его достижениям в этом рассказе, пусть не обижается, а дополнит мою историю. Это не следует понимать так, будто я лично хочу присвоить себе достижения всей группы, а всего лишь хочу правильно описать свою роль. То есть можно сказать, что я сделал больше, чем кто-либо, но не больше, чем все вместе взятые."

На российской и международной хакерской сцене имя ArkanoiD хорошо известно, и в ряде версий неофициальных хит-парадов компьютерного андерграунда он, наряду с такими персонажами, как Solar Designer, относится к числу наиболее квалифицированных хакеров на территории бывшего СССР. Попытки навести справки в андеграундной среде, скорее, дело запутали, нежели прояснили, - например, по некоторым слухам, ArkanoiD де-юре вообще не существует в природе, поскольку у него нет и никогда не было паспорта. По некоторой информации, его зовут Алекс Смирнов, однако нет совершенно никакой уверенности, что это его настоящее имя. В "Живом журнале" существует проживающий в Петербурге пользователь с похожим псевдонимом, но в день публикации статьи он обнародовал сообщение, в котором заявил о своей полнейшей непричастности ко всей этой истории.

Тем не менее, автор статьи, несомненно, является реальным лицом и, по всей видимости, действительно сыграл весьма существенную роль во взломе сети "Ситибанка" в 1994 году.

Новые лица

Буквально через несколько часов после того, как ArkanoiD опубликовал свою статью на сервере "Независимого обзора провайдеров", один из ведущих российских экспертов по информационной и сетевой безопасности Дмитрий Леонов разместил на своем сайте "Русский BugTraq" главу книги "Атака из Internet", написанную им в соавторстве с Ильей Медведковским, Павлом Семьяновым и Алексеем Лукацким. Там также идет речь о деле Левина и взломе "Ситибанка" - воспоминания одного из участников событий цитируются с сохранением авторской орфографии и пунктуации:

"…Продолжение истории было примерно в 94 году. Тогда ко мне в гости зашел мой знакомый, назовем его Буказоид, и очень туманно рассказал, что он нарыл в Спринте кучу интересных хостов. Я вспомнил про свое копание в недрах Спринта и быстро разговорил его :). Буказод, как оказалось, очень полюбил одну BBS, которую зачем-то установили в Ситибанке, нашел там кучу дыр, позволяющих устанавливать произвольные лимиты пользователям, и сидел там регулярно, используя ее для общения с друзьями из разных городов (благо платил за все Ситибанк).

…

Для удобства хакеров у серверов была команда help, а так же команды, показывающие конфигурацию, список известных IP-адресов по ARP, список известных сервисов (хостов в LAT и локальных сервисов), причем с комментариями. Я очень быстро наваял скрипт, который скачивал список сервисов, потом коннектился со всеми и записывал то, что они отвечали. ТАким образом было найдено куча серверов-шлюзов в другие сети, outdial`ы - доступ к модемам с возможностью звонить по всему миру, сервисы, позволявшие устанавливать соединения по X.25 от имени Ситибанка (только по Спринтнету и Тимнету), причем оплаченные соединенния, что позволяло соединяться с теми хостами, которые отказались принимать неоплаченные соединения или соединения из России, что позволило вновь воспользоваться ранее изученными шлюзами в Интернет из Спринта и outdial`ами Спринта :)

…

Наконец я нашел то, что искал - выход в Интернет. Один из роутеров, в Чили, к которому был подключен канал на какой-то местный банк, имел адрес этого банка на интерфейсе к нему. А из сетки того банка был открыт роутинг в Интернет. Зайдя телнетом на этот роутер, можно было с него дальше телнетом идти куда угодно. И обратно - можно было из Интернета зайти на этот роутер, а с него - во внутреннюю сеть Ситибанка и дальше, например, по X.25.

Буказоид тоже не дремал. Программировать ему было лень, поэтому он копал не вширь, а вглубь. Один из терминальных серверов имел занятную дырку - он не отслеживал отключение клиентов, попавших на него по X.25. Любой клиент, пришедший на него по X.25, оказывался подключенным к тому компьютеру, с которым работал ранее оказавшийся на том же порту товарищ если он забыл отрубиться от него. Для удобства, у серверов доступа была команда show users, показывавшая всех клиентов на всех портах, и адреса или имена компьютеров, к которым они были подключены. Заходишь на сервер, набираешь show users, отключаешься от него и начинаешь подключаться к тем портам, на которых кто-то висит. Если порт уже свободен, то оказываешься в нужном месте. Буказоид так быстро попал на парочку VAXов вместо их админов, завел себе там кучу логинов и занялся изучением VMS и деятельности админов Ситибанка. Собирал там какие-то файлы, читал переписку и т.д. Например, админы любили посылать друг другу большие списки с администраторскими паролями машин :)))

Естественно, на VAXах был замечательный контроль безопасности, результатом которого были огромные отчеты по всей подозрительной деятельности ... Буказоид нашел один такой - в нем были все следы его работы. Уверен, что тот отчет был распечатан, переплетен и поставлен на полку :)). Из их переписки выяснилось, что про проблемы с этим сервером доступа всем было известно ... Но никого это особо не волновало - его планировали заменить через полгода-год. дело в том, что считалось, что хакеры не могут залезть через Спринт - в американском Спринте было хорошо поставлено отслеживание хакеров и туда никто не совался. Но мир стал гораздо теснее. Кроме нас в Ситибанке копались хакера из Болгарии и других мест.

Естественно, не раз я и Буказоид оказывались подключенными через этот глючный сервер и к компьютерам, отвечающим за финансовые операции. Как вместо админов, так и пользователей, которые работали с некой системой "клиент-банк" через терминал. Можно было просто ввести номер счета и перевести со счета клиента деньги. Но наличие мозгов помогло избежать криминала - понятно было, что украсть деньги и остаться при этом незамеченным не получится, а если получится, то не получится выжить после этого :) Поэтому компьютеры с деньгами мы обходили стороной - не это было нужно.

Через некоторое время использование Ситибанка стало обычной рутиной - просто удобная измученная дыра для выхода в разные места. Примерно через полгода прогремел гром - Левин ограбил банк. Через пару дней ко мне прибежал наш общий знакомый с Буказоидом, и с ужасом в голосе поведал, что это он поведал Левину про тайну, получив за это $100. По счастливой случайности, я был с Левиным незнаком, поэтому меня пронесло и на допросы не таскали. Но урок был хороший - можно было загреметь за чужие грехи легко. Хотя сами мы УК не нарушали - в то время не было статей об несанкционированном доступе в УК, а денег мы не воровали :)"

Об авторе этого отрывка нам удалось выяснить, что его зовут Анатолий, он также проживал ранее в Петербурге и является известным специалистом в области телекоммуникаций.

Очевидно, под псевдонимом "Буказоид" в этом отрывке упоминается никто иной, как ArkanoiD, опубликовавший статью на "Независимом обзоре провайдеров". Сам отрывок был явно написан задолго до момента ее публикации, и может считаться независимым подтверждением правдивости изложенной там

истории.

Бородатая сенсация

Пристальное изучение вопроса приводит нас к довольно любопытному выводу - вся эта сенсационная история, оказывается, давным-давно является секретом полишинеля. И сам ArkanoiD, и его окружение уже несколько раз делали попытки "рассказать правду о деле Левина" и неоднократно контактировали с журналистами различных изданий, начиная еще с 1997 года. Однако падкие до жареного акулы пера подавали историю под таким соусом, что никто из серьезных людей в ее достоверность попросту не верил, а у самих горе-ньюсмейкеров выработалась стойкая идиосинкразия на общение с представителями второй древнейшей. Как пишет сам ArkanoiD:

"К вопросу о том, за что я не люблю журналистов. Я уже делал несколько попыток так или иначе рассказать эту историю - и каждый раз она была чудовищно переврана. В частности, особенно меня раздражает тот факт, что каждый (!) раз, когда мне случалось давать интервью, журналисты в конечной редакции - которую "по техническим причинам" "забывали" мне показать, решали "упростить" мой рассказ и представить дело так, что это я и был тем человеком, который продал Левину материалы исследовательской группы. Хотел бы сказать "бог им судья", но, будучи далек от христианской религии, скажу - плюньте в рожу этой мрази. Подобное обвинение ставит под сомнение не только мой профессионализм, а даже наличие элементарного здравого смысла. Разумеется, я хорошо понимал цену этой информации, и ни о какой подобной сделке и речи быть не могло. Да, я ошибся и моя ошибка меня многому научила - но идиотом я не был никогда."

Подобное отношение несложно понять, если ознакомиться, например, со статьей Курта Бранденбургера "Русская м@фия" в швейцарском журнале Facts:

"…Как выглядит человек, который долгое время лидирует в списке лучших хакеров? Коричневое кожаное пальто, темные очки, черные волосы до плеч, какая-то смесь из хиппи, Распутина и злодея из компьютерных фильмов. И этот человек со своим компьютером держит в страхе русские банки, теле- радиостанции и обладателей кредитных карточек?

…

Аркеной проникал в больничные карты городских больниц, взламывал коды кредитных карточек и манипулировал счетами новых русских. Как утверждает сам Аркеной, он делал это для своего удовольствия, а не с целью обогащения…"

После появления в печати подобных образчиков журналистского искусства неудивительно, что участники тех событий надолго прервали какие-либо контакты с прессой, а сегодня предпочитают рассказывать о них самостоятельно, отгородившись от журналистов посредниками. Если бы тон тогдашних публикаций был менее несерьезен, вполне вероятно, история могла развиваться и иначе - ведь на момент, когда они вышли из печати, сроки давности по американскому законодательству еще не истекли, и участники взлома "Ситибанка" могли бы быть привлечены к ответственности наряду с Левиным и его подельниками.

Тем не менее, и этого хватило, чтобы в околокомпьютерной среде история о взломе "Ситибанка" воспринималась как общеизвестная и чуть ли не классическая, а знаменитые 100 долларов, которые Левин заплатил за его секреты, стали притчей во языцех. Упомянутые публикации раскрывают ряд технических подробностей и дают представление о масштабе власти, которую русские хакеры в течение нескольких месяцев имели над сетью одного из крупнейших банков мира, - однако ничего принципиально нового, по сути, не сообщают.

Масштабы угрозы

Как теперь стало окончательно понятно, Владимир Левин не имел сообщников внутри банка, а сама возможность столь грандиозной операции оказалась реальной, в первую очередь, из-за раздолбайства банковских служащих и их пренебрежения элементарными нормами безопасности. Тем не менее, захват контроля над сетью "Ситибанка" потребовал длительной и кропотливой работы группы высококвалифицированных хакеров, преследовавших, впрочем, не корыстные, а исследовательские цели.

Возможно ли повторение подобной истории со стороны организованной преступной группировки, имеющей более корыстные устремления, нежели в описываемом случае? Авторы "Атаки из Internet" относятся к такой перспективе весьма скептически:

"...Проблема сетевых кракеров в том виде, как она обычно преподносится СМИ, на самом деле отсутствует. Да, много сил должно уделяться защите компьютерных систем от "псевдохакеров", которые считают себя профессионалами, умея запускать различные "нюки" (nuke) или подбирать пароли типа "guest". Они способны нанести этим определенный урон. Существуют, безусловно, и более квалифицированные группы кракеров, занимающиеся, например, взломом WWW-серверов для "увековечивания" собственного имени. Но у нас вызывает большое сомнение существование профессионалов, а тем более налаженной индустрии, которая допускает взлом любого более-менее защищенного хоста "на заказ". По собственному опыту мы можем предположить, что цена такого взлома должна быть в несколько раз больше, чем ценность находящейся там информации, поэтому в ход идут старые проверенные методы типа вербовки или подкупа.

Резюмируя, мы считаем, что сетевых кракеров, специализирующихся на вскрытии хостов за деньги или с целью использования полученной информации для собственного обогащения, практически не существует. Их квалификация должна быть настолько высока, что они наверняка являются хакерами, а не кракерами."

Впрочем, ArkanoiD с ними не вполне согласен: "В большинстве случаев действительно верно, что проще добиться решения задачи другими методами, но почему-то многие хотят именно так. А раз есть спрос, значит, наверняка возникнет и предложение..."

Автор: Сергей Рублёв © Lenta.Ru КОМПЬЮТЕРЫ, МИР 2738 07.11.2005, 14:38 220
URL: https://babr24.com/?ADE=25665 Bytes: 23944 / 23902 Версия для печати Скачать PDF

Телеграм: @tomsk24_link_bot
эл.почта: tomsk.babr@gmail.com

Прислать свою новость

ЗАКАЗАТЬ РАЗМЕЩЕНИЕ:

Рекламная группа "Экватор"
Телеграм: @babrobot_bot
эл.почта: eqquatoria@gmail.com

СТРАТЕГИЧЕСКОЕ СОТРУДНИЧЕСТВО:

эл.почта: babrmarket@gmail.com

Подробнее о размещении

Отказ от ответственности

Правила перепечаток

Соглашение о франчайзинге

Что такое Бабр24

Вакансии

Статистика сайта

Архив

Календарь

Зеркала сайта