GROUP IB

РУССКИЙ РЫНОК КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ

СОСТОЯНИЕ И ТЕНДЕНЦИИ

2011

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Данный отчет содержит результаты исследования состояния «русского» рынка компьютерных преступлений в 2011 году. В нем рассматриваются основные угрозы, связанные с различными видами хакерской активности, анализируются центральные тенденции в развитии «русского» рынка киберпреступности, даются оценки доли и финансовые показатели «русского» сегмента общемирового рынка киберпреступности, а также приводятся прогнозы относительно тенденций развития данного рынка в этом году.

Отчет был подготовлен аналитиками центра реагирования CERT-GIB и специалистами лаборатории компьютерной криминалистики компании Group-IB.

О КОМПАНИИ

Образованная в 2003 году международная компания Group-IB (www.group-ib.ru) — российский лидер рынка расследования компьютерных преступлений, предоставляющий весь комплекс услуг от реагирования на инцидент до постинцидентного консалтинга. На базе Group-IB осуществляет свою деятельность CERT-GIB, единственный в России коммерческий центр круглосуточного реагирования на инциденты информационной безопасности. Входит в LETA Group.

«РУССКИЕ» ХАКЕРЫ: ВОПРОСЫ ТЕРМИНОЛОГИИ

В связи с последним обращает на себя особое внимание значительные расхождения в трактовке специалистами понятия «русские хакеры». Отечественные 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 понятием «русского» рынка 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 понятием 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.

РЫНОК КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ

Рынок киберпреступности любой страны является составной частью ее теневой экономики. На данном рынке можно выделить четыре основных направления:

1. **ИНТЕРНЕТ-МОШЕННИЧЕСТВО.** Включает мошенничество в системах дистанционного банковского обслуживания, фишинговые атаки, хищение электронных денег. Следует отметить, что в это направление входят и услуги по обналичиванию похищенных денежных средств (на данную услугу приходится доля, занимающая до 40 % от всего направления).

2. **СПАМ.** Включает не только услуги рассылки нежелательных сообщений электронной почты, но и партнерские программы по нелегальной продаже медикаментов, контрафактной продукции и поддельного программного обеспечения.

3. **ВНУТРЕННИЙ РЫНОК** (Cybercrime to Cybercrime или C2C). Включает услуги по анонимизации интернет-активности и продаже трафика, эксплойтов, вредоносного программного обеспечения и загрузок.

4. **DDOS-АТАКИ.** Включает услуги по организации атак, направленных на отказ в обслуживании.

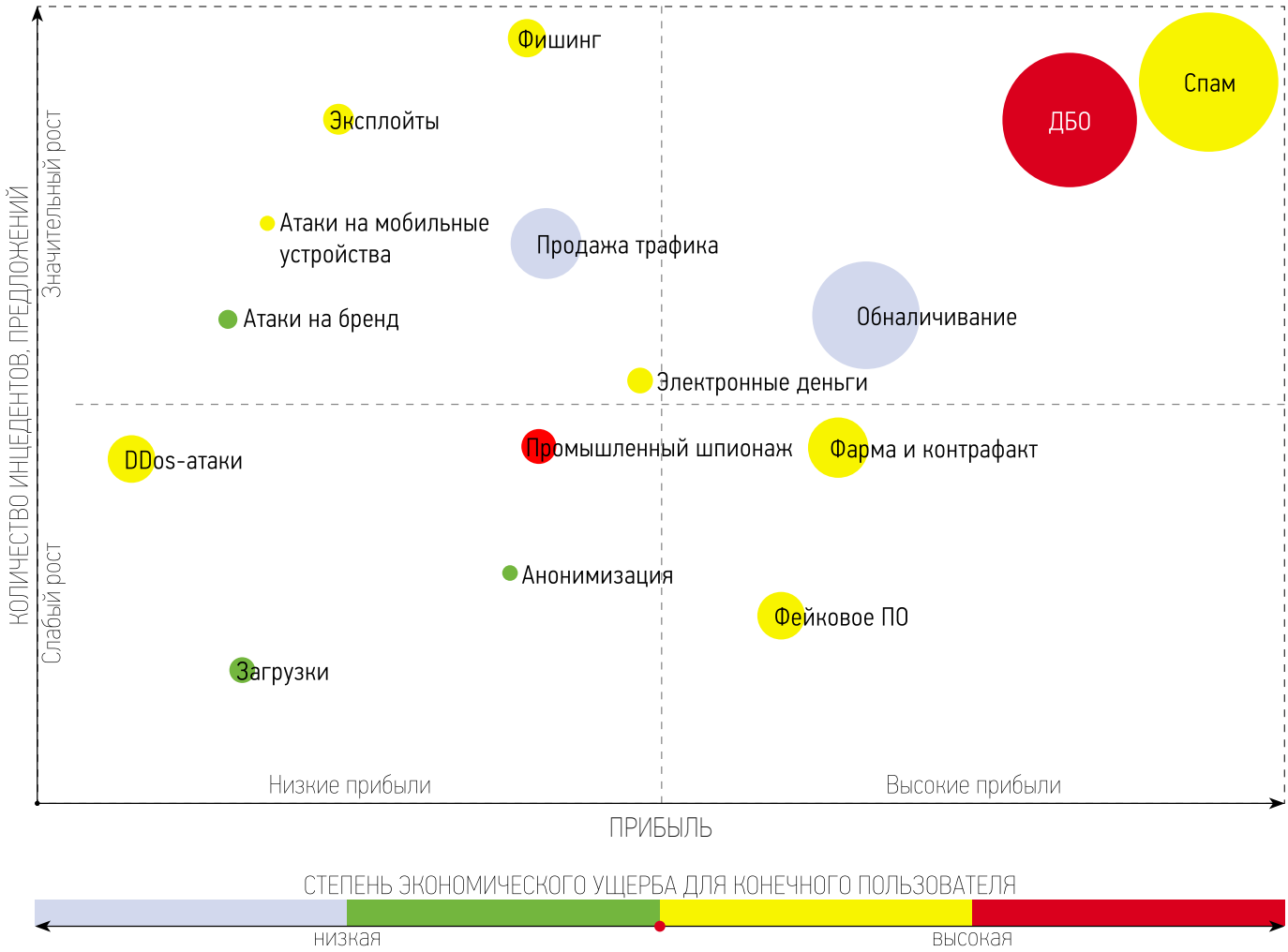
Помимо перечисленных направлений существует еще одно, которое включает услуги, не имеющие на сегодняшний день широкого спроса и предложения. Например, промышленный шпионаж, атаки на бренд, атаки на мобильные устройства и прочее. Это направление объединяет столь разные угрозы, что крайне сложно дать ему какое-либо единое название, поэтому в дальнейшем оно будет обозначаться как **«ИНОЕ»**.

РЫНОК КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ В РОССИИ: КОЛИЧЕСТВЕННАЯ ОЦЕНКА

Ниже представлены оценки рынка киберпреступности России по основным направлениям.

ТРЕНД	ДОЛЯ ОТ ОБЩЕГО ОБЪЕМА РЫНКА	СУММА
ИНТЕРНЕТ-МОШЕННИЧЕСТВО		
Мошенничество в системах интернет-банкинга	21.3 %	490 млн. $
Обналичивание денежных средств	16 %	367 млн. $
Фишинг	2.4 %	55 млн. $
Хищение электронных денег	1.3 %	30 млн. $
Итого:	41 %	942 млн. $
СПАМ		
Спам	24 %	553 млн. $
Медикаменты и различная контрафактная продукция	6.2 %	142 млн. $
«Поддельное» ПО	5.9 %	135 млн. $
Итого:	36.1 %	830 млн. $
ВНУТРЕННИЙ РЫНОК (C2C)		
Продажа трафика	6.6 %	153 млн. $
Продажа эксплойтов	1.8 %	41 млн. $
Продажа загрузок	1.2 %	27 млн. $
Анонимизация	0.4 %	9 млн. $
Итого:	10 %	230 млн. $
DDOS-АТАКИ		
DDoS-атаки	5.6 %	130 млн. $
Итого:	5.6 %	130 млн. $
ИНОЕ		
Иное	7.3 %	168 млн. $
Итого:	7.3 %	168 млн. $

На основании полученных данных была смоделирована матрица ***GIB Matrix***, отражающая состояние российского сегмента рынка киберпреступности:



Таким образом, анализ активности компьютерных преступников в 2011 году, проведенный аналитиками CERT-GIB, позволяет оценивать рынок киберпреступности в России в 2,3 млрд. долларов, что говорит о практически двукратном увеличении прошлогодних показателей.

Полученные данные позволили определить финансовые показатели «русского» рынка киберпреступности, который традиционно в два раза превосходит российский сегмент. Находясь территориально в различных регионах и совершая свои атаки по всему миру, «русские» хакеры заработали около 4,5 млрд. долларов. Эта сумма включает в себя и доходы российского сегмента.

Финансовые показатели мирового рынка компьютерной преступности в 2011 году эксперты Group-IB оценивают в 12,5 млрд. долларов. Оценка проводилась на основании данных, предоставленных нашими международными партнерами, а также опубликованных в открытых источниках.

ОБЩИЕ ТЕНДЕНЦИИ РАЗВИТИЯ

В 2011 году можно выделить следующие общие тенденции развития рынка компьютерных преступлений:

- Консолидация участников рынка, которая выражается в формировании ряда крупных киберпреступных группировок, функционирующих на постоянной основе. В итоге происходит отход от традиционной модели, которая основывалась на принципах дезорганизации, в пользу создания организованных групп с централизованной системой управления.
- Укрепление взаимосвязей между основными группировками, которое заключается во взаимовыгодном обмене скомпрометированными данными, предоставлении бот-сетей, схем обналичивания. Таким образом, возникают инциденты, в которых были задействованы сразу несколько киберпреступных групп, что создает определенные трудности при расследовании.
- Проникновение на рынок киберпреступности традиционных организованных преступных группировок, которые пытаются взять под свой контроль не только обналичивание похищенных денежных средств, но и весь процесс хищения. Подобная тенденция ведет к слиянию двух преступных миров и последующему перераспределению ресурсов из традиционных сфер контроля мафии (проституция, наркоторговля, незаконный оборот оружия и пр.) в пользу компьютерных преступлений. В условиях несовершенства существующего законодательства это, в первую очередь, грозит взрывным ростом атак на финансовый сектор экономики.
- Проникновение на рынок участников с низким уровнем технического образования. Таким образом, компьютерные преступления перестают быть уделом «технарей», так как требуют, в первую очередь, не специальных знаний, а капиталовложений. Появление данной тенденции привело к расширению

внутреннего рынка киберпреступности (C2C) и появлению на нем аутсорсинговых услуг (администрирование, обучение, консалтинг и т. д.).

- Рост и расширение внутреннего рынка. Данный рынок охватывает так называемые услуги Cybercrime to Cybercrime (C2C), предоставляемые на платной основе специализированными группами хакеров. Помимо традиционного роста объемов рынка данный год характеризуется становлением нового направления — ИТ-аутсорсинг.

Следствием вышеобозначенных тенденций является следующий факт: рынок киберпреступности в России переживает период динамического перехода от количественного состояния к качественному, что ведет к отходу от хаотической модели развития мира киберпреступности.

ОТРАСЛЕВЫЕ ТЕНДЕНЦИИ

1. Мошенничество в системах интернет-банкинга

Рост количества хищений. Как и предсказывалось в прошлогоднем отчете, 2011 год стал годом бурного роста данной отрасли киберпреступности. В основном этот рост обусловлен улучшением функциональности вредоносных программ, ориентированных на банковские системы, и формированием еще более устойчивых преступных групп, чей профессионализм и опыт росли с каждым месяцем и заработанным миллионом. В результате в декабре 2011 года крупнейшая «банковская» бот-сеть насчитывала около 2 млн компьютеров. Самыми крупными банковскими бот-сетями, которые успешно работали против российских банков, стали бот-сети, построенные на следующих вредоносных программах (расположены в порядке убывания в размере бот-сети):

- Carberp
- Hodprot
- Shiz
- Lurk
- Spy.Ranbyus
- Qhost

Удаленный доступ. Усиление мер защиты со стороны производителей систем ДБО и банков привело к тому, что для совершения успешного хищения злоумышленники начали активно экспериментировать со средствами удаленного доступа для проведения мошеннических операций прямо с компьютеров жертв. Наиболее успешными стали именно те преступные группы, в чьих руках оказался наиболее стабильный и удобный инструмент удаленного доступа. Для удаленного доступа злоумышленники использовали такие средства как TeamViewer, Hamachi, Mipko. Однако наибольшее распространение получил троян, который предоставлял доступ по протоколу Microsoft Remote Desktop.

Автоподмена и автозалив. С 2009 года Group-IB предупреждала об автоматической подмене реквизитов платежного поручения в момент подписания документа и его отправки, а также о возможностях полностью автоматизированного процесса формирования и отправки мошеннического платежного поручения вредоносной программой. Однако эти функциональные возможности начали активно использоваться только с осени 2011 года. Их появление позволяет преступникам избежать необходимости удаленного подключения либо копирования информации с пользовательского компьютера для обхода средств защиты (виртуальные клавиатуры, PIN-коды, VPN-туннели, сетевая фильтрация). Пока среди всех вредоносных программ, которые используются против клиентов российских банков, такой функциональностью обладает только «банковская» троянская программа Carberp.

«Благотворительность». Появление автоподмены и автозалива потребовало тщательного тестирования. Злоумышленники нашли идеальный способ: в течение нескольких месяцев они автоматически переводили по 1 рублю на счета разнличных благотворительных фондов или религиозных организаций. С помощью такой «благотворительности» новый способ мошенничества был успешно протестирован.

Физические лица. В 2010 году жертвами хищений в системах интернет-банкинга были в основном юридические лица, тогда как 2011 год стал годом всплеска хищений у физических лиц. Для данного вида хищений злоумышленники активно использовали техники веб-инжектов, а также троянские программы, перенаправляющие пользователя на фишинговый ресурс. В результате только за последний квартал 2011 года жертвами таких троянских программ стали десятки тысяч физических лиц, а общая сумма похищенных у них средств составила 73,5 млн. долларов.

Веб-инжекты. Эта техника широко известна и реализована во всех популярных «банковских» троянах уже давно. Однако активное его использование против клиентов российских банков началось только в 2011 году. Причиной начала использования веб-инжектов стал массовый переход от «толстого» клиента, когда на компьютер пользователя устанавливалась специальная банковская программа, к «тонкому» клиенту, когда все операции осуществляются через веб-браузер. Кроме того, хорошим стимулом для использования этой функциональности киберпреступниками стало увеличение количества физических лиц, использующих интернет-банкинг.

Фишинг. Банковский фишинг большого распространения в прошлом году не получил. После ликвидации в Москве в первом квартале 2011 года группы фишеров, использование такого рода атак практически не встречалось. Однако в конце лета эту же схему опробовала другая группа, которой удалось добиться неплохих результатов на преступном поприще. В результате ее деятельности ежедневно появляются как минимум 1–2 фишинговых ресурса, нацеленных на клиентов нескольких крупнейших банков.

Новые игроки. В апреле 2011 года прекратила свое существование бот-сеть, построенная на троянской программе Hodprot (классификация NOD32), работавшая с 2009 года. Вместо нее злоумышленники предпочли новую троянскую программу Carberp.

Многие эксперты в области ИБ заявляли, что к хищениям у клиентов российских банков причастны такие вредоносные программы, как Zeus и SpyEye. Но до конца 2011 года не было зафиксировано ни одного реального хищения с указанными вредоносными программами. Тем не менее, в ноябре–декабре 2011 года были обнаружены первые рабочие экземпляры Zeus и SpyEye, которые обладали модулями для работы именно с российскими системами интернет-банкинга. Исследование этих бот-сетей показало, что эти модули находились в стадии тестирования и активного распространения не получили. Мы предполагаем, что появление этих программ обязательно найдет свое отражение в 2012 году.

DDoS-атаки. Начиная с конца 2010 года количество DDoS-атак на банки после хищений больших сумм резко сократилось. Эта же тенденция продолжилась и в 2011 году. Она связана с тем, что проведение DDoS-атак стало служить сигналом для служб безопасности банков о совершенных хищениях. В результате мошеннические операции быстро обнаруживались и блокировались.

2. Спам

Партнерские программы[1]. Общие тенденции данной отрасли сохранялись на протяжении всего 2011 года.

- наиболее распространенный и наиболее простой способ монетизации спама — работа на партнерские программы;
- наиболее распространенный способ извлечения прибыли, применяемый партнерскими программами, — продажа контрафактной фармацевтической продукции;
- затем идут продажа контрафактного программного обеспечения (под видом лицензионного), продажа дешевых копий престижных аксессуаров (одежды, наручных часов и др.), реклама сайтов знакомств, в том числе и мошеннических, и т. д.;
- другой, менее популярный способ монетизации спама — продажа услуг по рассылке чужих сообщений различных категориям пользователей и сдача в аренду программного обеспечения, предназначенного для рассылки спама.

[1] Партнерская программа — организация, предлагающая пользователям (партнерам) за вознаграждение рекламировать веб-сайты, продающие определенные виды товаров или услуг. Вознаграждение каждого партнера, как правило, пропорционально стоимости товаров или услуг, купленных привлеченными им посетителями рекламируемых веб-сайтов. При этом партнерская программа обеспечивает каналы доставки товаров или услуг потребителям, возможность приема онлайн-платежей от пользователей (в том числе и по банковским картам), разработку шаблонов рекламируемых веб-сайтов и т. д.

При этом общий объем рассылаемого спама не меняется в результате закрытий отдельных партнерских программ или в результате невыполнения ими обязательств по выплатам спамерам, так как крупные игроки на этом рынке работают сразу на несколько партнерских программ и в случае возникновения проблем переключают свои ресурсы на другие программы.

3. DDoS-атаки

Количество и мощность атак. По сравнению с предыдущими периодами количество DDoS-атак в 2011 году выросло. Основными жертвами традиционно стали интернет-магазины и другие представители сферы онлайн-бизнеса. Однако следует отметить, что средняя мощность атак по сравнению с 2010 годом стала меньше, а для атак в основном использовались бот-сети численностью не более 10 000 узлов.

Политика. В 2011 году резко увеличилось количество «политических» DDoS-атак, которые осуществлялись с целью заблокировать определенные сайты СМИ, блоги и форумы. Это объясняется повышенной политической активностью в России в связи с парламентскими выборами и предстоящими выборами Президента.

Аресты. Летом 2011 года был произведен громкий арест Игоря Артимовича, выступившего исполнителем DDoS-атаки на крупную платежную систему Assist. Этот арест был широко освещен в прессе, благодаря чему общественность, наконец, узнала, что такое DDoS-атаки и чем они опасны, а заказчики и исполнители DDoS-атак убедились, что данное преступление может быть успешно расследовано. Следует отметить, что благодаря данному случаю правоохранительные органы получили ценный опыт в противодействии преступлениям такого рода.

Банковский спад. В 2011 году значительно уменьшилось количество DDoS-атак на банковские сайты и системы интернет-банкинга. Во-первых, это связано с их неэффективностью с точки

зрения проведения мошенничеств. Во-вторых, банки приложили значительные усилия для того чтобы обезопасить свою сетевую инфраструктуру, в частности и в области фильтрации «мусорного» трафика.

HTTPS. Новой тенденцией в 2011 году стали атаки по протоколу HTTPS, в предыдущие годы встречавшиеся достаточно редко. При проведении данного вида атак для достижения необходимого результата (отказ в обслуживании) необходим минимум ресурсов. А оборудование для фильтрации и отражения подобного вида атак имеет высокую стоимость и поэтому редко встречается в наличии у хостеров и интернет-провайдеров.

ПРОФАЙЛЫ CERT-GIB

В 2011 ГОДУ СПЕЦИАЛИСТАМИ КОМПАНИИ GROUP-IB И АНАЛИТИКАМИ ЦЕНТРА РЕАГИРОВАНИЯ CERT-GIB БЫЛИ ВЫДЕЛЕНЫ СЛЕДУЮЩИЕ ДЕЛА, В КОТОРЫХ ЦЕНТРАЛЬНУЮ РОЛЬ ИГРАЛИ ХАКЕРЫ, ВЫХОДЦЫ ИЗ РОССИИ И СТРАН СНГ.

ЛИЧНОЕ ДЕЛО

Хорохорин Владислав (a.k.a BadB)

Родился 29 сентября 1982 года в г. Донецке, Украина. Прописан в г. Москве. Постоянное место жительства: г. Нетания, Израиль. Гражданство: Россия, Украина, Израиль.

Владелец онлайн-магазинов, специализирующихся на продаже скомпрометированных данных пользователей банковских карт — Dumps.name и BadB.biz. Более 8 лет активного участия в кардинге.

BadB впервые привлек внимание USSS (Секретной Службы США) в 2003 году после ареста в Балтиморе американского кардера китайского происхождения — Жиана Пин Вона (Jian Ping Wong). Среди криминальных связей последнего агентами USSS был особо выделен некий BadB. Интерес USSS к BadB вспыхнул с новой силой после ареста Воа, он же Роман Вега, — духовного вдохновителя русскоязычного кардерского движения и одного из самых активных членов сообщества CarderPlanet. Среди данных, проанализированных агентами USSS, на компьютере Воа были обнаружены многочисленные упоминания о профессиональных мошеннических связях с BadB. Арест кардера Rdetty из Сиэттла в 2009 году и обнаружение на его компьютере дополнительной доказательной базы против BadB сподвиг американские спецслужбы к началу целенаправленных действий по отлову и нейтрализации BadB.

Выделенный агент внедрения USSS вышел на BadB, приобрел у него несколько партий скомпрометированных данных владельцев банковских карт американского и израильского происхождения, после чего провел ряд дополнительных оперативно-следственных мероприятий по закреплению полученной доказательной базы.

Эта информация была передана голландским властям для получения доступа к серверам веб-ресурсов Хорохорина, Dumps.name и BadB.biz, хостинг которых осуществлялся на территории Нидерландов. Полученные от голландцев копии дисков серверов

сайтов Dumps.name и BadB.biz были проанализированы и прикреплены к обвинительному заключению американского суда.

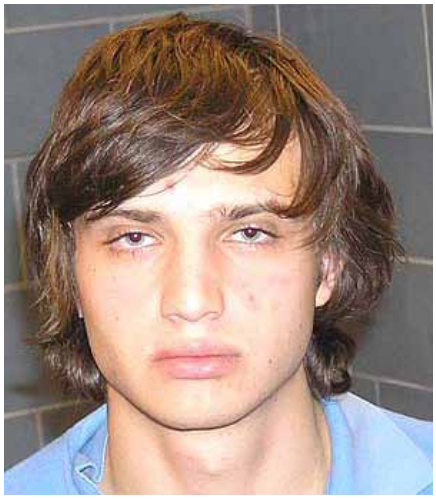
Кроме этого, американские спецслужбы заручились поддержкой израильских коллег для прослушивания личных телефонных переговоров и перехвата интернет-коммуникаций Хорохорина. Ранее аналогичные запросы были адресованы администрациям электронных почтовых служб Yahoo и Google с целью получения доступа к личной корреспонденции Хорохорина.

Обвинение, составленное на основании собранной информации, было представлено на суд присяжных в Американском суде округа Колумбия 12 ноября 2009 года. Вердикт суда был рассекречен только в августе 2010 с целью его направления французским правоохранительным органам. 7 августа 2010 года Хорохорин был задержан французскими пограничниками в аэропорту Ниццы перед самым вылетом в Москву.

Против Хорохорина выдвинуты обвинения в мошенничестве и в краже с отягчающими обстоятельствами. Если он будет признан виновным по обоим пунктам, то ему по совокупности грозит до 12 лет тюрьмы. Кроме того, каждое из этих двух обвинений подразумевает штраф в размере до 250 тысяч долларов.

На текущий момент Хорохорин содержится под стражей на территории Франции. Американские власти делают все возможное для его экстрадиции в США.

Юридические интересы Хорохорина представляет американское адвокатское бюро Bukh&Associates, которым руководит личный адвокат Хорохорина — Аркадий Бух, также представляющий интересы другого предполагаемого киберпреступника Олега Николаенко. Как и в случае с Николаенко, защита настаивает на выдаче Хорохорина российской стороне.



ЛИЧНОЕ ДЕЛО

Николаенко Олег (a.k.a Mega-D, Docent, King of Spam).

Родился 13 июля 1987 года (в некоторых используемых документах возможен подлог даты рождения: 13 июня 1985 года) в г.Рогань Харьковской обл., Украина. Прописан в г. Видном Московской области. Гражданство: Россия, Украина.

Предполагаемый администратор и владелец бот-сети Mega-D, также известной как Ozdok. Специализация бот-сети: рассылка спама. В период активности Mega-D располагал более 510 000 зараженными компьютерами (ботами). Операционная мощность на момент наибольшей активности: 10 млрд спам-сообщений в день, что составляло около трети всего мирового спама.

Олег Николаенко был арестован в Лас-Вегасе, США в ноябре 2010 года Федеральным бюро расследований по обвинению в нарушении закона США о борьбе со спамом (CAN-SPAM Act). Аресту Николаенко предшествовало задержание двух американских спамеров — Джоди Смита и Ланса Аткинсона, выдавших агентам ФБР ключевую информацию по мошеннической деятельности Николаенко.

ФБР обвиняет Николаенко не только в нарушении антиспам-законов, но и в пособничестве разнообразным мошенническим схемам, в основе которых лежало массовое использование почтовых рассылок: распространение контрафактной продукции широкой номенклатуры, а также нелегальных лекарственных и наркосодержащих препаратов.

На текущий момент Николаенко находится в г. Милуокки, штат Висконсин, США в ожидании судебного решения по предъявленным ему обвинениям.

По некоторым данным Олег Николаенко близок к сделке с американским правосудием на условиях выплаты крупного штрафа и выдачи российской стороне с возможностью отбывания наказания на территории Российской Федерации.

Юридические интересы Николаенко представляет американское адвокатское бюро Bukh&Associates, которой руководит личный адвокат Николаенко — Аркадий Бух.

ЛИЧНОЕ ДЕЛО

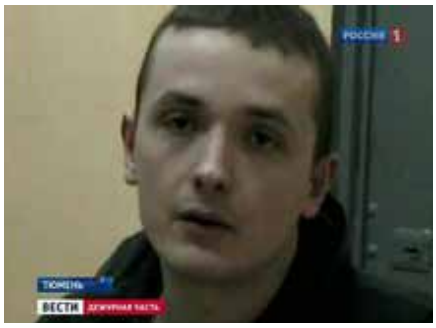
Аникин Евгений

Родился 2 ноября 1985 года рождения, уроженец г. Абакана, Республика Хакасия. Прописан в пос. Мошково Новосибирской области. Проживает в г. Новосибирске. В 2008 году окончил Новосибирский государственный университет. Гражданство: Россия.

Евгений Аникин входил в состав интернациональной группы хакеров, похитивших 9,5 млн долларов со счетов платежной системы WorldPay (процессинговое подразделение Royal Bank of Scotland). Идентификаторы к этим счетам были похищены путем взлома сервера в американском филиале Royal Bank of Scotland. Аникин с соучастником нашли группу лиц, занимающихся подделкой пластиковых карт. Этот же дуэт вербовал «кассиров» — исполнителей завершающего этапа мошеннической операции, которые осуществляли снятие денежных средств через банкоматы на территории разных стран и пересылку их в общий «котел».

Выпускник хакасского Института бизнеса и мехмата НГУ был задержан в Санкт-Петербурге вместе с подельником Виктором Плещуком. В северной столице против Аникина было возбуждено уголовное дело по факту хищения денежных средств (кража в особо крупном размере). После утверждения обвинительного заключения городской прокуратурой дело было направлено в Новосибирск для рассмотрения по существу. Дело по статье 158 УК РФ было рассмотрено 7 и 8 февраля Заельцевским районным судом Новосибирска.

Санкция статьи предусматривала до десяти лет колонии. Государственный обвинитель требовал до пяти лет лишения свободы, но подсудимый признал вину полностью и заключил соглашение о возмещении ущерба с потерпевшей стороной. Исходя из обстоятельств дела, суд приговорил Евгения Аникина к пяти годам лишения свободы условно.



ЛИЧНОЕ ДЕЛО

Глотов Максим (a.k.a “двуличный” хакер)

Родился 17 августа 1987 года в г. Богданович Сверловской области. Прописан в г. Богдановиче Свердловской области. Образование: окончил Российский профессионально-педагогический университет (РГППУ) по специальности «Прикладная информатика в экономике». Гражданство: Россия.

По версии следствия Андриан Степанов и Максим Глотов с августа 2007 года по май 2009 года совместно с другими лицами под различными псевдонимами, используя вредоносные программы, совершили неправомерный доступ к охраняемой законом компьютерной информации — аутентификационным данным 41 агента ЗАО «ОСМП» и ЗАО «Eport», которые использовались ими для доступа к лицевым счетам в системе электронных платежей.

Максим Глотов считается автором программы OSMP Grabber. Она устанавливается на компьютеры частных предпринимателей — владельцев терминалов ОСМП, и отправляет злоумышленнику реквизиты (номер терминала, имя пользователя, пароль) учетной записи агента в платежной системе ОСМП.

В последние годы программа приобрела широкую известность, «ванночки» с деньгами продавали на форумах со скидки до 80%. Их опустошение осуществлялось даже с помощью спамерских рассылок: «пополни счет мобильного телефона за 50%» с выводом WM через анонимные кошельки.

Регулярно получая несанкционированный доступ к чужим данным, Глотов с подельниками похищали денежные средства с помощью изменения информации агентов платежных систем. Подложные действия Глотова повлекли за собой несанкционированное списание с агентских счетов денежных средств на общую сумму более 10 млн. рублей.

Благодаря программе OSMP Grabber стала возможна схема залива денег не через традиционных «дропов» или подставных физических лиц-обнальщиков, а через юридических лиц. Таким образом, терминалы ОСМП использовались в качестве буфера в схеме обналичивания средств с чужих банковских карточек.

Первый раз Глотова задержали в Екатеринбурге на съемной квартире. На операцию по задержанию ушло несколько месяцев оперативной работы. Было принято решение не помещать Глотова под стражу, ограничившись подпиской о невыезде. Воспользовавшись этим, Глотов пришел на первое заседание суда, вышел в перерыв в коридор и скрылся.

Сначала Глотов уехал в Курск, а после в Тюмень, сделал пластическую операцию и подготовил поддельные документы на новое имя — водительское удостоверение и паспорт гражданина РФ. Повторно Глотова опознали и задержали в ноябре 2010 года.

Максим Глотов до и после хирургического вмешательства

На данный момент против Максима Глотова и Адрияна Степанова возбуждено уголовное дело №1-742/2011 по обвинению в мошенничестве и неправомерном доступе к компьютерной информации, а также в создании и распространении компьютерных вирусов и пособничестве при подделке паспорта и водительского удостоверения. Дело находится на рассмотрении в Железнодорожном районном суде г. Екатеринбурга.

Глотову грозит до 10 лет лишения свободы и крупный денежный штраф.

ЛИЧНОЕ ДЕЛО

Сабельников Андрей (a.k.a AndreSabre)

Родился 6 августа 1980 в г. Санкт-Петербурге. Прописан в г. Светлогорске Ленинградской области. В 2003 году окончил факультет вычислительных систем и программирования Санкт-Петербургского государственного университета аэрокосмического приборостроения. Гражданство: Россия.

23 января 2012 года компания Microsoft подала в один из судов штата Вирджиния иск против гражданина РФ Андрея Сабельникова, где обвиняла его в создании вредоносного программного обеспечения Kelihos. Kelihos — название бот-сети по классификации Microsoft, которая в «Лаборатории Касперского» называется Hlux.

В иске указывается, что Сабельников использовал вирус с целью контроля, поддержания и развития огромной бот-сети. Старший юрист отдела Microsoft по борьбе с киберпреступлениями Ричард Боскович указывает, что их обвинения основываются на данных, полученных при анализе кода Kelihos.

Бот-сеть Kelihos использовалась для незаконного получения личных данных, расположенными более чем на 41 000 компьютеров по всему миру, также с его помощью в огромных количествах рассылались спам-сообщения и проводились DDoS-атаки. До сентября 2011 года бот-сеть рассылала примерно по 3,8 млрд спам-сообщений в сутки.

Kelihos — это работающий по принципу peer-to-peer бот-сеть, состоящая из нескольких уровней, которые включают в себя узлы разных типов: маршрутизаторы (компьютеры, командующие ботами и контролирующие динамику структуры пиринговой сети), контроллеры (инфицированные компьютеры, чей публичный IP-адрес используется ботом для рассылки спам-сообщений, получения адресов электронной почты и «вылавливания» приватной информации о пользователе в сетевом потоке), а также рабочие узлы.

Питерский фотограф-любитель Андрей Сабельников попал в поле зрения специалистов по безопасности после того, как вы-

яснилось, что Kelihos подгружает необходимые данные с зарегистрированного на Сабельникова домена sabelnikov.net (в настоящее время сайт на этом домене не работает).

Сабельников на данный момент является внештатным программистом в одной из консалтинговых компаний, однако до недавнего времени он работал софтверным инженером и проектным менеджером в российской компании Agnitum, специализирующейся на разработке межсетевых экранов, антивирусов и защитного программного обеспечения и кроме всего прочего выпускающей известный межсетевой экран Outpost Firewall Pro. Также в Microsoft сообщают, что выйти на Сабельникова удалось благодаря показаниям Доминика Александра Пьятти, жителя Чехии, владельца хостинговой компании dotFREE Group, которая оказалась причастна к регистрации 3723 доменов в зоне cz.cc, использовавшихся для управления бот-сетью. Пьятти согласился сотрудничать со следствием, чтобы избежать судебного преследования.

Сам Сабельников отрицает свою причастность к незаконным действиям, указанным в заявлении Microsoft, о чём он также упоминает в своём блоге http://sabelnikov.livejournal.com/.

На текущий момент бот-сеть Kelihos активна и, используя незначительно измененную схему работы, продолжает вредоносную активность.

АТАКА НА ASSIST

Также в 2011 году началось первое в России дело, когда в организации DDoS-атак были выявлены предполагаемые исполнитель и организатор. Ущерб от нападения хакера на процессинговую компанию Assist, от которого пострадала авиакомпания «Аэрофлот», превышает 1 млн. рублей.

25 июня 2011 года основатель процессинговой компании ChronoPay Павел Врублевский арестован по подозрению в организации DDoS-атаки на конкурента. Ранее в июне 2011 года сотрудники ФСБ арестовали Игоря Артимовича, подозреваемого в техническом исполнении DDoS-атаки на серверы компании Assist. Артимович признался в содеянном и дал обвинительные показания о причастности Врублевского к этому правонарушению.

Санкцию на арест Врублевского выдал Лефортовский суд Москвы по ходатайству Следственного управления ФСБ России. «Суд постановил избрать в отношении Врублевского, 1978 года рождения, меру пресечения в виде заключения под стражу», – заявила агентству РАПСИ пресс-секретарь суда Надежда Савенко.

В декабре 2011 года Врублевский был выпущен из СИЗО и в настоящее время находится под подпиской о невыезде.

По версии следствия, Врублевский в 2010 году организовал DDoS-атаку на сервера процессинговой компании Assist, что привело к блокировке платежной системы, а ее клиенты не могли приобрести билеты на сайте «Аэрофлота». По данным «Аэрофлота», атака началась 16 июля 2010 года, и компания смогла возобновить продажи электронных билетов только через семь дней. Таким образом Врублевский хотел дискредитировать Assist, считают в ФСБ. Его компания ChronoPay также претендовала на заключение выгодного контракта с «Аэрофлотом» по продаже электронных авиабилетов и пыталась избавиться от конкурента, однако поставленных целей Павел Врублевский не добился, так как «Аэрофлот» подписал контракт с Альфа-Банком.

Это первый случай в России и во многих других странах мира, когда в деле фигурируют и предполагаемый исполнитель, и предполагаемый организатор DDoS-атак.

КОМПЬЮТЕРНЫЕ ПРЕСТУПЛЕНИЯ В РОССИИ: ВОПРОСЫ ЮРИДИЧЕСКОГО ПРОТИВОДЕЙСТВИЯ

В настоящее время преступления в сфере компьютерной информации имеют широкое распространение на всей территории Российской Федерации, стран СНГ и мировых держав.

Немаловажную роль в создании препятствий для предотвращения и расследования данных видов преступлений играет наличие определенных пробелов в системе российского законодательства. В отличие от других стран, в законодательстве которых используется четкий понятийный аппарат и прописаны жесткие санкции за совершение компьютерных преступлений, наше законодательство требует значительного совершенствования. Также следует отметить, что за рубежом большое внимание уделяется обучению сотрудников правоохранительных органов и судей основным вопросам сферы информационных технологий и безопасности, что позволяет им самостоятельно выносить суждения по тем или иным аспектам компьютерных преступлений.

В итоге из-за несовершенства правовых норм Российской Федерации, отсутствия жестких санкций, устойчивой правоприменительной практики и систематического повышения квалификации по вопросам противодействия компьютерным преступлениям злоумышленники несут ответственность несоразмерную совершенным деяниям.

Например, Евгений Аникин и Виктор Плещук, взломавшие компьютерную систему американской корпорации RBS WorldPay и похитившие со счетов 10 миллионов долларов, были признаны российским судом виновными, но приговорены только к условным срокам. В то время как за совершение общеуголовных преступлений, например, за хищение с нанесением ущерба на сумму 10 000 – 50 000 рублей, осужденные отбывают реальные сроки в местах лишения свободы.

В настоящее время идет разбирательство по делу, связанному с DDoS-атакой на сайт процессинговой компании Assist. В итоге понесенный ущерб составил более миллиона рублей. В ходе следствия был установлен предполагаемый заказчик атаки, который дал признательные показания в организации хакерской атаки.

Суд санкционировал его арест. Размеры ущерба и упущенной выгоды в данном случае превышают размер особо крупного ущерба по преступлениям против собственности. Однако, несмотря на это, позднее мера пресечения была заменена на подписку о невыезде.

Приведенные выше примеры показывают, что законодателями и, соответственно, судебными органами не осознается вся глубина и опасность преступлений в сфере компьютерной информации.

Президентом Российской Федерации Дмитрием Медведевым был внесен на обсуждение проект Федерального закона «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации». Данный проект был принят Государственной думой РФ 17.11.2011 г., и Федеральным законом от 07.12.2011 г. №420-ФЗ введен в действие. Вышеуказанный закон затронул, в том числе, статьи Главы 28 Уголовного кодекса РФ.

Среди наиболее значимых изменений этой части Кодекса, принятие которых положительно скажется на эффективном противодействии преступлениям в сфере компьютерной информации, следует выделить внесение дополнительных квалифицирующих признаков и увеличение тяжести санкций. Вместе с тем поправки в Главу 28 УК РФ были внесены без учета мнения специализированных правоохранительных органов (имеющих опыт расследования преступлений в сфере компьютерной информации) и отраслевых организаций, в связи с чем имеют ряд спорных моментов.

Для усиления противодействия организованной компьютерной преступности со стороны российских правоохранительной и судебной систем предлагается реализовать:

1. Внести в законодательную базу дополнительный понятийный аппарат, связанный с вопросами информационной безопасности и информационных технологий. Например, необходимо внести (возможно, под иным наименованием) понятие «бот-сеть», которое является и в ближайшем будущем будет

оставаться основным инструментом совершения большинства преступлений в сфере информационных технологий.

2. Изменить существующее в УК РФ понятие «компьютерная информация», которое не отражает в полной мере сущности компьютерной информации. Таким образом, возникает возможность неверной трактовки понятия.
3. Ужесточить санкции за совершенные преступления с использованием компьютерных технологий.
4. Внести изменения и дополнения в уголовно-процессуальное законодательство:

   a. Внести понятие «цифровые доказательства», описать процедуры и процессуальные действия, связанные с их получением, закреплением, исследованием и др.

   b. Выделить в отдельное определение место совершения преступления в сфере компьютерной информации и установить определенное место расследования данного вида преступлений.
5. Организовать на федеральном и региональном уровнях программы повышения квалификации для судебных, прокурорских, следственных и правоохранительных органов, в рамках которых проводить семинары по вопросам, связанным с расследованием преступлений в сфере компьютерной информации.
6. Разработать и внести на рассмотрение ООН документ, устанавливающий принципы международного взаимодействия против преступлений в сфере информационно-коммуникационных технологий и компьютерной информации, и в то же время в отличие от Будапештской конвенции отстаивающий суверенитет государств-участников.

Реализация данных мер позволит существенно повысить степень раскрываемости преступлений в сфере компьютерной информации, изменить существующую правоприменительную практику и наладить должное международное взаимодействие в данной сфере.

РЫНОК КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ В РОССИИ: ПРОГНОЗЫ НА 2012 ГОД

Анализ рынка киберпреступности в России в 2011 году позволяет спрогнозировать следующие основные тенденции его развития.

Мошенничество в системах интернет-банкинга

Рост. В 2012 году мы по-прежнему прогнозируем рост атак на системы интернет-банкинга, так как данная область деятельности продолжает приносить преступникам сверхприбыли. Но в отличие от 2011 года этот рост будет прерывистым и в основном обеспечен хищениями у физических лиц. Начиная со второго квартала 2012 года и до конца лета, мы прогнозируем постепенный спад по количеству хищений. Это будет обусловлено заменами игроков и используемых вредоносных программ по направлению мошенничества в системах интернет-банкинга.

Автоподмена и автозалив. Именно эта техника должна стать доминирующей в 2012 году совместно с использованием веб-инжектов.

Замена вредоносных программ. Учитывая текущее состояние и уровень развития преступных групп вредоносная программа Carberp потеряет свои лидирующие позиции, но, возможно, появятся ее клоны, как это было ранее с программой Zeus. Кроме этого, на рынке появятся и новые игроки с новыми троянскими программами, которые при должном уровне развития займут свою нишу в российском сегменте хищений в системах интернет-банкинга.

Фишинг. Как показала практика, работа с фишиновыми ресурсами является трудоемкой задачей, однако даже люди с небольшой квалификацией и маленьким стартовым капиталом могут развить это направление до еще более крупных масштабов. В итоге, эта схема может стать очень популярной и количество людей вовлеченных в нее будет неуклонно расти.

Спам

Рост. Объем рассылаемых нежелательных сообщений будет расти, при этом отключение управляющих серверов бот-сетей, используемых для рассылки спама, приведет лишь ко временному уменьшению количества рассылаемых сообщений.

Стабильность. Наиболее крупные «подпольные» партнерские программы не прекратят свое существование и не будут вытеснены более мелкими игроками.

DDoS-атаки

Фильтрация трафика. В 2012 году «ботоводы» встретятся с определенными сложностями – значительная часть «мусорного» трафика будет блокироваться, не доходя до предполагаемой жертвы, так как на промежуточных узлах появляется все больше фильтрующего оборудования, анализирующего трафик.

Жертвы. Продолжит рост количество атак на ресурсы, использующие HTTPS-протокол. Наиболее частыми жертвами останутся все те же ресурсы, связанные с онлайн-торговлей. А DDoS-атаки в банковской сфере, вероятно, окончательно сойдут на нет из-за их низкой эффективности.

GROUP IB

107023, Russia, Moscow,
Mazhorov lane, house 14,
building 2.
Tlf.: +7 (495) 661-55-38
E-mail: info@group-ib.ru
www.group-ib.ru