кардинг по новому

лось ака серверный олень

одни хакеры ломают программы, другие — платежные системы. они не вламываются как грабители среди бела и дня и не кричат руки вверх мать вашу! они действуют скрытно, заметают следы и их очень-очень трудно найти. хоте узнать как реально работают кардеры? тогда вот эта статья!

введение

Back in the old days… опс, а чего это я вдруг по-английски заговорил? А! понятно! Всю ночь мылился с зарубежными кардерами, так как наши не канают в этом ни хрена (или канают, но молчат как партизаны). Испания. Нидерланды. Швеция. Австралия. Я говорил со всеми и многие поделись вполне реальными рецептами взлома, которые мне еще долго систематизировать и укладывать в голове. Но ближе к делу. Давным-давно, когда никакого Интернета еще и проекте не было, но кредитными картами народ уже пользовался во всю, проверка подлинности кредитки представляла большую проблему, поскольку технические ресурсы не позволяли магазинам при каждой покупке звонить в банк и проверять остаток денег на счету. Стоимость междугородных звонов существенно превышала цену пары пачек сигарет или бутылки колы. Существовал определенный порог, ниже которого проверка подлинности не производилась и продавец верил клиенту на слово (конкретное значение порога каждый магазин выбирал самостоятельно). Подделать карту не имея специального (и весьма дорогостоящего!) оборудования было очень сложно и хотя существовала вероятность купить трехтомник Кнута за 50$ при балансе всего в 10$ или даже 1$, злоумышленника было легко найти, ведь карта выдается не просто так, а только тем, у кого есть счет в банке.

Появление Интернет-магазинов породило множество проблем. Удаленный сервер не может "пощупать" кусок пластика и все, что он видит — последовательность цифр, определяющую номер карты. Разумеется, она не случайна и не всякая комбинация чисел будет воспринята с благодарностью. В номер карты прежде всего входит контрольная сумма, страхующая от ошибки набора, а так же некоторая другая информация, описывающая тип банка-эмиттера, тип самой карты и т. д. То есть просто взять и ввести что ни будь от балды не получится. Нас просто пошлют подальше вот и все. Однако, если расшифровать алгоритм кодирования номеров, можно сгенерировать вполне правдоподобный номер, который визуально ни чем не отличается от подлинного. Конечно, магазин может послать в банк запрос — а существует ли такой номер вообще, но... это же пока придет ответ! А цивилизованный клиент ждать не любит! Он просто пожмет плечами и пойдет в другой магазин. Конкуренция ведь!

Поскольку, алгоритм кодирования номеров долгое время держался в строжайшем секрете, а расшифровать его по одним лишь номерам карт было практически невозможно, карты быстро завоевали популярность и получили массовое распространение. Неразвитость систем связи существенно затрудняла распространение хакерской информации и если даже кто-то (например, уволенный банковский работник) был готов рассказать что и как, это никому не вредило, т.к. круг вовлеченных людей был очень мал. Но с появлением BBS все изменилось. Алгоритм кодирования просочился в массы и хакеры создали множество автоматических генераторов, некоторые из которых живы до сих пор (правда, уже не работают).

Любой подросток мог скачать генератор с борды и забыть, что такое отсутствие карманных денег. Ущерб от краж стремительно возрастал, но банки долгое время делали вид, что ничего не происходит, дескать их система прочна как бронепоезд и хрен вам ее взломать. Кардерами занималась полиция. Заказы приходили по реальным адресам, и хотя их было можно до некоторой степени замаскировать (например, оформить посылку на имя друга), полностью спрятать хвосты в воду не удавалось. А вот кражи из-за рубежа (особенно из России) проходили спокойно и безнаказанно. Поимка жулика требовала слишком много юридической волокиты и у чиновников был всегда наготове железный отмаз: "у нас тут людей на улицах режут, а вы со своими крадерами". Конечно, кое-кого все-таки ловили и вроде бы даже судили условно, но пойманных единицы из тысяч!

В настоящее время генераторы практически полностью утратили актуальность, поскольку практически все Интернет-магазины без исключения (и, естественно, банкоматы) всегда проверяют подлинность карты, отправляя запрос в банк, тем более что современные технические средства это позволяют.

А вот другой пример "исторического" взлома. Каждый из нас наверняка видел как в фильмах в банкомет вставляется какое-то устройство с бегущими цифрами, а в конце достается пачка хрустящих купюр. Что это такое? Оказывается, это генератор PIN-кодов, подключаемый в обход клавиатуры банкомета. Подобрать полный номер кредитки нереально, поскольку это займет слишком много времени, да и будет слишком наглядно. На банк обрушится лавина запросов и банкомет будет немедленно заблокирован. Но если подсмотреть номер чужой карты, то подобрать PIN вполне реально, если, конечно, делать это не вручную, а с помощью электроники. Банкометы, естественно, предусматривают блокировку карты после определенного количества неправильных попыток, но в древности защитная схема была плохо отработана и ее удавалось обойти. Теперь же все это в прошлом. Очевидные дыры уже давно заткнуты и просто так не взламываются, однако, кардеры сдаваться не собираются и можно сказать даже процветают. Настало время познакомится с современными методиками взлома.

тайники электронных магазинов

Совершая покупку по кредитке, мы неизбежно "засвечиваем" ее номер. Многие магазины запоминают его в специальной базе на тот случай если мы вдруг придем сюда еще раз и нам, как постоянным покупателям, сделают скидку. Разумеется, это не единственная причина для сохранения номеров, но одна из. Нас уверяют, что никакие данные никому не передаются и никогда используются нам во вред. Может быть, это действительно так, может быть действительно налоговые органы удерживаются от соблазна порыться в готовой базе и устроить серьезную разборку, как это так, человек платит налогов на 10$, а каждую неделю совершает покупок на 10.000$. Ясно только одно — раз эта база как-то взаимодействует с Интернетом она не полностью изолирована от внешнего мира и в нее можно проникнуть и похитить РЕАЛЬНЫЕ номера кредитных карт, которые выдержат ЛЮБУЮ проверку.

Конкретные методики взлома могут варьироваться от атаки на операционную систему, под которой вращается сервер, до "инъекции" SQL/PHP-команд в строку формы запроса. Главное — забросить свой shell-код на удаленный узел, а все остальное, как говориться, дело техники. Подробнее об этом можно прочитать, в частности, в моих "записках исследователя компьютерный вирусов", электронную копия которой лежит на ftp://nezumi.org.ru

Пресса регулярно сообщает о том, что при аресте очередного хакера у него обнаружили сотни и даже тысячи краденных номеров. Естественно, когда взламывается база, какой смыл уносить с собой только часть? Если уж брать так все. Вот хакеры и берут. Тем более, Интернет каналы у них по настоящему скоростные. Правда, воспользоваться награбленным удается далеко не всегда и не всем. Дело в том, что если владелец оригинальной карты обнаружит недостаток средств и побежит в банк, карта будет немедленно заблокирована, и при первом же обращении к ней полиция побежит искать мошенника по адресу, указанному при совершении покупки в Интернет-магазине. Обналичить деньги через банкомет так же не получается, поскольку банкомету требуется "живая" карта, а не только ее номер, а вот карты-то у похитителя и нет. Так что опасность подобных краж все-таки сильно преувеличена. Во всяком случае ни одному хакеру разбогатеть так и не удалось. Прямо как в анекдоте, теоретически мы миллионеры, а практически можем купить только пиво, да и то не без риска.

Правда, есть люди, которые занимаются обналичиванием ворованных денег, естественно, удерживая за это свой процент, который колеблется от 30% до 60% от общей суммы, но их немного. К тому же никто из них не собирается гарантировать хакеру какой бы то ни было "безопасности". Так что это слишком рискованный бизнес и лучше в него не ввязываться. Намного проще и безопаснее пойти бананами торговать.

шпионаж за соседями

При заполнении формы на сайте Интернет-магазина вся конфиденциальная информация должна передаваться по специальным протоколам, заведомо устойчивым к перехвату (например, по SSL), однако, некоторые магазины этим требованием пренебрегают и номер карты передается по сети открытым текстом. Можно ли его перехватить? Теоретически возможно, практически же… тоже возможно, но для этого придется попотеть.

Начнем с того, что даже если мы захватим один из промежуточных маршрутизаторов (что уже является огромной проблемой) выделить из общего потока гигабайтного трафика жалкие несколько цифр скорее всего не удастся. Если же атаковать сам Интернет-магазин, то ничего перехватывать вообще не нужно. Просто взять базу и уйти!

А вот в локальной сети кое-что выловить все-таки можно. Достаточно установить сниффер и грабить весь пролетающий трафик. Пассивные снифферы грабят только текущий

сегмент, активные — и все остальные. Об этом мы уже неоднократно писали в предыдущих номерах Хакера, так что не будем лишний раз повторяться. В крупной организации, локальная сеть которой насчитывать сотни узлов, а сотрудники из разных отделов зачастую даже не знакомы друг с другом, подобные кражи случаются достаточно часто. Вася покупает в Интернет-магазине новый диск или регистрируется на порно-сервере, чтобы посмотреть на голых телок и хоть немного отвлечься от работы, а Петя ворует номер его кредитки и дальше использует ее по своему усмотрению. Чаще всего Вася не стремиться раздувать большой скандал, поскольку ему тогда тоже достанется, да и доказать, что кредитку своровал именно Петя, а не кто-то еще практически невозможно, особенно если Петя использовал ее для доступа на другой порно-сайт, например, с голыми мужиками. Пускай они ему совершенно фиолетовы, но сам факт! Пусть Вася докажет, что это не он гей. А Петя тем временем будет покупать диски и прочую мишуру...

Аналогичным образом можно действовать и в сетях кабельного Интертена, который чаще всего строится на обычном Ethernet. Про беспроводные сети и точки доступа не стоит и говорить. Их ломают только так!

обвитый проводами

А что насчет банкометов? Можно ли их хакнуть? На первый взгляд нет, потому что они оборудованы камерами слежения и соединены с банком выделенным бронированным кабелем, закопанным глубоко под асфальт, причем протокол передачи заведомо устойчив к перехвату и даже если мы сможем врезаться в линию банкомет ←→ банк, это мало что даст. Максимум — мы просто устроим тотальный DoS, нарушив работу банкомета, но денежек все равно не получим. На самом деле, все это не более чем теория. Реальные хакеры рассказали мне (и я склонен верить им), что в действительности сплошь и рядом для передачи данных используются готовые каналы связи, в том числе телефонные линии и Интернет, а сам кабель по пути своего следования заходит то в одни, то в другие распределительные шкафы и самое главное! Протокол обмена все-таки неустойчив к перехвату. Поскольку, вся система проектировалась в те далекие времена, когда процессоры, мощнее чем Intel 4004 стоили огромную кучу денег и занимали целый шкаф, разработчики просто не могли использовать "тяжелые" алгоритмы шифрования, которые современные компьютеры взламывают за считанные минуты. Но дело даже не в этом. Хакеры нашли эффективные способы повторного снятия денег даже без знания ключа. Это сложно объяснить на пальцах, тем более, что деталей я не понял и сам (ну что делать, не криптогрфы мы), но приблизительная картина выглядит так:

В ходе совершения транзакции банк и банкомет обмениваются зашифрованными пакетами, содержащими помимо всего прочего еще и поле синхронизации. Это просто 16-битное число, увеличивающее на единицу с каждым отправленным/принятым пакетом. Поскольку оно так же зашифровано, то ни предсказать, ни подделать его невозможно. Можно только… сбить счетчик синхронизации, послав несинхронный пакет. Несмотря на наличие поля контрольной суммы, поле синхронизации в него не попадает, а поскольку здесь используется простейшее потоковое шифрование, то искажение поля синхронизации никак не воздействует на остальные поля и потому такой пакет будет воспринят банкометом как правильный, но вот счетчик синхронизации будет сброшен. Это значит, что мы можем повторить посылку ранее посланных пакетов, перехваченных нами, и банкомет послушно снимет деньги с карты еще раз. Естественно, чтобы поля синхронизации совпали, мы должны сбрасывать счетчик до начала легального снятия денег клиентов и перед повтором этой операции. Поскольку, число повторов ограничено только количеством денег на счету жертвы, нам совершенно все равно сколько она снимает — один доллар или сто. Мы может снять сколько угодно!

Основная проблема — как все-таки перехватить канал связи? Конечно, можно залезть в распределительный шкаф, предварительно сорвав замок, но это будет совсем не по-хакерски. В случае с телефонной линей все проще. Цифровые АТС неплохо исследованы хакерами и имеют множество дыр, через которые можно подключиться к любому каналу. Про Интернет вообще не стоит и говорить! Взломать провайдера хоть и сложная, но вполне осуществимая задача.

летучие голландцы

Вместо того, чтобы обчищать чужие магазины многие жулики предпочитают создавать свои. В штатах и Европе эта деятельность поставлена на широкую ногу и буквально ошеломляет своим размахам. Такое впечатление, что жульничество в конце 20 века стало нормой жизни.

Некоторые (и их меньшинство) просто подыскивают раскрученный Интернет-магазин или любой другой сайт, работающий с кредитками (например, порно), создают его визуальную

копию и размещают ее на близком по написании домене так, чтобы ошибшиеся в написании покупатели попадали в их загребущие лапы. Остается просто считать номер кредитки и отправить клиента ожидать заказа, который ему, естественно не придет. Или… все-таки придет? Некоторые жулики, рассчитывающие на долговременное существование, действительно высылают заказ, усыпляя бдительность клиента, а через некоторое время обчищают его счет до последнего цента.

Как вариант можно прибегнуть к массовой рассылке с предложением перейти по ссылке. Маловероятно, чтобы все пользователи вчитывались в ее написание, тем более что дырявый Outlook Express позволяет легко маскировать ссылки. Человек думает, что переходит к сайту A, а на самом деле его направляют на B.

Еще можно внедриться в файл hosts, хранящий IP адреса некоторых доменных имен, однако, для этого хакеру необходимо получить статус администратора на атакуемой машине, но разве это проблема? Просто рассылаем заманчивый файл, не открыть который просто невозможно, и пожинаем урожай.

Впрочем, все эти пути незаконны и небезопасны. А вот вполне честный путь. Человек покупает у нас скажем пачку сигарет за 6$, а с него карточки каждый месяц снимается $100. Как? За что? Почему? Караул!!! Грабят среди бела дня!!! Помогите хоть кто ни будь!!!

И нечего так кричать! Никто никого не грабит. $100 это за льготную подписку на журнал о вкусной и здоровой пище. Было же сказано в двухсот страничном соглашении, что все покупатели автоматически получают членство… Ага, да вон там на сто десятой странице мелким шрифтом. Если кто не прочитал — так это его личные проблемы. Мы ничего не воруем, мы ведем честный бизнес, а за такие наезды мы еще и в суд можем подать. Короче, уйдите и не отвлекайте службу поддержки своими дурацкими вопросами.

Я как-то купил в одном магазине диск своей любимой группы. Через месяц получил внушительную посылку в которой помимо диска было много всего… Вот, думаю, как же здорово на западе магазины работают. Столько бонусов за первую покупку! Ага! Как же! Бонусы! Это был реальный товар, который мне всучили, воспользовавшись тем, что мне лень было читать все, что они там пишут. И главное — не придерешься. Все предельно честно.

Многие люди склонны считать, что воруют в основном на порно-сайтах. Как сказать. Это смотра какой сайт. Не все порно-сайты созданы жуликами и не все не-порно сайты созданы честными людьми. Часто бывает так: заходишь на сайт, торгующий электронными книгами, музыкой или кинофильмами, оплачиваешь товар, а вместе с ним кучу всего в придачу.

социальная инженерия

Среди множества объявлений, предлагающих работу, зачастую попадаются вполне приемлемые варианты. Вас готовы принять в любое время, только предварительно необходимо завести кредитную карту на которую будет поступать зарплата и естественно сообщить ее номер для проверки, а то ведь мало ли что… Если такая карта у вас уже есть, то это вообще хорошо! Ну да, кому хорошо, а кому не очень. Стоит ли говорить, что после этого "фирма" снимает все ваши деньги и исчезает, а вы даже не знаете кому идти жаловаться. Никто не будет искать виртуальную фирму, существующую только в электронных проводах и сетевых картах.

Список методик "безболезненного" отъема денег довольно обширен и разнообразен. Далеко не всегда удается установить, что имеешь дело с обманщиком. Например, вам могут предложить 100% работающий генератор номеров (не троян) за… $1.000. А чего вы хотели? Такие генераторы обычно стоят даже дороже. Вот несколько наугад сгенерированных номеров. Проверьте их — они работают! Интернет-магазины принимают их к оплате! Да нет же, это не троян. Я точно говорю. Вот исходные тексты, вот откомпилированный файл. Смотрите, никакого подвоха тут нет и воровать с вашего компьютера никто ничего не собирается! Ну и так далее в том же духе, пока клиент не выложит $1000 за совершенно бесполезную программу. Да, в нее вложено большое количество реально работающих номеров. Все это — кредитные карты злоумышленника. Естественно, они работают! В смысле отовариваются. Правда на них лежит совсем немного денег и сразу же после сделки злоумышленник немедленно блокирует все карты, так что покупатель остается с носом. Вот такое наказание за жадность. А кому жаловаться? "Я купил генератор и только собирался похарествовать как обнаружил, что меня кинули на $1.000. Гражданин прокурор, разберитесь с ними пожалуйста!" Смешно? Конечно, чисто теоретически обиженный покупатель может нанять братков, но это уже совсем из другой оперы.

заключение

Мошенничество с кредитными картами совершается ежесекундно и сдавать своих позиций кардеры не собираются. Напротив, они наступают, занимая все новые и новые территории. Однако… Лично я никогда не занимался кардерстом, поскольку оно слишком близко подошло к обыкновенному воровству за котором не стоит никакого исследовательского духа, только стремление к деньгам и жажда наживы, а настоящие хакеры в первую очередь стремятся к знаниям.