

1. Компьютерные преступления

Что такое «компьютерное преступление»?

Уголовный кодекс РФ содержит три состава преступлений, называемых преступлениями в сфере компьютерной информации, – ст. 272, 273 и 274 (глава 28). Термин же «компьютерные преступления» несколько шире, чем «преступления в сфере компьютерной информации». Он также охватывает те преступления, где компьютерная техника, программы, компьютерная информация и цифровые каналы связи являются орудиями совершения преступления¹ или объектом посягательства. К таким преступлениям относятся: мошенничество с применением банковских карт (кардинг*), мошенничество с выманиванием персональных данных (фишинг*), незаконное пользование услугами связи и иной обман в области услуг связи (фрод, кража трафика), промышленный и иной шпионаж, когда объектом являются информационные системы, и т.д.

В разных источниках имеется несколько определений «компьютерного преступления» – от самого узкого (только три вышеупомянутых состава) до самого широкого (все дела, касающиеся компьютеров). Для целей форензики четкого определения компьютерного преступления и не требуется. Форензика как бы сама есть определение. Компьютерным можно называть любое преступление, для раскрытия которого используются методы компьютерной криминалистики.

В зарубежной литературе и во многих официальных документах кроме/вместо «computer crime» также часто употребляется термин «cyber crime» – киберпреступность, киберпреступление. Определения этого термина разные, более широкие и более узкие.

Для целей настоящей книги мы будем использовать следующее определение.

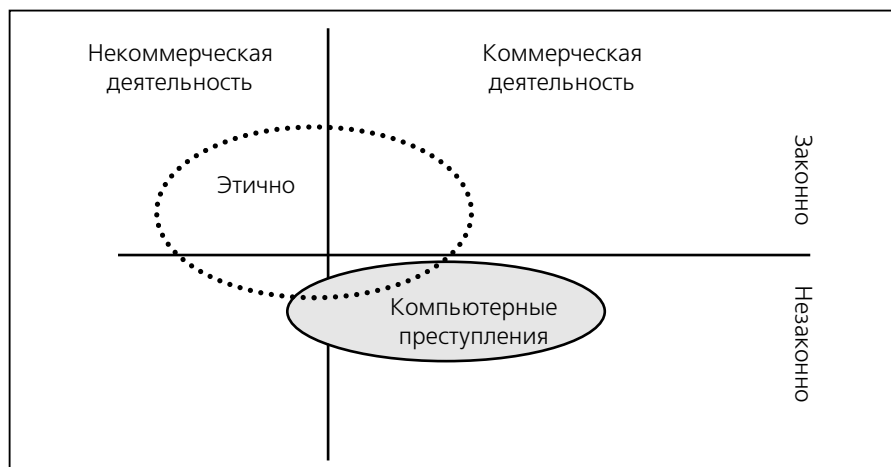
Компьютерное преступление (киберпреступление) – уголовное правонарушение, для расследования которого существенным условием является применение специальных знаний в области информационных технологий.

Компьютер и компьютерная информация могут играть три роли в преступлениях, которые автор относит к компьютерным:

- объект посягательства;
- орудие совершения;
- доказательство или источник доказательств.

Во всех трех случаях требуются специальные знания и специальные методы для обнаружения, сбора, фиксации и исследования доказательств.

¹ Понятно, что из разряда компьютерных следует исключить такие преступления, где компьютерная техника используется не в качестве таковой, а всего лишь как материальная ценность, тяжелый объект, потребитель электроэнергии и т.п.



«Правовое поле»

Избыточная криминализация

Не всякое общественно опасное деяние объявляется уголовно наказуемым. Некоторые из них государство предпочитает не криминализировать, поскольку тогда не будет возможности соответствующие преступления раскрывать, расследовать и осуществлять правосудие — настолько их будет много. Например, употребление алкоголя — очевидно, что общественно опасно. Многие страны в свое время пробовали вводить сухой закон, но никто в этом не преуспел. То есть бессмысленно бороться уголовно-правовыми методами с массовыми явлениями, для которых никак не хватит производительности у существующих правоохранительных и судебных органов. Однако в отношении некоторых общественно опасных деяний такая логика не принимается во внимание законодателями. В результате в Уголовном кодексе РФ немало составов, расследований по которым не проводится, даже если есть заявление от потерпевшего. Или еще хуже — расследования проводятся лишь по избранным случаям из массы аналогичных. В качестве примера можно привести распространение порнографии (ст. 242 УК) или нарушение тайны связи (ст. 138 УК).

Существуют разные точки зрения на вопрос, следует ли криминализовать общественно опасное деяние, если заранее известно, что не хватит производительности правоохранительных органов на уголовное преследование. С одной стороны, сам факт криминализации и редкие случаи привлечения к ответственности несколько уменьшат количество проявлений. С другой стороны, очевидная для всех необязательность и неисполняемость одного закона будет способствовать неисполняемости других.

К большому сожалению, значительная часть компьютерных преступлений относится именно к таким деяниям — криминализированным, но не обеспеченным ресурсами для раскрытия и расследования. Причем ресурсов не просто не хватает, не просто меньше, чем требуется. Их много меньше, чем нужно для полноценного уголовного преследования соответствующих преступлений. То есть их не хватило бы даже на малую часть, даже при идеально функционирующих правоохранительных органах.

В этой ситуации для работников правоохранительных органов не остается иного выхода, кроме как самостоятельно расставлять приоритеты, сообразуясь со степенью общественной опасности преступления и иными обстоятельствами (см. параграф «Приоритетность расследования»).

Криминалистическая характеристика

Для тех, кто, успешно сдав экзамен по криминалистике, уже все забыл, напомним: криминалистическая характеристика — это система типичных признаков преступления того или иного вида.

Сталкиваясь в очередной раз с преступлением, следователь или оперуполномоченный вспоминает похожие дела из своей практики, предполагает, что данное преступление — типичное и пытается применять те же самые подходы, методы, способы поиска доказательств, которые уже приносили успех в аналогичных делах. Чем более типично данное преступление, тем скорее такой подход принесет успех. Если же личный опыт невелик, следует обратиться к коллективному опыту коллег. Именно такой формализованный опыт, система знаний о типичном преступлении определенного класса и называется криминалистической характеристикой.

Она включает следующее:

- способ совершения преступления, предмет посягательства;
- личность вероятного преступника и вероятные его мотивы;
- личность вероятного потерпевшего;
- механизм образования следов;
- обстановка и другие типичные обстоятельства.

В литературе имеется несколько вариантов состава криминалистической характеристики, у разных криминалистов разные представления о необходимой степени ее подробности. Но все варианты более-менее похожи. Автор будет придерживаться вышеуказанного состава.

Большинство исследователей [8, 12, 41] пишет о криминалистической характеристике трех видов преступлений, деля все рассматриваемые преступления по составам трех статей УК — 272, 273 и 274. Вряд ли стоит настолько обобщать. Одной «компьютерной» статьей УК охватывается сразу несколько преступных деяний, сильно отличающихся по личности

преступника, по способу, по оставляемым следам. Например, психически неуравновешенный программист создал и распустил по Сети вирус, чтобы навредить всему миру, который он ненавидит. Другой пример: сотрудник рекламного агентства использует зомби-сеть* (ботнет) для рассылки спама* в соответствии с полученным заказом. Оба они совершают преступление, предусмотренное статьей 273 УК — создание или использование вредоносных программ. Но что может быть общего в характеристиках этих двух преступлений?

Некоторые юристы договариваются даже до того, что рассматривают обобщенную криминалистическую характеристику для всех трех упомянутых составов [40].

В российском УК только три статьи, описывающих преступления в сфере компьютерной информации. В украинском УК — тоже три, в белорусском — семь, в казахском — одна, в киргизском — две, в эстонском — семь. При этом составы, по большому счету, одни и те же. Почему же криминалистических характеристик должно быть непременно три?

Разумеется, при анализе отталкиваться надо не от статей УК, а наоборот — группировать преступления по признаку общности их криминалистической характеристики.

Обсудим отдельные элементы криминалистической характеристики, а затем более подробно — криминалистическую характеристику каждого из видов компьютерных преступлений.

Статистика

Поскольку криминалистическая характеристика выводится из опыта, требуется большое количество совершённых и расследованных преступлений каждого типа. С компьютерными преступлениями дело обстоит не так, как с квартирными кражами или угонами автотранспорта. Их совершается относительно немного, а выявляется и расследуется — и того меньше. Поэтому приведенную в источниках статистическую информацию следует воспринимать не как свыше данную истину, а лишь как первое приближение к будущим характеристикам, которые появятся после накопления значительного опыта.

Кстати, об опыте. Некоторые авторы приводят в криминалистической характеристике статистические данные о личности преступника или обстановке. Например, столько-то процентов преступников моложе 25 лет, столько-то процентов из них мужского пола, такая-то часть работает в отрасли ИТ и связи и т.д. Автор считает подобную статистику несостоятельной. Как полагают все эксперты (и критикуемые источники в том числе), большая часть компьютерных преступлений остается латентной. Раскрывается меньшая часть из них, причем раскрываются лишь простейшие их виды. А криминалистическая характеристика относится ко всем преступ-

лениям — и простым, и сложным. Статистика же подсчитывается только по раскрытым.

Возьмем для примера такой сложный вид преступления, как построение зомби-сетей*. Он должен квалифицироваться по статье 273 УК. Однако раскрытий такого рода преступлений в России вообще не было, а по всему миру было 3 или 4 случая. А теперь подумаем, какое значение для поиска «зомбиводов» будет иметь утверждение, что «40% преступников имели среднее специальное образование»? Учитывая, что статистика эта подсчитана только по раскрытым эпизодам ст. 273 УК, а из них около 3/4 — это навешивание 273-й статьи «в нагрузку» к нарушению авторских прав (строго говоря, неправомерное).

В данной работе автор не только отказался от классификации компьютерных преступлений по статьям УК, но и не использует для криминалистической характеристики судебно-следственную статистику. Автор, сам служивший в органах внутренних дел, слишком хорошо знает, как эта статистика пишется...

Личность вероятного преступника

Оценивая вероятного преступника, важнее всего для нас установить уровень его компетенции в области ИТ. Этот параметр является критическим. В технических методах борьбы, в соревнованиях «спрятать-найти» или «стереть-восстановить» уровень специальных знаний является решающим.

Когда квалификация подозреваемого неизвестна, ее следует предполагать высокой.

С той же целью специалисту или следователю имеет смысл до поры скрывать свой собственный уровень познаний в ИТ перед подозреваемым.

Приведем пример. Изымая компьютер во время обыска (если застали его включенным), специалист должен решить, следует ли применить штатную процедуру выключения или выключить компьютер грубым прерыванием электропитания. С одной стороны, при грубом обесточивании может пропасть некоторое количество данных, как правило, не очень существенных. Но лучше бы их сохранить. С другой стороны, у некоторых хакеров* (в дурном значении этого слова) есть противная привычка оснащать свой компьютер логической бомбой*, срабатывание которой связано с командой выключения компьютера (shutdown). Поэтому при использовании штатного выключения есть риск уничтожить все улики собственными руками. Какой вариант выбрать, зависит от того, как мы оцениваем уровень квалификации владельца компьютера. При невозможности оценить этот уровень компьютер выключается прерыванием электропитания, то есть в расчете на наличие логической бомбы.

Далее приведем описание нескольких типичных образов компьютерных преступников.

«Хакер» (наименование условное). Основной мотивацией этого типа нарушителей являются: исследовательский интерес, любопытство, стремление доказать свои возможности, честолюбие. Средства защиты компьютерной информации, ее недоступность они воспринимают как вызов своим способностям. Некоторые исследователи [12. С. 31-39] полагают необходимой чертой этого типа хорошие знания в области ИТ и программирования. Однако практика опровергла это предположение. Среди обвиняемых по соответствующим составам средний уровень знаний оказался невысок. Другие исследователи [4, 11, 57] наряду с многознающими «хакерами» вводят отдельную категорию «script kiddies*». Это те, кто движим теми же мотивами, но не в состоянии придумать свое и поэтому просто бездумно используют готовые инструменты, сделанные другими. Автор полагает возможным объединить их в единую категорию, поскольку мотивы одинаковы, а знания — вещь наживная.

Первой чертой личности «хакера» является *эскапизм* — бегство от действительности, стремление уйти от реальности, от общепринятых норм общественной жизни в мир иллюзий, или псевдодеятельность. Компьютерный мир, особенно вместе с Интернетом, является прекрасным альтернативным миром, в котором возможно найти интересное занятие, защиту от нежелательных социальных контактов, реализовать креативный потенциал и даже заработать денег. С другой стороны, человек, который чем-то сильно увлечен в реальном мире, вряд ли сможет найти достаточное количество времени и сил, чтобы стать хорошим специалистом в специфических областях ИТ.

Эскапизм является предрасполагающим фактором для возникновения компьютерной или сетевой зависимости [13]. Такая зависимость (в слабой или сильной форме) является второй чертой личности вероятного преступника. Компьютерная зависимость (аддикция) может начаться с обычного увлечения, которое аддикцией не является. Зависимость в более тяжелой форме ближе к психической девиации, а в тяжелой форме некоторые полагают такую аддикцию болезнью (причем эпидемического характера), которую следует лечить. Исследованию феномена компьютерной/сетевой зависимости посвящены десятки научных работ, как из области медицины, так и социологии [14-17]. Компьютерная, или сетевая аддикция характеризуется неспособностью человека отвлечься от работы в Сети, раздражительностью при вынужденных отвлечениях, готовностью пренебречь ценностями (материальными и социальными) реального мира ради мира виртуального, пренебрежением своим здоровьем. Исследования показывают, что

страдающие сетевой зависимостью люди в то же время отличаются высоким уровнем абстрактного мышления, индивидуализмом, интровертностью, эмоциональной чувствительностью и некоторой степенью нонконформизма.

Эти черты приводят к тому, что «хакер» имеет узкий круг общения и предпочитает всем другим контактам сетевые. Искать его сообщников и источники информации о нем следует прежде всего среди его виртуальных знакомых. Контакты и социальные связи в реальном мире «хакер» субъективно оценивает как менее комфортные и не склонен доверять своим офлайновым* знакомым.

Другое следствие эскапизма — неуделение внимания многому, что существует лишь в реальном мире и никак не отражено в Сети. Например, такой специалист может довольно чисто уничтожить следы, оставляемые на компьютерных носителях (всевозможные компьютерные логи, временные файлы, информацию в свопе и т.д.), но ему даже не придет в голову мысль про логи телефонных соединений, с помощью которых он выходил в Сеть. Один знакомый автору подозреваемый вполне серьезно утверждал, что его преступление «абсолютно недоказуемо», поскольку все мыслимые следы уничтожены. Но преступление оказалось «абсолютно доказуемым», поскольку подозреваемый отчего-то совершенно забыл про существование пяти свидетелей, которым сам же всё подробно описывал и показывал.

Второй чертой личности является некриминальная в общем направленность мыслей «хакера». Исследовательский интерес и честолюбие редко сочетаются с антиобщественными установками, предельной опасливостью, боязнью правоохранительных органов. Это, как правило, выливается в уделение малого внимания заметанию следов, непринятие мер конспирации. Часто у него даже отсутствует само осознание того факта, что совершается уголовное преступление.

Следует упомянуть, что эскапизмом и сниженной социализированностью страдает большинство ИТ-специалистов. Собственно, некоторый отрыв от реальной жизни — это побочный эффект большого опыта в компьютерной сфере. Поэтому поиск по указанным критериям даст не только возможного преступника, но и вполне законопослушных ИТ-специалистов.

«Инсайдер» (наименование условное). Несколько более распространенным типом компьютерного злоумышленника является человек, не слишком хорошо владеющий знаниями в области ИТ, зато владеющий доступом в информационную систему (ИС) в силу служебного положения. Уже стало общим местом утверждение, что большая часть «взломов» компьютерных систем совершается изнутри. Это действительно так. По-

этому при расследовании неправомерного доступа «инсайдер» — первая версия, которую следует рассматривать. Даже если неправомерный доступ был явно снаружи, скорее всего, он стал возможным из-за сговора с местным сотрудником.

Если для «внешнего» хакера обнаружить уязвимость в информационной системе представляет собой задачу, то для сотрудника предприятия почти все уязвимости видны с самого начала. И если информационная система (ИС) имеет отношение к деньгам, ценностям или платным услугам, то сотрудник постоянно пребывает под искушением. Однако руководители и даже сотрудники службы безопасности, чьим попечениям доверена такая ИС, часто страдают странным дефектом зрения: они опасаются и уделяют внимание защите от внешних злоумышленников и в то же время слепо доверяют собственным сотрудникам, забывая, что разница между первыми и вторыми — только в их возможностях. У сотрудников возможностей напасть несравненно больше.

Итак, типичный «инсайдер» совершает компьютерное преступление (лично или в форме подстрекательства, совместно с «внешним» соучастником) с использованием сведений, полученных в силу служебного положения. Такие сведения — пароли, знания о конфигурации ИС, знания о ее уязвимостях, о принятых процедурах. В ряде случаев этими сведениями он владеет «официально», то есть они ему необходимы для выполнения работы. Но чаще бывает, что реальный доступ сотрудников к конфиденциальной информации значительно шире, чем формальный или чем необходимый. То есть «инсайдер» знает об ИС больше, чем ему положено.

Например, в одной компании-операторе связи имел место инцидент с неправомерным доступом в базу данных. Были изменены данные об объеме оказанных клиенту услуг, от чего компания понесла существенные убытки. Как оказалось, преступником являлся один из сотрудников, вступивший в сговор с клиентом, с которого и «списал» часть задолженности за услуги. Он имел свой собственный логин* в указанную базу данных, но предпочел воспользоваться логином своего начальника. Это не составило особого труда, поскольку тот держал пароль на листочке, прилепленном к монитору. Свалить вину на коллег — характерное поведение для «инсайдера».

Указать иные признаки личности вероятного преступника типа «инсайдер» автор не берется. Некоторые исследователи полагают [39, 40, 48], что «инсайдер» непременно должен считать себя обиженным, обойденным по службе, недостойно вознаграждаемым. Как ни странно, но среди современного «офисного планктона» таковыми считают себя почти все. А среди так называемых «топ-менеджеров» (а равно «стук-менеджеров» и «гарк-менеджеров») — через одного. Если есть искушение украсть, и че-

ловек этому искушению поддастся, он сам себе осознанно или неосознанно найдет «обиды», вспомнит о «недоплате», о социальной розни и сочинит другие оправдания. Поэтому автор полагает, что такая черта личности вероятного преступника, как наличие обид, в криминалистической характеристике является излишней.

«Белый воротничок» (наименование условное). Этот тип преступника представляет собой давно и хорошо известного казнокрада, но только сменившего инструменты своей деятельности на компьютер. Украсть у государства или у частной компании можно сотней способов. Кроме банального хищения здесь возможны взятки, коммерческий подкуп, незаконное использование информации, составляющей коммерческую тайну, различные виды мошенничества и так далее. В отличие от «инсайдера», этот тип злоумышленника имеет минимальную квалификацию в сфере ИТ и компьютер как орудие совершения преступления не использует. Компьютер здесь выступает только как носитель следов, доказательств совершения преступления.

По своим мотивам «белые воротнички» могут быть разделены на три группы:

1. Злоупотребляющие своим служебным положением из чувства обиды на компанию или начальство. Их следует искать среди долго проработавших сотрудников. Причем для возникновения мотива мести совсем не обязательно наличие действительной обиды со стороны работодателя. В значительной части случаев, как отмечалось выше, обиды эти оказываются вымышленными. Такой обиженный, обойденный и недостойно оплачиваемый злоумышленник чаще всего ворует, чтобы «компенсировать» якобы недополученное от работодателя. Но бывают и бескорыстные мстители, которые не приобретают выгоды от своих незаконных действий либо по этическим соображениям (реже), либо для снижения вероятности раскрытия преступления (чаще).

2. Беспринципные расхитители, не имеющие моральных барьеров и ворующие только потому, что представилась такая возможность. Для подобных «белых воротничков» характерен недолгий срок службы на должности до начала злоупотреблений. Довольно часто за таким имеется криминальное прошлое.

3. Квазивынужденные расхитители, попавшие в тяжелое материальное положение, в материальную или иную зависимость от лица, требующего совершить хищение или мошенничество. Как правило, подобные проблемы трудно скрыть от окружающих — крупный проигрыш, наркомания, семейный кризис, неудачи в бизнесе. Эта группа расхитителей менее осторожна, они не могут долго подготавливать свои преступления, как это делают первые и вторые.

«Е-бизнесмен» (наименование условное). Этот тип вероятного преступника не является квалифицированным ИТ-специалистом и не имеет служебного положения, которым можно злоупотребить. С самого начала он планирует именно криминальное предприятие, отлично осознаёт его противозаконность. Решение совершить правонарушение именно в компьютерной (сетевой) среде, а не в офлайне* он принял не из-за своих особых знаний в этой области и не из-за внутренней тяги к компьютерам, а исключительно на основе рационального анализа. Он посчитал, что так будет выгоднее.

«Выгода» компьютерного преступления обычно связана с его технической или организационной сложностью. На простые уловки попадает мало жертв, от простых средств нападения большинство информационных систем давно защищены. Успешные компьютерные преступления отличаются технической сложностью, участием нескольких сообщников с «разделением труда», многоходовостью. Поэтому чертой личности «е-бизнесмена» является наличие организаторских способностей и предпринимательской инициативы.

Что же касается его незаконопослушности, асоциальности, нонконформизма, то автор полагает эти характеристики не обязательными. На этапе начального накопления капитала, в условиях так называемой «переходной экономики» многие виды бизнеса предусматривают те или иные нарушения законодательства и асоциальную направленность. С этой точки зрения владелец зала игровых автоматов не более асоциален, чем отмывающий деньги через онлайн-казино. А оптимизатор налоговых платежей не менее законопослушен, чем отмыватель электронных кошельков.

Указанному типу преступников отвечает большинство кардеров*, спамеров* и фишеров*.

«Антисоциальный тип» (наименование условное). Также отмечались интернет-мошенники, которые руководствовались не только извлечением прибыли. Более того, их преступный доход часто бывал меньше, чем средняя зарплата специалиста той же квалификации. Мотивом для совершения мошенничества являлась антисоциальная психопатия (социопатия) таких лиц и их патологическая тяга к ведению подобных «игр». Социопатия признана отдельным видом психического расстройства [61, W27] и зарегистрирована под названием «antisocial personality disorder» или «dissocial personality disorder» в классификаторе болезней ВОЗ (ICD, №F60.2). Обычно такие типы действуют импульсивно и не склонны к планированию, особенно долгосрочному.

Подобное расстройство вообще часто приводит к совершению преступления, не только компьютерного, причем мошенничества чаще, чем насилия. Интернет-мошенничество не требует особых технических зна-

ний, вполне достаточно умения пользоваться готовыми программными инструментами.

Оперативность

Некоторые отмечают особое значение оперативности действий при раскрытии и расследовании компьютерных преступлений. Ссылаются на относительно быструю по сравнению с другими видами преступлений утрату доказательств, а также на оперативность связи между сообщниками, которые могут быстро предпринять действия по уничтожению улик и иному воспрепятствованию следственным органам.

Давайте посмотрим, действительно ли это так.

Компьютерная информация бывает короткоживущей. Бывает она и долгоживущей. Даже всерьез говорят [W03] о компьютерной археологии (цифровой археологии), то есть поиске и изучении «древней» компьютерной информации ради получения исторических и обществоведческих сведений. Неоднократно отмечались случаи, когда человек, казалось бы, безвозвратно утративший информацию со своего компьютера, находил ее в Сети и таким образом восстанавливал.

Логи* хранятся не вечно. Но насколько долго? Здравый смысл подсказывает, что хранить их стоит до тех пор, пока они могут пригодиться. В зависимости от содержания логов, этот период полезности соответствует периодичности подсчета статистики, сроку действия клиентского договора, периодичности оплаты услуг, сроку исковой давности. В некоторых случаях длительность хранения логов установлена нормативными актами. Например, постановление Правительства РФ №538 [L01] устанавливает трехлетний срок хранения сведений об абонентах и их «расчетах за оказанные услуги связи, в том числе о соединениях, трафике и платежах». Многие предприятия хранят логи до истечения сроков исковой давности. Некоторые хранят информацию столько времени, на сколько хватает места на диске. В общем, сроки хранения во многих случаях могут быть весьма значительными и даже превышать сроки хранения бумажных документов. В отличие от бумажных, электронные документы обходятся в хранении и обработке несравненно дешевле.

Что касается оперативной связи между сообщниками по компьютерным преступлениям, то все используемые ими способы связи никак не оперативнее обычного телефона, которым пользуются все преступники на протяжении последних десятилетий. Вспомним также об отнюдь не повсеместном доступе к компьютеру и к Сети, об относительно медленной электронной почте, о разнице во времени между сообщниками из разных стран. Заключим в результате, что для среднего «компьютерного» преступника скорость связи с сообщниками вряд ли отличается от скорости связи для среднего мошенника или взяточника.

Возможность быстрого уничтожения цифровых следов и прочих доказательств в ряде случаев, безусловно, присутствует. Стереть один файл можно столь же быстро, как смыть в унитаз один грамм героина. Но вот стирание (а тем более, затирание с гарантией от восстановления) содержимого всего диска занимает десятки минут. В случаях, когда информация находится на удаленных компьютерах, добавляется еще время получения доступа к ним. Уничтожить основные доказательства такого занятия, как фишинг*, займет не один час, если не позаботиться обо всем заранее. Вспомним, что могут успеть за один час преступники, совершившие офлайн-преступления: выбросить в реку пистолет, заменить капот и радиатор после наезда на пешехода, отдать родственнику полученные в виде взятки деньги, выстирать испачканную кровью одежду, сжечь фальшивый паспорт, иногда даже убрать сообщника.

Видно, что оперативность действий по фиксации и изъятию доказательств для расследования компьютерных преступлений столь же важна, как для многих иных преступлений. Поэтому отличительной особенностью компьютерных преступлений не является.

Для иллюстрации темы оперативности вот случай, рассказанный сотрудником управления «К» одного из субъектов Федерации.

Был выявлен и доставлен в управление подозреваемый в совершении неправомерного доступа (ст. 272 УК). После установления места его жительства одного из сотрудников срочно отправили туда для проведения неотложного (ч. 5 ст. 165 УПК) обыска и изъятия компьютера — предполагаемого орудия совершения преступления, на котором надеялись обнаружить основные доказательства. Поскольку для задержания (ст. 91-92 УПК) подозреваемого оснований не нашлось, после допроса он был отпущен домой. На следующее утро оказалось, что в силу некоторых обстоятельств, описывать которые здесь неуместно, упомянутый выше сотрудник так и не произвел обыска в квартире подозреваемого. Разумеется, все подумали, что доказательства с этого компьютера утрачены. Уже без особой спешки, получив судебную санкцию на обыск, отправились к подозреваемому. Была еще слабая надежда, что он по незнанию просто отформатировал свой диск и информацию можно будет восстановить. Каково же было удивление оперативников, когда при обыске они обнаружили не только компьютер подозреваемого с нетронутой информацией, но и еще один компьютер — компьютер сообщника, который подозреваемый принес в свою квартиру, чтобы переписать на него всю ценную информацию со своего. Таким образом, задержка в несколько часов не привела к утрате компьютерной информации, к тому же позволила выявить сообщника.

Конечно, описанный случай не слишком типичный. Но и не единственный в своем роде.

Автор делает следующий вывод. **Необходимость особой быстроты в действиях не является отличительной чертой тактики раскрытия компьютерных преступлений.**

Приоритетность расследования

Ввиду большого количества компьютерных преступлений никто уже всерьез не рассчитывает на возможность расследовать их все. На каких именно фактах стоит сосредоточиться правоохранительным органам и службам безопасности, зависит от следующих факторов:

- Вид и размер ущерба. Очевидно, что более общественно опасными являются те из компьютерных преступлений, которые подразумевают насилие (по сравнению с теми, которые лишь наносят материальный ущерб). Также более приоритетными являются преступления, посягающие на права несовершеннолетних и иных менее защищенных субъектов.
- Распространенность. Как известно, раскрытие преступления и наказание преступника также в некоторой мере воздействуют на потенциальных правонарушителей. Поэтому раскрывать часто встречающиеся типы преступлений при прочих равных важнее, чем редкие типы преступлений.
- Количество и квалификация персонала. В зависимости от того, сколько имеется сотрудников и насколько они квалифицированы, стоит браться за те или иные компьютерные преступления. Слишком сложные начинать расследовать бесполезно.
- Юрисдикция. Предпочтительными являются преступления, не требующие задействовать иностранные правоохранительные органы. Наиболее быстрый результат получается при расследовании преступлений, локализованных в пределах одного города.
- Политика. В зависимости от текущих политических установок, могут быть признаны более приоритетными некоторые виды компьютерных преступлений. Не потому, что они более общественно опасны, но потому, что их раскрытие повлечет больший пиар-эффект или большее одобрение начальства.

Автор вовсе не считает указанную выше приоритезацию целиком правильной, справедливой и подлежащей исполнению. Автор лишь констатирует, как обстоит дело на практике. Потерпевшему, эксперту, специалисту или иному лицу следует учитывать, что правоохранительные органы берутся не за любые компьютерные преступления или проявляют разную степень энтузиазма в зависимости от вышеперечисленных обстоятельств.

Далее рассмотрим самые распространенные виды компьютерных преступлений и дадим их криминалистическую характеристику. Будут описаны лишь те элементы, которые специфичны для рассматриваемого вида компьютерных преступлений.

Как уже указывалось выше, классификация преступлений по статьям УК с научной точки зрения несостоятельна. Одни составы слишком широкие, другие слишком узкие. Например, формулировка статьи 272 охватывает и случай, когда малолетний script kiddie* завладевает копеечным логином* на доступ в Интернет, и случай, когда иностранный шпион получает доступ к компьютеру с государственной тайной. Напротив, статья 187 УК (изготовление или сбыт поддельных кредитных либо расчетных карт и иных платежных документов), казалось бы, специальная статья для кардеров*, охватывает лишь очень незначительную часть кардерской деятельности, в то время как основная деятельность кардеров — это статьи 159 (мошенничество) и 165 (причинение имущественного ущерба путем обмана или злоупотребления доверием).

На основании изложенного автор будет классифицировать компьютерные преступления отнюдь не по статьям УК, а по схожести их криминалистических характеристик.

Онлайн-мошенничество

Способ

Такая форма торговли, как интернет-магазин, нашла широкое применение среди бизнесменов по целому ряду причин. Он, в частности, отличается **низкими затратами** на организацию торговли. Стоимость веб-сайта с соответствующим бэк-офисом* не идет ни в какое сравнение со стоимостью содержания реальной торговой площади. К тому же зависимость текущих затрат интернет-магазина от его оборота если и не очень близка к пропорциональной, то значительно ближе к ней по сравнению с магазином реальным. Это значит, что при отсутствии (нехватке) покупателей убытки будут невелики. Например, цена готового, стабильно работающего интернет-магазина начинается с 15-20 тысяч долларов. По сравнению с реальным (офлайновым*) магазином, тем более в крупном городе, это просто смешные деньги.

Именно эта особенность интернет-торговли привлекла сюда мошенников. Затратив относительно небольшую сумму, злоумышленник может создать видимость нормального торгового предприятия и заняться мошенничеством или обманом потребителей. Десятки-другие жертв вполне окупают сделанные затраты. Для магазина на улице такое было бы невымыслимо.

Кроме фиктивных интернет-магазинов мошенники используют и другие предлоги для получения платежей:

- лже-сайты благотворительных организаций, религиозных организаций, политических партий и движений, которые якобы собирают пожертвования;

- спам-рассылки и сайты с просьбой о материальной помощи под трогательную историю о бедной сиротке, жертве войны, заложнике и т.п.;
- сайты фиктивных брачных агентств и отдельные виртуальные невесты;
- мошеннические онлайн-овые* «банки» и «инвестиционные фонды», обещающие дикие проценты по вкладам;
- рассылки и сайты о якобы обнаруженных уязвимостях и черных ходах в платежных системах, позволяющие умножать свои деньги, например, переслав их на особый счет (в том числе мошенничества II порядка, построенные на том, что жертва думает, будто она обманывает обманщика);
- мошеннические сайты и рассылки, предлагающие удаленную работу (на такую чаще всего клюют сетевые эскаписты) и требующие под этим предлогом какой-либо «вступительный взнос».

Все такие преступления имеют одну и ту же криминалистическую характеристику и сводятся к размещению информации в Сети, анонимному взаимодействию с жертвой и получению от нее денег с последующим исчезновением из Сети.

Одно из мошеннических писем, полученное автором.

```
Message-ID: <005401c60d0a$bd889c4b$ba13f6ba@csuftmeslrimef>
Reply-To: «=?windows-1251?B?zOj140jr?=?» <ryletsale@37.com>
From: «=?windows-1251?B?zOj140jr?=?» <ryletsssale@mail.ru>
To: <fnn@optics.npi.msu.su>
Subject: =?windows-1251?B?yuDqIO7h++Pw4PL8IPDz6+Xy6vM=?=
Date: Thu, 29 Dec 2005 21:33:59 +0300
MIME-Version: 1.0
Content-Type: multipart/alternative;
        boundary="-----_NextPart_000_00D6_01C2A75B.03B7B128"
X-Priority: 3
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook Express 5.50.4522.1200
X-MimeOLE: Produced By Microsoft MimeOLE V5.50.4522.1200
X-RBL-Warning: mail from 194.67.23.194 refused (RelayWatcher)
X-Lookup-Warning: MAIL lookup on ryletsssale@mail.ru does not match
194.67.23.194
X-MDRcpt-To: fnn@optics.npi.msu.su
X-Rcpt-To: fnn@optics.npi.msu.su
X-MDRemoteIP: 194.67.23.194
X-Return-Path: ryletsssale@mail.ru
X-Spam-Checker-Version: SpamAssassin 2.63 (2004-01-11)
X-Spam-Report:
* 3.0 MDAEMON_SPAM_BLOCKER MDAEMON: message marked by Spam Blocker
* 0.0 HTML_MESSAGE BODY: HTML included in message
* 1.2 DATE_IN_PAST_96_XX Date: is 96 hours or more before Received: date
X-Spam-Status: No, hits=4.2 required=5.0 tests=DATE_IN_PAST_96_XX,
HTML_MESSAGE,MDAEMON_SPAM_BLOCKER autolearn=no version=2.63
X-Spam-Level: ****
```


X-Spam-Processed: optics.npi.msu.su, Fri, 29 Dec 2006 21:35:05 +0300
 X-MDRedirect: 1
 X-MDaemon-Deliver-To: optics@fnn.ru

Я предлагаю вам программу, которая позволит играть в казино и ВЫИГРЫВАТЬ, абсолютно без риска собственными финансами. Если казино наживаются на наших страстях, то почему бы и нам не нажиться на их слабости?! Причем сделать это абсолютно законным способом, без риска быть уличенным в мошенничестве... Если Вы желаете приобрести программу для того чтобы использовать ее на практике или просто для всеобщего развития(программа очень интересная, кроме теории и комбинаций, есть тренировочная версия игры в рулетку, чтобы вы могли попробовать или вернее сказать закрепить материал на практике с виртуальными деньгами, когда вы увидите что система работает, то можете переходить на настоящую игру. Вышлите 500 рублей с помощью программы индекс-деньги на мой счет 4100189014963, затем напишите мне на емейл ryletsale@37.com

что деньги вы перечислили со своего счета(номер вашего счета и время перевода) на мой. После этого я в течение 24 часов высылаю вам по емейл программу. Если Вы боитесь высалать деньги по причине участвовавших обманов, то предлагаю другой вариант Вы пишете на указанные мною адрес, с возможность ознакомления программой перед покупкой. Я высылаю ВАМ маленькую часть для ознакомления, если Вас она заинтересует, то переводите деньги на счет и получаете полностью.

Если отвлечься от легенды, то жертвам предлагается перевести 500 рублей при помощи сетевой платежной системы на определенный счет. У мошенника есть минимум сутки на то, чтобы собрать деньги без риска получить обвинение в обмане. Фактически даже больше: при помощи заранее приготовленных правдоподобных оправданий реально растянуть срок до трех суток. Только после этого администрация платежной системы начнет получать первые жалобы на обман.

Предложение разослано при помощи современных спамовых технологий, массово и одновременно. Из порядка миллиона разосланных копий будут получены от 2 до 4%. Если хотя бы 1% получивших письмо поведутся на обман, мошенник заработает порядка 100 тысяч рублей, что с лихвой покрывает все издержки.

Обстановка

Такие особенности, как **сохранение анонимности** владельца веб-сайта или рассылки и **большой промежуток времени** между приемом заказа и его исполнением, позволяют мошенникам надеяться на успех своего криминального предприятия.

Таким образом, в соответствии с особенностями криминального «бизнес-плана», мы имеем три группы признаков фальшивого интернет-магазина:

- видимая сильная экономия на веб-сайте, рекламе, персонале, услугах связи и другом; мошенник вместо полноценного магазина ограничивается одним лишь «фасадом», дизайн сайта и товарный знак часто заимствованы, заказы обрабатываются явно вручную, не используется банковский счет;
- стремление скрыть личность владельца там, где она должна указываться, — при регистрации доменного имени, приобретении услуг связи, подключении телефонного номера, даче рекламы и т.п.;
- применяются только такие способы оплаты, где возможно скрыть личность получателя платежа, невозможна оплата курьеру при получении;
- период между заказом товара и его доставкой максимально растянут;
- отсутствуют дешевые товары.

Преступник

Вероятны типы преступников: «хакер» и «е-бизнесмен» (см. главу «Личность вероятного преступника»).

Потерпевший

Очевидно, что потерпевший ранее уже пользовался услугами интернет-магазинов, поскольку само использование этого вида торговли для обычного человека непривычно; требуется время, чтобы решиться и привыкнуть покупать товары таким способом.

Столь же очевидно, что потерпевший является пользователем одной из платежных систем, которые использовали мошенники.

Также потерпевшему свойственно до последнего момента надеяться, что его все-таки не обманули или это было сделано неумышленно. Даже через год некоторые из обманутых покупателей все еще могут поверить, что деньги им вернут. Например, уже выявлен и задержан владелец фальшивого онлайн-магазина. Известен один из его клиентов — тот, который и обратился в правоохранительные органы. Чтобы найти остальных потерпевших, имеет смысл возобновить работу веб-сайта, на котором размещался мошеннический магазин и вывесить там объявление с просьбой к жертвам мошенника обратиться к следователю, ведущему дело. Автор уверен, что значительная часть обманутых клиентов все-таки посетит уже давно закрывшийся веб-сайт в надежде, что для них еще не все потеряно.

Следы

Схема всех онлайн-мошенничеств такова:

- размещение (рассылка) информации;
- взаимодействие с жертвой;
- получение денежного перевода.

Все три этапа предусматривают оставление обильных следов технического характера. Хотя мошенники, очевидно, постараются предпринять меры для своей анонимизации. Относительно получения денег мошенников кроме анонимизации спасает быстрота: перевод полученных средств между различными платежными системами осуществляется достаточно быстро, но требует много времени для отслеживания.

При размещении мошенниками подложного интернет-магазина можно рассчитывать на обнаружение следующих видов следов:

- регистрационные данные на доменное имя; логи от взаимодействия с регистратором доменных имен; следы от проведения платежа этому регистратору;
- следы при настройке DNS-сервера, поддерживающего домен мошенников;
- следы от взаимодействия с хостинг-провайдером, у которого размещен веб-сайт: заказ, оплата, настройка, залив контента;
- следы от рекламирования веб-сайта: взаимодействие с рекламными площадками, системами баннерообмена, рассылка спама;
- следы от отслеживания активности пользователей на сайте.

При взаимодействии с жертвами обмана мошенники оставляют такие следы:

- следы при приеме заказов — по электронной почте, по ICQ, через веб-форму;
- следы от переписки с потенциальными жертвами.

При получении денег мошенники оставляют такие следы:

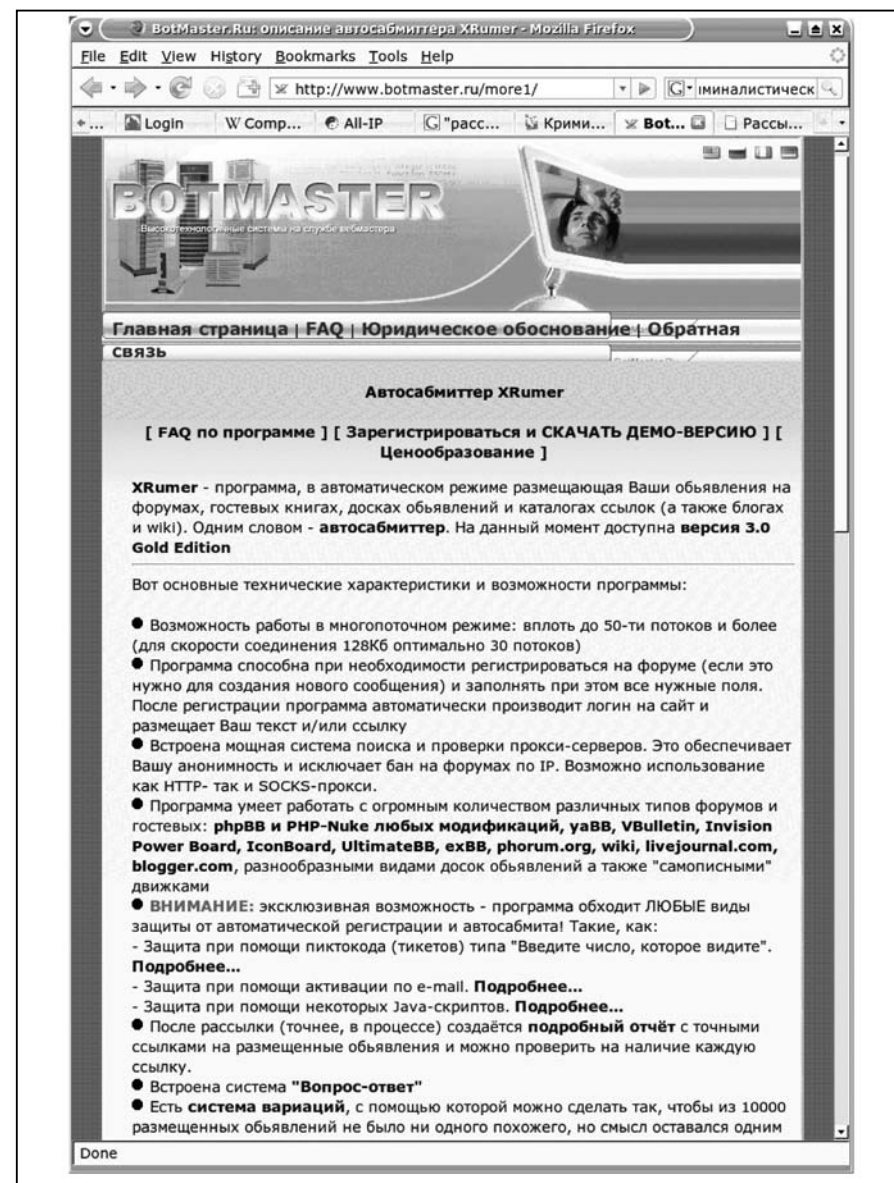
- следы при осуществлении ввода денег в платежную систему (реквизиты, которые указываются жертве);
- следы при переводе денег между счетами, которые контролируются мошенниками;
- следы при выводе денег;
- следы от дистанционного управления мошенниками своими счетами, их открытия и закрытия;
- следы от взаимодействия мошенников с посредниками по отмыванию и обналичиванию денег.

Клевета, оскорбления и экстремистские действия в Сети

Способ

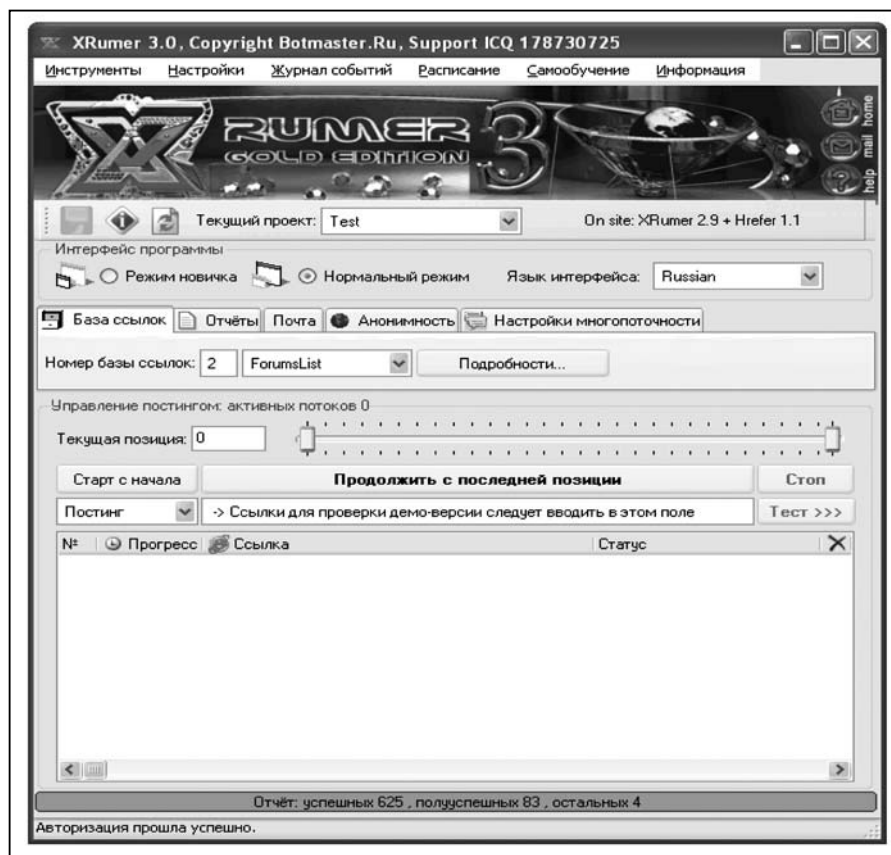
Преступление заключается в размещении на общедоступном, как правило, популярном ресурсе в Интернете оскорбительных, клеветнических или экстремистских материалов.

Ресурсы могут быть следующими: веб-форумы и доски объявлений, веб-страницы*, сообщения в телеконференциях* (newsgroups), массовая



Веб-сайт, предлагающий программу для самостоятельной массовой рассылки (постинга) сообщений по веб-форумам и электронным доскам объявлений

рассылка (спам*) по электронной почте, ICQ, SMS и другим системам обмена сообщениями. Иные средства применяются редко.



Скриншот вышеуказанной программы

В некоторых случаях злоумышленник ограничивается одним-двумя ресурсами. Скорее всего, это непрофессионал, который не может или не хочет оценить охваченную аудиторию. Мало какой ресурс охватывает сразу много пользователей. В других случаях информация размещается на многих ресурсах одновременно, и ее размещение периодически повторяется, как того велит теория рекламы.

Однократное размещение информации злоумышленник может осуществить собственными силами. Для массового размещения ему придется либо привлечь профессионалов-спамеров*, либо найти, подготовить и задействовать соответствующее программное средство для массовой рассылки или спам-постинга.

Предметом посягательства являются честь, достоинство личности, деловая репутация, национальные и религиозные чувства. В некоторых

случаях целью такой кампании может быть провоцирование ложного обвинения другого лица в клевете, оскорблениях, экстремизме; но такое встречается редко.

Преступник

Все эти преступления неспроста объединены в одну главу. У них общий не только способ, но и мотивы. Унижение чести и достоинства физического лица, нанесение ущерба деловой репутации юридического лица, оскорбление национальных и религиозных чувств групп людей — все это, как правило, делается не из корыстных, а из личных побуждений. Дело в том, что сама такая идея — оскорбить, оклеветать, опорочить, поглумиться над национальностью в Сети — может прийти в голову лишь сгоряча, человеку, который не привык строить трезвый расчет.

Разумеется, возможны случаи, когда клевета в Интернете — это часть более крупной пиар-кампании, проводимой с определенными корыстными целями. Но такие случаи редки. В России они еще реже.

Когда есть выбор, какую версию предпочесть, «личную», «деловую» или «политическую», лучше начинать с личной. Опыт автора говорит, что большинство правонарушений в Интернете (не только оскорбления, но и DoS-атаки) сейчас диктуются личными мотивами. Корыстные соображения встречаются реже. Деловых людей в Сети пока мало и деловых интересов — тоже. Зато личные обиды и амбиции льются через край.

Понятно из этого, что злоумышленника надо начинать искать среди личных недоброжелателей потерпевшего.

Квалификация типичного преступника для обсуждаемого вида правонарушений находится в четко очерченных рамках.

С одной стороны, он достаточно плотно общается в Интернете, чтобы придавать значение его воздействию на иных людей. Человек, знакомый с глобальной компьютерной сетью лишь поверхностно, вряд ли придаст большое значение тому, что написано на каком-то там веб-сайте. Его круг общения и его референтная группа¹ находятся вне Сети. Его субъективная оценка значимости и достоверности информации из Сети — низкая. К тому же он понимает, что ему будет сложно совершить указанные действия в малознакомой среде.

С другой стороны, уровень знаний о сетевых технологиях такого злоумышленника не может быть высоким, поскольку тогда он осознал бы, как много следов оставляет каждое действие и сколько есть способов его обнаружить. Новички, попав в Интернет, как правило, опасаются «большого брата» и побаиваются за свою приватность. Пользователь средней

¹ Референтная группа — реальная или условная социальная общность, с которой индивид соотносит себя как с эталоном и на нормы, мнения, ценности и оценки которой он ориентируется в своем поведении и в самооценке.

квалификации уверен, что в Интернете можно легко достичь анонимности, если только принять соответствующие меры. А сетевой профессионал знает, что никакие меры анонимности не обеспечивают.

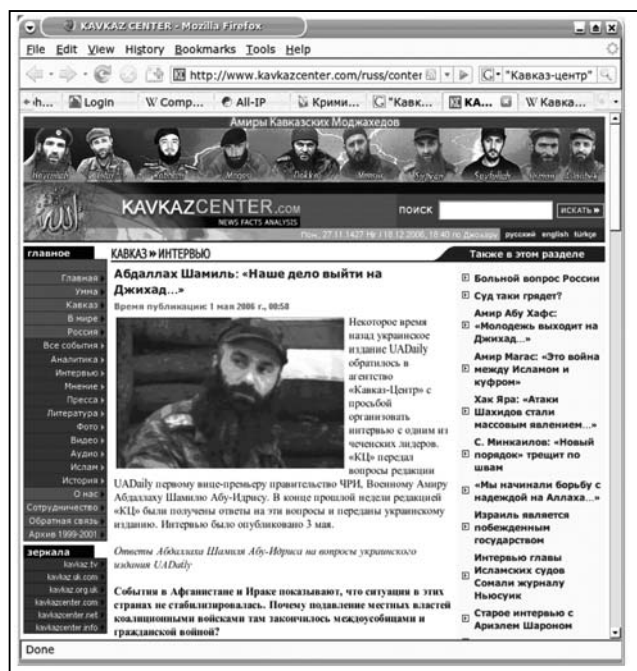
То есть вероятный преступник довольно много времени проводит в Интернете, но знает о нем не слишком много.

Такое движущее чувство, как обида, обычно развивается постепенно. И если уж подозреваемому пришло в голову разместить клевету или оскорбления именно в Интернете, логично предположить, что там же, в Интернете, его светлое чувство обиды росло и развивалось. Имеет смысл разыскать на веб-сайтах и в переписке предшествующие споры, претензии, негативную информацию, в ответ на которую подозреваемый затеял свою кампанию.

Обстановка

Несколько слов об экстремизме. Признать тот или иной материал экстремистским (равно как возбуждающим межнациональную рознь или, скажем, порнографическим) можно, лишь проведя экспертизу. А до той поры распространение материала защищено правом на свободу слова.

Автору лишь пару раз пришлось видеть в Интернете истинно экстремистский материал, то есть по которому было позже вынесено заключение эксперта. Несравненно чаще приходилось сталкиваться с «экстремизмом» со стороны операторов связи, сотрудники которых отключали клиентов и



Экстремистский веб-сайт, который давно не могут закрыть российские власти. В настоящее время размещен в Швеции, у провайдера «prq Inet»

закрывали сайты, опираясь исключительно на собственные представления о политике и религии. Подлинная цитата из Правил оказания услуг одного крупного российского хостинг-провайдера: «запрещается размещение информации, пропагандирующей фашизм и коммунизм». Точка.

Был даже случай в практике автора, когда за отключение якобы экстремистского сайта (оценка его содержания произведена исключительно техническими сотрудниками провайдера) было возбуждено уголовное дело против отключившего сайт по статье 144 УК (воспрепятствование законной профессиональной деятельности журналистов), поскольку «экстремистский» веб-сайт был зарегистрирован как СМИ.

Следы

Если размещение информации преступник проводил лично и вручную, следы зависят от способа размещения. Они описаны в разделах 2 и 4.

При размещении информации лично, но с использованием автоматизации будут также следы от поиска, настройки и пробных запусков соответствующей программы. Существуют общедоступные бесплатные и платные программы для рассылки спама по электронной почте, по телеконференциям, для массового постинга в веб-форумы и доски объявлений.

При заказе размещения (рассылки) у специализирующихся на этом профессионалов, то есть спамеров*, искать следы размещения на компьютере подозреваемого бессмысленно. Лучше искать следы его контактов со спамерами: объявления спамеров, переписка с ними, телефонные переговоры, следы подготовки размещаемого текста, перевода денег. Найденные спамеры, если их склонить к сотрудничеству, дадут изобличающие показания, и никаких технических следов размещения информации искать уже не понадобится.

Кроме того, злоумышленник наверняка будет сам просматривать размещенные им тексты как с целью контроля, так и ради отслеживания реакции других. В случае личных некорыстных мотивов он должен испытывать удовлетворение при просмотре своих сообщений. При просмотре образуются соответствующие следы.

DoS-атаки

Способ

DoS-атака* или атака типа «отказ в обслуживании» является одним из видов неправомерного доступа, а именно такого, который приводит к блокированию информации и нарушению работы ЭВМ и их сети. Иные виды неправомерного доступа (копирование информации, уничтожение информации), а также использование вредоносных программ могут быть этапами осуществления DoS-атаки.

Такие атаки принято разделять на два типа [19]: атаки, использующие какие-либо уязвимости в атакуемой системе и атаки, не использующие уязвимостей. Во втором случае своеобразным «поражающим фактором» атаки является перегрузка ресурсов атакуемой системы — процессора, ОЗУ, диска, пропускной способности канала.

Преступник

В настоящее время встречаются DoS-атаки как с личными, так и с корыстными мотивами. Еще 2-3 года назад личные мотивы превалировали [19]. Но сейчас наблюдается четкая тенденция возрастания числа DoS-атак с корыстными мотивами — в целях вымогательства или недобросовестной конкуренции.

Организовать DoS-атаку на типичный веб-сайт не представляет из себя сложной задачи, она под силу ИТ-специалисту средней квалификации, имеющему в своем распоряжении среднее же оборудование и средней ширины канал связи. Соответственно, на черном рынке DoS-атака на обычный веб-сайт стоит десятки долларов за сутки. На более крупный или более защищенный объект — первые сотни долларов за сутки. Возможны оптовые скидки. Заказать атаку может себе позволить даже один обиженный индивидум. Инструмент для осуществления распределенных DoS-атак — зомби-сети* (ботнеты) — также имеются в продаже на черном рынке по сравнительно низкой цене, порядка десятков долларов за тысячу зомби-хостов. И цена эта в последнее время снижается.

С другой стороны, в Сети появляется все больше и больше чисто информационного бизнеса, благополучие которого целиком и полностью зависит от доступности его сайта или другого сетевого ресурса. Это онлайн-магазины, онлайн-аукционы, онлайн-казино, букмекерские конторы и некоторые другие виды предприятий. Остановка работы веб-сайта в таких условиях означает полную остановку бизнеса. Несколько недель простоя могут полностью разорить предприятие. Естественно, при таких условиях находятся желающие пошантажировать владельца и получить с него выкуп за прекращение DoS-атаки. Несколько лет назад подобных предприятий (е-бизнеса) с существенными доходами еще не было. Соответственно, не было и DoS-вымогательства.

Итак, можно выделить два типа преступлений, связанных с DoS-атаками, — с целью доставить неприятности владельцу или пользователям атакуемого ресурса и с целью получить выкуп.

В первом случае, как и при клевете и оскорблениях, следует искать «обиженного». При этом непосредственным исполнителем может быть как он сам, так и нанятый профессионал.

Во втором случае мы имеем дело с хладнокровным криминальным расчетом, и преступление мало чем отличается от офлайн-вымога-

тельства или недобросовестной конкуренции. Тип возможного преступника «е-бизнесмен» описан выше, в главе «Личность вероятного преступника».

Обстановка

Один тип DoS-атаки основан на использовании уязвимостей в программном обеспечении атакуемого ресурса. Другой тип — так называемый флуд* — не использует никаких уязвимостей и рассчитан на простое исчерпание ресурсов жертвы (полоса канала, оперативная память, быстродействие процессора, место на диске и т.п.). Как легко понять, ко флуду нет неуязвимых, поскольку любые компьютерные ресурсы конечны. Тем не менее разные сайты подвержены флуду в разной степени. Например, CGI-скрипт, работающий на веб-сайте, может быть написан неоптимально и требовать для своей работы слишком много оперативной памяти. Пока такой CGI-скрипт вызывается раз в минуту, эта неоптимальность совершенно незаметна. Но стоит злоумышленнику произвести вызов CGI-скрипта хотя бы сто раз в секунду (никаких особых затрат со стороны злоумышленника для этого не требуется, всего 300 пакетов в секун-

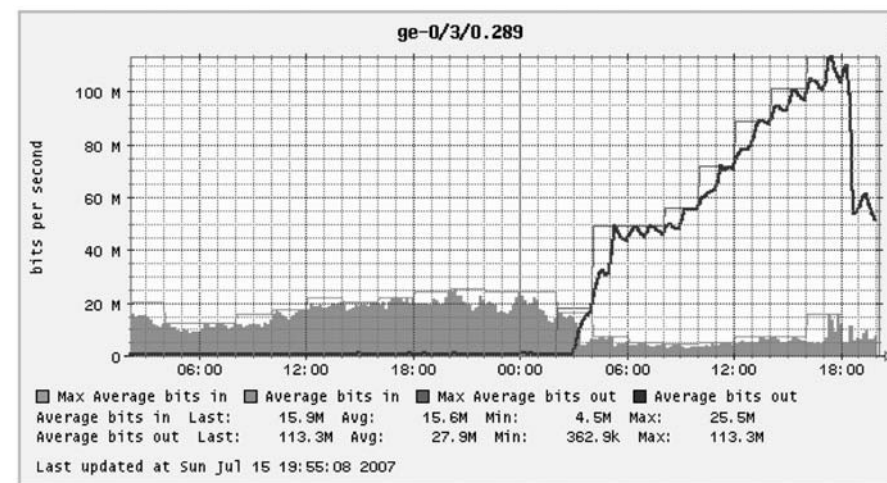


График загрузки канала при DoS-атаке.

Распределенная атака на сайт «Библиотека Мошкова» 15.07.07. Атака представляла собой массу HTTP-запросов, сгенерированных зомби-компьютерами. До 3:00 мы видим характерный веб-трафик: исходящий превышает входящий на порядок. С началом атаки входящий трафик постепенно (не все зомби входят в атаку одновременно) возрос с 1 Мбит/с до 100 и более. Исходящий же трафик, напротив, упал, поскольку сервер не справляется с нагрузкой. Около 18:00 трафик атаки стал снижаться вследствие принятых мер — фильтрации известных адресов зомби-сети

ду, порядка 5 Мбит/с) — и неоптимальность CGI-скрипта приводит к полному параличу веб-сайта.

То есть запас по производительности и есть первичная защита от DoS-атаки.

Обычные хостинг-провайдеры* держат на одном сервере по несколько десятков клиентских веб-сайтов. По экономическим причинам большого запаса производительности они сделать не могут. Отсюда следует, что типичный веб-сайт, размещенный у хостинг-провайдера, уязвим даже к самому простейшему флуду.

Потерпевший

Потерпевшим в подавляющем большинстве случаев выступает юридическое лицо.

Коммерческие организации редко бывают заинтересованы в официальном расследовании, поскольку для них главное — устранить опасность и минимизировать убытки. В наказании злоумышленника они не видят для себя никакой выгоды. А участие в судебном процессе в роли потерпевшего часто негативно отражается на деловой репутации.

Выступить потерпевшим организация-владелец атакуемого ресурса может в следующих случаях:

- когда есть уверенность, что не наказанный злоумышленник будет повторять атаки;
- когда предприятию надо отчитываться за понесенные убытки или перемены в оказании услуг перед партнерами, клиентами, акционерами;
- когда руководитель предприятия усматривает в атаке личные мотивы, личную обиду, когда уязвлено его самолюбие.

В прочих случаях не приходится рассчитывать на заинтересованность потерпевшего в раскрытии преступления.

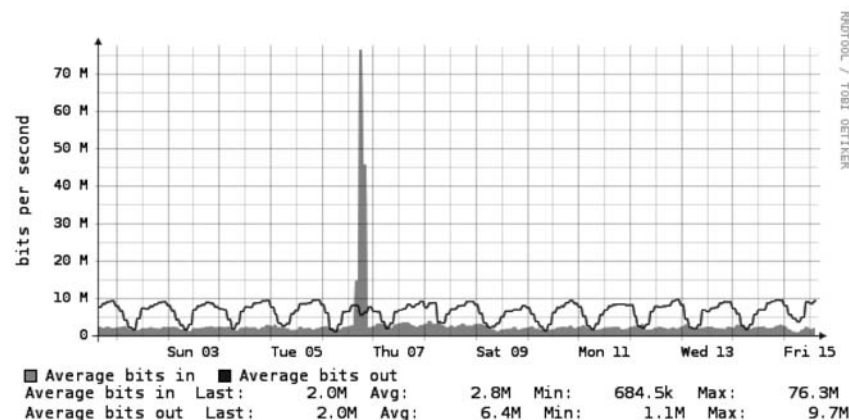
Следует помнить, что многие DoS-атаки воздействуют сразу на целый сегмент Сети, на канал, на маршрутизатор, за которым могут располагаться много потребителей услуг связи, даже если непосредственной целью атаки является лишь один из них. Для целей расследования необходимо установить, на кого именно был направлен умысел преступника. Формальным же потерпевшим может выступить любой из пострадавших от атаки.

Вместо формального потерпевшего мы здесь опишем особенности личности специалиста, который обслуживает атакованную информационную систему и отвечает за ее защиту. Понимание его личности поможет понять причины и механизм совершения преступления.

Типичный профессиональный системный администратор — человек, в реальном мире ничего из себя не представляющий (даже далеко не всегда высокооплачиваемый), но в мире виртуальном — царь и бог. Подобное

двойное положение сильно способствует развитию комплексов неполноценности и стремлению компенсировать в виртуальности свою ничтожность в реальном мире. Поскольку речь идет о молодом человеке, значительную часть времени вынужденном проводить за компьютером (иначе профессионализм не приобрести), данный комплекс часто усугубляется половой неудовлетворенностью. Теперь представьте, что может натворить такой системный администратор с болезненным желанием продемонстрировать свою власть. При условии, что руководитель компании в технических вопросах вовсе не разбирается или не интересуется ими.

Автор вспоминает случай из своей практики, когда DoS-атака на веб-сайт была заказана одним из посетителей веб-форума на нем. Неосторожное слово, ответная грубость, перепалка — в результате администратор форума закрыл доступ пользователю, которого он считал виновным, и в дальнейшем удалял все его аккаунты. Обиженный решил отомстить. Причем руководствовался, по-видимому, женской логикой, потому что мстить решил не обидевшему его человеку, а веб-сайту. Как выяснилось в ходе расследования, он заказал DoS-атаку на этот сайт. Атака была мощной, а сайт, сервер и сеть в целом не были рассчитаны на большие перегрузки, работали вблизи предела своей производительности. В результате атаки «упал» не только целевой веб-сайт, но и несколько десятков веб-сайтов, живших на том же сервере. А также потеряли работоспособность соседние сервера, использовавшие тот же канал связи. Пострадавшими были: магистральный



Пример исходящей DoS-атаки типа флуд на фоне типичного веб-трафика с дневной периодичностью. В период атаки (серый пик 6 числа) виден провал в профиле входящего трафика (черная линия) — он образуется за счет перегруженности канала

провайдер, у которого оказался целиком забит флудом* канал связи, оператор дата-центра, несколько хостинг-провайдеров, чьи сервера соседствовали с целевым, а также все их клиенты — всего более сотни лиц.

Описанную DoS-атаку было бы значительно легче предотвратить, чем отразить или преодолеть ее вредные последствия. Стоило администратору веб-форума быть немного сдержаннее или хотя бы задуматься о последствиях, и атаки удалось бы избежать.

Можно сказать, что для потерпевшего от DoS-атаки (точнее, сотрудников юрилица-потерпевшего) характерно провоцирующее поведение в онлайн-взаимоотношениях.

Следы

При подготовке и проведении DoS-атаки образуются следующие следы технического характера:

- наличие инструментария атаки — программных средств (агентов), установленных на компьютере злоумышленника или, чаще, на чужих используемых для этой цели компьютерах, а также средств для управления агентами;
- следы поиска, тестирования, приобретения инструментария;
- логи (преимущественно статистика трафика) операторов связи, через сети которых проходила атака;
- логи технических средств защиты — детекторов атак и аномалий трафика, систем обнаружения вторжений, межсетевых экранов, специализированных антифлудовых фильтров;
- логи, образцы трафика и другие данные, специально полученные техническими специалистами операторов связи в ходе расследования инцидента, выработки контрмер, отражения атаки. (Следует знать, что DoS-атака требует немедленной реакции, если владелец желает спасти свой ресурс или хотя бы соседние ресурсы от атаки. В ходе такой борьбы обе стороны могут применять различные маневры и контрманевры, из-за чего картина атаки усложняется.);
- следы от изучения подозреваемым (он же заказчик атаки) рекламы исполнителей DoS-атак, его переписки, переговоров и денежных расчетов с исполнителями;
- следы от контрольных обращений подозреваемого к атакуемому ресурсу в период атаки, чтобы убедиться в ее действенности.

При профессиональном осуществлении атаки используются зомби-сети* или иной специализированный инструментарий. Естественно, он не одноразовый. Исполнители не заинтересованы в простаивании своих мощностей и могут осуществлять несколько атак одновременно, либо осуществлять теми же программными агентами параллельно с атакой другие функции, например, рассылку спама*.

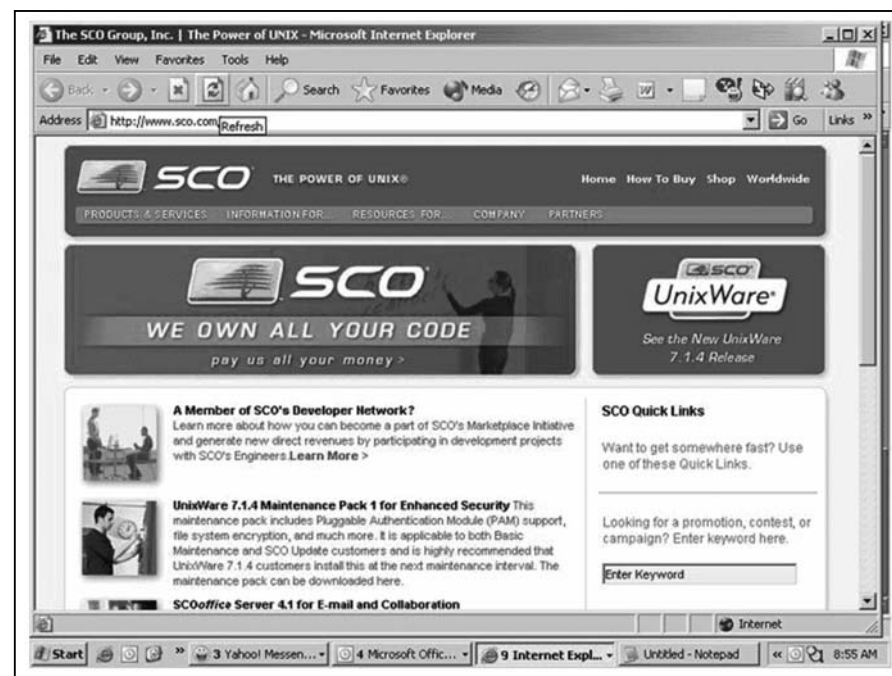
Дефейс

Способ

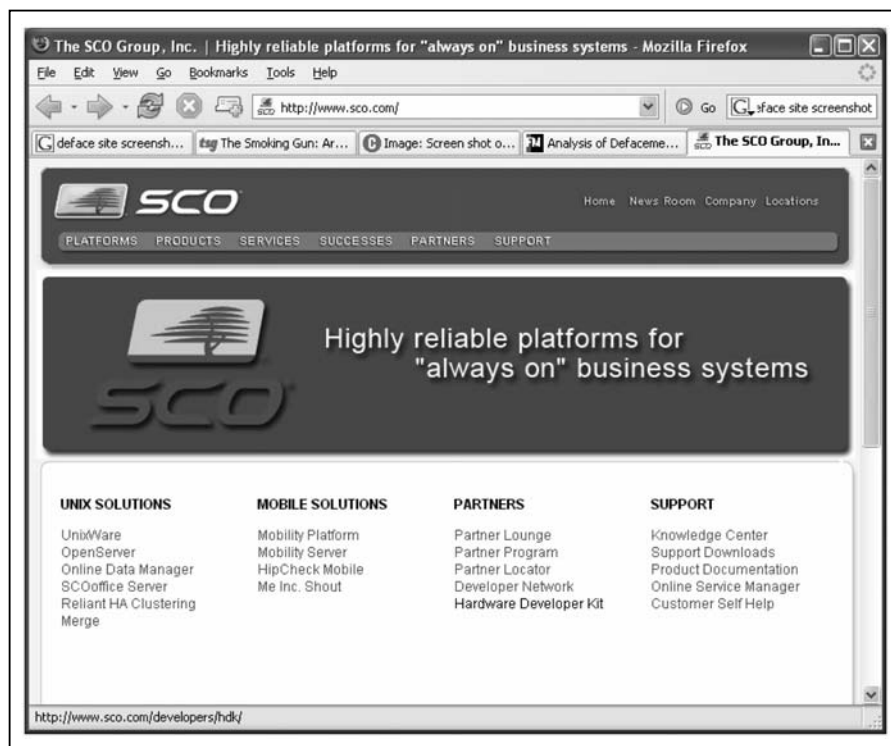
Данное правонарушение состоит в том, что злоумышленник тем или иным способом изменяет внешний вид публичного веб-сайта потерпевшего, чаще всего его титульную страницу. Технически это можно осуществить, получив доступ на запись к директории, где хранятся данные веб-сервера. Также часто дефейс производят, воспользовавшись уязвимостью в самом веб-сервере или одном из его CGI-скриптов. Бывает, что злоумышленник изменяет веб-страницу, воспользовавшись штатной функцией, под аккаунтом одного из законных пользователей.

Следует отличать дефейс от подмены веб-сайта при помощи атаки на DNS или изменения DNS-записи для сайта жертвы. Это иной способ, хотя цель атаки может быть такой же, как при дефейсе.

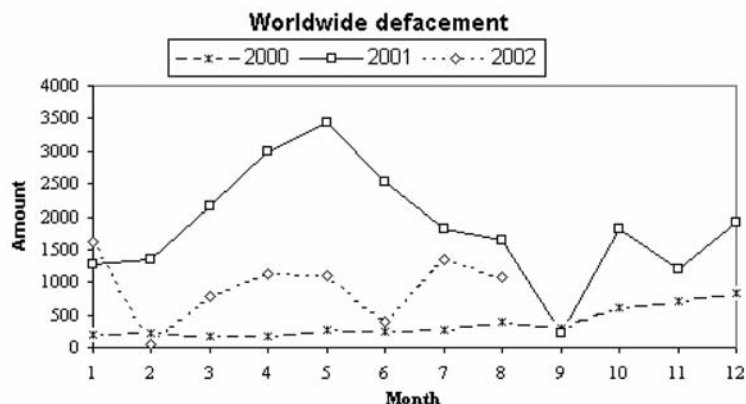
Явление это достаточно распространенное. Фиксируются тысячи подобных инцидентов ежемесячно. Можно предположить, что не все дефейсы попадают в статистику, поскольку для владельца взломанного веб-сайта выгодно скрыть такой инцидент.



Дефейс веб-сайта «SCO» 29.11.2004. Сделан, скорее всего, по идеологическим мотивам. Измененная титульная страница прожила около трех часов. О новости сообщили все СМИ, интересующиеся компьютерно-сетевой тематикой



Для сравнения — обычный вид веб-сайта «SCO». Как видно, в данном случае злоумышленник лишь частично изменил внешний вид титульной страницы сайта. В большинстве случаев при дефейсе внешний вид страницы изменяется кардинально



Количество зафиксированных дефейсов в 2000-2002 годах по месяцам.
Источник — [65] со ссылкой на www.zone-h.org

Преступник

Мотивы для дефейса бывают следующие (перечислены в порядке убывания частоты):

- стремление продемонстрировать публично свою квалификацию;
- политические, религиозные, иные идеологические мотивы;
- личная неприязнь, личный конфликт с потерпевшим или кем-либо из его работников;
- стремление дискредитировать владельца веб-сайта, испортить ему деловую репутацию в целях конкурентной борьбы, повлиять на его капитализацию в целях биржевой спекуляции;
- стремление продемонстрировать наличие уязвимости в ПО, привлечь к ней внимание.

Вероятный преступник соответствует модели «хакер» или реже — «инсайдер».

Следы

На взломанном компьютере следов остается не много, злоумышленник старается по возможности уничтожить их. Не следует удивляться, если следов там вообще найти не удастся. Больше следов можно найти на компьютерах, которые хакер использует в качестве промежуточных узлов для исследования атакуемого веб-сайта и доступа к нему. Также пригодятся статистические данные транзитных провайдеров (см. главу «Статистика трафика» в разделе 2). А на собственном компьютере злоумышленника следов должно быть еще больше — там должны найтись переработанная или заново изготовленная веб-страница, а также ее промежуточные варианты, средства для осуществления несанкционированного доступа, средства для поиска и эксплуатации уязвимостей на целевом веб-сайте и промежуточных узлах.

Помимо этого, злоумышленнику еще необходимо привлечь общественное внимание к дефейсу. В противном случае акция может остаться незамеченной — измененные сайты недолго остаются в таком состоянии, владелец обычно быстро восстанавливает первоначальный вид.

Следовательно, злоумышленник сразу после «взлома» или незадолго до него каким-либо способом оповестит мир о своем преступлении. Это могут быть сообщения по электронной почте, статья в телеконференции или на веб-форуме. Все эти действия оставят дополнительные следы.

Злоумышленник также будет периодически проверять результат дефейса и отслеживать реакцию общественности на него. Эти действия он может совершать со своего компьютера, без особых мер для анонимизации.

Потерпевший

Чаще потерпевшим является юридическое лицо. Обычно предприятие-потерпевший не заинтересовано в разглашении информации об инциденте. Но если широкая огласка уже произошла, позиция потерпевшего может измениться, поскольку необходимо чем-то компенсировать ущерб деловой репутации и как-то оправдаться перед акционерами и клиентами. Быстро найти и привлечь к ответственности злоумышленника — это все-таки некоторая компенсация в плане репутации и общественных связей.

К данному преступлению относится все, сказанное о потерпевших в предыдущей главе ("DoS-атаки").

Вредоносные программы

Способ

Антивирусные аналитики отмечают явную тенденцию к коммерциализации вредоносного ПО. Еще 5-7 лет назад почти все вирусы и черви создавались без явной корыстной цели, как полагают, из хулиганских побуждений или из честолюбия.

А среди современных вредоносных программ большинство составляют программы, заточенные под извлечение выгоды. Основные их разновидности (с точки зрения предназначения) суть следующие:

- троянские программы для создания зомби-сетей*, которые затем используются для рассылки спама, DoS-атак, организации фишеровских сайтов и т.п.; нередко они снабжены механизмом самораспространения;
- так называемое spyware*, то есть черви и троянцы для похищения персональных данных — паролей и ключей к платежным системам, реквизитов банковских карточек и других данных, которые можно использовать для мошенничества или хищения;
- так называемое adware*, то есть вредоносные программы, скрытно внедряющиеся на персональный компьютер и показывающие пользователю несанкционированную рекламу (иногда к классу adware причисляют не только вредоносные, но и «законопослушные» программы, которые показывают рекламу с ведома пользователя);
- руткиты*, служащие для повышения привилегий пользователя и сокрытия его действий на «взломанном» компьютере;
- логические бомбы*, которые предназначены для автоматического уничтожения всей чувствительной информации на компьютере в заданное время или при выполнении (при невыполнении) определенных условий;
- так называемое «ransomware» — подвид троянских программ, которые после скрытного внедрения на компьютер жертвы шифруют файлы,

содержащие пользовательскую информацию, после чего предъявляют требование об уплате выкупа за возможность восстановления файлов пользователя.

Следует отметить, что так называемые кряки* — программы, предназначенные для обхода технических средств защиты авторского права, — не относятся ко вредоносным. Как по букве закона, так и по техническим особенностям создания и применения, они стоят особняком. Создание кряков имеет смысл рассматривать отдельно (см. главу «Нарушение авторских прав в офлайне»).

Преступник

Как современная вредоносная программа является лишь средством, технологическим элементом для криминального бизнеса, так и современный вирусописатель работает не сам по себе, а исполняет заказы других. Это может быть прямой заказ, когда программист-вирмейкер* получает техническое задание, исполняет его и отдает готовый продукт заказчику. Это может быть не прямой заказ, когда вирмейкер*, зная потребности черного рынка, старается их удовлетворить своим продуктом, который затем и реализует (лицензирует пользователям) самостоятельно.

Давно не отмечалось случаев, когда один человек исполнял весь преступный замысел целиком — писал вредоносную программу, применял ее, использовал результат применения для извлечения дохода.

Таким образом, создатель вредоносной программы — это почти всегда член преступной группы. Его деятельность не имеет смысла в отрыве от заказчиков и пользователей вредоносной программы.

Кроме создания вредоносных программ уголовно наказуемо и их применение. Лицо, использующее такую программу, тоже в большинстве случаев не реализует результаты своего труда непосредственно, а продает или передает их дальше, другим членам преступной группы.

Наконец, третий тип — это реализаторы результатов применения вредоносных программ, то есть спамеры*, вымогатели, кардеры*, мошенники.

Приведем примеры типичных криминальных «коллективов».

Спамеры. Первый сообщник создает и совершенствует программное обеспечение для скрытного внедрения на компьютеры пользователей (троянцы*). Второй, купив у первого право на использование указанной программы, рассылает ее в массовом порядке, принимает сигналы и учитывает успешно внедрившиеся экземпляры троянцев, объединяет их в структурированную зомби-сеть*. Готовую сеть (целиком или частично, насовсем или на время) он продает третьему сообщнику, который с ее помощью осуществляет рассылку спама. Заказы на рассылку принимает четвертый сообщник, который ищет заказчиков при помощи того же спама, часть полученных от заказчиков денег перечисляет третьему в оплату

его услуг. Пятый занимается сбором и верификацией адресов электронной почты для рассылок. Собранные базы адресов (или подписку на такие базы) он продает либо четвертому, либо третьему сообщнику.

Кардеры. Первый из сообщников (точнее, первая группа, одного человека тут не хватит) занимается сбором атрибутов банковских карт*. Он может служить продавцом или официантом и незаметно снимать данные с карточек клиентов. Он может быть менеджером в фирме или банке и получать доступ к базе данных карточек в силу служебного положения. Он может получать номера карточек, внедряя вредоносные программы-шпионы (spyware) или через фишинг*. Добыв некоторое количество номеров (или даже дампов*) банковских карт, первый сообщник сбывает их второму. Второй исполняет роль организатора криминального бизнеса. Он аккумулирует у себя данные и распределяет их исполнителям. Третий сообщник исполняет по заказам второго верификацию реквизитов карт, то есть проверяет их действительность и пригодность для платежей. Четвертый сообщник создает и поддерживает платный веб-сайт или лжемагазин или интернет-казино* с возможностью оплаты услуг карточками. Он имеет несколько договоров с биллинговыми компаниями, время от времени меняет их, а также свою вывеску. Это механизм для отмыwania денег. Пятая группа сообщников — так называемые набивщики. Они получают от второго партии номеров банковских карт по несколько десятков и вводят их через отмывочное предприятие четвертого сообщника под видом разных клиентов. При этом они должны при помощи технических средств эмулировать доступ из разных стран и с разных компьютеров. За свою работу они получают сдельную оплату, реже — процент с доходов. Шестой сообщник представляет собой иной канал реализации, он занимается так называемым вещевым кардингом. Получая от второго «отборные», наиболее перспективные номера кредиток, он использует их для покупок в настоящих интернет-магазинах. Покупается в основном дорогая, нетяжелая и ликвидная техника — мобильные телефоны, видеокамеры, компьютерные комплектующие, некоторые автозапчасти и т.п. Естественно, заказываются они вовсе не на его адрес. Для получения заказов существует седьмая группа сообщников — дропы. Это граждане из благополучных стран, поскольку большинство интернет-магазинов не доставляют заказы вне США, Канады и ЕС, а если и доставляют, то проверяют таких покупателей очень тщательно. Работа дропов состоит в том, чтобы подтвердить по телефону сотруднику магазина, что заказ сделал он, получить посылку и тут же переслать ее шестому сообщнику (иногда — другому дропу, для пушного запутывания следов). Дропы вербуются десятками из малообеспеченных слоев общества типа студентов или негров. Обычно дроп выполняет всего десяток-другой операций с интервалом в несколько недель. Он получает оплату сдельно или в виде процента от

стоимости товара. Наконец, восьмой сообщник занимается получением и реализацией посылок от дропов.

Фишеры. Первый сообщник занимается размещением подложных веб-сайтов банков и иных учреждений. В состав программ такого сайта входит система для моментальной отсылки введенных клиентом конфиденциальных данных злоумышленнику, естественно, не напрямую, чтобы трудно было его вычислить. Второй изготавливает эти сайты, составляет подложные письма и рассылает их, но не самостоятельно, а пользуясь для этого услугами спамеров*. Третий сообщник занимается реализацией полученных данных (номера карт с пин-кодами или пароли к платежным системам) кардерам или иным криминальным структурам. Бывает, что реализацией пин-кодов преступная группа занимается самостоятельно. Тогда предусмотрен четвертый сообщник, который изготавливает «пластик», то есть копии банковских карт для офлайновых магазинов и банкоматов, а также пятая группа, которая собственно снимает из банкоматов деньги, получая для этого карты и пин-коды у четвертого.

Видно, что вредоносное ПО во всех случаях играет роль инструмента для одного из этапов большого преступного замысла. И создатель, и применитель вредоносных программ также исполняют общий замысел.

Отмечались и иные способы использования добытых при помощи вредоносных программ конфиденциальных данных. Например, в конце 2006 года был зарегистрирован случай массовой кражи атрибутов доступа программы ICQ, которая осуществлена при помощи вредоносной программы, массово разосланной пользователям. «Красивые» номера ICQ через посредников поступили в продажу. А из остальных злоумышленники попытались выжать деньги оригинальным способом. Они под видом прежних владельцев ICQ-аккаунтов обращались к их знакомым (используя контакт-лист, украденный вместе с паролем или скачанный с сайта) и просили денег «взаймы». Есть сведения, что некоторый процент пользователей ICQ откликнулся на такую просьбу.

Итак, вероятный преступник по делам о создании и использовании вредоносных программ — это член преступной группы, работающий в этой группе на основе найма или за процент от дохода или как самостоятельный создатель орудий преступления. То есть с точки зрения экономики вирусописатель продает в одних случаях свою рабочую силу, в других — свой труд, а в третьих — результат своего индивидуального труда.

Как правило, это профессиональный программист, вставший на преступный путь уже после выбора профессии. Его движущим мотивом являются деньги. Мотивы, характерные для типа «хакер», то есть самоутверждение и исследовательский интерес, могут иметь значение лишь на первом этапе, при вовлечении его в преступную деятельность. Корыстный же мотив — всегда основной.

Звонилки (dialers)

Одним из видов мошенничества является недобросовестное использование платных телефонных линий. Абонировав соответствующий номер с высокой оплатой за «разговор» со стороны вызывающего абонента, мошенники всяческими способами пытаются спровоцировать вызовы на него со стороны абонентов. Помещают этот номер в заведомо ложной рекламе, отправляют SMS и совершают исходящие вызовы с этого номера, чтобы абонент перезвонил, сами совершают звонки на свой номер, пользуясь несовершенством биллинга оператора, навязывают ложную информацию о вызовах телефонной сети, а также вставляют (загружают) этот номер во вредоносные программы-звонилки (dialer), которые заставляют модем пользователя совершать вызов.

По условиям договора оператор вызывающего абонента платит за такой звонок оператору вызываемого абонента, а потом пытается получить деньги со своего абонента.

Опишем более подробно один из самых распространенных типов такого мошенничества — с использованием вредоносной программы-звонилки (dialer, диалер, программа дозвона).

Большинство звонилок относятся к классу троянских программ. Одни из них имеют обычный для троянцев механизм скрытного внедрения на компьютер или маскируются под полезные программы. Другие таких механизмов не имеют и рассчитаны на однократный запуск самим пользователем, который введен в заблуждение методами социальной инженерии. Например, на веб-сайте, содержащем многочисленные ссылки на порнографию, некоторые ссылки ведут на такую программу с пояснением «запустите для просмотра видео». Обманутый пользователь кликает на гиперссылку, тем самым скачивая программу-звонилку, и запускает ее. Будучи запущенной, она скрытно внедряется на компьютер пользователя (возможно, при этом даже показывает ему видео) и впоследствии активизируется, набирая при помощи модема платный номер¹. Злоумышленники получают через оператора деньги за совершенный звонок, а потерпевшему потом предоставляется разбираться со своим оператором связи, доказывая, что он не звонил в Лихтенштейн и не получал услугу «для взрослых».

Следует заметить, что среди подобных программ-диалеров есть и невредоносные, которые не скрывают своего присутствия и своего предназначения и показывают пользователю, какой звонок и по какому тарифу будет произведен. Они также иногда используются для обмана потребителей, но не вызывают столько проблем у абонентов и не влекут обвинения в мошенничестве и в использовании вредоносных программ.

¹ При соединении с таким номером пользователь часто даже получает интернет-соединение и, думая, что соединился со своим провайдером, не замечает подмены и остается на связи долгое время.

Итак, большинство программ-звонилок являются вредоносными, поскольку внедряются на компьютер и производят свои действия без уведомления пользователя и разрешения от него. Многие потерпевшие настаивают на возбуждении уголовного дела по факту заражения такой программой, поскольку считают, что это позволит им не оплачивать стоимость звонка оператору связи.

Но на сегодняшний день суды не признают вредоносные программы стихийной силой, а их действия — форс-мажорными обстоятельствами. Поэтому заразившимся такими программами пользователям все же приходится оплачивать звонки. Впрочем, иногда оператор связи склонен «прощать» такую задолженность абонента — не по закону, а по справедливости.

Одни из программ-звонилок имеют собственный механизм распространения, чаще всего рассылают себя по электронной почте по списку адресов, найденных на зараженном компьютере. Другие самостоятельно распространяться не умеют, и злоумышленник вынужден размещать их на веб-сайтах, маскировать под что-то безобидное и рекламировать свой сайт.

Количество заражений подобными программами медленно снижается, поскольку все меньше компьютеров используют модем, все больше — выделенные линии связи.

Следы

При изготовлении вредоносных программ можно обнаружить следующие цифровые следы:

- исходный текст вредоносной программы, его промежуточные варианты, исходные тексты других вредоносных или двойного назначения программ, из которых вирмейкер заимствовал фрагменты кода;
 - антивирусное ПО различных производителей, на котором создатель вредоносной программы обязательно тестирует свою, а также средства для дизассемблирования и отладки;
 - программные средства для управления вредоносными программами (многие из них работают по схеме «клиент-сервер», одна из частей внедряется на компьютер жертвы, а другая часть работает под непосредственным управлением злоумышленника);
 - средства и следы тестирования работы вредоносных программ под различными вариантами ОС;
 - следы контактирования с заказчиками или пользователями вредоносной программы, передачи им экземпляров и документации, оплаты.
- При распространении и применении вредоносных программ можно обнаружить следующие цифровые следы:
- средства и следы тестирования работы вредоносной программы под различными вариантами ОС;

- контакты с создателем или распространителем-посредником вредоносной программы;
- программные средства для управления вредоносной программой, данные о внедрениях этой программы к жертвам, результаты деятельности (пароли, отчеты о готовности, похищенные персональные данные);
- средства распространения вредоносной программы или контакты с теми, кто подрядился ее распространять.

Кроме того, на компьютере жертвы должна найтись сама вредоносная программа (ее серверная или клиентская часть). Очень часто обнаруживает ее сам потерпевший при помощи антивирусного ПО. При этом вредоносная программа может быть уничтожена по команде пользователя или автоматически, в соответствии с настройками антивируса. Хотя исполняемый код вредоносной программы, обнаруженный в ходе экспертизы, является доказательством по делу, в случае его уничтожения потерпевшим без этого доказательства можно обойтись. Лог антивируса, а также следы деятельности вредоносной программы, будучи исследованы в ходе экспертизы, позволят эксперту категорично утверждать, что на исследуемом компьютере была установлена определенная вредоносная программа, хотя исполняемого кода этой программы и не обнаружено. Лучше поручить такую экспертизу предприятию, которое производит или обслуживает соответствующее антивирусное ПО.

Кардерство

Способы

Объем мошеннического рынка в области банковских карт* очень велик. Его можно оценить так. В каждом банке установлен лимит приемлемых потерь при карточных операциях. Он колеблется в пределах 0,1–0,5%. Это значит, что не менее 0,1% всего мирового оборота по карточным операциям достается кардерам*.

С банковскими (платежными) картами возможно несколько видов мошенничества. Их всех можно уложить в единую схему:

получение — распределение — реализация

На первом этапе данные о банковских картах получают разнообразными способами. На втором этапе они сортируются, проверяются, классифицируются, возможно, проходят через оптовых посредников (скупка в розницу, продажа оптом, продажа в розницу). На третьем этапе данные банковских карт реализуются, то есть конвертируются в деньги.

Указанная цепочка никогда не исполняется одним человеком. Каждый из этапов связан со своими особыми навыками, опытом в соответствующей области, служебным положением, доступом к технике. Поэтому криминальная цепочка всегда включает не менее трех сообщников.

Получение

Наборы данных банковских карт, которые представляют ценность:

- (1) номер, срок действия, имя владельца, код¹ cvv или cvv2
- (2) дампы* карты
- (3) дампы + пин-код

Третий вариант — самый привлекательный для кардеров. Этот набор данных можно конвертировать в наличные самым быстрым способом и получить при этом максимальную сумму.



Портативные считыватели, используемые мошенниками для скрытого снятия дампа карты в местах оплаты

Способы получения данных банковских карт:

- дистанционный неправомерный доступ к серверу, на котором такие данные хранятся или обрабатываются, например, к серверу магазина или банка — способ, наиболее часто предполагаемый несведущими людьми, но очень редко встречающийся на практике;
- доступ к таким данным с использованием своего служебного положения и недостатков в системе защиты информации предприятия — очень часто владельцы конфиденциальной информации предпринимают излишние меры защиты от внешних угроз, но пренебрегают защитой от угроз внутренних;
- (редко) перехват интернет-трафика, когда данные карты передаются в открытом виде (по протоколу HTTP или по электронной почте);
- получение данных банковских карт, или снятие дампа* при обслуживании клиентов в предприятиях торговли и питания — похож на пре-

¹ Card Verification Value

дыдущий способ, но особенность в том, что информация копируется непосредственно с карты при физическом контакте с ней;

- выманивание данных карт и иногда пин-кодов у владельцев методами фишинга*;
- получение дампов и пин-кодов при помощи фальшивых банкоматов или приставок к банкоматам (скиминг*);
- получение самой карточки мошенническим способом («ливанская петля» и др.);
- обычная кража карты у ее держателя (бывает, что пин-код записан на ней или на листке, лежащем в том же бумажнике).

Реализация

Реализация данных с банковских карт, то есть обращение их в деньги, может производиться следующими способами:

- вещевой кардинг — приобретение в интернет-магазинах или в реальных магазинах (при наличии дампа карты) ликвидных товаров, чаще на продажу, реже на заказ, последующая их реализация;
- совершение фиктивных покупок в интернет-магазинах или приобретение услуг платных сайтов по сговору с их владельцами; при помощи данных чужой карты производится оплата, биллинговое предприятие* (оно не участвует в сговоре) учитывает платеж и переводит магазину за вычетом своей комиссии, магазин переводит обусловленную долю кардеру;
- игра в интернет-казино*; нанятые кардером игроки регистрируют в интернет-казино много аккаунтов* на имя владельцев карт, вносят с карт депозит, играют, а затем для тех аккаунтов, где образовался выигрыш, проводят процедуру вывода средств;
- использование иных интернет-сервисов, где возможно получение денег, например, организующих показ любительского видео;
- (редко) вымогательство у магазина, банка, иного предприятия, несущего ответственность за сохранность данных; за утрату и разглашение данных о картах клиентов предприятие может подвергнуться санкциям со стороны платежной системы, получить большой ущерб деловой репутации, может стать ответчиком по искам клиентов — за избавление от этих неприятностей многие готовы заплатить кардерам-вымогателям;
- обналичивание в банкоматах; когда есть дамп карты и пин-код, то изготавливается твердая копия карты (так называемый «белый пластик», потому что внешнее оформление для банкомата не требуется), с которой в банкоматах снимается максимально возможная сумма за минимально возможное время.

Ниже приводятся немного более подробные пояснения к перечисленным способам приобретения и реализации данных банковских карт.

Скиминг

Наиболее лакомый кусок для кардеров — это полная копия (дамп) магнитной полосы карты вместе с ее пин-кодом. Такие данные позволяют



Приставка к банкомату, замаскированная под конструктивную часть и осуществляющая скрытое копирование магнитной полосы карты

снять со счета весь остаток средств плюс весь кредитный лимит. Обычно это десятки тысяч долларов. Ради подобного куша кардеры готовы на многое. Даже банковские работники, обнаружив, что имеют (или могут



Видеокамера, осуществляющая снятие вводимого клиентами пин-кода, замаскированная под лоток с рекламой [95]

получить) доступ к пин-кодам клиентов, не всегда выдерживают искушение связаться с кардерами и совместно очистить клиентские счета.

В 1980-х и 1990-х была популярна установка фальшивых банкоматов и торговых терминалов. Многие из них даже выдавали клиентам деньги или товары. Ныне такие банкоматы встречаются реже.

Более распространены «приставки» к легальным банкоматам, которые незаметно для клиента считывают данные с магнитной полосы и «подсматривают» вводимый пин-код [95, 96, 97].

О распространенности подобного способа говорит то, что производители банкоматов сейчас предусматривают в картоприемнике механизм для неравномерного протягивания карты. Карта втягивается в банкомат и экстрагируется из банкомата рывками, чтобы затруднить считывание магнитной полосы возможным шпионским устройством. Впрочем, ответные технические меры уже придуманы.



Накладка на клавиатуру банкомата, снимающая вводимый пин-код [97]

Использование интернет-казино

Если бы такие казино легко и быстро выплачивали игрокам выигрыши, они были бы идеальным каналом отмычки денег для кардеров. Но в онлайн-казино легок и прост только ввод денег. А для их вывода (получения выигрыша) надо затратить немало усилий и времени; в результате далеко не факт, что игрок вообще получит свои деньги. Это не следствие жадности онлайн-казино. Это следствие действий кардеров. Если какое-либо казино начнет без формальностей выплачивать выигрыши, оно вскоре обнаружит, что кардеры составляют подавляющее большинство его игроков. От чего такое казино немедленно будет объявлено пособником со всеми вытекающими неприятными последствиями.

Поэтому для выплаты денег казино требует подтверждения личности игрока, а также пользуется только неанонимными системами платежей. От игрока, пожелавшего получить выплату, скорее всего, потребуют прислать скан-копию паспорта и какого-либо документа, подтверждающего место жительства, например, квитанции об оплате коммунальных услуг. Возможно, от игрока захотят получить номер телефона ради дополнительного подтверждения его личности. Выплата производится на именной банковской счет (при этом не всякий банк будет признан благонадежным) или при помощи именного чека, который отправляется по почте. В общем, онлайн-казино выработали ряд процедур, затрудняющих кардерам жизнь.

Те в ответ придумали контрмеры. Немало умельцев предлагают услуги по изготовлению скан-копий паспортов и иных документов за разумную цену (\$20-40), телефонные номера в «благонадежных» странах с переводом входящих звонков на любой номер в любой стране, банковские счета, принимающие платежи, адресованные произвольным физическим лицам, и другие подобные услуги.

Также наблюдается разделение труда в области работы с самими интернет-казино. Регистрацию аккаунтов* игроков обычно поручают отдельным людям. На черном рынке кардерских товаров и услуг продаются и покупаются такие аккаунты, как пустые, так и уже «отыгранные», то есть готовые для вывода денег.

Фиктивные покупки

Типичный интернет-магазин или платный веб-сайт для получения платежей от своих клиентов использует услуги так называемого билингового предприятия — финансового учреждения, которое принимает данные банковских карт, совершает транзакции и переводит полученные деньги (за вычетом своей комиссии) на банковский счет интернет-магазина. У билинговой фирмы имеется собственная служба безопасности, препятствующая проведению мошеннических операций. Именно поэтому банки отка-

2000Charge - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
https://secure.2000charge.com/secure/eu/ Go
Secure Order Form - 128bit Encrypt... PrimeCups - Exclusive Videos of Girl... 2000Charge
PrimeCups.Com - €39,95 Per 1 Month
Sie erwerben hiermit einen Zugang für die Dauer von 30 Tage zum Preis von € 39,95.
Diese Mitgliedschaft wird nach Ablauf zum 30 Tage
Zugang zum Preis von €39,95 und erneuert sich automatisch alle 30 Tage.
Sie koennen die Mitgliedschaft jederzeit kündigen.
2000Charge ist ein autorisiertes Abrechnungsinstitut für "PrimeCups.Com"
1. Adresse:
Ihre Daten werden streng vertraulich behandelt und sind SSL verschlüsselt.
Wählen Sie ihr Land: Deutschland
Vorname:
Nachname:
Strasse:
PLZ und Stadt:
Land und Bundesland: Deutschland (Bitte hier auswählen)
Telefonnummer:
(Ihre Telefonnummer wird ertl. zur Kaufverifikation verwendet.)
E-Mail:
Wir werden Ihre Zahlung per E-Mail bestätigen.
2. Bankangaben:
Banktyp: (Bitte auswählen)
Bankleitzahl:
Kontonummer:
3. Geben Sie bitte hier das gewünschte Passwort ein:
(Buchstaben/Zahlenkombination, min. 4/ max. 10 Zeichen)
Bitte achten Sie auf Gross- und Kleinschreibung!
Transferring data from www.classic.ben.ru... secure.2000charge.com

Веб-страница билинговой фирмы, на которую пользователь переадресуется со страницы платного веб-сайта для оплаты услуг при помощи банковской карты. На верху страницы мы видим наименование предприятия, в чью пользу берется платеж, и сумму

зываются работать с мелкими онлайн-магазинами напрямую и предпочитают взаимодействовать именно с билинговыми предприятиями-посредниками. Билинговое предприятие отказывает в обслуживании тем онлайн-магазинам, у которых процент отозванных транзакций (chargeback) превышает некоторый уровень, обычно 1%. Может отказать в обслуживании и по иной причине, если сочтет интернет-магазин подозрительным.

Веб-сайт типичного онлайн-магазина даже не имеет интерфейса для ввода платежных реквизитов. Посетитель веб-сайта вводит их прямо на веб-странице билинговой фирмы, естественно, пользуясь защищенным (HTTPS) соединением.

Один из способов реализации данных банковских карт состоит в сговоре между кардером и владельцем онлайн-магазина. Часто такие магазины или платные веб-сайты устраиваются специально ради приема платежей по чужим картам. Сообщники вместе пытаются обмануть билинговое предприятие, сделать так, чтобы возвратов было не больше установленного количества.

Для ввода реквизитов карт в интерфейс билинговой системы обычно нанимаются отдельные люди, набивщики. Это «чернорабочие» кардерского мира. Тем не менее от них требуется владеть определенными навыками. Набивщик должен использовать для каждой новой карты новый прокси-сервер или сокс-сервер, желательно, расположенный в той стране, в которой живет держатель карты. Он должен побеспокоиться, чтобы его компьютер соответствовал типичной конфигурации компьютера клиента.

При взаимодействии с веб-интерфейсом билинговой системы браузер пользователя сообщает следующие данные:



Система оплаты услуг без банковских карт — следствие массового кардерства

- марка и версия браузера;
- язык браузера;
- версия ОС;
- разрешение экрана;
- воспринимаемые типы данных;
- воспринимаемые языки;
- воспринимаемые кодировки данных;
- referer, то есть адрес веб-страницы, с которой пользователь перешел на данную веб-страницу;
- некоторые другие настройки.

Понятно, что если во время такого взаимодействия передаются реквизиты банковской карты Джона Смита из США, а язык браузера выставлен украинский, то система заподозрит неладное. Также возникнет подозрение, если с одного и того же IP-адреса будут введены карточные реквизиты двух разных людей из разных стран.

Поэтому набивщики получают необходимые инструкции и, если надо, ПО для своей работы.

Именно из-за нашествия кардеров стали появляться альтернативные системы оплаты услуг в Интернете. Некоторые платные веб-сайты уже не принимают банковских карт. Оплата производится через телефонный звонок по платной линии или иным подобным способом. У таких способов больше накладные расходы, но это дешевле, чем постоянно решать проблемы, создаваемые из-за кардинга.

Реальный пластик

На кардерском жаргоне «реальным пластиком» именуются полноценные твердые копии банковских карт. На них должен присутствовать цветной рисунок, голограмма, иметься эмбоссированное (выдавленное) имя держателя и магнитная полоса с нужными данными.

Для этого способа реализации требуется дамп* карты. Пин-код не нужен. По дампу изготавливается твердая копия карты. Она должна не только нести верные данные на магнитной полосе, но и выглядеть соответственно. Рисунок карты, конечно, не обязан совпадать с оригинальным, но он должен присутствовать и быть хорошего качества: не смазываться, не отслаиваться. Желательно, чтобы название банка и карты соответствовало коду (первые 6 цифр номера карты); впрочем, продавцы редко обращают на это внимание.

К такой поддельной карте реализатору желательно иметь поддельный документ. Продавец или кассир не обязан спрашивать у покупателя удостоверение личности, но может это сделать, если возникнут подозрения. А они, скорее всего, возникнут, поскольку кардер с «реальным пластиком» пойдет покупать не корзину продуктов в супермаркете, а что-нибудь по-

дороже, что можно будет перепродать хотя бы за 40-50% стоимости. Совершить много покупок по поддельной карте не удастся, одна, две, может быть, три — и держатель карты спохватится и заблокирует ее.

Бывает, что фальшивый документ изготавливают на имя держателя карты. Это надежнее, но дороже. Ведь поддельная карта может быть использована не более 2-3 раз. После этого она в лучшем случае будет заблокирована, а в худшем — попадет в стоп-лист. Соответственно, и поддельный документ нужно будет выбросить вместе с картой. Другой вариант — «постоянный» документ, вместе с которым можно использовать несколько разных карт. В соответствии с именем в документе наносится (эмбоссируется) имя на карте. То есть имя на карте будет соответствовать документу, но не будет соответствовать имени на магнитной полосе. В этом случае затраты ниже, но выше риск, поскольку продавец может сравнить имя на чеке и имя на карте.

Образец же подписи на поддельной карте можно нарисовать такой, какой удобно.

Пластиковые заготовки для банковских карт, оборудование для нанесения изображений, эмбоссирования и записи магнитной полосы имеется в свободной продаже. Но приобретать его целесообразно, только если собираешься изготавливать карты сотнями. Единичные экземпляры выгоднее заказывать на стороне. Полное изготовление банковской карты на черном рынке обойдется в 100-200 долларов.

Белый пластик

Карта, имеющая только записанную магнитную полосу, именуется у кардеров «белым пластиком». Ее изготовление обходится совсем недорого. Однако область использования ограничена лишь банкоматами. Разумеется, необходимо знать пин-код.

Набор дампы карты + пин-код стоит на черном рынке дорого, зато с его помощью можно выжать карточный счет досуха, сняв в банкомате весь остаток и весь кредитный лимит.



Заготовки
для банковских карт

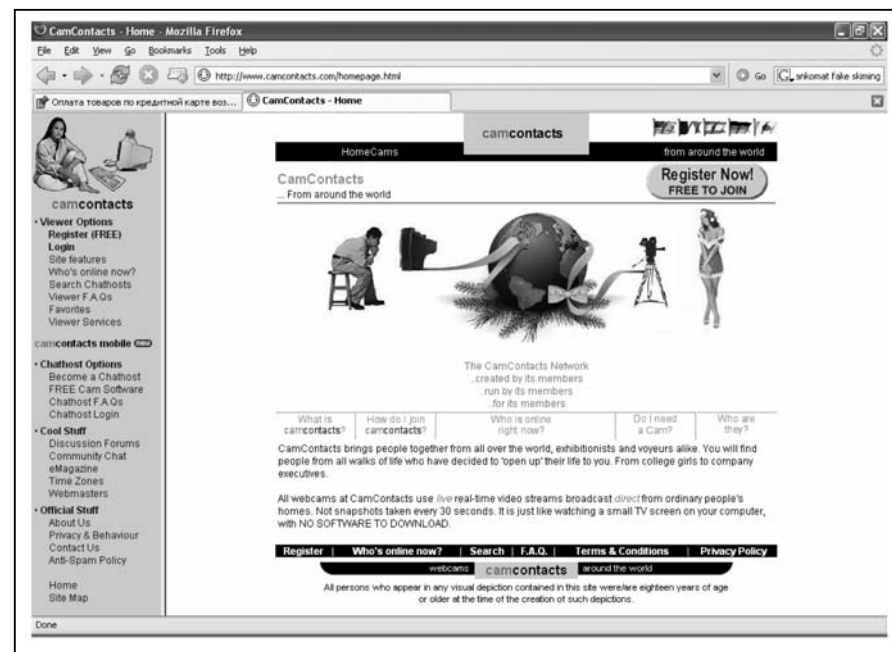
Многие банки ставят ограничения для банкоматных транзакций — по географии, по максимальной сумме за раз и по максимальной сумме за день. Это несколько усложняет кардерам жизнь. Карту могут успеть заблокировать и занести в стоп-лист, пока еще не все деньги с нее сняты.

Кроме реализации в банкоматах возможны варианты покупки товаров по «белому пластику» в магазинах. Естественно, лишь по сговору с продавцом.

Посреднические онлайн-сервисы

Инструментом кардера может стать почти любой интернет-сервис, где предусмотрена выплата денег клиентам.

Некоторое распространение имеют посреднические сервисы по обмену видео. Суть их состоит в том, что одни пользователи желают транслировать видеоизображение через Интернет, а другие желают его потреблять. (Разумеется, как правило, речь идет об эротическом видео, но посредник предпочитает об этом «не знать».) Посредник организует этот процесс, сводит покупателя с продавцом и осуществляет расчет между ними. Себе берет процент за посредничество.



Один из многочисленных сайтов, предлагающих посредничество в продаже онлайн-видео. Такие сайты привлекательны для кардеров в качестве метода обналичивания

Поскольку от покупателей принимаются платежи по банковским картам, а выплаты продавцам производятся чеком или банковским переводом, есть возможность «отмывания». Кардер регистрируется на таком посредническом сайте как покупатель, как продавец и начинает продавать услуги самому себе.

Это также не простой путь. Службы безопасности знают, как притягательны для кардеров подобные сервисы, и всячески стараются воспрепятствовать. Выплаты обставляются различными условиями наподобие интернет-казино. Кардеры, разумеется, находят ответные меры.

Почему мошенничество?

В заключение несколько слов о квалификации кардерских действий.

В УК РФ имеется специальная статья 187, на первый взгляд, специально ориентированная на кардеров: «изготовление или сбыт поддельных кредитных либо расчетных карт и иных платежных документов». Но диспозиция статьи сформулирована без учета сегодняшних технологий кардинга. Юристы расходятся во мнении, что считать «сбытом» банковской (расчетной) карты. Одни юристы [20] утверждают, что сбытом можно считать лишь действия, предполагающие переход карты (как вещи) к иному владельцу. При таком подходе привлечь к уголовной ответственности по этой статье можно только одного члена преступной группы — того, который непосредственно печатает твердые копии карт, да и то лишь в том случае, если расплачивается ими не сам. Другие юристы [W04] полагают, что «сбыт» состоит также в использовании поддельной карты в качестве средства платежа. Но и в том, и в другом случае из этого состава выпадает использование лишь данных банковских карт, без изготовления твердых копий, а ведь эти случаи составляют большинство.

Законодательство здесь сильно отстало от развития технологий. Впрочем, вряд ли стоит его «подтягивать». Платежные системы активно переходят от карт с магнитной полосой к чиповым картам. Для новой технологии и методы мошенничества будут новыми.

Для всех кардерских действий, которые сводятся к получению денег или материальных ценностей, годится статья 159 УК «мошенничество». Те случаи, когда с помощью чужой карты приобретается не имущество, а услуга, можно также квалифицировать как мошенничество в отношении держателя карты, если деньги были списаны. А если не списаны, то подойдет статья 165 УК «причинение имущественного ущерба путем обмана или злоупотребления доверием».

Мошенничество с трафиком

Автоматизированные системы расчетов (биллинговые системы), а также средства сбора данных для таких систем (предбиллинг, mediation) операторов связи всегда являлись объектом интереса мошенников, казнокрадов и прочих криминальных элементов. Изменив данные в биллинговой системе, можно осуществить мошенничество, хищение, растрату на значительную сумму. Сложность таких систем велика, доступ к ним имеют сразу многие лица из персонала и даже клиентов предприятия, поэтому всегда имеется достаточно технических возможностей получить доступ и изменить данные.

Мошенничество с данными биллинга достаточно распространено. Оно распространено настолько, что существуют нормативы списания средств на такие злоупотребления. На рынке есть особые программные продукты для выявления и пресечения подобного рода действий, они именуются «fraud management systems». Само название свидетельствует о том, что речь идет не о предотвращении мошенничества вообще, а лишь о разумном снижении убытков от такого мошенничества.

Расследование подобных преступлений требует специальных знаний в двух областях. Во-первых, в области бизнеса отрасли связи. Порядок пропуска трафика, его техническая организация, взаиморасчеты между операторами, особенности тарифов — все это область специальных знаний. Во-вторых, требуются знания в области ИТ, поскольку все биллинговые системы — это компьютерные информационные системы, и организация несанкционированного доступа к ним является предметом соответствующих специальных знаний.

Автору неизвестны случаи, когда мошенничество с трафиком было совершено «снаружи», то есть без содействия сотрудника пострадавшей компании либо сотрудника иного оператора связи. Теоретически такие случаи возможны, но на практике они, видимо, очень редки.

Есть две типичные схемы подобного мошенничества. В первом случае сотрудник оператора связи вступает в сговор с ее клиентом (или несколькими клиентами) и тем или иным способом изменяет данные об оказанных услугах (объеме, времени, тарифах). Во втором случае «выгодоприобретателем» от мошенничества выступает другой оператор связи, который получает незаконный доход или экономию за счет манипуляций с тарифами, типом трафика и т.п. В этом случае сговор с сотрудником пострадавшего оператора не обязателен, хотя и желателен.

Следует заметить, что деяние, называемое «мошенничеством с трафиком», не всегда является правонарушением. Иногда это всего лишь нарушение условий межоператорского договора. А иной раз — и вовсе правомерная оптимизация затрат при помощи, например, альтернативных путей пропуска трафика.

Нарушение авторских прав в офлайне

Способ

Обсуждаемое преступление соответствует частям 2 и 3 ст. 146 УК. В данной главе речь идет лишь о тех случаях, когда распространение произведения происходит не через сеть, а в офлайне* — путем передачи (продажи) носителя или путем инсталляции с такого носителя.

Распространенностью этого состава в российской криминальной статистике мы обязаны легкости его раскрытия. Торговля на улицах контрафактными дисками и обилие рекламы услуг «черных инсталляторов» позволяет обнаружить и раскрыть такое преступление очень быстро, в любой день, когда возникнет желание.



Объявления «черных инсталляторов»

Преступник

Подозреваемый в большинстве случаев известен, поскольку задерживается на месте после проведения проверочной закупки.

В некоторых случаях преступником является не непосредственный продавец, а директор или товаровед магазина, выставивший в продажу контрафактные экземпляры. Хотя чаще хитрый директор фирмы, прекрасно зная о контрафактности реализуемых программ, делает крайним продавца или инсталлятора.

Потерпевший

Потерпевшим является правообладатель. Большинство правообладателей на популярные продукты — зарубежные. Не все они имеют представительства в России. Не все из них охотно соглашаются выступать потерпевшими.

Российские правообладатели также не всегда соглашаются писать заявление о возбуждении уголовного дела.

По части 2 ст. 146 возбудить дело можно только по заявлению правообладателя. Без такого заявления возбудить дело можно лишь по части 3 этой статьи — при особо крупном размере, более 250 000 рублей.

Для установления принадлежности авторских прав на то или иное произведение часто назначается автороведческая экспертиза. На разрешение эксперту ставится следующий вопрос: кто является вероятным правообладателем для представленного произведения (фонограммы, фильма, программы для ЭВМ)? Или в такой формулировке: какие имеются признаки на экземпляре произведения, указывающие на принадлежность авторских прав на это произведение? Автор полагает, что подобную экспертизу правильнее называть не автороведческой, а компьютерно-технической или программно-технической.

Вывод эксперта об авторе и правообладателе может носить лишь предположительный характер. То, что данное лицо является правообладателем на данное произведение, — это факт юридический, а не технический. Исключительные права на произведение могут быть переданы по договору другому лицу, но произведение от этого не изменится ни на бит. Эксперт лишь ищет на экземпляре произведения какие-либо указания на правообладателя, уведомления об авторских правах, которые принято там ставить. А строго установить правообладателя — это задача следователя. Принадлежность исключительных прав на произведение устанавливается документами — авторским договором, договором об уступке исключительных прав, свидетельством о регистрации прав на продукт и т.д.

В некоторых случаях правообладатели делегируют некоторые свои полномочия ассоциациям, занимающимся защитой интеллектуальной

собственности на коллективной основе. Такая ассоциация может считаться законным представителем потерпевшего. Для этого она должна представить соответствующий договор.

Следы

Из следов технического характера здесь присутствует разве что установленное «черным инсталлятором» программное обеспечение. Соответствующий носитель следует отправить на экспертизу для установления состава установленного ПО и его вероятного правообладателя.

Автор еще раз хотел бы здесь подчеркнуть, что установление контрафактности программного обеспечения (будь оно в виде развертки на жестком диске или в виде дистрибутива на пиратском CD) не может являться предметом программно-технической экспертизы. Равно как и любой другой экспертизы. Контрафактность — это вопрос правоотношений между правообладателем и пользователем: заключен ли авторский договор, уплачены ли деньги, соблюдены ли условия договора (лицензии). Исследование экземпляра самой программы этих обстоятельств установить невозможно. Программно-техническая экспертиза может лишь выявить признаки контрафактности, которые сами по себе ничего не доказывают и могут служить лишь косвенным доказательством. Это обстоятельство подтверждено постановлением Верховного суда [L02]: «Понятие контрафактности экземпляров произведений и (или) фонограмм является юридическим. Поэтому вопрос о контрафактности экземпляров произведений или фонограмм не может ставиться перед экспертом».

Также не может быть предметом КТЭ установление стоимости экземпляров ПО. Стоимость устанавливается товароведческой или экономической экспертизой, либо принимается равной цене этого ПО, если оно продается за одинаковую цену всем потребителям (подробнее об этом — в главе «Стоимость ПО» раздела 5).

Часто для установления стоимости экземпляров ПО или прав на его использование пользуются данными, которые представлены потерпевшим, например, его официальным прайс-листом. Это неправильно. Программное обеспечение, в отличие от иного рода товаров, может продаваться за существенно разную цену. Разница в цене в 3-5 раз на одну и ту же программу для разных классов потребителей является на рынке ПО обычным делом.

К тому же более ранние версии ПО после выхода более свежих версий обычно снимаются с продажи совсем. Стоимость версии, которая на момент совершения преступления не продавалась, не может быть приравнена к стоимости более свежей версии. При обновлении расширяется функциональность ПО, исправляются ошибки, улучшается дизайн и иные потребительские свойства продукта. Поэтому стоимости новой и

старой версии не могут быть равны. Некоторые производители даже готовы передавать пользователям право на использование устаревших версий бесплатно или за символическую цену. Для определения стоимости версии ПО, изъятой из продажи, необходимо назначать экономическую или товароведческую экспертизу. В ней желательно участие не только экономиста, но и специалиста по ИТ или программированию — для учета специфики такого товара, как ПО.

Политизированность

Общественная опасность нарушений авторских и смежных прав ныне оценивается как достаточно высокая. Во всех странах заметна тенденция к ужесточению наказаний за такие нарушения, и следовательно, к повышению оценки их общественной опасности. Не секрет, что указанное ужесточение в большинстве стран проводится под давлением США, на территории которых сосредоточено большинство крупных правообладателей и экономика которых сильно зависит от соответствующих доходов. С макроэкономической точки зрения массовое нарушение авторских прав сводится к перераспределению доходов между более развитыми и менее развитыми странами. И размер этих доходов достаточно велик, чтобы существенно влиять на благополучие экономики в целом. Поэтому вопрос об авторских правах, а также иных правах интеллектуальной собственности — это вопрос политический. Политизированность неизбежно влияет на организацию раскрытия и расследования таких дел.

С одной стороны, это означает, что борьба с нарушениями авторских прав, ее размер, интенсивность и направленность регулируются высшим государственным руководством. Отсутствие такой борьбы отрицательно повлияет на отношение со стороны развитых стран, где расположено большинство правообладателей. Другая крайность — излишне рьяная борьба с нарушениями авторских и смежных прав — может нанести ущерб национальной экономике из-за сильного увеличения платежей иностранным правообладателям или невозможности пользоваться высокотехнологичной продукцией.

С другой стороны, политические партии и общественные деятели не могут не уделять внимания вопросам авторских прав и соответствующим нарушениям. В зависимости от своих позиций они склонны по-разному освещать события, лоббировать решения, использовать уголовные и гражданские дела, связанные с авторскими правами, в пропагандистских целях.

Понятно, что большинству сотрудников правоохранительных органов не нравится роль инструмента в этой политической и идеологической борьбе. Поэтому они предпочитают в делах, связанных с авторскими правами, воздерживаться от проявления инициативы, а лишь исполнять «от сих до сих» полученные сверху указания.

Нарушение авторских прав в Сети

Способ

Неправомерное воспроизведение охраняемых произведений в онлайн-не* осуществляется путем размещения их на общедоступных веб-серверах, FTP-серверах или в файлообменных сетях*.

Хотя заголовок говорит лишь об авторских правах, на самом деле все нижесказанное относится и к иным правам интеллектуальной собственности — смежным правам, патентным правам, правам на товарные знаки и т.п.

«Размещение на общедоступных серверах» — это нестрогое выражение. Конкретное правомочие, которое подозреваемый осуществляет, не имея на то разрешения, сформулировано так: «Сообщать произведение таким образом, при котором любое лицо может иметь доступ к нему в интерактивном режиме из любого места и в любое время по своему выбору (право на доведение до всеобщего сведения)» — абзац одиннадцатый пункта 2 статьи 16 Закона РФ «Об авторском праве...». Это правомочие было специально внесено в закон в 2004 году для учета тех случаев, когда произведение распространяется через веб-сайт или FTP-сайт.

Иногда произведение размещается не в глобальной компьютерной сети, а в локальной. При этом варианте качественных отличий нет, если только круг пользователей локальной сети не ограничивается одной семьей. Все, что превышает этот круг, уже не может считаться «для личного пользования». Большую популярность имеют так называемые домовые сети, охватывающие подъезд, жилой дом или пару домов. Там часто встречаются сервера, содержащие большое количество музыки, фильмов и программного обеспечения.

Преступник

Размещением контрафакта в Сети обычно занимаются не из корыстных побуждений. В большинстве случаев правонарушитель действует, либо вообще не задумываясь о противоправности, либо руководствуясь нонконформизмом.

Случаи корыстной мотивации, пожалуй, исчерпываются получением дохода от рекламы, которая размещена на веб-сайте, содержащем популярный, но контрафактный контент (так называемый варез*). Веб-мастер обычно получает доход со своего веб-сайта через размещение на нем рекламы. Доход тем больше, чем выше посещаемость ресурса. Разместить на сайте популярный варез — верный путь быстро поднять посещаемость. Многие так и поступают, либо не задумываясь о нарушении прав, либо надеясь на «авось пронесет».

Потерпевший

Контрафактных произведений в Сети такое количество, что правоохранительные органы не занимаются этими правонарушениями в инициативном порядке. Инициатором всегда выступает потерпевший.

Потерпевшим может быть как сам правообладатель, так и организация по коллективному управлению авторскими и смежными правами или общественная организация-объединение правообладателей. В последнем случае должен быть представлен договор, в котором правообладатель уполномочивает такую организацию представлять свои интересы в случае нарушения авторских прав.

Подобные организации бывают чрезвычайно активны и настойчивы. Но иногда они заинтересованы вовсе не в уголовном преследовании виновного, а всего лишь в прекращении распространения по Интернету защищаемого произведения. После того, как контрафактная программа или иное произведение убрано с сайта, заявитель может потерять к делу всякий интерес и прекратить сотрудничество с правоохранительными органами.

Бывает и другая крайность, когда организация, защищающая авторские права своих членов, предоставляет правоохранительным органам не только информацию об обнаруженном нарушении, но и протокол осмотра и заключение своего эксперта о контрафактности. Понятно, что к доказательствам, которые собраны заинтересованной стороной, надо относиться критически, а заключение эксперта, который находится в служебной или иной зависимости от потерпевшего (представителя потерпевшего), вообще не может быть признано доказательством в силу УПК. Но иногда следователь, чтобы уменьшить себе работу, идет на поводу у представителя потерпевшего и фактически строит дело только на полученных от него документах. Автор неоднократно сталкивался с такой практикой и, конечно же, считает ее недопустимой.

В качестве примера можно привести Некоммерческое партнерство поставщиков программных продуктов (НП ППП) — организацию, созданную российскими правообладателями и ведущую работу по защите их авторских и смежных прав. Такая работа, безусловно, полезна. Но следует помнить, что указанное партнерство фактически является заинтересованным лицом, хотя формально не выступает в качестве потерпевшего или представителя потерпевшего в конкретном уголовном деле. Поэтому эксперты, предоставленные этой организацией, не могут считаться независимыми, если только потерпевший входит в число членов НП ППП. То же относится к разработанной ими методике проведения экспертиз [94] и к регулярно публикуемым каталогам цен на программные продукты — все эти материалы следует рассматривать наравне с материалами, предоставленными потерпевшим, то есть заинтересованной стороной.

Следы

При доведении до всеобщего сведения образуются такие следы технического характера:

- записи в логах веб- или FTP-сервера при записи файлов на сервер (upload);
- записи в логах веб- или FTP-сервера при получении файлов потребителями — свидетельствует об интерактивной доступности файлов иным лицам;
- следы на компьютере, с которого подозреваемый записывал файлы на общедоступный сервер, локальные копии этих файлов;
- архивы и логи сообщений электронной почты и ICQ, в которых подозреваемый сообщал другим пользователям о доступности файлов по определенному сетевому адресу.

Кроме того, подозреваемый может иметь договор с оператором связи, на ресурсе которого производилось размещение произведения.

Фишинг

Способ

Фишинг (phishing) — это выманивание у потерпевших их конфиденциальных данных методами социальной инженерии. Как правило, речь идет о номерах банковских карт, их пин-кодах, паролях к системе управления банковским счетом (онлайн-банкинг) и другой информации, которую можно потом обратить в деньги. Наибольшей популярностью у фишеров пользуются самые распространенные банки и платежные системы: «Citi bank» «eBay» и «PayPal».

Выманивание данных происходит при помощи подложных сообщений электронной почты и/или подложных веб-сайтов. Как правило, пользователя стараются напугать, например, закрытием его счета или приостановкой оказания услуг, если он не выполнит предложенную мошенником процедуру. Часто, если не всегда, ссылаются на якобы произошедшую аварию, утрату аутентификационных данных, иные чрезвычайные обстоятельства, даже на действия мошенников-фишеров.

Хотя вероятность обмануть каждого адресата невелика, но за счет массовой рассылки и охвата огромной аудитории фишерам удается собрать некоторое количество ценных сведений с каждой рассылки. Фишинг стал экономически выгоден лишь после появления дешевых технологий спам-рассылки.

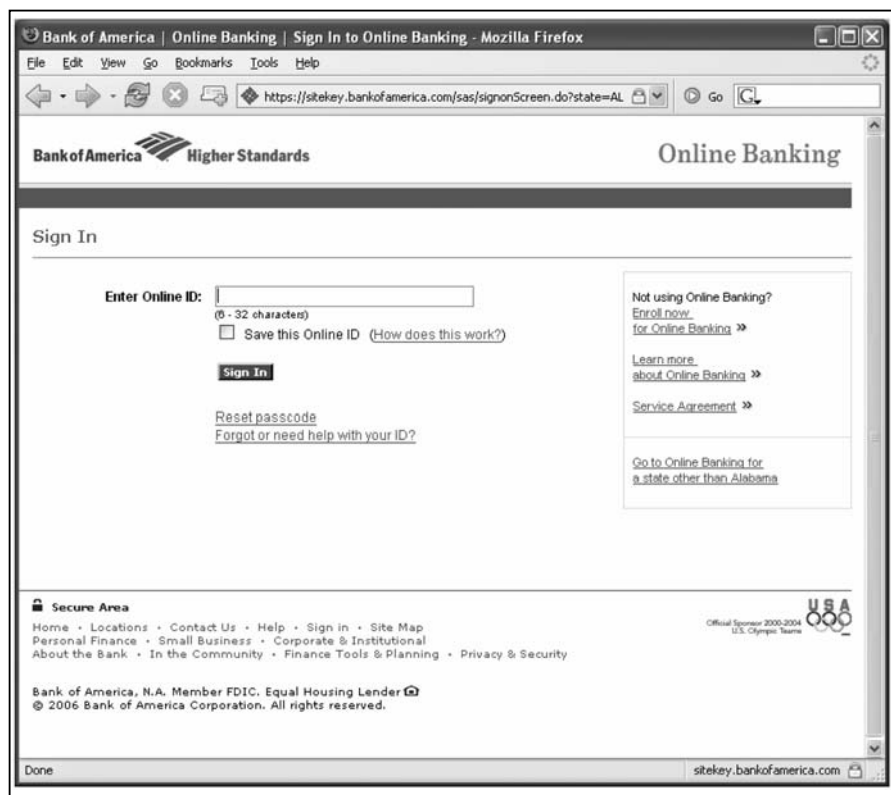
Фишинг после своего возникновения стал необычайно популярен среди мошенников. Исследователи отмечают [73, W05] его высокую доходность, изощренность, глобальность, возможность и выгодность его использования против клиентов самых разнообразных банковских, платежных и даже некоммерческих систем.



Типичное фишинговое письмо о якобы заблокированном аккаунте в системе управления банковским счетом (онлайн-банкинг). Ссылка ведет на подложный сайт, где пользователю будет предложено ввести свои конфиденциальные данные. Ссылка http://sigotama.com/www.bankofamerica.com/BOA/sslencript218bit/online_banking/index.htm лишь слегка похожа на настоящий адрес банка — www.bankofamerica.com



Фишинговый веб-сайт, копирующий страницу авторизации подлинного веб-сайта



Для сравнения — подлинная страница авторизации банка. Обратите внимание на защищенный режим соединения (HTTPS), фишерский же сайт использует протокол HTTP, без шифрования и аутентификации

Логотипы банков и платежных систем, их веб-сайты подделываются с максимально возможной точностью. Чтобы ввести жертву в заблуждение, мошенники различными способами маскируют URL своего сайта, делая его максимально похожим на подлинный URL. Часто для этого регистрируется новый домен для каждой новой рассылки. Подложные ссылки маскируются и иными способами.

Вот еще пример фишингового письма.



Письмо фишера. Видимый текст на самом деле является графическим вложением. С этой картинки поставлена гиперссылка на подложный сайт

Естественно, видимая гиперссылка ведет не на указанный сайт, а на другой, подложный, URL которого виден из исходного текста сообщения.

Исходный код сообщения:

```
...
From: «Fifth Third Bank» <customerservice-num74936499573ver@security.53.com>
To: «Abuse» <abuse@wimax.ru>
X-Virus-Scanned: Norton
User-Agent: MIME-tools 5.503 (Entity 5.501)
X-Mailer: MIME-tools 5.503 (Entity 5.501)
X-Priority: 3 (Normal)
MIME-Version: 1.0
```

```
Content-Type: multipart/related;
  boundary="WO1_WNI98HTQGVW7PI"
Date: Thu, 11 Jan 2007 11:57:32 +0300
X-Original-Message-ID: <auto-000001001154@mail1.wimax.ru>
Subject: [ABUSE]Fifth Third Bank - we need to update your informa-
tion!
  -Thu, 11 Jan 2007 03:57:25 -0500
Status: R
X-Status: NT
X-KMail-EncryptionState:
X-KMail-SignatureState:
X-KMail-MDN-Sent:
```

```
--WO1_WNI98HTQGVW7PI
Content-Type: text/html; charset=us-ascii
Content-Transfer-Encoding: 7bit
```

```
<HTML><HEAD>
<META http-equiv=Content-Type content="text/html; charset=utf-8">
<META content="MSHTML 6.00.2800.1522" name=GENERATOR></HEAD>
<BODY bgcolor="#FFFFFF" text="#A7DF6E">
<a href=http://www.53.com.bankingportal.id1568110.gdotbotns.net/conf>
</a>
</p><p><font color="#FFFFFF">Send an ambulance. boor autobiography
She had taken the time to interlace its stout steel loops with
barbed wire.</font></p><p><font color="#FFFFFF">He had tried stand-
ing on the right leg and had found he could, for short times, but
doing so produced a low, primal agony that lasted for hours. He and
his first wife had honeymooned on Maui. I said I didn't call looking
at things in my own house snooping. You've been working so hard. The
bag won't be zipped. The letter was an exhaustive (and ultimately
exhausting) manual of where Mrs Roman D. You see, I began by loving
only the part of you that makes such wonderful stories, because
that's the only part I had?? the rest of you I didn't know anything
about, and I thought that part might really be quite unpleasant.
colloq</font></p>
</BODY>
</HTML>
```

```
--WO1_WNI98HTQGVW7PI
Content-Type: image/gif; name="cater.gif"
Content-Transfer-Encoding: base64
Content-ID: <JI4UU2RCCX>
```

```
R01GODlhWAJ9AfXJAPv4/9ENDfb2+u/v9dTU1JycnZOTk4+PkfPz8+Pj49fX2cPDw3t7f
GNjY+vr69vb3M/P0MzMzLy8vLe3uKysrKOjo4uLjBQanLOzs4KCgnVldWxsBf1dXVVVVU
xMTENDQzs7OzQ0NCsrKyIi
IhwCHBMTewAAAAAAAAAAAAAAAAAAAA
...
```

Посмотрим на сведения о домене, на котором живет фишерский сайт:

```
$>whois gdotbotns.net
```

Whois Server Version 2.0

Domain names in the .com and .net domains can now be registered with many different competing registrars. Go to <http://www.inter-nic.net> for detailed information.

```
Domain Name: GDOTBOTNS.NET
Registrar: REGISTER.COM, INC.
Whois Server: whois.register.com
Referral URL: http://www.register.com
Name Server: NS1.DOTOB.NET
Name Server: NS1.IGARNS.NET
Name Server: Q1.OXIDIZER-NS.NET
Status: clientDeleteProhibited
Status: clientTransferProhibited
Updated Date: 10-jan-2007
Creation Date: 08-jan-2007
Expiration Date: 08-jan-2008
```

```
>>> Last update of whois database: Thu, 11 Jan 2007 07:48:22 EST <<<
```

```
...
Registration Service Provided By: GotNameDomains.com
Contact: gmgr@gotnamedomains.com
```

Domain name: gdotbotns.net

```
Administrative Contact:
  5920 St
  Marie Domzalski (ra50sso50n@yahoo.com)
  +1.2152881490
  Fax: -
  3546 Belgrade St.
  Philadelphia, PW 19134
  US
```

```
Technical Contact:
  5920 St
  Marie Domzalski (ra50sso50n@yahoo.com)
  +1.2152881490
  Fax: -
  3546 Belgrade St.
  Philadelphia, PW 19134
  US
```

Registrant Contact:

5920 St
 Marie Domzalski (ra50sso50n@yahoo.com)
 +1.2152881490
 Fax: -
 3546 Belgrade St.
 Philadelphia, PW 19134
 US

Status: Locked

Name Servers:
 ns1.dotorb.net
 ns1.igarns.net
 q1.oxidizer-ns.net

Creation date: 08 Jan 2007 21:05:18
 Expiration date: 08 Jan 2008 21:05:18
 ...

Как видно, доменное имя активировано в тот же день, когда производилась рассылка, а зарегистрировано за два дня до того. Надо ли говорить, что указанный в реестре почтовый адрес владельца домена (Белградская улица, город Филадельфия, США) не существует?

Вишинг (vishing) аналогичен фишингу. Только вместо направления жертвы на подложный сайт ее просят позвонить по подложному телефонному номеру, который якобы принадлежит банку или другой доверяемой инстанции. В телефонном разговоре (или при автоматизированном общении с использованием тонального набора) у жертвы выманивают конфиденциальную информацию.

В условиях массового перехода на IP-телефонию несложно получить в пользование анонимный трудно отслеживаемый номер телефона. Имеется также возможность перехватить вызовы на чужой номер, то есть на подлинный номер банка.

Фарминг — разновидность фишинга. Отличие в том, что подлинный ресурс (обычно веб-сайт банка) подменяется на подложный не методами социальной инженерии, а число техническими методами — при помощи атаки на DNS, внедрения пользователю вредоносной программы и т.п.

Выманивание персональных данных можно производить и более изощренным способом. Например, злоумышленник создает развлекательный ресурс. При регистрации на этом ресурсе от пользователя требуется сообщить свой адрес электронной почты, а также выбрать пароль. С некоторой вероятностью пользователь использует тот же пароль, что и для своего почтового аккаунта. Это даст возможность злоумышленнику просматривать электронную почту жертвы, в которой могут попасться конфиденциальные данные.

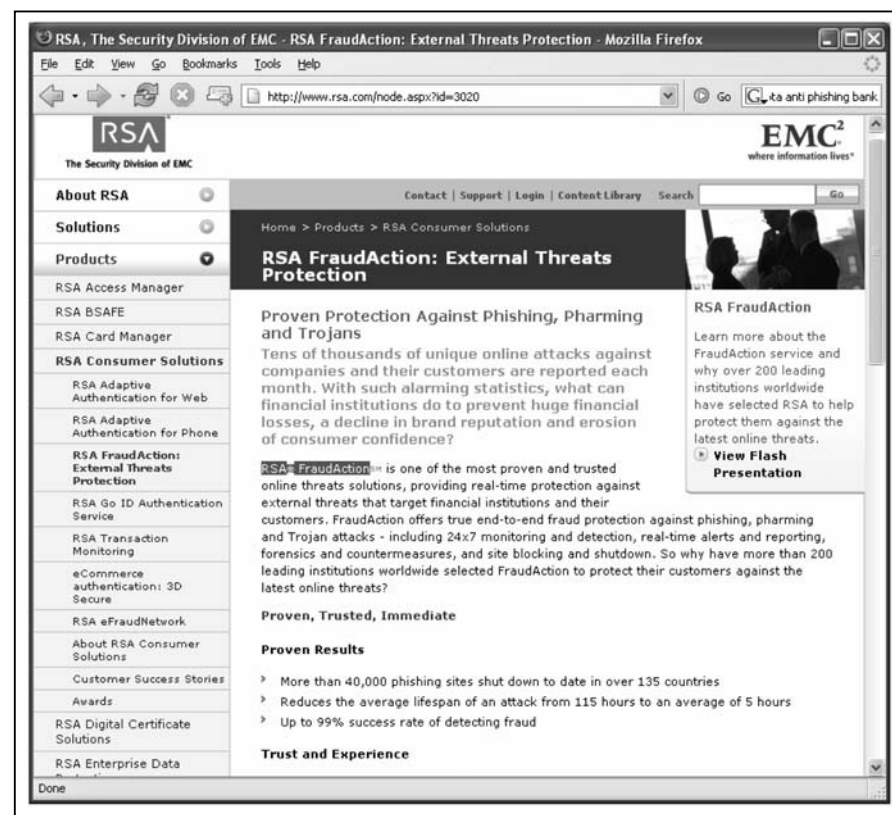
Преступник

Фишинг и реализация его результатов не под силу одному человеку. Этим занимаются преступные группы, состоящие как минимум из двух членов. Первый сообщник или группа сообщников занимается выманиванием конфиденциальных данных, которые передаются или продаются второму сообщнику или группе сообщников для реализации.

Вероятный тип преступника — «е-бизнесмен» (см. главу «Личность вероятного преступника»).

Потерпевший

Сами фишерские уловки рассчитаны на людей неосведомленных, не сведущих в информационных технологиях и невнимательно относящихся к предупреждениям банков, платежных систем и других инстанций. Таковых — большинство.



Одна из онлайн-антифишинговых служб — «RSA FraudAction», бывшая «Cyota»

Установить потерпевших, которые сами не обратились в правоохранительные органы, можно следующими способами:

- проверить обращения в банк или иное предприятие, на клиентов которого было рассчитано мошенничество, — большинство обманутых не считают нужным обращаться в правоохранительные органы или думают, что произошло не мошенничество, а ошибка в расчетах, они вместо этого обращаются в банк;
- если есть доступ к статистике трафика или логам фишерского веб-сайта, можно установить и проверить всех пользователей, обращавшихся к этому сайту (конечно, не все из них стали жертвами мошенничества, но значительная часть);
- при помощи клиентской службы банка или самостоятельно разослать всем клиентам банка уведомления об имевших место попытках мошенничества с просьбой проверить свои счета и с обещанием вернуть украденные деньги.

Банк или платежная система также могут выступать в качестве потерпевшего по делу о фишинге. Могут, но не всегда желают, поскольку такой процесс отрицательно сказывается на деловой репутации. Однако они всегда заинтересованы в предотвращении дальнейших мошеннических действий против своих клиентов. Многие банки и платежные системы сами занимаются отслеживанием деятельности фишеров или поручают это специальным агентствам. Накопленной информацией о деятельности фишеров они с удовольствием поделятся с правоохранительными органами.

Киберсквоттинг

Определение

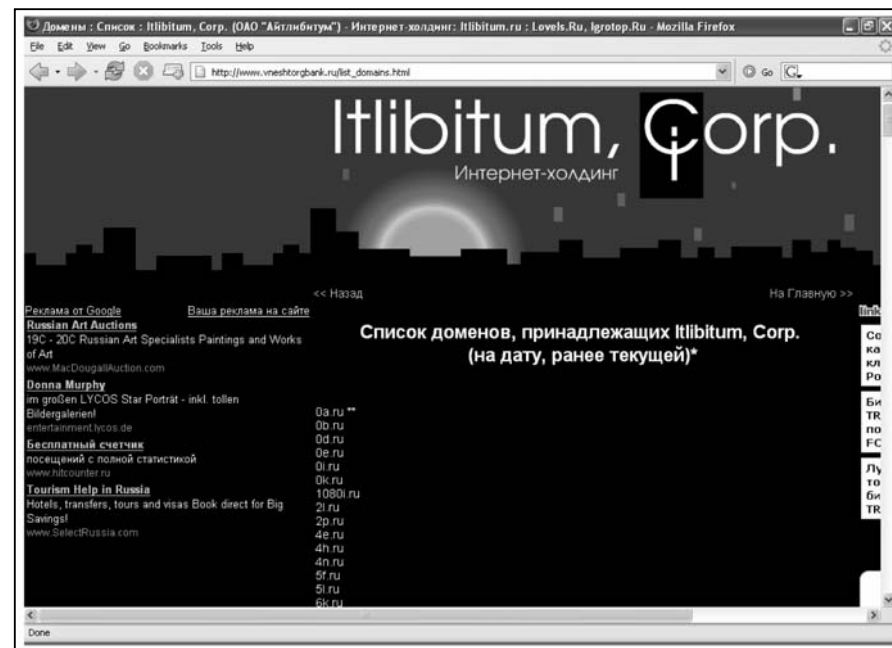
Этим термином именуется приобретение доменного имени с целью его недобросовестного использования либо с целью не допустить его добросовестного использования другим лицом.

Доменное имя в подавляющем большинстве стран является объектом купли-продажи, и стоимость его может существенно возрастать в зависимости от разных факторов.

Сразу после появления доменных имен, в 1980-х, они не имели коммерческой ценности. Но с развитием так называемого «е-бизнеса», во второй половине 1990-х годов, стало ясно, что хорошее доменное имя дает существенную прибавку числа клиентов. Следовательно, доменное имя имеет стоимость, является активом компании, может покупаться и продаваться. По данным компании «comScore Networks», в 2006 году объем розничных продаж через Интернет в США превысил 100 млрд. долларов. В странах Евросоюза в этом же году объем продаж составил около

130 млрд. Оценочная стоимость самых популярных доменных имен достигает десятков миллионов долларов. Зафиксированы реальные сделки с доменными именами на суммы в несколько миллионов.

Естественно, в таких условиях появляются желающие заработать на перепродаже доменных имен — киберсквоттеры.



При запросе веб-сайта www.vneshtorgbank.ru мы попадаем не на сайт банка, а на страницу киберсквоттера, который предлагает к продаже это имя и еще много других имен — всего в списке 490 доменов

Правовая оценка

Далеко не всегда киберсквоттинг криминален. Сам по себе захват доменного имени преступлением не является. Даже когда он производится в целях недобросовестной конкуренции, это нарушение рассматривается в гражданском порядке или по внесудебной процедуре, установленной регистратором.

Уголовное преступление совершается тогда, когда на основе киберсквоттинга происходит вымогательство (ст. 163 УК), мошенничество (ст. 159 УК) или принуждение к совершению сделки (ст. 179 УК). Изредка возможны и некоторые другие виды преступлений — обман потребителей, уклонение от уплаты налогов и т.д.

Большинство случаев киберсквоттинга не попадают в сферу уголовных преступлений. Захват домена с целью продажи или воспрепятствования его использованию может являться нарушением прав на товарный знак или иное средство индивидуализации, актом недобросовестной конкуренции, иным злоупотреблением правом, наносящим ущерб. Во всех подобных случаях заявитель отсылается к гражданскому порядку разрешения споров.



Фрагменты фальшивого сайта Генпрокуратуры *grpf.info*

О вымогательстве можно вести речь лишь тогда, когда киберсквоттер угрожает распространять при помощи захваченного домена сведения, порочащие потерпевшего или причиняющие ему существенный вред, например, распространять негативные сведения от его лица.

Хороший пример такого поведения все желающие могли наблюдать в 2003 году, когда неустановленные лица зарегистрировали доменное имя *grpf.info* и разместили под ним сайт, якобы принадлежащий Генеральной прокуратуре РФ (у прокуратуры тогда своего сайта не было). Среди прочей информации, сведений о руководителях и новостей на лжесайте были размещены отчеты об исполнении политических заказов, расценки на «услуги» прокуроров и другие подобные материалы [W07, W08, W09].

Также можно припомнить историю с предвыборными сайтами кандидата в мэры Москвы — *lugkov.ru* (сайт сторонников) и *lujkov.ru* (сайт противников).

По имеющимся у автора сведениям, подобными публичными скандалами закончилось всего несколько случаев. В большинстве случаев публичный человек или организация, шантажируемые возможностью такого лжесайта, предпочитали не доводить дело до его появления и решать вопрос тем или иным способом.

Другое

Платежи через Интернет

Это, конечно же, не вид преступления. Однако некоторые чисто офлайн-преступления превращаются в компьютерные, если для передачи денег используются платежные системы Интернета, либо договоренность о платеже достигается через Интернет. В той части, которая касается такого платежа, расследование должно использовать методы компьютерной криминалистики. С другой стороны, многие компьютерные преступления включают в способ совершения осуществление платежа через подобные системы.

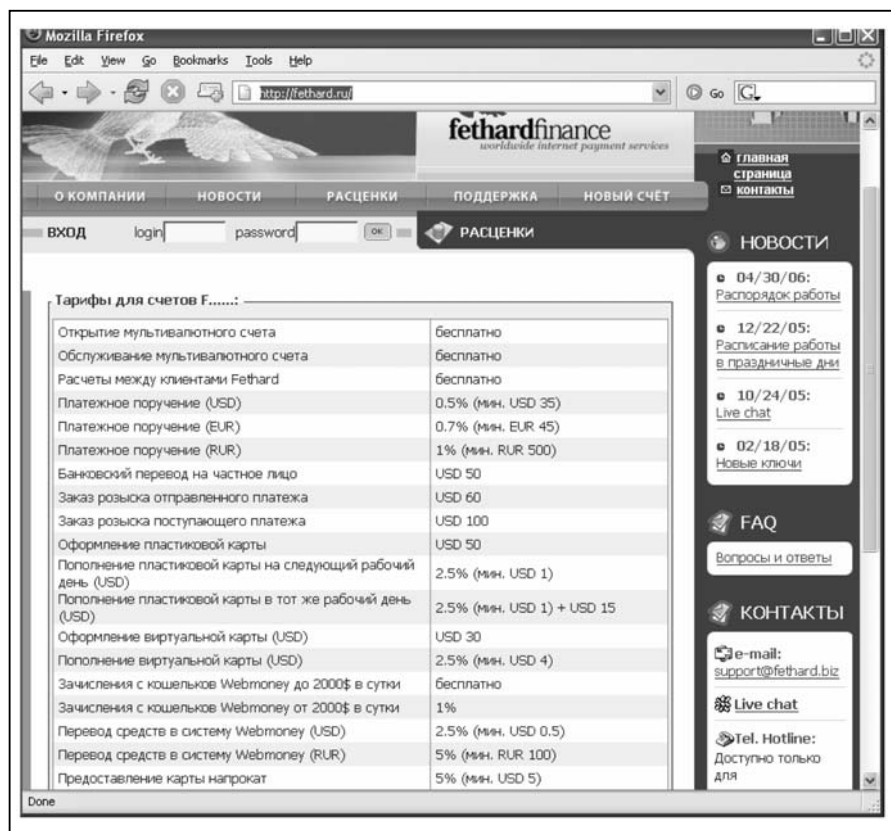
Наряду с банковскими платежными системами и методами платежа, которые подчиняются законодательству той или иной страны и имеют механизмы для расследования проведенных операций, существуют и чисто сетевые платежные системы, которые банками не являются и не столь подвержены контролю со стороны государственных органов. Можно назвать такие системы, как «WebMoney», «PayPal», «E-gold», «Яндекс-Деньги» и другие. Как правило, они связаны между собой различными гейтами и частными посредниками, поэтому можно быстро конвертировать средства из одной системы в другую, затрудняя тем самым отслеживание и блокирование криминальных транзакций. Именно такая квазианонимность и скорость перевода средств привлекают различного рода

злоумышленников к использованию сетевых платежных систем.

Правда, у многих правоохранительных органов есть что называется «оперативные позиции» в таких платежных системах и среди посредников. Иногда их удается задействовать, и тогда транзакции можно не только отследить, но и провести в удобное время удобным для следствия способом, задокументировать или вернуть.

Существуют и вторичные услуги — управление счетами таких платежных систем, ввод и вывод средств из них, в том числе анонимный.

Из-за множественности таких систем, их трансграничности, легкости перевода средств из одной в другую существует реальная возможность остаться анонимным как для плательщика, так и для получателя платежа. Конечно, это не принципиальная анонимность, а трудность отслеживания платежей и переводов.



The screenshot shows the website of Fethard, a provider of internet payment services. The main content is a table titled 'Тарифы для счетов F.....' (Rates for F... accounts). The table lists various services and their associated costs or fees. The website interface includes a navigation menu with links like 'главная страница' (main page), 'контакты' (contacts), 'о компании' (about company), 'новости' (news), 'расценки' (rates), 'поддержка' (support), and 'новый счет' (new account). There is also a login section with fields for 'login' and 'password'.

Тарифы для счетов F.....	
Открытие мультивалютного счета	бесплатно
Обслуживание мультивалютного счета	бесплатно
Расчеты между клиентами Fethard	бесплатно
Платежное поручение (USD)	0.5% (мин. USD 35)
Платежное поручение (EUR)	0.7% (мин. EUR 45)
Платежное поручение (RUR)	1% (мин. RUR 500)
Банковский перевод на частное лицо	USD 50
Заказ розыска отправленного платежа	USD 60
Заказ розыска поступающего платежа	USD 100
Оформление пластиковой карты	USD 50
Пополнение пластиковой карты на следующий рабочий день (USD)	2.5% (мин. USD 1)
Пополнение пластиковой карты в тот же рабочий день (USD)	2.5% (мин. USD 1) + USD 15
Оформление виртуальной карты (USD)	USD 30
Пополнение виртуальной карты (USD)	2.5% (мин. USD 4)
Зачисления с кошельков Webmoney до 2000\$ в сутки	бесплатно
Зачисления с кошельков Webmoney от 2000\$ в сутки	1%
Перевод средств в систему Webmoney (USD)	2.5% (мин. USD 0.5)
Перевод средств в систему Webmoney (RUR)	5% (мин. RUR 100)
Предоставление карты напрокат	5% (мин. USD 5)

Перечень услуг одной из посреднических фирм по осуществлению интернет-платежей, вводу и выводу средств. Размер комиссионного вознаграждения явно превышает обычный, но при этом обеспечивается относительная анонимность

Приведем пример из практики. Группа кардеров* для вывода средств, полученных преступным путем, использовали следующий метод. Средства сосредотачивались на нескольких счетах сетевых платежных систем «PayPal» и «E-gold». Как только набиралась заметная сумма, она немедленно перечислялась посреднику — специально созданной ради анонимизации интернет-платежей фирме, которая имела собственные счета в обеих упомянутых платежных системах. По поручению кардеров посредник раз в три месяца открывал новый банковский счет в одном из прибалтийских банков (там не слишком строго проверяют документы у вкладчиков, можно назваться Иваном Петровым или Джоном Смитом, и банкиры поверят на слово). На такой счет сбрасывались криминальные деньги. Банковскую карту от каждого счета вместе с пин-кодом посредник отсылал главарию кардеров по почте на абонентский ящик. Деньги снимались через банкоматы. Все указания как платежным системам, так и посреднику давались через веб-интерфейс или по электронной почте с использованием анонимизирующих прокси-серверов. В результате добытые преступным путем деньги доходили до кардеров с задержкой всего в пару недель и с потерей порядка 40%, зато с высокой степенью анонимности.

Многие сетевые платежные системы выпускают (в сотрудничестве с банками) собственные платежные карты, через которые можно относительно просто вывести деньги, сняв их в любом банкомате. На 2006 год известно о выпуске таких карт для систем:

- Gcard (<http://moneymakergroup.ru/-Gcard--t82.html>)
- Rupay (<http://news.proext.com/money/12310.html>)
- Fethard (<http://fethard.ru>)
- Webmoney (<http://cards.webmoney.ru>)
- Roboxchange (<http://cashcards.ru/WebClient/?Lang=ru&>)

Для выпуска карты формально требуется предъявить паспорт или прислать его скан-копию. Но проверка именно формальная, никаких серьезных препятствий для получения карты на чужое имя не существует. Не говоря уже о том, что аккаунты в таких системах свободно продаются и покупаются, можно воспользоваться чужим аккаунтом для заказа карты, которая высылается по почте.

Подобная опция дает злоумышленнику возможность использовать счет «WebMoney» или «E-gold» для получения криминальных платежей, например, доходов от кардерской деятельности, платы от потерпевшего по мошенничеству или вымогательству. Зачисленная на электронный кошелек сумма быстро переводится через два-три промежуточных аккаунта на карточный счет, при этом используется веб-интерфейс управления счетом, который, в принципе, позволяет анонимизировать пользователя. Затем деньги с карты снимаются в банкомате, каковая операция также допускает анонимность.

В порядке противодействия указанным способам, в зависимости от обстоятельств, перед правоохранительными органами могут стоять следующие задачи:

- воспрепятствовать регулярной деятельности злоумышленников, максимально затруднив обналичивание денег с их электронных кошельков;
- воспрепятствовать обналичиванию конкретного платежа на электронный кошелек;
- вернуть конкретный платеж отправителю;
- установить лицо, получающее деньги с конкретного электронного кошелька или получившее конкретный платеж.

Упомянутые выше карты для обналичивания средств с электронных кошельков эмитируются не самими платежными системами (хотя и несут их логотип), а банками. Банки же вполне подконтрольны властям и при наличии судебной санкции не только сообщают всю информацию о карточном счете, но и заблокируют его или вернут платеж.

Когда требуется отследить платеж через банковскую карту, следует обращаться за содействием в соответствующий банк. При наличии судебного решения банк обязан предоставить любую информацию. Чтобы отследить, заблокировать или вернуть платеж внутри сетевой платежной системы, следует обращаться к руководству этой системы. В отличие от банков, они не обременены многочисленными обязанностями перед вкладчиками и ограничениями, поэтому вполне могут себе позволить, например, закрыть счет мошенника и конфисковать все его средства даже без объяснения причины. На сотрудничество с властями электронные платежные системы также идут менее охотно, чем банки. У одних правоохранительных органов могут иметься с ними «хорошие отношения», другие же на свой запрос получают отказ.

Терроризм и кибервойна

Интернет все в большей степени используется для распространения СМИ. Заметна отчетливая тенденция возрастания доли информации, получаемой средним человеком через Сеть. А чем больше информации люди получают через киберпространство, тем более привлекательным оно становится для ведения информационной войны [35, 37, 38, W13].

Информационная война может быть частью войны обыкновенной или вестись отдельно от нее, без развязывания боевых действий. Терроризм же, в отличие от войны, имеет своим обязательным элементом массовую информацию. Современная доктрина определяет терроризм как проведение деструктивных действий с целью запугивания и принуждения, то есть оказания влияния на поведение людей посредством страха [36]. При этом задуманное влияние оказывает не сам теракт (убийство,

взрыв, похищение), а сопровождающее его информационное воздействие через СМИ. То есть без резонанса в СМИ террористический акт перестает быть таковым и превращается в заурядное преступление.

Для ведения информационной войны или информационного обеспечения терактов противник может использовать сетевые СМИ и популярные интернет-ресурсы пассивно — просто сливая в них подготовленную информацию. Но возможно и активное использование Интернета: создание и поддержание собственных интернет-ресурсов, подавление информационных ресурсов противников, провоцирующие действия, навязчивая реклама (спам) и так далее.

Указанные активные действия в Сети могут подпадать под соответствующие статьи УК.

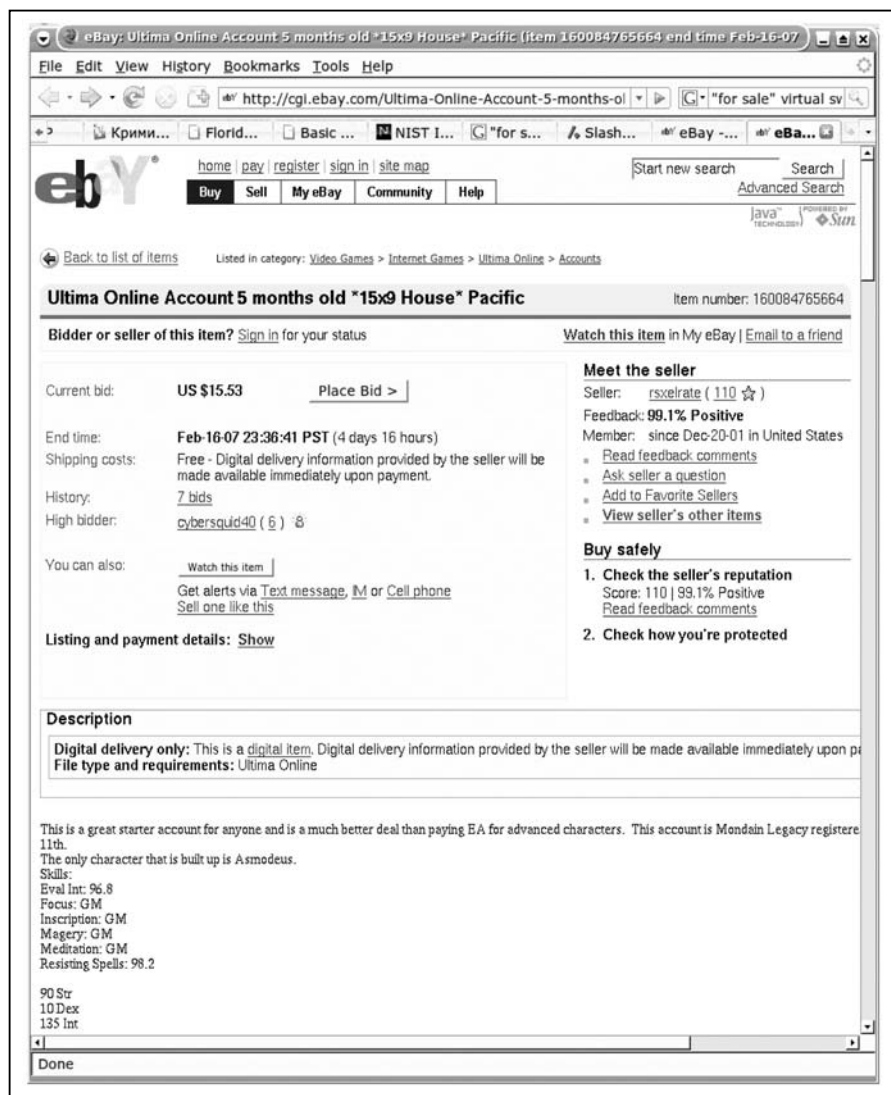
Мошенничество в онлайн-играх

Онлайновые многопользовательские игры, называемые также многопользовательскими мирами или MUD, популярны с начала 1990-х. Однако лишь в начале 2000-х годов они стали коммерциализироваться. Некоторые создатели игр получают основной доход от абонентской платы игроков или продажи лицензий на ПО. Другие проекты делают ставку на торговлю виртуальными предметами, виртуальной недвижимостью и иными предметами и услугами, находящимися целиком внутри виртуального мира. Достаточное число игроков и развитые технические средства делают такие проекты коммерчески успешными.

На аукционах виртуальных предметов совершается сделок на сотни тысяч долларов ежедневно. Продаются виртуальные предметы (оружие, броня, драгоценности, артефакты), персонажи, местная виртуальная валюта, недвижимость виртуального мира (дома, магазины, участки земли под застройку), прочие ценности (разрешения и лицензии от властей виртуального мира, членство в кланах, карты и т.п.) [58].

А там, где появляются ликвидные ценности существенного размера, появляются и мошенники, желающие такие ценности похитить.

В виртуальных мирах возможны различные методы обмана и злоупотреблений. Похищение у персонажей различных ценных виртуальных предметов, а также персонажей целиком. Продвижение персонажа по уровням с использованием недозволенных методов, в том числе уязвимостей в ПО игры (так называемый читинг*). Генерация и дублирование ценных виртуальных предметов. Обман других игроков с целью выманивания у них виртуальных ценностей. Нарушение установленной монополии на различные виды деятельности в виртуальном мире, что ведет к недополучению дохода владельцами игры. Продажа игрокам неразрешенных программных приспособлений для получения игровых преимуществ. И многие другие.



Одно из многочисленных объявлений о продаже ценностей из виртуальных миров за реальные деньги. В данном случае продается персонаж с некоторым количеством виртуального имущества

В некоторых зарубежных странах прошли первые судебные процессы, касающиеся хищения виртуальных предметов и персонажей. В России же интересы игроков не подлежат судебной защите, согласно ст. 1062 ГК. Исключения редки: для некоторых из видов упомянутого типа мошенни-

чества могут использоваться вредоносные программы или неправомерный доступ к игровому серверу. Например, для кражи пароля от игрового персонажа. Но это случай редкий, и относится он к иным видам преступлений, описанным выше.

Автор не исключает, что по мере развития виртуальных миров, нарастания количества их участников, по мере совершенствования возможностей персонажей и, следовательно, возрастания денежных интересов игроков и устройств такие интересы станут защищаться на государственном уровне, возможно, будут приняты и специальные законы.

Уже сейчас фиксируются сделки с предметами, принадлежащими виртуальному миру, на суммы в десятки тысяч долларов. Уже сейчас есть отдельные лица, зарабатывающие на жизнь участием в таких виртуальных мирах. Прослеживается четкая тенденция к возрастанию размера интересов игроков. Следовательно, скоро потребуются законодательная защита таких интересов.

Использование RBL

RBL (real-time black lists) — это черные списки для защиты от спама, основанные на протоколе DNS. RBL — это как раз тот случай, когда цель не оправдывает средства, когда лекарство становится вреднее болезни.

Исходное предназначение RBL — противодействие рассылке спама. Черный список представляет собой базу данных IP-адресов (реже — доменов), доступную всем пользователям (реже — лишь подписчикам) по протоколу DNS. В запросе указывается IP-адрес. В ответе сообщается, числится ли данный адрес в списке. Большинство мейл-серверов имеют встроенную возможность взаимодействия с любым RBL. При открытии SMTP-сессии принимающий сервер запрашивает RBL, и если IP-адрес передающего мейл-сервера числится, то электронная почта отвергается¹. Подчеркнем, что входящая почта отвергается без ее принятия, без анализа заголовков или содержания писем, только на основании IP-адреса передающего сервера.

Предполагается, что в RBL должны заноситься источники спама. То есть IP-адреса, с которых часто рассылается спам либо имеется потенциальная возможность этого (например, открытый транслятор электронной почты). Практика показывает, что когда мейл-сервер использует RBL, содержащий источники спама, это приводит к избавлению от значительной части поступающего спама — от 30 до 70%. При этом число ложных срабатываний (то есть случаев, когда отвергается нормальное письмо) хотя и ненулевое, но находится в приемлемых рамках — от 0,1% до 4%, в зависимости от качества используемого черного списка [W22].

¹ Разумеется, эта опция не включена по умолчанию. Фильтрация почты по RBL включается лишь администратором сервера, вполне осознанно.

Далее следует рассказать про RBL, отличающиеся от традиционных. Ввиду наблюдавшегося роста их популярности у некоторых их владельцев появилась идея использовать черные списки в других целях. В некоторые RBL заносятся не источники спама, а IP-адреса провайдеров, политика которых не одобряется держателями черного списка. К неодобряемым чертам провайдеров относятся обычно следующие: (а) предоставление хостинга веб-сайтам, которые рекламируются при помощи спама (так называемые spamvertized-ресурсы); (б) предоставление каких-либо услуг лицу, распространяющему программы или БД, предназначенные для рассылки спама; (в) отказ отключить клиента, обвиненного в вышеуказанных деяниях; (г) отказ отключить субпровайдера, который отказался отключить клиента по одному из вышеуказанных деяний.

Предполагается, что клиенты таких провайдеров, испытывая неудобства в связи с недоставкой своей почты, станут оказывать давление на своих провайдеров, способствуя таким образом изменению их политики в желаемом направлении. Описанные RBL принято называть черными списками второго рода [W23].

Понятно, что занесение в RBL сетей провайдеров является методом реализации убеждений (политических, моральных, нравственных) тех лиц, которые такие черные списки содержат. Не отрицая прав на собственные убеждения и на их пропаганду, тем не менее следует указать, что это не имеет отношения к коммерческой деятельности и, как правило, экономически не обосновано.

От спама использование RBL второго рода также не защищает.

Непосредственные неудобства пользователям создаются не самим RBL, а тем, что некоторые мейл-серверы настроены на его использование. Владелец отвергающего почту мейл-сервера как бы «не отвечает» за факт наличия адреса отправителя в используемом черном списке. Как правило, они не связаны договорными отношениями, а в законодательстве о создании препятствий в передаче электронной почты напрямую не говорится.

Использование чужих RBL для работы мейл-серверов, как правило, не регламентировано внутренними документами компании-провайдера. Часто все подобные настройки делаются рядовыми сотрудниками провайдера без санкции руководства, которое такими «техническими деталями» не интересуется.

В человеческом обществе исторически сложилось так, что в случае вымогательства под угрозой причинения вреда третьему лицу (заложнику) моральная ответственность за последствия ложится не на вымогателя, а на того, кто не исполнил его требования. А действия держателей RBL второго рода как раз и есть аналог захвата заложника: провайдера вынуждают исполнять требования (зачастую незаконные) под угрозой причинения вреда непричастным лицам — его клиентам и клиентам клиентов.

Изобразим схематически отношения между субъектами, вовлеченными в историю с описанным кибервымогательством. Участников можно свести к пяти субъектам.

- отправитель почты;
- администратор передающего мейл-сервера;
- получатель почты;
- администратор принимающего мейл-сервера;
- держатель черного списка.

На самом деле схема несколько сложнее. Над администраторами серверов, как правило, стоят их владельцы (руководители предприятий). В большинстве случаев администраторы делают настройки на использование деструктивных RBL без ведома своего руководства.

Владелец передающего (внесенного в чёрный список) сервера является объектом вымогательства. Его клиент-отправитель письма является непричастным заложником, которому наносится вред. Получателю письма вред также наносится (пунктирная стрелка), но он об этом не знает.

Схема кибервымогательства при помощи RBL немного сложнее, чем классическая схема с заложником. Здесь разнесены субъект, выдвигающий требования, и субъект, непосредственно причиняющий вред непричастному. Держатель черного списка использует администратора принимающего сервера втемную, стараясь не раскрывать ему истинную схему, вводя в заблуждение относительно истинного содержания его RBL.

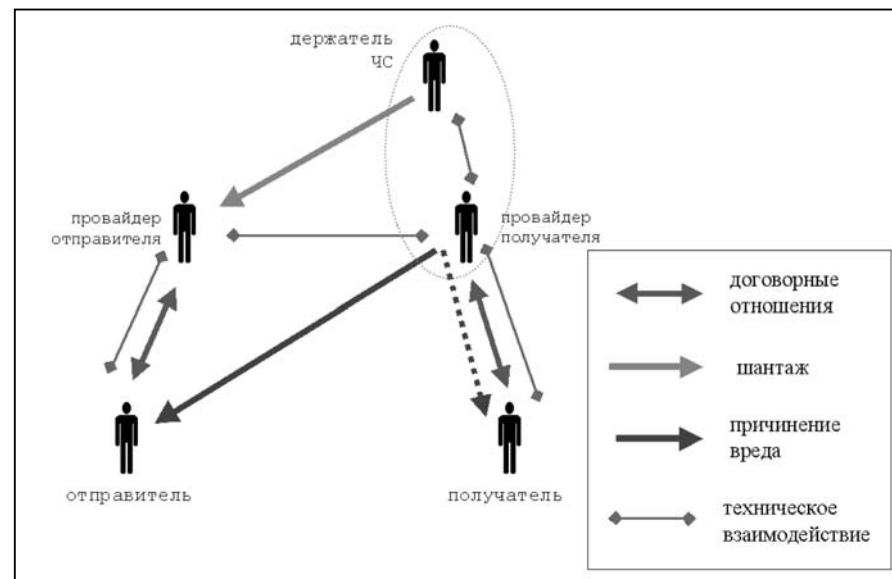


Схема взаимоотношений при шантаже с использованием черного списка (RBL)

Как следует квалифицировать действия держателя RBL второго рода? Сами держатели не отрицают, что их метод подразумевает причинение вреда непричастным. Это официально опубликованная политика таких черных списков, как «Spamhaus», «Sorbs» и «Spews» (ныне не существующего). Держатели RBL выдвигают следующий тезис. Не запрещено публиковать любые списки. Их черный список выражает их собственные «личные» убеждения. Следовательно, его обнародование защищается положениями о свободе слова. Каждый пользователь использует RBL под свою ответственность, на свой собственный риск, о чем имеется предупреждение, опубликованное там же, где и политика RBL.

Действительно, публиковать личные убеждения не может быть запрещено. Однако держатели RBL второго рода делают все, чтобы их деструктивный RBL был похож на обычные RBL первого рода, предназначенные для защиты от спама. Предупреждения относительно политики черного списка и вреда непричастным, мягко говоря, не афишируются. Они изложены хотя и на публичном веб-сайте, но не слишком вразумительно и где-нибудь в конце страницы мелким шрифтом. Держатели RBL второго рода рекламируют свой список как «антиспамовый». Естественно, администратор мейл-сервера, задумав защититься от спама при помощи RBL, просто включает имеющиеся в образцах списки, не изучая подробностей политики каждого из них. Проконтролировать же, какая почта отвергается, не представляется возможным из-за особенностей технологии — напомним, что письмо не принимается, соединение отвергается еще до начала передачи письма. Исследования показывают, что подавляющее большинство пользователей таких RBL были искренне убеждены, что там содержатся лишь источники спама. Подавляющее большинство пользователей отказались от их использования, как только узнали правду.

Таким образом, можно утверждать, что умысел держателя RBL второго рода направлен именно на введение в заблуждение пользователей. Действия держателя RBL могут быть квалифицированы как сознательное причинение вреда непричастным путем обмана или злоупотребления доверием с целью принуждения жертвы к определенным действиям (часто незаконным) в соответствии со своими политическими целями. Вымогательством это считаться не может, поскольку нет требования передачи выкупа. Следовательно, это может быть квалифицировано по ст. 179 УК (принуждение к совершению сделки или к отказу от ее совершения). Аналогичный состав преступления имеется и в законодательстве других стран.

Как следует квалифицировать действия пользователя черного списка? Здесь два варианта.

Если пользователь не знал особенностей RBL второго рода, принимал его за RBL первого рода и использовал именно в качестве такового, то он сам — потерпевший от мошеннических действий, поскольку отвержение валидной электронной почты наносит вред как отправителю, так и получателю, а следовательно, и их провайдером.

Если же пользователь RBL знал принцип его работы и сознавал, что использование RBL не защищает от спама, а ведет к недоставке валидной почты, то его действия следует квалифицировать как соучастие (ч. 2 ст. 33 УК — соучастие в форме исполнения). Разумеется, сказанное не относится к случаю, когда лицо использует RBL для фильтрации только своей личной почты.

Накрутка

Описанные ниже действия не всегда можно квалифицировать как мошенничество или иное уголовное преступление. Впрочем, даже тогда, когда квалификация возможна, пострадавшие предпочитают не обращаться в правоохранительные органы, а защищаться своими средствами, поскольку это эффективнее.

Накрутка является одним из видов мошенничества с целью хищения средств, ассигнованных на рекламу в сети Интернет, или иного обмана, связанного с рекламой.

По мере все большей коммерциализации Интернета, по мере увеличения рекламных бюджетов мошенничество с рекламой становится все привлекательнее. Как профессиональные мошенники могут затеять проект с целью обмана рекламодателей или рекламораспространителей, так и обычные владельцы интернет-проектов могут соблазниться легкими, но не вполне честными деньгами.

Доход многих интернет-проектов складывается из поступлений за рекламу. А эти поступления пропорциональны количеству посетителей веб-сайта (или количеству посетителей из целевой аудитории). Таким образом, поднять посещаемость сайта означает пропорционально поднять свои доходы. Между веб-сайтами за посетителей идет нешуточная борьба.

Среди методов увеличения посещаемости есть и не вполне честные методы и даже откровенно мошеннические.

Одним из источников посещаемости веб-сайта (для некоторых — главным источником) являются поисковые системы и интернет-каталоги. Количество пользователей, пришедших по ссылкам из поисковой системы или каталога, сильно зависит от позиции ресурса в результатах поиска или в каталоге. А позиция эта зависит от релевантности запросу (для поисковых систем), от индекса цитируемости или от посещаемости (для каталогов). Поднять свой ресурс в рейтинге можно, симитировав высокую посещаемость сайта — это и называется накруткой счетчика.



Веб-счетчик — инструмент подсчета посещаемости. Показывается на рейтингуемой веб-странице, но запрашивается с рейтингового сервера. Измеряет число посетителей и другую статистику для определения рейтинга сайта

#	Рейтинг: заглавных страниц / сайтов	Загл. страница	хосты	посетители	хиты	стат.
1	АНЕКДОТ.РУ - "Анекдоты из России"	14 484	16 401	21 385		
2	АНЕКДОТОВ.NET - Анекдоты, Фото, Приколы + В И Д Е О	7 540	8 249	10 693		
3	100% лучшие ФОТО - ПРИКОЛЫ III new!	7 332	8 234	10 291		
4	УМОРА.РУ Антистресс Позитив Портал УМОРА.РУ	5 432	6 351	9 184		
5	Анекдоты @mail.ru: Анекдоты, истории, афоризмы, гороскоп...	5 155	5 586	6 239		
6	+10... С В Е Ж И Х . А Н Е К Д О Т О В (super!)	4 988	5 394	6 052		
7	ДЕСЯТКА НОВЫХ И СМЕШНЫХ историй на АНЕКДОТ.РУ	3 690	3 936	4 355		
8	ХОХМА - Юмор, SEX-истории, ФОТО приколы, тосты, МОЗГОЛО...	3 051	3 228	3 964		
9	ЕЖЕДНЕВНЫЕ прикольные картинки, анекдоты, истории и вид...	2 722	3 137	4 345		
10	Юмор, Фото-Видео Приколы, МЕГА-ЗРОТИКА, ежедневно III	2 652	2 718	3 502		
11	АНЕКДОТЫ на Острые ру - это не для тупых...	2 427	2 826	3 782		
12	MULT.RU Мультифильмы без бабки	2 417	2 495	3 157		
13	+10... С В Е Ж И Х . П Р И К О Л О В (super!)	2 287	2 382	2 605		
14	СМС ПРИКОЛЫ, ПРИКОЛЬНЫЕ СМС ШУТКИ, ЛЮБОВНЫЕ СМС, SMS ПО...	1 965	2 054	2 511		
15	Триникси - Вселенная Развлечений. Фото, видео, флэш	1 753	1 804	2 699		
16	Анекдоты изПодтишка. 145 новых анекдотов.	1 522	1 545	1 912		
17	Юмор, смех, приколы и хорошее настроение.	1 452	1 538	2 132		
18	АНЕКДОТЫ и ФОТО ПРИКОЛЫ на SPYNET.RU	1 439	1 454	1 789		

Один из рейтингов. Ресурсы упорядочены по посещаемости.

Самые популярные привлекают больше посетителей.

А чем больше посетителей, тем выше позиция в рейтинге.

Один из методов быстро вырваться вперед — накрутить себе посещаемость

Другой способ использования накрутки — непосредственный обман рекламодателя или рекламодателя.

При размещении рекламы в Интернете используются три схемы расчета — плата за показ, плата за клик и процент с продаж. В первом случае владельцу рекламной площадки рекламодатель или рекламодатель (посредническое рекламное агентство) платит пропорционально числу показов рекламного баннера на веб-странице. Во втором случае плата пропорциональна числу пользователей, перешедших на рекламируемый ресурс по гиперссылке, то есть кликнувших на рекламном баннере*. В третьей схеме рекламодатель или владелец рекламной площадки получает от рекламодателя процент с продаж тому клиенту, который пришел по ссылке. Есть и вариант оплаты рекламы по фиксированному тарифу — обусловленная сумма в месяц или в день. Но в этом случае тариф зависит от посещаемости ресурса, на котором реклама размещается.

Первый и второй способы дают возможность для обмана путем манипуляции со статистикой просмотров или статистикой переходов по рекламному баннеру.

Технические методы накрутки статистики весьма разнообразны. Как разнообразны и защитные контрмеры, применяемые рекламодателями и рекламодателями, а также поисковыми системами и интернет-каталогами. В ходе накрутки для противодействия этим контрмерам мошенники могут прибегать к использованию зомби-сетей*, вредоносных программ (типа adware*), использовать неправомерный доступ к чужим информационным системам (в том числе к тем, которые ведут статистику) — словом, совершать компьютерные преступления.

Впрочем, большинство случаев накрутки счетчиков, фальсификации статистики или иного недозволенного повышения своих показателей (рейтинга, релевантности, индекса цитируемости) нельзя квалифицировать как уголовные преступления. Это всего лишь нарушение условий договоров, связывающих рекламодателей, рекламодателей и владельцев рекламных площадок. С такими нарушениями рекламодатели и посредники должны разбираться самостоятельно, собственными средствами, а возникшие из этого споры относятся к разряду гражданских дел.

Заключение к разделу 1

Теория уголовного права и криминалистика оперируют различными критериями при классификации преступлений. В Уголовном кодексе преступления объединены в статьи по общности объекта преступления, в главы — по общности родового объекта преступления. Криминалистика же характеризует преступления совсем иными параметрами — способ совершения, личность преступника, личность потерпевшего, методы раскрытия и так далее. Оттого и классификация другая. Общую криминалистическую характеристику могут иметь преступления из разных глав УК (например, клевета и возбуждение национальной розни). А преступления, объединенные в одну статью УК, с точки зрения криминалистики, существенно отличны друг от друга (например, нарушение авторских прав в Сети и в офлайне).

Отсюда понятно, что является ошибочным строить криминалистические характеристики преступлений, классифицируя их по критериям уголовного права.

В данном разделе были рассмотрены наиболее распространенные на сегодняшний день виды компьютерных преступлений. Следует помнить, что вследствие развития индустрии ИТ способы совершения киберпреступлений быстро меняются, возникают новые, а старые постепенно сходят на нет.