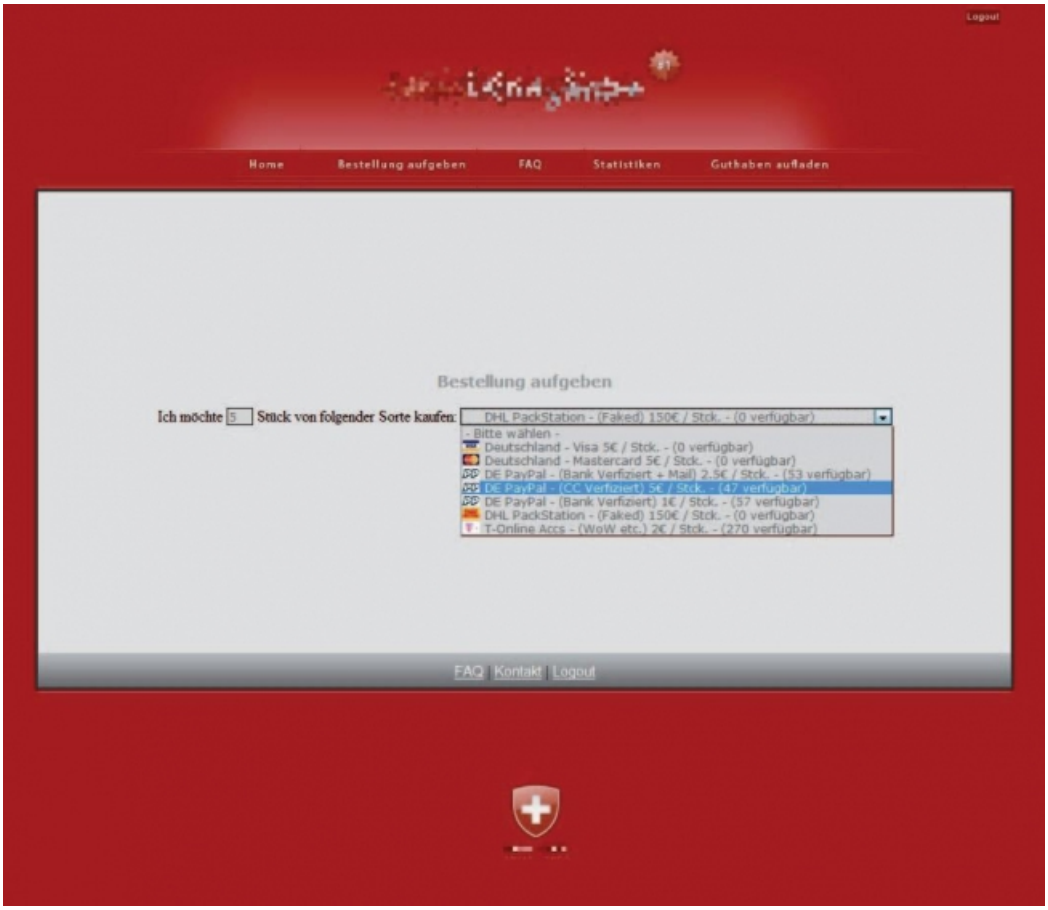
Нелегальная интернет-экономика активно развивается

На днях мне в руки попалось интересное исследование о преступниках, которые зарабатывают на краже данных у самых обычных пользователей сети Интернет. Авторы материала, Марк-Орель Эстер и Ральф Бенцмюллер из G Data Security Labs, на нескольких десятках страниц проанализировали основные сегменты нелегальной торговли и специфики данных, на которых можно заработать. Правда, этому материалу не хватает ответственной специфики - но может быть это и правильно, так как практически все российские хакеры работают "на экспорт". :)

Структура рынка

Интересно, что основным товаром на "черном" интернет-рынке являются не какие-то секретные данные, а информация самых обычных пользователей - данные их аккаунтов к платным сетям и игровым сервисам, интернет-магазинам и интернет-банкам и т.д. Логин-пароль к провайдеру ШПД не особенно интересен, так как не представляет особенной ценности, а вот параметры пластиковой карточки в цене как никогда. Правда, работают эти данные только для карт, где не подключен 3DSecure - с этой технологией безопасности еще никому справиться не удавалось. Продают такие данные массово и большими пакетами, поскольку и воруются они чуть ли не квадратно-гнездовым методом с помощью "ботнетов": сетей, состоящих из чужих компьютеров, зараженных специальными вирусными программами.

Примечательно то, что на такие данные существует платежеспособный спрос - преступникам всегда приятно получить дешевле то, что стоит дорого. :) Таким образом, современная нелегальная экономика в Сети оценивается в несколько десятков миллиардов долларов в год. Справедливости ради надо отметить, что само ее наличие "кормит" огромное число сотрудников спецслужб, частных детективов, сотрудников СБ банков, а также экспертов частных криминалистических компаний. В этой экономике, к слову, есть все признаки, присущие реальной экономической среде: производители, продавцы, поставщики услуг, «мошенники» и клиенты. Для многих заработок денег подобными киберпреступлениями — всего лишь переходная ступень на пути к организованной преступности, пусть даже (или потому что) для этого не требуются личные контакты с другими людьми.



Нелегальный магазин, продающий данные аккаунтов

У подобной нелегальной экономики есть свои "информационные базы" - это дискуссионные форумы (так называемые «борды», от англ. board), где главные обсуждаемые темы — это ботнеты, спам, кража данных и т. д. Форумы сообщества могут быть самыми разными — на большинстве, конечно, тусуются так называемые «скрипт-кидди» (новички, желающие стать настоящими хакерами, от англ.

script kiddie), и только в небольшом количестве реально продаются и покупаются данные кредитных карт, краденые товары и всё, на что есть платежеспособный спрос. Чем более незаконным является предмет обсуждения, тем более тщательные меры принимают владельцы форумов для предотвращения доступа на них не просто незарегистрированных пользователей, а тех, за кого никто не поручится и которых никто не знает. :)

Владельцы таких "торговых баз" предоставляют участникам нелегального киберсообщества черный рынок, где те могут продавать и покупать товары и услуги. Продаваться может всё, что угодно — от краденых данных кредитных карт до адресов электронной почты и ботнетов (сетей, состоящих из зараженных компьютеров). Например, можно купить, а лучше арендовать ботнет, а потом использовать его для проведения DDoS-атак. На все есть ориентировочные и среднестатистические цены. Полагаю, читатели этого текста смогут сходу набросать как минимум десяток таких адресов, правда? Конечно, конкурирующие форумы часто «дефейсят» или даже подвергают DoS-атакам. :)

Всё происходит следующим образом: кто-то предлагает определенный товар, например наборы данных для доступа к пользовательским аккаунтам eBay. Продавец называет сумму за каждый аккаунт. Если покупатель желает приобрести все предлагаемые аккаунты или большинство из них, то продавец может сделать оптовую скидку. Кроме того, продавец, как правило, указывает приемлемую для него форму оплаты. Для совершения сделки потенциальный покупатель обычно отвечает на объявление о продаже через форум или обращается к продавцу напрямую, используя указанные им контактные данные. Разумеется, вопросы купли-продажи или обмена «товаром» участники этих сообществ также обсуждают напрямую посредством служб мгновенного обмена сообщениями, таких как MSN, ICQ, Yahoo Messenger и Jabber.

В число товаров, предлагаемых на продажу в нелегальной экономике, входит всевозможная информация. Спросом пользуются данные для создания аккаунтов, кражи личности и осуществления другой деятельности, полезной и необходимой для нелегального сообщества. Ассортимент предлагаемых товаров достаточно широк — от личных данных (фамилия и имя, адрес и т. д.) до банковских реквизитов и дампов баз данных с сотнями и тысячами наборов пользовательских данных. «Дампами баз данных» называют копии баз данных интернет-магазинов и форумов, где хранятся пользовательские данные - это один из самых востребованных и ликвидных товаров на рынке. Большим спросом также пользуются адреса так называемых «магазинов для кардеров». Это магазины, где из-за недостаточно тщательной проверки данных кредитных карт можно оплачивать покупки через Интернет краденными кредитками.

Большинство участников нелегальной экономики весьма озабочены сокрытием и маскировкой оставляемых ими в Интернете данных, по которым их можно отследить и установить личность.

Интернет-магазин, продающий кредитки, аккаунты PayPal и многое другое

Поэтому почти все посетители нелегальных форумов и сайтов пользуются прокси-серверами. Жители

Восточной Европы предпочитают пользоваться прокси-серверами, зарегистрированными в таких странах, как Германия, Нидерланды и Швейцария. С другой стороны, немецкие киберпреступники предпочитают использовать польские, российские и украинские серверы. Списки бесплатных прокси-серверов публикуются на разных сайтах сообщества, однако у таких серверов есть существенный недостаток — низкая скорость. Поэтому многие предпочитают использовать коммерческие прокси-серверы или систему Tor. Кстати, содержание "аномайзера" тоже хороший бизнес - главное не вести логов. :) А предлагаемый ассортимент услуг достаточно широк — от простых прокси-серверов, пригодных для анонимного веб-серфинга, до SSH-сокетов и OpenVPN, которые скрывают IP-адрес пользователя при использовании любых программ, включая программы для мгновенного обмена сообщениями (например, IRC или Skype).

Кражи личности и фишинг

Основными инструментами получения нелегальных данных являются компьютерные вирусы - до сих пор защитные комплексы стоят не более чем на половине компьютеров, подключенных к Сети с помощью фиксированного ШПД. Одни хакеры предлагают доверчивым пользователям доступ к порнографическому контенту и используют эксплойты для заражения их компьютеров. Другие рассылают вредоносные программы в виде вложений электронных писем — для заражения компьютера пользователю иногда достаточно открыть письмо или щелкнуть по ссылке. Многие троянские программы также распространяются через файлообменные сети под видом обычных программ, игр и др.

Сайт, где вредоносные программы предлагаются в качестве услуги

После установки троянская программа скачивает из Интернета исполняемый файл бота, после чего компьютер становится частью ботнета. После заражения компьютера обычно происходит следующее: данные, которые могут принести выгоду, копируются с компьютера и продаются. Данные учетных записей выставляются на продажу на черном рынке. После использования всех «полезных» данных компьютеры становятся ботами для рассылки спама или проведения DDoS-атак.

Товар	Мин. цена	Макс. цена
Средство удаленного администрирования — цена зависит от функциональных возможностей	20,00 €	100,00 €
Программа-вор — см. выше	5,00 €	40,00 €

Фальшивое удостоверение личности или водительские права — цена зависит от качества подделки	50,00 €	2500,00 €
Исполняемый файл бота — цена зависит от функциональных возможностей и от разработчика	20,00 €	100,00 €
Исходный код бота	200,00 €	800,00 €

Кстати, зараженные компьютеры можно «приобрести» оптом на нелегальных форумах. Цены зависят от места проживания злополучных владельцев этих компьютеров. Особо ценятся зараженные компьютеры в Западной Европе, Северной Америке и Австралии. Это объясняется наличием в этих странах хорошо развитой инфраструктуры Сети - высокая скорость, высокое проникновение доступа в Сеть, низкая увлеченность пользователей защитой своих компьютеров. Торговцы предлагают зараженные компьютеры партиями по 1000 штук. Однако мало кто из покупателей знает, что ботнеты в статическом состоянии редко выживают - для их нормального функционирования постоянно нужны "новообращенные" машины, поэтому бот из 10-20 тыс. машин без "подпитки" долго не протянет.

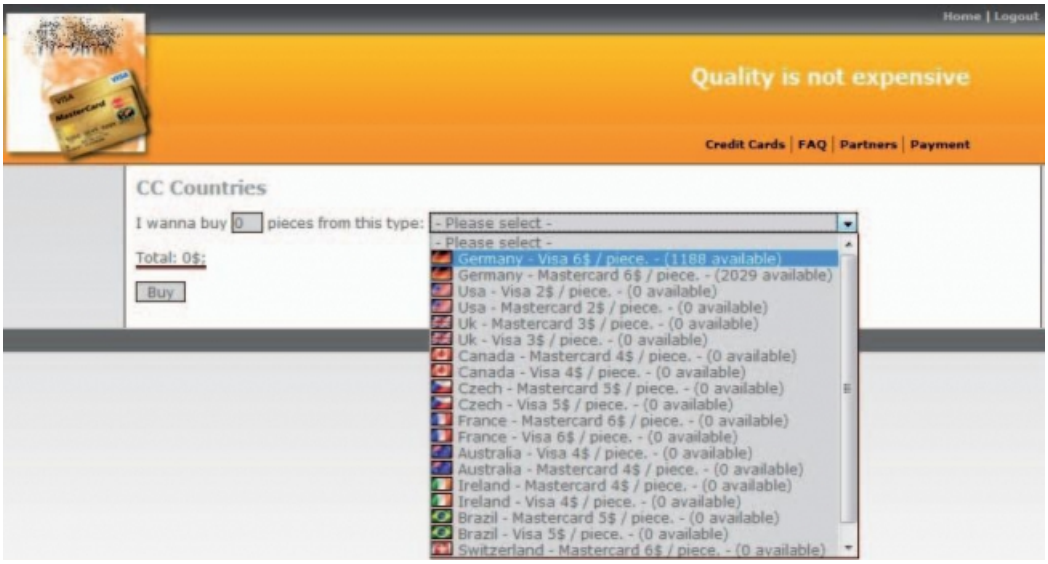
Услуга	Мин. цена	Макс. цена
Веб-хостинг — цена зависит от набора услуг (от небольшой веб-площадки до множества серверов)	5,00 €	9999,00 €
Шифрование вредоносных программ	10,00 €	40,00 €
DDoS-атака, почасовая стоимость	10,00 €	150,00 €
Боты, установленные на 1000 компьютеров — цена зависит от географического местоположения компьютеров	50,00 €	250,00 €
Рассылка 1 миллиона электронных писем на определенные адреса (например, особо ценятся адреса любителей игр)	300,00 €	800,00 €

Конечно же, почти каждый знаком с одним из аспектов существования нелегальной экономики, а именно со спамом (навязчивыми рекламными сообщениями). Среди киберпреступников спам весьма популярен, и не в последнюю очередь из-за возможности заработать неплохие деньги. Рассылка 1 миллиона электронных писем обходится владельцу ботнета в 250-700 долларов. Даже если использовать ботнет скромных размеров, состоящий из 20 тыс. ботов (компьютеров-зомби), и отправлять с каждого бота по 2 письма в секунду, то вся рассылка займет всего 25 секунд. Этим объясняется огромная заинтересованность владельцев ботнетов в их постоянном расширении путем добавления новых зараженных компьютеров. Списки электронных адресов можно запросто приобрести в интернет-магазинах на большинстве нелегальных форумов, а также у поставщиков услуг массовой рассылки. Такие списки обычно организованы по категориям или источникам. Продавцы нередко утверждают, что на предоставляемые адреса раньше никогда не отправлялся

спам. Однако это всего лишь означает, что данный список адресов еще не продавался, а вовсе не то, что эти адреса до этого никогда не использовались спамерами. :)

Данные	Мин. цена	Макс. цена
База данных — цена зависит от типа содержимого и степени наполнения; покупается вся база данных	10,00 €	250,00 €
Данные кредитных карт — цена зависит от полноты наборов данных. (Номера кредиток вместе с датами их истечения стоят недорого; чем полнее наборы данных, тем выше цена.)	2,00 €	300,00 €
1 миллион адресов электронной почты — проверенные адреса и адреса специальных групп стоят дороже	30,00 €	250,00 €

Интересно, что в 2010 г. вредоносные файлы содержались в 2,2% электронных сообщений, что в 2,6 раза больше, чем в 2009-м (тогда на вредоносные программы приходилось только 0,85% трафика). Массированные вредоносные рассылки, наблюдавшиеся летом и в начале осени 2010-го, во многом обусловили высокий процент вредоносного спама по итогам года. Пик таких рассылок пришелся на август. В 2011 году процент вирусов в спаме за год еще не подсчитан (поскольку год не кончился), но он явно превосходит показатели 2010 года.

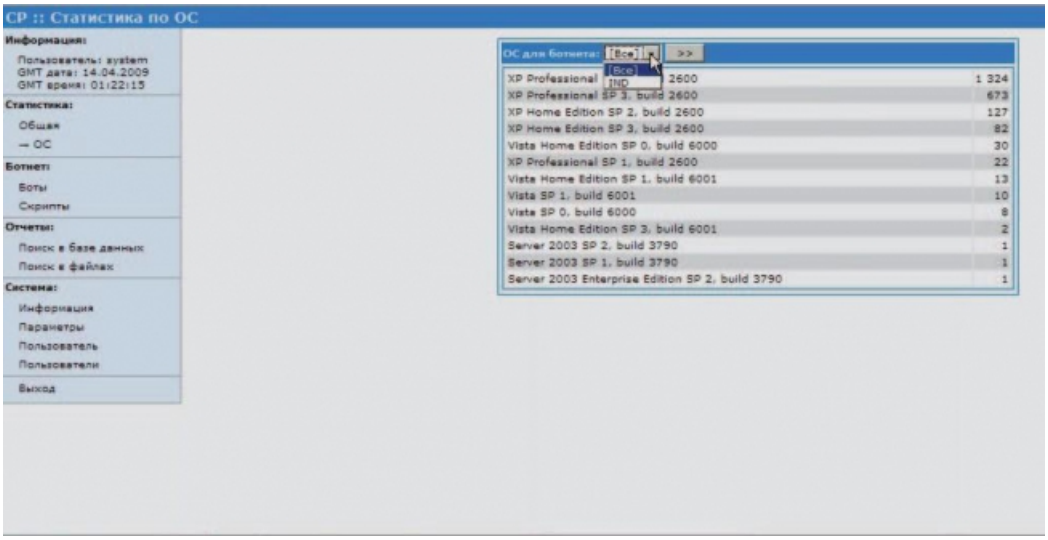


Интернет-магазин, где продаются данные кредитных карт

Правда, активность кибермошенников в прошлом году была притушена правоохранительными органами. Так, в начале 2010 г. была закрыта часть командных серверов ботнета, строящегося с помощью вредоносной программы Email-worm.Win32.Iksmas, также известной как Waledac. Летом прошлого года испанская полиция арестовала владельцев одного из крупнейших ботнетов — Mariposa, который был создан с помощью червя P2P-worm.Win32.Palevo. Червь распространяется через каналы пиринговых сетей, инстант-мессенджеры и с использованием функции autorun, т. е. через любые переносные устройства — от фотокамеры до флэшки. Основным способом "монетаризации" Palevo была продажа и использование персональных данных владельцев зараженных машин: логинов и паролей от различных служб, в первую очередь интернет-банкинга.

Осенью 2010 года прошли массовые аресты преступников, связанных с использованием вредоносной программы ZeuS. В конце сентября в США были арестованы 20 человек — выходцы из России, Украины и других стран Восточной Европы — денежных мулов, которые занимались отмыванием денег, украденных с помощью этого троянца. По схожему делу была захвачена группа лиц и в Великобритании. В середине октября была поставлена точка в истории еще одного весьма

известного ботнета, созданного при помощи троянской программы Bredolab. На самом деле говорить следует не об одном ботнете, а о нескольких, управляемых из сотни центральных серверов. Все они были отключены от Интернета в результате операции, проведенной голландской и французской киберполицией. На момент выключения ботнета его крупнейший сегмент состоял более чем из 150 000 зараженных машин. Часть "новообращенных" зомби-машин этих крупных ботнетов была навербована с помощью социальных сетей.



Веб-интерфейс ботнета

Но преступников это... конечно не остановило. :) В этом году их интересует полезная информация, которую можно добыть о пользователях в многочисленных социальных сетях. Современные вредоносные программы все больше нацелены на кражу пользовательских учетных записей от чего угодно: банковских и платежных систем, электронной почты, социальных сетей и т. д. Однако это далеко не всё и далеко не самое ценное, чем владеют пользователи. Уже сейчас представители нелегальной экономики эксплуатируют специальные шпионские программы - их интересует сам пользователь: его местоположение, работа, увлечения, знакомые, данные о его состоянии, семье, цвете волос и глаз и т. д. "Их будет интересовать каждый документ и каждая фотография, которая хранится на зараженном компьютере. Не правда ли, такой набор данных похож на то, что так стремятся заполучить социальные сети и продавцы интернет-рекламы? Эта информация действительно нужна всем, потенциальных покупателей таких данных — множество. Ее дальнейшее использование может быть весьма разнообразным, но, вне всякого сомнения, спрос на нее есть, и в будущем он будет расти", - говорится в отчете о глобальных вирусных угрозах от начала 2011 года, который был подготовлен экспертами Global Research&Analisys Team (GReAT) в сотрудничестве с подразделениями Content&Cloud Technology Research и Anti-Malware Research "Лаборатории Касперского".

Аккаунты (учетные записи)	Мин. цена	Макс. цена
Учетная запись Steam — цена зависит от количества установленных игр	2,00 €	50,00 €
Учетная запись игры World of Warcraft — цена зависит от полноты данных и от уровня персонажей	5,00 €	30,00 €
Учетная запись упаковочного пункта — цена зависит от полноты данных и от того, поддельные или краденые эти данные	50,00 €	150,00 €
Учетная запись PayPal — чем полнее набор данных, тем выше цена	1,00 €	25,00 €

Учетная запись Click & Buy — см. выше	10,00 €	35,00 €
Учетная запись электронной почты с частными письмами — цена зависит от продавца	1,00 €	5,00 €

Эти выводы подтверждают и специалисты G Data Security Labs. По их мнению, фишинг является не просто "все более популярным", а чуть ли не одним из основных направлений криминогенной активности. В нелегальном сообществе можно найти всё, что угодно. К примеру, просматривая нелегальные форумы, можно наткнуться на предложения о продаже аккаунтов Facebook и Twitter или их обмене на другие товары или услуги - правда, такой товар стоит не так уж и много. В российском сегменте Сети более интересны аккаунты социальных сетей с привязанными к ним платежными кошельками, которые не требуют отдельной авторизации для проведения платежей или вывода игровой валюты. Притчей во языцех стали атаки на системы дистанционного банковского обслуживания - они были отмечены в России на примерах системы "Телебанк" от ВТБ24 и "Альфа-Клик" от "Альфа-банк". А ведь "ловили" пользователей на банальные подставные страницы, "заманивали" на которые с помощью почтового спама. Глупо, конечно, постоянно говорить о том, что "каждый пользователь интернет-банкинга, социальной сети или иного интернет-сервиса должен оберегать свои личные данные и принимать разумные меры безопасности при их вводе или передаче". Но приходится повторяться. Разумного пользователя должно насторожить требование ввести слишком много транзакционных данных на (предполагаемом) сайте своего банка или отключенное шифрование при передаче данных. А еще проще сделать прямые закладки к своим банковским сервисам и переходить, для их использования, только по ним.

Как получить награбленное?

Какими бы разнообразными не были используемые средства и стратегии, все они, в конечном счете, предназначены для одной цели: заработать деньги для преступника. Ирония состоит в том, что украсть в киберпространстве данные не так сложно, как монетизировать свои усилия. Если вы, конечно, не работаете "на заказ". Во всех остальных случаях есть как проблемы со сбытом, так и с получением денег - именно поэтому в чести электронные системы "цифровой наличности", которые дерут с клиентов немыслимые в реальном мире комиссионные (т.н. "плата за риск"), а также можно найти множество полуфабрикатов для преступной деятельности. Вирусы, данные кредиток, базы данных и т.д. Их похищают на автомате, а вот спрос куда как ниже предложения.

Но как же вывести наличность? Исследователи из G Data Security Labs отмечают несколько основных способов для этого. Один из вариантов "отмывки" - загрузка и "откачка" денег из интернет-казино. Но это должен быть совсем "черный" сервис, чтобы его администраторы и служба безопасности ни о чем не догадались. :) Можно превратить виртуальные деньги в реальные так, чтобы было неясно, откуда они пришли. Во многих случаях через Интернет покупаются товары с использованием краденых данных кредитных карт или виртуальной валюты, заработанной рассылкой спама. Чтобы преступника не схватили при получении товаров, эти товары адресуют в так называемые «дроп-зоны» (англ. drop zone, букв. "зона сброса"). Получает их не сам преступник, а какой-нибудь посредник, обычно нанятый посредством спам-письма в качестве курьера или сотрудника по логистике, который сразу же отправляет полученные товары на другой адрес. Неудивительно, что дроп-зоны пользуются огромным спросом в преступном сообществе. Спрос, как известно, рождает предложение — подобные услуги можно в изобилии найти на нелегальных сайтах. Процесс всегда стандартный: после заказа товаров их отправляют на какой-то адрес в России или иной стране; полученные товары забирают с почты и отсылают на адрес настоящего получателя. А то и цепочка может быть куда как более длительной и, в итоге, приведет нас на практически анонимный абонентский ящик в крупном пересылочном пункте, где никто никого не помнит и за все платилось наличными.

Дроп-зоны, предлагаемые на форуме

Кроме того, используются комбинации вышеописанных приемов. Например, используется следующий способ: кибермошенник использует краденые данные кредиток для покупки товаров в интернет-магазине, а эти товары затем доставляются на абонентский ящик, данные доступа к которому были украдены у какого-то ни о чем не догадывающегося третьего лица. Мошенник забирает полученные товары, продает их на интернет-аукционе, а затем переводит деньги на свой частный и совершенно анонимный счет.

Уже давно прошли те времена, когда хакерское сообщество состояло в основном из юношей, использующих Интернет для забавы и удовлетворения своей технической любознательности. Термин «хакер» уже нельзя применять по отношению к представителям нового поколения участников этой нелегальной экономики. Это самые настоящие преступники, обладающие техническими знаниями и навыками в определенной области - ими движут корыстные мотивы, а обороты в этой «индустрии» исчисляются многими миллиардами долларов. Деньги либо крадутся у жертв, либо зарабатываются на спаме. Участники сообщества нередко являются членами профессионально организованных преступных группировок, где каждому отведена своя роль.

Стоит ли пугаться обычным пользователям? Пугаться, наверное, нет, а вот опасаться - вполне стоит. Обеспечение защиты персональных компьютеров от киберпреступников уже стало суровой необходимостью. Всякий, кто пользуется Интернетом, не защитив свой компьютер при помощи хорошего антивируса и файрволла (брандмауэра), рискует стать жертвой таких преступников. В наше время, когда интернет-аукционы и интернет-банкинг стали частью повседневной жизни, риски значительно возросли.