Информационные технологии и компьютерные преступления в сети Интернет

Яппаров Рауф Мидхатович,
доцент кафедры оперативно-розыскной деятельности ОВД Уфимского юридического института МВД России, полковник полиции

В настоящее время ЭВМ настолько прочно вошли в нашу жизнь, что с каждым днем все больше и больше граждан хранят в них свою «виртуальную собственность». И если многие из них весьма трепетно относятся к таковой в реальном мире, то сосредоточенным в сложных кибернетических устройствах, каковыми являются персональные ЭВМ, они явно не уделяют должного внимания. Большинство правообладателей интеллектуальной собственности, находящейся в их персональных компьютерах, продолжают считать, что никому нет дела до информации, сосредоточенной в ПЭВМ, что в файлах нет ничего ценного для хакера, и что все вирусные атаки пройдут мимо. Это далеко не так. За последние годы интенсивного развития телекоммуникационных технологий преступные структуры, постоянно изобретая новые вредоносные программы, превратили Интернет в высокодоходное занятие, своеобразный криминальный бизнес, который приносит миллиардную прибыль.

В данной статье мы хотели бы дать характеристику наиболее распространенным способам криминального обогащения в сфере Интернет, а также методы и формы противодействия данным противоправным проявлениям. Для этого мы предлагаем проанализировать современное состояние борьбы с киберпреступностью с двух позиций: какая информация, сосредоточенная на компьютерах пользователей, представляет интерес для хакеров и каким образом происходят непосредственно сами хищения интеллектуальной собственности. Отметим, что в подавляющем большинстве случаев для совершения кражи информации пользователей сети Интернет преступники используют специализированные вредоносные программы или методы социального инжиниринга[1], либо и то, и другое в совокупности — для большей эффективности.

По результатам проведенного нами исследования, можно выделить 4 группы сведений, которые наиболее часто подвергаются атакам с помощью вредоносных программ. Подчеркиваем, что это далеко не весь спектр данных, интересующих криминальные элементы. Это, в частности, информация, позволяющая получить:

- доступ к различным финансовым операциям (онлайн-банкингу[2], пластиковым картам, электронным деньгам), интернет-аукционам[3] и т.д.;
- доступ к почтовым ящикам, которые являются неотъемлемой частью ICQ-аккаунтов[4], как и все найденные на компьютере адреса электронной почты;
- пароли, коды для доступа к интернет-пейджерам[5], сайтам и др.;
- пароли, коды к онлайн-играм.

1. Социальная инженерия — это метод управления действиями человека без использования технических средств воздействия. Метод основан на использовании психологических особенностей человека, его восприятии окружающей среды и нравственного состояния.
2. С помощью услуги «Онлайн-Банкинг» клиенты Банка могут в режиме реального времени контролировать состояние своих счетов.
3. Интернет-аукцион (он же «онлайновый аукцион») — аукцион, проводящийся посредством интернета. В отличие от обычных аукционов, интернет-аукционы проводятся на расстоянии (дистанционно) и в них можно участвовать, не находясь в определённом месте проведения, делая ставки через интернет-сайт или компьютерную программу аукциона.
4. Аккаунт — это учётная запись, где хранится персональная информация пользователя для входа на сайт.
5. Интернет-пейджер, то есть программа для моментального обмена сообщениями, главной функцией которого является вызов заданного пользователя (этот процесс состоит из двух стадий — определения доступности пользователя и установления канала связи).

Целью любой вредоносной программы является контроль за действиями пользователя (например, запись последовательности всех нажатых клавиш), либо целенаправленный поиск ключевых данных в пользовательских файлах или системном реестре. Полученные данные вредоносная программа в итоге передает своему изобретателю или лицу, намеревающемуся совершить преступление. Подобные «творения» относятся к программам типа Trojan-Spy или Trojan-PSW. «Заразиться» такими программами можно самыми различными путями: при просмотре вредоносного сайта, по почте, в чате, форуме, через интернет-пейджер или иным способом «во время путешествия» в сети Интернет. В качестве примера давайте рассмотрим одну из модификаций широко распространенного программного продукта Trojan-PSW.Win32. LdPinch, который занимается кражей паролей к интернет-пейджерам, почтовым ящикам, FTP[6] и другой информации.

Эта вредоносная программа, оказавшись на компьютере, рассылает всем «друзьям» по контакт-листу сообщения типа: «Смотри «далее идет ссылка_на_вредоносную_программу» Классная вещь!)». В результате практически каждый получатель данного сообщения идет по этой вредоносной ссылке и запускает «троянца». И так далее: заразив один компьютер, «троянец» рассылает себя дальше по всем контакт-листам, обеспечивая хакера всеми необходимыми пользовательскими данными для проведения дальнейших преступных операций. Происходит это из-за высокого уровня доверия к ICQ-сообщениям: получатель не сомневается, что сообщение пришло от его знакомого и добросовестно отвечает ему.

Особое опасение вызывает тот факт, что подобные вредоносные программы начинают сочетать с мето-

6. FTP (англ. FileTransferProtocol — протокол передачи файлов) — протокол, предназначенный для передачи файлов в компьютерных сетях. FTP позволяет подключаться к серверам и просматривать содержимое каталогов, загружать файлы с сервера или на сервер, передавать файлы между серверами.

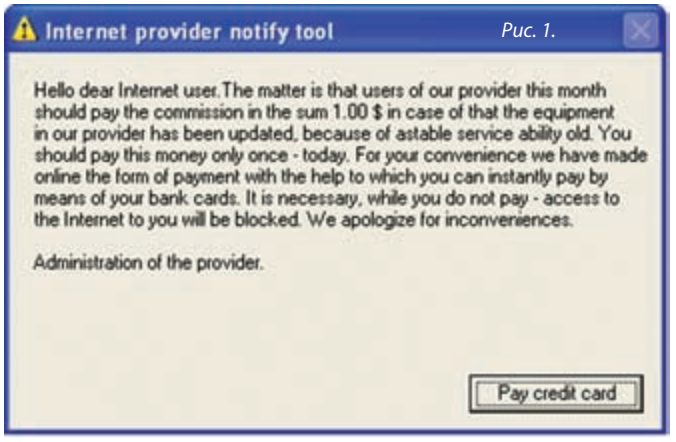

Рис. 1.

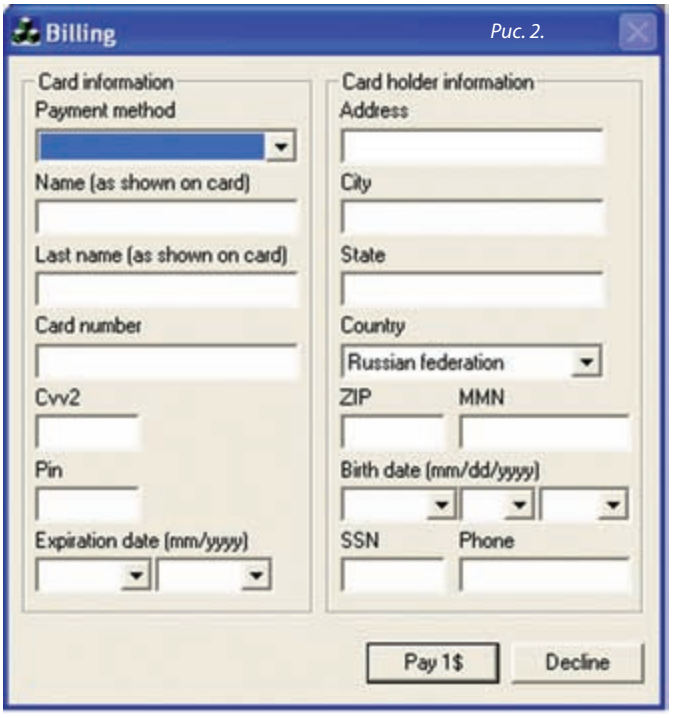

Рис. 2.

дами социального инжиниринга. В большинстве случаев хакеры одновременно с вредоносными программами вынуждают пользователя компьютера совершить определенные действия, необходимые для достижения ими преступного умысла[7]. Например, при запуске вредоносная программа Trojan-Spy.Win32.Agent.ih выводит следующее диалоговое сообщение (см. рис. 1):

Примерный перевод текста указывает пользователю на необходимость заплатить всего 1 $ за пользование услугами интернета провайдеру[8]. При этом отметим, что сообщение составлено по всем правилам социального инжиниринга, а это:

- пользователю не оставляют времени для размышлений, так как заплатить необходимо быстро, не раздумывая, в день получения письма;
- предлагается заплатить символическую плату — всего лишь 1 доллар, что резко увеличивает шансы мошенников, так как мало кто будет что-либо выяснять из-за одного доллара;
- для стимулирования действий пользователя злоумышленники угрожают: если не заплатишь, администратор заблокирует доступ к Интернету.

При этом, чтобы минимизировать подозрения пользователя в истинности намерений, в качестве отправителя указана администрация провайдера, которая якобы уже проявила заботу о своем пользователе и подготовила все необходимое, осталось только оплатить и не тратить драгоценное время на оформление документации и отправку сообщения. Вполне логично предположить, что администрация провайдера знает адрес электронной почты своего пользователя. Законопослушному пользователю просто не оставляют выбора, и он нажимает кнопку «Pay 1 $», что приводит к появлению следующего диалогового окна (см. рис. 2). Естественно, что после заполнения всех полей и нажатия кнопки «Pay 1 $» никакой оплаты не происходит, а вся информация о вашей кредитной карте отправляется по почте к мошенникам.

Методы социального инжиниринга используются и отдельно от вредоносных программ. Красноречивым подтверждением этого является фишинг[9] — атака, направленная на клиентов того или иного банка, использующих для управления своего счета систему онлайн-банкинга. Так, например, в рассылаемых от имени банка фальшивых письмах авторы могут утверждать, что учетная запись клиента заблокирована по той или иной причине, и что для ее разблокирования необходимо ввести учетные данные пользователя. При этом в теле письма приводится специальным образом сформированная ссылка. Приводимая ссылка создается хакерами таким образом, что на экране пользователя она отображается как реально существующий сетевой адрес сайта банка (на самом же деле ссылка при ее активации приведет на сайт лица, намеревающегося совершить преступление). Введенные данные опять же попадут не в банк, а к преступнику, который получит данные клиента, а вместе с ними и возможность доступа к его счету.

Похожим образом рассылаются и письма от имени различных служб поддержки, социальных служб и т. п.

Однако преступники «охотятся» не только за данными пользователей кредитных карт. Их интересуют и такие данные, как списки электронных адресов пользователей компьютеров. Неоценимую помощь в этом хакерам оказывают вредоносные программы, которые получили название SpamTool. Эти программы занимаются сканированием файлов данных на компьютере пользователя и ищут там все адреса электронной почты, хранящиеся в операционной системе. Собранные адреса тут же отфильтровываются по заданным критериям (например, удаляются принадлежащие антивирусным компаниям) и отсылаются лицу, намеревающемуся совершить преступление.

Существуют и куда более циничные способы проникновения вредоносных программ в компьютеры пользователей. Отмечены случаи, когда преступники предлагают оплачивать владельцам сайтов загрузку их «посетителям» вредоносных программ. Так, например, поступали с сайтом iframeDOLLARS.biz. Согласно расположенной там «партнерской программе», веб-мастерам предлагалось установить на собственных сайтах эксплойты[10] для дальнейшей автома-

7. URL: http://www.securelist.com/ru/descriptions/ old98678.
8. Провайдер, (англ. Internet Service Provider, ISP, букв. «поставщик Интернет-услуги») — организация, предоставляющая услуги доступа к Интернету и иные связанные с Интернетом услуги.
9. Фишинг (англ., от fishing — рыбная ловля, выуживание) — вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей — логинам и паролям.
10. Эксплойт (брешь в безопасности) — это компьютерная программа или скрипт, использующий специфические уязвимости операционной системы, с помощью которых могут быть получены расширенные права доступа.

Рис. 3.

тической загрузки посетителям вредоносных программ. «Партнерам по бизнесу» авторы предлагали вредоносные программы купить по цене 61 $ за 1000 заражений[11].

Безусловно, основная причина совершения хищений пользовательской информации имеет корыстную направленность. В конечном итоге практически вся украденная информация продается либо напрямую используется для материального обогащения. Но получить данные кредитных карт и электронные адреса пользователей — это только часть дела, далее злоумышленникам необходимо вывести награбленное из платежной системы, то есть реализовать полученную информацию.

Способы обналичивания преступно нажитых средств путем использования интернет-технологий весьма разнообразны. Если результатом проведенной фишинг-атаки стали, например, параметры для доступа к системе онлайн-банкинга или электронному кошельку пользователя, то средства могут быть выведены через цепочку виртуальных электронных обменных пунктов, например путем перевода одной электронной валюты в другую через электронные платежные системы либо с помощью аналогичных услуг «представителей» киберкриминала[12]. В самом крайнем случае можно приобрести товар непосредственно в интернет-магазине[13].

Во многих случаях этап легализации преступно нажитых средств является самым опасным для преступника, так как приходится указывать какие-либо «свои» идентификационные признаки, например адрес для доставки товара, номер индивидуального счета/электронного кошелька и т. д.

Изощренность в достижении преступных замыслов толкает мошенников на поиск новых путей решения проблем такого рода. Одним из таких направлений приложения усилий современного преступного мира является привлечение людей, которых на языке киберкриминала называют «дропами»[14]. Эти люди нужны для того, чтобы преступники избежали уголовной ответственности, получили деньги или товар, оставаясь вне подозрения, а правоохранительные органы пошли по ложному «следу». При этом сами «дропы» зачастую и не знают, для чего их используют.

Существуют самые абсурдные способы вовлечения «дропов» в криминальный бизнес. В частности, их может нанять на работу якобы международная компания, разместившая на интернет-сайтах объявления о трудоустройстве. С такими работниками даже заключается трудовой договор. Но в случае их задержания сотрудниками правоохранительных органов при передаче денег те ничего вразумительного о своих работодателях сказать не могут. Договор, впрочем, как и все указанные в нем реквизиты, оказывается, безусловно, фальшивым. Преступник или, зачастую, организованная преступная группа не ищут «дропа», их поставкой занимается «дроповод» — лицо, на которое замкнуты все «работники» организации. Естественно, каждому в этой криминальной цепочке приходится платить, но «безопасность» в этом случае стоит того. Что же касается украденных адресов электронной почты путем сканирования операционной системы, то их можно потом продать на «черном» рынке за немалые деньги тем же «спамерам», использующим эти данные в социальных сетях Интернета в своих рассылках[15].

Другой представляющий оперативный интерес криминальный промысел — учетные записи онлайн-игр, которые приобретают все большую популярность. В процессе таких игр многие пользователи «покупают» себе с помощью электронных денег виртуальное оружие, заклинания, всевозможную защиту и другие атрибуты. Отмечены случаи, когда виртуальные ресурсы продаются за тысячи вполне реальных долларов. И все эти богатства злоумышленники, получив их абсолютно бесплатно путем взлома данных учетных записей, могут продать желающим по очень низким ценам, чем и объясняется рост популярности вредоносных программ, занимающихся кражей игровой виртуальной собственности. В настоящее время количество модификаций таких вредоносных программ, ворующих пароли от известных игр, может достигать 1500.

Один из наиболее распространенных способов обогащения в сфере Интернет считается злоупотребление доверием. Любой бизнес, расширяясь, постоянно ищет новые области своего применения. Не является исключением в данном случае и киберкриминал. Через сети Интернета продается все больше товаров и предлагается такое же количество услуг, постоянно появляются новые. Преступность оперативно внедряет в них мошеннические схемы из реального мира. Задача мошенника – склонить «клиента» к добровольной сделке, и для этого в подавляющем большинстве случаев используется фиктивное занижение цен. Как правило, в таких схемах для привлечения покупателей ставка де-

11. www.iframedollars.biz

12. Электронные платежные системы — это технологии, позволяющие производить расчеты напрямую между контрагентами с помощью электронной связи.

13. Интернет-магазин (электронный магазин) — это каталог товаров, в котором перечислены свойства 2 (характеристики) каждого товара, имеются фотографии, и, конечно, указана цена. В электронном магазине вы ищете необходимые товары и формируете свой заказ, а также вводите информацию, необходимую для оплаты, времени и места доставки выбранных товаров. Доставка осуществляется курьером или почтой.

14. http://www.itsec.ru/

15. Спам (англ.) — массовая рассылка коммерческой, политической и иной рекламы (информации) или иного вида сообщений лицам, не выражавшим желания их получать.

лается на значительно более низкие цены по сравнению с существующими на потребительском рынке. Вся аргументация таких цен в подобных интернет-магазинах весьма и весьма сомнительна. Но многие «покупатели» верят этим аргументам: «А почему бы им не продавать товар дешево, если он достался бесплатно!».

Так, например, один из интернет-магазинов на своем сайте предлагал ноутбуки по приемлемой цене, обосновывая это следующими положениями (см. рис. 3):

- продажа конфиската (таможенный конфискат);
- продажа товаров, купленных по украденным ранее кредитным картам;
- продажа товара, купленного в кредит через подставных лиц.

При заказе товара «клиента» просят внести предоплату, а иногда и заплатить стоимость товара полностью, после чего телефоны или адреса преступников перестают отвечать, а деньги, безусловно, никто не возвращает. При этом способы обмана покупателя разнообразны. Например, широко распространена доставка купленного в интернет-магазинах товара с помощью курьеров. В этом случае мошенники могут требовать предоплату только за доставку, аргументируя свое требование тем, что курьер часто приходит по адресу, где никто ничего не заказывал и затраты на курьера приходится покрывать интернет-магазину. В этом случае покупатель оплачивает затраты за доставку, а товар, естественно, не доставляется.

Такие интернет-магазины – это далеко не единственные ловушки для обманутых пользователей, в сфере компьютерной информации находят свою вторую жизнь практически все криминальные идеи из реального мира. В качестве очередного примера можно рассмотреть еще один из «проектов» мошенников, когда «клиенту» предлагают вложить определенную сумму денег под очень привлекательный процент (см. рис. 4). Комментарии, как говорится, здесь излишни. В один момент люди, доверяющие таким «инвестиционным» сайтам, превращаются из «инвесторов» в обманутых вкладчиков. Способов мошенничества и здесь предостаточно: постоянно обнаруживаются ложные обменные сайты для электронных денег, клиенты которых также лишаются своих средств, периодически появляются интернет-пирамиды (аналог сетевого маркетинга из реального мира), рассылается «спам» о существовании секретных специализированных электронных кошельков, которые удваивают или утраивают полученные суммы и т.д.

Как мы уже сказали ранее, все подобные мошеннические схемы используют психологию, менталитет[16] населения, склонного к легкой наживе.

С середины 2006 года в России появились новые вирусные технологии, направленные на вымогательство денег пользователей сети Интернет. Так, вредоносная программа Trojan. Win32. Krotten модифицировала реестр компьютера пользователя таким образом, что нормальная работа системы становилась невозможной. Появляющийся периодически «информер» выдвигал требование о переводе некоему владельцу сайта через СМС-сообщение определенной суммы денег за пользование ресурсами сети, взамен в сообщении гарантировалось восстановление работоспособности компьютера. Некоторые пользователи компьютеров, обладая достаточной квалификацией, восстанавливали исходное рабочее состояние системы самостоятельно, другие — переустанавливали операционную систему, что в конечном итоге позволяло избавиться от этой вредоносной программы. Однако основная масса пользователей склонялась в пользу «платить», обосновывая свое решение экономией времени или средств либо по морально-этическими соображениям, так как выскакивающий постоянно баннер носил преимущественно эротический характер. В результате после нескольких «неудачных» попыток ввода предлагаемого мошенниками пароля пользователь приходил к правильному выводу — это обман и нужна квалифицированная помощь, но его деньги уходили безвозвратно. Распространялся Trojan. Win32. Krotten в чатах, на форумах под видом программ, позволяющих получать бесплатную IP-телефонию, бесплатный доступ к сети Интернет, к сотовым коммуникациям и т. д.

Рис. 4.

Достаточно было только «кликнуть» мышкой на появляющийся рекламный баннер, и пользователь становился очередным «владельцем» вредоносной программы.

Рыночная экономика инициирует появление все новых и новых методов, форм, способов криминального обогащения в сфере компьютерной информации, а наша психология (менталитет) и другие факторы определяют вектор его развития. Почему же в интернет-сфере такие преступления как вымогательство, мошенничество, кража и другие популярны среди лиц, их совершающих? Ответ на этот вопрос банально прост: в надежде восстановить утерянные или испорченные данные пользователи компьютеров, зачастую и сами склонные к противоправным действиям, возможным благодаря пробелам в законодательстве, нередко согласны выполнить любые условия «доброжелателей» или немного отступить от требований закона. Предрасположенность определенного контингента лиц к добровольной передаче данных и нарушению законов, халатность в работе на компьютерах, характерные для части населения, зачастую являются инициирующими факторами преступного обогащения и осложняют процесс привлечения к уголовной ответственности злоумышленников.

16. http://www.securelist.com/ru/images/vlpub/0610_bmw_pic3.png.