



«Русский» рынок компьютерных преступлений в 2010 году: состояние и тенденции

Москва, 2011

Этот документ подготовлен Group-IB исключительно в целях информации. Содержащаяся в настоящем документе информация получена из источников, которые, по мнению Group-IB, являются надежными, однако Group-IB не гарантирует точности и полноты информации для любых целей. Group-IB не несет ответственность за какие-либо убытки или ущерб, возникшие в результате использования любой третьей стороной информации, содержащейся в настоящем документе, включая опубликованные мнения или заключения, а также за иные последствия. Этот документ или любая его часть не может распространяться без письменного разрешения Group-IB либо тиражироваться любыми способами. Copyright © Group-IB

Оглавление

ВВЕДЕНИЕ	3
ОСНОВНЫЕ ПОЛОЖЕНИЯ.....	4
ВОПРОСЫ ТЕРМИНОЛОГИИ.....	5
ОБЩИЕ ТЕНДЕНЦИИ РАЗВИТИЯ РЫНКА КИБЕРПРЕСТУПНОСТИ.....	6
ОСНОВНЫЕ УГРОЗЫ	7
<i>Галопирующий рост DDoS-атак</i>	<i>7</i>
<i>Направленные атаки на финансовый сектор</i>	<i>7</i>
<i>Резкий всплеск случаев смс-мошенничества</i>	<i>8</i>
<i>Использование приемов социальной инженерии: новая волна</i>	<i>9</i>
<i>Целевые атаки на объекты критической инфраструктуры</i>	<i>9</i>
ОБЗОР АКТУАЛЬНЫХ УСЛУГ «РУССКОГО» РЫНКА КИБЕРПРЕСТУПНОСТИ	10
ОСНОВНЫЕ СОСТАВЛЯЮЩИЕ «РУССКОГО» РЫНКА КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ.....	10
БОТ-СЕТИ КАК ОСНОВНАЯ СОСТАВЛЯЮЩАЯ РЫНКА КИБЕРПРЕСТУПНОСТИ	10
БОТ-СЕТИ И ОСНОВНЫЕ УСЛУГИ РЫНКА.....	11
ПРОДАЖА ЗАГРУЗОК	11
ПРОДАЖА ТРАФИКА	12
ПАРТНЕРСКИЕ ПРОГРАММЫ И ЧЕРНЫЙ ФАРМБИЗНЕС.....	13
ДРУГИЕ УСЛУГИ, СВЯЗАННЫЕ СО СПАМОМ.....	13
ФИНАНСОВЫЕ ПОКАЗАТЕЛИ РЫНКА КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ	15
КИБЕРУГРОЗЫ 2011 ГОДА: ОСНОВНЫЕ ТЕНДЕНЦИИ.....	17
ЗАКЛЮЧЕНИЕ	18

Список таблиц и иллюстраций

Таблица 1. Цены на услуги по продаже 1000 загрузок.....	12
Рисунок 1. Способы оплаты покупок онлайн 2008-2010 гг., опрос RUметрики.....	8
Рисунок 2. Схемы извлечения прибыли из DDoS-атак, мошенничества в системах ДБО и рассылки спама с использованием бот-сетей.....	10
Рисунок 3. Схема продажи трафика.....	12
Рисунок 4. Схема онлайн-фармбизнеса.....	13
Рисунок 5. Прогнозируемые финансовые показатели российского и русского сегментов рынка киберпреступлений (в млрд долларах США).....	15

Введение

Данный отчет содержит результаты исследования состояния «русского» рынка компьютерных преступлений в 2010 году. В нем рассматриваются основные угрозы, связанные с различными видами хакерской активности, анализируются основные услуги, предлагаемые компьютерной мафией, даются оценки доли «русского» сегмента общемирового рынка киберпреступности, а также приводятся прогнозы относительно тенденций развития данного рынка в этом году.

Отчет был подготовлен аналитиками отдела расследования и специалистами лаборатории компьютерной криминалистики компании Group-IB при содействии экспертов Центра вирусных исследований и аналитики ESET и аналитиков компании LETA.

О компаниях

Group-IB (www.group-ib.ru) — первая в России и в странах СНГ компания, профессионально и комплексно занимающаяся расследованием обстоятельств компьютерных преступлений, нарушений информационной безопасности и компьютерной криминалистикой. Входит в LETA Group.

ESET (www.esetnod32.ru) — международный разработчик антивирусного программного обеспечения и решений в области компьютерной безопасности для корпоративных и домашних пользователей. Компания ESS Distribution, обладающая эксклюзивными правами на все продукты компании ESET в странах СНГ, входит в LETA Group.

LETA (www.leta.ru) — один из лидеров рынка информационной безопасности в России. Является первым российским оператором типизированных ИТ-услуг, обеспечивающим заказчикам комплексные решения в области информационной безопасности. Входит в LETA Group.

Основные положения

1. «Русский» рынок киберпреступности представляет собой рынок компьютерных преступлений, совершаемых как гражданами РФ, так и гражданами стран СНГ и Прибалтики, а также гражданами других стран мира, но являющимися выходцами из стран бывшего СССР. Российский рынок является составной частью «русского» и представляет собой рынок компьютерных преступлений, совершаемых исключительно гражданами РФ.
2. Расширение рынка и параллельное снижение цен на предлагаемые услуги привело в 2010 году к росту количества хакерских атак по всему миру и увеличению финансовых показателей.
3. Эксперты Group-IB оценивают финансовые обороты мирового рынка компьютерных преступлений в 7 млрд долларов, а долю российского сегмента рынка киберпреступности в 1,3 млрд долларов. Общие доходы всего «русского» рынка компьютерных преступлений составили сумму, превышающую первую почти в 2 раза. Находясь территориально в различных регионах и совершая свои атаки по всему миру, «русские» хакеры заработали в 2010 году около 2,5 млрд долларов.
4. При соответствующих факторах развития информационных технологий и рынка киберпреступлений можно спрогнозировать, что уже в текущем году «русские» хакеры заработают около 3,7 млрд долларов, а в 2013 году удвоят данный показатель. Приблизительно половина доходов «русского» сегмента рынка компьютерных преступлений будет приходиться на российских злоумышленников.
5. За 2010 год основными угрозами со стороны хакеров стали:
 - галопирующий рост количества и сложности DDoS-атак;
 - направленные атаки на финансовый сектор и рост инцидентов в системах ДБО;
 - резкий всплеск случаев смс-мошенничества на территории стран СНГ;
 - использование приемов социальной инженерии в целях хищения персональной информации и интернет-мошенничества;
 - целевые атаки на объекты критической инфраструктуры.
6. Для того чтобы снизить активность хакеров, действующих на территории СНГ и стран Балтии, необходимо регулярно проводить усовершенствование законодательной базы и повышение уровня компетенций правоохранительных органов, осуществляющих борьбу с преступлениями в сфере компьютерных технологий. Также важным фактором противодействия киберпреступникам является разработка и внедрение инновационных технических средств и решений, которые позволят реализовать проактивный отклик на выявленные инциденты и практически мгновенную реакцию на угрозы информационной безопасности.

Вопросы терминологии

Эксперты в области расследования компьютерных преступлений, используя общий термин «хакеры», предпочитают классифицировать компьютерных злоумышленников по роду их специфической деятельности, а также по национальной принадлежности.

В связи с последним обращает на себя особое внимание значительные расхождения в трактовке специалистами понятия «русские хакеры». Отечественные компьютерные криминалисты этим термином предпочитают называть злоумышленников-граждан РФ, осуществляющих свою преступную деятельность на территории нашей страны. В США и Европе под словом «русские» традиционно понимают не только граждан России, но также всех граждан и эмигрантов из стран бывшего СССР, которых объединяют общие история и язык. Данная особенность нашла свое отражение в трактовке западными специалистами термина «русские хакеры», когда им обозначают компьютерных злоумышленников, например, из Прибалтики, Украины или стран Средней Азии.

Поэтому одной из задач исследования является оценка не только рынка киберпреступности в России, но и анализ состояния всего «русского» сегмента общемирового рынка.

Итак, в дальнейшем в данном отчете под термином «русский» рынок киберпреступности будет пониматься рынок компьютерных преступлений, совершаемых как гражданами РФ, так и гражданами стран СНГ и Прибалтики, а также гражданами других стран мира, но являющимися выходцами из стран бывшего СССР. При анализе финансовых показателей данного сегмента будут учитываться не только преступления, совершаемые «русскими» хакерами на территории стран проживания, но и те, которые были совершены ими в других регионах мира.

Под термином российский рынок киберпреступности будет пониматься рынок компьютерных преступлений, совершаемых исключительно гражданами РФ. При анализе финансовых показателей данного сегмента будут учитываться только преступления, совершаемые российскими хакерами на территории РФ.

Общие тенденции развития рынка киберпреступности

В 2010 году можно выделить следующие общие тенденции развития рынка компьютерных преступлений:

- увеличение степени профессионализации его участников. С каждым годом приходится отмечать профессиональный рост хакеров, которые затрачивают значительные ресурсы для совершенствования преступных схем, методов и инструментов. Это, в первую очередь, связано с тем, что все больше участников рынка воспринимают свою преступную деятельность в качестве основного источника заработка.
- расширение рынка за счет появления новых участников. Возможность получить многомиллионный доход и отсутствие жесткого преследования хакеров в ряде стран мира порождают ежегодное увеличение численности участников рынка киберпреступности. В России ситуация дополнительно усугубляется большим количеством выпускников технических вузов и внутренней нестабильной экономической ситуацией, в результате которой упомянутая масса специалистов не может найти высокооплачиваемый легальный заработок.
- снижение цен на востребованные услуги. Появление новых участников ведет к росту конкуренции в этой отрасли, поэтому констатируется снижение цен и даже появление скидок для «оптовых» покупателей. Заказчикам могут предоставить тестовый период использования услуги и даже гарантии возврата денег.
- рост внутреннего рынка киберпреступности. Данный рынок охватывает так называемые услуги Cybercrime to Cybercrime. (C2C), когда хакеры оказывают услуги для своих же коллег. Например, при хищениях из систем дистанционного банковского обслуживания (ДБО) злоумышленники заказывают услуги у «нальщиков» (преступников, обеспечивающих обналичивание похищенных денежных средств). В качестве иного примера можно привести случаи, когда создатель вредоносного ПО заказывает у другого злоумышленника «загрузки». Данный рынок охватывает крупные движения денежных средств в различных платежных системах и требует особого изучения для понимания общей картины рынка киберпреступности.
- направленность на сверхмонетизацию. Период 2003-2009 был знаковым по переходу киберпреступности на 100% монетизацию ее деятельности. Прошедший год показал, что теперь злоумышленники нацелены в первую очередь на получение сверхприбыли. Так, в 2010 году специалистами Group-IB было зафиксировано единоразовое хищение посредством мошенничества в системе ДБО в размере 1 млн долларов. Параллельно преступники продолжили разработку схем, направленных на дальнейшую монетизацию собственной деятельности. Например, счета мобильных телефонов в 2010 году фактически стали одним из видов платежных систем, чем приковали к себе внимание киберпреступности. Как только появилась возможность монетизировать мобильный счет (перевод денег на пластиковые карты, монетизация через короткие номера с помощью смс-агрегаторов и другие типы вывода денежных средств) — появились соответствующие атаки (вирусы семейства Winlock, троянские программы для мобильных телефонов и т.д.).

Следствием вышеобозначенных тенденций является следующий факт — услуги, предлагаемые на рынке киберпреступности, стали более доступными, с чем связаны рост количества хакерских атак по всему миру и увеличение финансовых показателей. При этом рынок киберпреступности развивается по законам классического рынка: рыночное образование цен, монополии, конкуренция и т.п.

Основные угрозы

2010 год характеризуется активизацией компьютерных злоумышленников, а также продолжающейся профессионализацией данного рынка во всем мире. За исследуемый период основными угрозами со стороны хакеров стали:

- галопирующий рост количества и сложности DDoS-атак;
- направленные атаки на финансовый сектор и рост инцидентов в системах ДБО;
- резкий всплеск случаев смс-мошенничества на территории стран СНГ;
- использование приемов социальной инженерии в целях хищения персональной информации и интернет-мошенничества;
- целевые атаки на объекты критической инфраструктуры.

1. Галопирующий рост DDoS-атак

Помимо совершенствования технологий создания вредоносного программного обеспечения, в прошедшем году констатируется рост количества и сложности распределенных атак отказа обслуживания (DDoS-атаки). В 2010 году была зафиксирована DDoS-атака мощностью потока 100 Гбит/сек, которая является самой мощной атакой за все время наблюдений. Она в 2 раза превосходит самую мощную атаку в 2009 году. Другим примером, отражающим современную силу атак такого типа, можно назвать необычайно мощную атаку на известный сайт Wikileaks.

В прошлом году был поставлен абсолютный рекорд по суммарному объему DDoS-трафика, который превысил трафик за все вместе взятые года предыдущих исследований.

7

Одновременно с ростом сложности таких атак фиксируется снижение их стоимости. Поэтому теперь за подобными услугами на рынок киберпреступности обращаются не только крупные заказчики, но и не столь обеспеченные. Именно с данным фактом связан галопирующий рост количества DDoS-атак по всему миру.

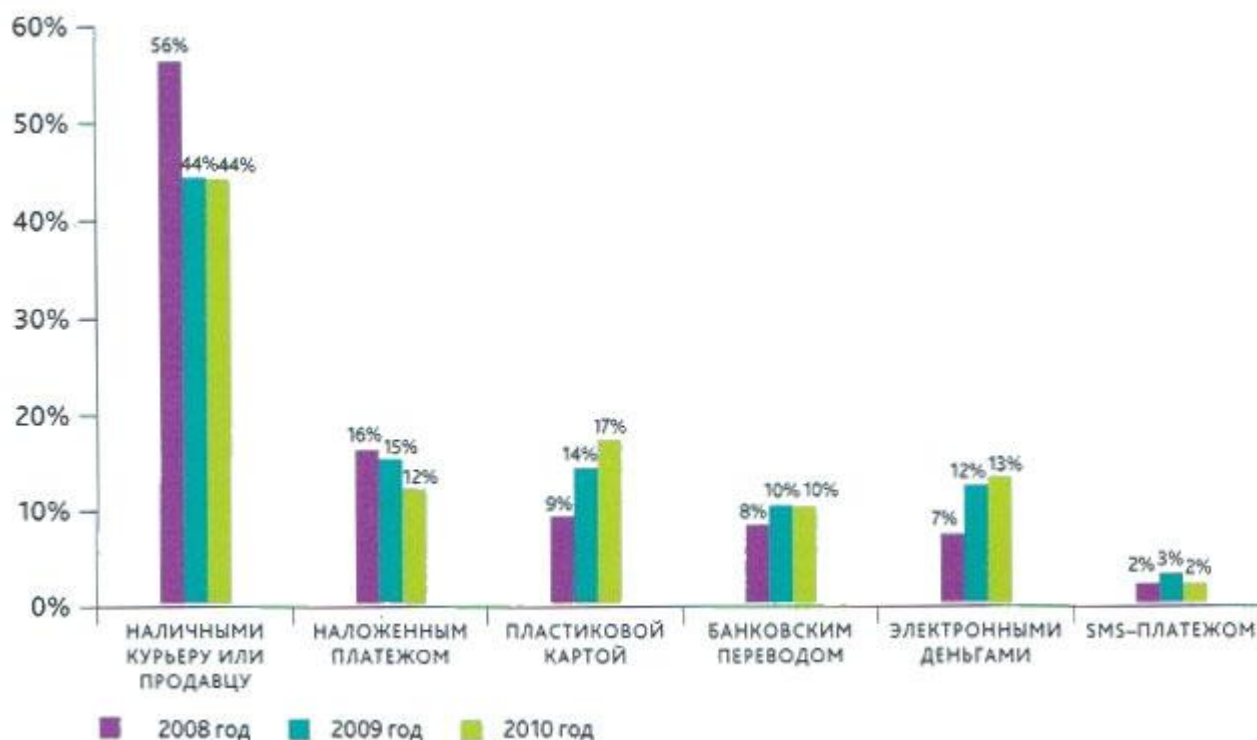
2. Направленные атаки на финансовый сектор

FinCEN (Департамент Казначейства США по борьбе с финансовыми преступлениями) обозначил тренд киберпреступлений в финансовой сфере как самый быстрорастущий — количество таких преступлений увеличилось на 115 % за 2010 год. Самым опасным признано мошенничество в системах ДБО. По ущербу мошенничество в ДБО в России в 2010 году стало лидером среди угроз информационной безопасности и фактически является угрозой для экономики РФ, банковской отрасли, среднего и малого бизнеса. Распространение банковских троянов и регулярные направленные атаки хакеров на финансовый сектор обусловлены возможностью получения многомиллионных прибылей. При этом под угрозой находятся денежные средства как юридических, так и физических лиц. Это связано с растущей динамикой использования систем интернет-банкинга и интернет-платежей. Несмотря на то, что лидерство среди методов оплаты покупок в Рунете еще принадлежит платежам наличными деньгами, эта категория неумолимо снижается в последние годы, что сопровождается ростом объема платежей пластиковыми картами и электронными деньгами. Это говорит о повышенной популярности электронной торговли.¹ Оплата банковскими картами уже сейчас показывает уверенный рост по сравнению с другими платежными инструментами. Банковская карта сродни мобильному телефону — это удобный, а

¹ Платежи банковскими картами — просто, быстро, удобно // Интернет в цифрах. № 4. 2010.

главное, массовый способ оплаты услуг. Распространение платежей в Интернете посредством банковских карт привлекают мошенников. Уже сейчас схемы кражи денег с банковских счетов весьма разнообразны: скимминг, шимминг, фишинг, вирусы и многочисленные способы мошенничества.

Рисунок 1. Способы оплаты покупок онлайн 2008-2010 гг., опрос RUMетрики



Источник: Интернет в цифрах. № 4. 2010

3. Резкий всплеск случаев sms-мошенничества

Всеобщее внедрение и распространение мобильной связи, привело к бурному росту преступлений в этом направлении. Рост новых технологий, таких как мобильный интернет, возможность перевести деньги со счета одного номера на счет другого, возможность пополнить счет практически в любом уголке страны, а также использование мобильной связи для оплаты различных услуг, привело к появлению новых методов отъема денег. Прошлый год характеризуется ростом так называемого sms-мошенничества. Применительно к сфере информационной безопасности следует отметить взрывной рост распространения вредоносного программного обеспечения, направленного на вымогательство денег у пользователя. Данное вредоносное ПО блокирует возможность пользоваться компьютером или делает его использование некомфортным (например, половина экрана закрыта изображением с требованием отправить sms на короткий номер). Разблокировать компьютер можно, только получив код, который направляется (и то не всегда) в ответ на отправку платной sms на короткий номер. Необходимо отметить, что данный вид мошенничества имеет ярко выраженный локальный характер и широко распространялся в 2010 году на территории стран СНГ. Это связано с тем, что в странах Запада отсутствуют контент-провайдеры, позволяющие функционировать подобным схемам, а антивирусные компании предоставляют интернет-сервисы для бесплатной разблокировки зараженных компьютеров.

Так же в качестве некоторых трендов можно отметить:

4. Использование приемов социальной инженерии: новая волна

Очередная важная тенденция мира киберпреступности в 2010 году обусловлена популяризацией социальных сетей. Более половины людей в мире младше 30 лет состоят в социальных сетях, а Facebook превзошел Google по объемам еженедельного трафика в США. Данный интерес к подобным сервисам со стороны пользователей привел к возникновению тенденции распространения вредоносного ПО и управления его установкой через популярные социальные сервисы. Механизм передачи инструкций вредоносным программам через системы мгновенной передачи текстовых сообщений знаком хакерам ранее, но массового характера внедрения этой методики фиксировать еще не приходилось. Например, криминалистами были обнаружены загрузчики вирусов, которые использовали сервис сообщений Facebook как средство отдачи указаний и контроля за установкой. Массовый характер заражений компьютеров приводит к эпидемиям, что позволяет хакером создавать многомиллионные ботнеты.

5. Целевые атаки на объекты критической инфраструктуры

В прошедшем году специалистами в области расследования нарушений информационной безопасности были зафиксированы беспрецедентные по сложности хакерские атаки, благодаря которым преступникам удавалось нанести урон ИТ-инфраструктуре крупных объектов национальных экономик. Инцидент, связанный с червем Stuxnet, был признан компьютерными криминалистами всего мира одним из самых дорогих и высокотехнологичных за всю историю создания вирусов. Это первый случай, получивший широкую огласку в СМИ, иллюстрирующий факт применения вирусов для осуществления диверсий и террористических атак. Исследования степени защищенности крупных промышленных объектов показали, что на данный момент уровень информационной безопасности предприятий стратегических отраслей не соответствует новым видам киберугроз. При этом состояние защиты российских предприятий значительно ниже, чем в среднем по миру.

Обзор актуальных услуг «русского» рынка киберпреступности

Основные составляющие «русского» рынка компьютерных преступлений

В рамках отчета выделены следующие составляющие рынка компьютерных преступлений России, представляющие наибольшую общественную опасность:

- DDoS-атаки: сетевые атаки, направленные на отказ в обслуживании;
- мошенничество в системах дистанционного банковского обслуживания (ДБО): неправомерная отправка электронных платежных поручений с целью хищения денежных средств;
- спам: массовая рассылка нежелательных сообщений электронной почты;
- продажа трафика: услуги по установке вредоносных программ на большое количество компьютеров и услуги по перенаправлению посетителей на определенные веб-сайты (относится к внутреннему рынку киберпреступности);
- партнерские программы (нелегальная продажа медикаментов, продажа контрафактного ПО, загрузок и т.п.) (относится к внутреннему рынку киберпреступности).

Рассматриваемые в отчете составляющие «русского» рынка киберпреступности взаимосвязаны:

- формирование бот-сетей непосредственно связано с продажей трафика;
- бот-сети используются для рассылки спама, осуществления DDoS-атак и мошенничества в системах ДБО;
- рассылка спама используется для продвижения услуг продаваемых через партнерские программы;
- DDoS-атаки часто осуществляются при проведении неправомерных электронных платежных поручений и т. д.

10

Бот-сети как основная составляющая рынка киберпреступности

Рассматриваемые составляющие «русского» рынка компьютерных преступлений, использующие бот-сети, можно представить в виде следующих схем услуг:

Рисунок 2. Схемы извлечения прибыли из DDoS-атак, мошенничества в системах ДБО и рассылки спама с использованием бот-сетей



Источник: Group-IB

DDoS-атаки, мошенничество в системах ДБО и рассылка спама как составляющие рынка компьютерных преступлений следует рассматривать с точки зрения формирования программной составляющей бот-сетей, окончательным формированием бот-сетей и извлечением прибыли из них.

Формирование программной составляющей бот-сетей можно представить в форме следующих услуг:

1. покупка вредоносного программного обеспечения, используемого на узлах бот-сети (цена подобного программного обеспечения: 3000 – 10000 долларов);
2. шифрование исполняемых файлов вредоносной программы для затруднения детектирования этой программы антивирусными средствами (цена подобной услуги: 20 – 30 долларов);
3. аренда серверов для управляющего центра бот-сети. Как правило, используются так называемые «абузоустойчивые» хостинг-провайдеры, которые лояльно относятся к наличию управляющих серверов бот-сетей на своих площадках (цены от 150 – 200 долларов).

Окончательное формирование заключается в расширении бот-сети за счет покупки установок вредоносных программ на компьютеры в сети Интернет для различных регионов, а также за счет участия в партнерских программах (участие бесплатное, стоимость трафика указана ниже).

Бот-сети и основные услуги рынка

11

Извлечение прибыли из сформированных бот-сетей происходит следующим образом:

- с помощью проведения DDoS-атак: оказание DDoS-услуг и шантаж угрозой DDoS-атаки (средняя цена DDoS-атаки: 70 – 90 долларов за сутки атаки по данным объявлений из открытых источников, 300 – 500 долларов за сутки атаки по данным объявлений на закрытых ресурсах; разница в ценах появляется из-за отличий в качестве оказываемых DDoS-услуг и сложности типовых задач);
- с помощью мошенничества в системах ДБО: неправомерная отправка электронных платежных поручений на крупные суммы денег, их вывод («залив») и легализация (средний ущерб от инцидентов подобного рода — от 70 до 100 тысяч долларов);
- с помощью рассылки спама: оказание услуг по рассылке спама с использованием баз адресов электронной почты и программ мгновенного обмена сообщениями, а также услуг по рассылке спама в социальных сетях (цена базы e-mail в 1 миллион адресов — 500 – 1000 долларов, стоимость 1000 аккаунтов в социальных сетях для рассылки спама — 30 – 50 долларов).

Продажа загрузок

Часто бот-сети используются для продажи загрузок программного обеспечения — в этом случае узлы бот-сети загружают программы, предоставляемые заказчиками (как правило, это троянские программы или блокираторы Windows). При этом загрузки в различных регионах мира имеют разные ценовые категории: наиболее дешевыми регионами считаются азиатские страны и Южная Америка, загрузки в странах Европы и в США стоят дороже. Услуги по продаже загрузок только в определенных странах пользуются большим спросом у злоумышленников, зарабатывающих на мошенничествах в системах ДБО, т. к. позволяют сформировать бот-сеть из компьютеров,

используемых в бухгалтерской деятельности в странах, для которых у злоумышленника есть готовые схемы вывода и легализации денежных средств.

Типовые цены на услуги по продаже 1000 загрузок («зараженных» компьютеров) в различных регионах мира представлены в Таблице 1.

Таблица 1. Цены на услуги по продаже 1000 загрузок

Регион	Цена
Азия	10 – 12 долларов
Южная Америка	10 – 12 долларов
США	100 – 140 долларов
Европа	70 – 130 долларов
Россия	20 – 40 долларов

Источник: Group-IB

Продажа трафика

Продажа трафика может осуществляться в форме продажи посещений веб-страниц для привлечения посетителей на различные веб-сайты (онлайн-магазины медикаментов, порносайты и т.п.) или для увеличения количества посетителей с уязвимыми версиями веб-браузеров, заходящих на страницы с эксплоитами, приводящими к загрузке и запуску вредоносных программ на пользовательских компьютерах (в том числе используемых для создания бот-сетей). Продажа посещений веб-страниц часто связана со взломом популярных интернет-порталов, на страницы которых внедряется код, перенаправляющий веб-браузер посетителя на страницу заказчика услуг по продаже посещений. Взломанные интернет-порталы продаются как ресурсы с установленными шеллами (скриптами для удаленного управления системой): стоимость 10 шеллов в среднем составляет от 900 до 3000 долларов.

12

Рисунок 3. Схема продажи трафика



Источник: Group-IB

Партнерские программы и черный фармбизнес

Данный вид киберпреступной деятельности специально выделен как отдельное направление в отрасли киберпреступности, ибо среди партнерских программ он был одним из первых и до сих пор сохраняет лидирующие роли. Черный фармбизнес заключается в перепродаже контрафактных медикаментов и медикаментов, реализация которых законодательно регулируется (медикаменты получают от более крупных онлайн-магазинов или реализуются непосредственно через партнерские программы). Существование фармбизнеса основано на рекламе виагры, стероидов и других медикаментов посредством рассылки спама, применением черных методов раскрутки (черная SEO) и привлечением посетителей онлайн-магазинов покупкой трафика, описанной выше. Спам-рассылка по базе объемом 10 миллионов адресов стоит около 350 – 1500 долларов. По подобной схеме можно организовывать любой тип незаконного бизнеса.

Рисунок 4. Схема онлайн-фармбизнеса



Источник: Group-IB

Другие услуги, связанные со спамом

Спам-рассылки активно используются киберпреступниками для увеличения продаж нелегального программного обеспечения (операционных систем, офисных программ и т. д.) и распространения вредоносного программного обеспечения в форме поддельных антивирусных программ и межсетевых экранов.

Поддельные антивирусные программы и межсетевые экраны используются для вымогательства денег у пользователя под видом платного удаления компьютерных вирусов или якобы для легализации обнаруженного нелегального программного обеспечения и различных аудио- и видеопроизведений. Зачастую принцип работы таких программ схож с работой блокираторов Windows — программа не позволяет пользователю продолжить работу с компьютером до совершения оплаты.

Не редко продвижение услуг, рекламируемых посредством спама, осуществляется с помощью партнерских программ: в рамках партнерских программ множество пользователей, не имеющих прямого отношения к рекламируемым услугам, независимо друг от друга производят рассылку спама, содержащего ссылки на товары и услуги, и получают доход, зависящий от количества привлеченных в онлайн-магазин клиентов.

Финансовые показатели рынка компьютерных преступлений

Рынок киберпреступности любой страны входит в состав ее теневой экономики, количественную оценку которой можно дать приблизительно, основываясь на косвенных фактах. Однако следует отметить, что благодаря обозначенной выше высокой активности злоумышленников и совершенствованию технологий и методов атак мировой рынок компьютерных преступлений показал в 2010 году впечатляющие темпы роста финансовых показателей.

В октябре 2010 года на конференциях Securing Our eCity и Digital Crimes Consortium были впервые озвучены представителями американских компетентных организаций предварительные оценки оборота киберпреступности в мире на 2010 год — около 6 млрд долларов. **Итоговое число эксперты Group-IB оценивают в 7 млрд долларов.**

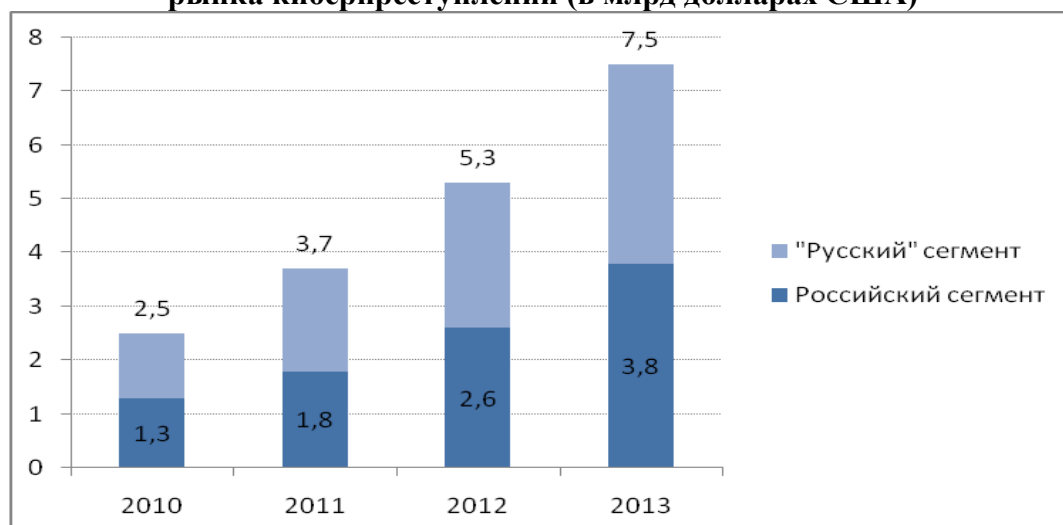
Стоит отметить, что рынок компьютерных преступлений, традиционно сосредоточенный на продаже похищенных банковских и карточных реквизитов, сменил свою основную бизнес-модель в 2010 году. Теперь на рынке представлен гораздо более широкий выбор похищенной конфиденциальной информации, предлагается изготовление фишинговых сайтов, аренда бот-нетов и даже услуги его администрирования.

Специалисты Group-IB оценивают долю **российского сегмента рынка киберпреступности в 1,3 млрд долларов**. Общие доходы всего «русского» рынка компьютерных преступлений составили сумму, превышающую первую почти в 2 раза.

15

Находясь территориально в различных регионах и совершая свои атаки по всему миру, **«русские» хакеры заработали около 2,5 млрд долларов**. Эта сумма включает в себя и доходы российского сегмента. Соответственно, на долю русскоязычных злоумышленников приходится до трети всех доходов от компьютерных преступлений в мире.

Рисунок 5. Прогнозируемые финансовые показатели российского и русского сегментов рынка киберпреступлений (в млрд долларах США)



Источник: Group-IB

Group-IB

107023, Москва, Мажоров переулок, дом 14, строение 2

+7 495 661-55-38

www.group-ib.ru

При соответствующих факторах развития информационных технологий и рынка киберпреступлений можно спрогнозировать, что уже в текущем году «русские» хакеры заработают около 3,7 млрд долларов, а в 2013 году удвоят данный показатель. Приблизительно половина доходов «русского» сегмента рынка компьютерных преступлений будет приходиться на российских злоумышленников.

Киберугрозы 2011 года: основные тенденции

Анализ мирового рынка киберпреступности и его «русского» сегмента позволяет спрогнозировать следующие основные тенденции в области киберугроз.

- В 2011 году основные атаки хакеров придутся на системы интернет-банкинга. Многомиллионные прибыли, получаемые преступниками в ходе такого мошенничества, заставят злоумышленников разрабатывать новые виды банковских троянов и совершенствовать механизмы бесследной кражи денег у клиентов банков.
- В этом году предполагается дальнейшее увеличение количества и мощности DDoS-атак. Цены на данную услугу на рынке компьютерных преступлений падают, что означает рост спроса на организацию таких атак. К тому же преступники зачастую используют DDoS-трафик при мошенничестве в системах ДБО, что в связи с общим трендом киберпреступлений также свидетельствует о дальнейшем росте количества подобных инцидентов.
- Растущая популярность социальных сетей и сервисов мгновенных сообщений способствуют дальнейшей эксплуатации преступниками методов социальной инженерии для распространения вредоносного ПО, что позволит хакером проводить лавинообразные заражения компьютеров доверчивых интернет-пользователей.
- Пример Stuxnet позволяет предположить появление в этом году подобных инцидентов, направленных на нанесение ущерба крупным промышленным объектам. Кибертерроризм и промышленный шпионаж с помощью информационных технологий становятся реальными угрозами, анализ которых требует серьезных усилий со стороны всего экспертного сообщества.
- Хотя экспертам приходилось и ранее сталкиваться с хакерскими атаками, вызванными политическими мотивами, хактивизм станет в этом году более популярным явлением. Если раньше хакеры в основном охотились за критически важными корпоративными данными, то с ростом хактивизма увеличатся случаи хищения политической информации и ее использования в целях дискредитации политических соперников. На примере фанатских волнений в Москве в конце 2010 года и революционных событий в странах арабского Востока в первом квартале 2011 года можно проиллюстрировать силу хактивистов, демонстрирующих общественно-политическую позицию в сети Интернет и побуждающих собственных сторонников к реальным протестным акциям.

Заключение

Несмотря на активное противодействие компьютерным злоумышленникам со стороны правоохранительных органов и специалистов в области пресечения и расследования нарушений информационной безопасности, рынок киберпреступности показал в прошедшем году активный рост, что отразилось в количестве преступлений и объемах прибыли, полученной хакерами. При этом на долю русскоязычных злоумышленников приходится до трети всех доходов от компьютерных преступлений в мире. Общемировой рынок киберпреступности характеризуется профессионализацией, расширением предоставляемых услуг и повышением их доступности, что приведет к увеличению ущерба от деятельности хакеров в 2011 году.

Особо следует отметить, резкий рост «русского» сегмента рынка компьютерных преступлений. Данный факт связан со слабостью законодательства и правоприменения в странах постсоветского пространства, высоким уровнем технического образования, языковой общностью и экономической нестабильностью.

Основываясь на данных IDC, рынок информационной безопасности составил в 2010 году около 13 млрд долларов. Для сравнения, мировой рынок компьютерной криминалистики составил всего 1,8 млрд долларов. Данная цифра в разы уступает финансовым показателям международной киберпреступности и ненамного опережает доходы российских хакеров.

Основа мирового рынка противодействия компьютерным преступлениям состоит в том, что все публичные компании обязаны объявлять о совершенных преступлениях против них. Это делается для защиты акционеров и правильной оценки рисков вложений в компанию. Соответственно для уменьшения этих рисков эмитенты вынуждены вкладывать деньги, как в технические, так и в организационные меры по расследованию преступлений.

18

В России власти пока не требуют такого подробного раскрытия информации. Но учитывая, что именно в России проблематика киберпреступлений носит особо острый характер, то необходимо ввести требования публичного информирования об инцидентах информационной безопасности. Введение подобного требования государством поможет резко улучшить системы защиты в российских корпорациях и заставит их внедрять системы расследований. К сожалению, без давления государства отечественные компании не хотят вкладывать средства в защиту, которая была бы адекватна актуальным киберугрозам. Пример Ф3-152 и СТО БР ИББС показывает, что именно прямые указания государства способны повлиять на рост уровня информационной безопасности.

Для того чтобы снизить активность хакеров, действующих на территории СНГ и стран Балтии, необходимо регулярно проводить усовершенствование законодательной базы и повышение уровня компетенций правоохранительных органов, осуществляющих борьбу с преступлениями в сфере компьютерных технологий. Также важным фактором противодействия киберпреступникам является разработка и внедрение инновационных технических средств и решений, которые позволяют реализовать проактивный отклик на выявленные инциденты и практически мгновенную реакцию на угрозы информационной безопасности. Ужесточение наказаний, активизация межгосударственной работы, привлечение к сотрудничеству отраслевых ассоциаций и популяризация фундаментальных политик информационной безопасности будут способствовать к снижению современных темпов роста «русского» рынка киберпреступности.