Автор: Артур Скальский © Lenta.Ru ИНТЕРНЕТ , МИР 4023 10.10.2004, 18:41 431

Борьба с преступлениями, совершаемыми с использованием сети Интернет. Доклад Управления "К".

Развитие информационной инфраструктуры, широкое внедрение современных автоматизированных систем управления и связи, обработки и хранения информации является неотъемлемым атрибутом современной России. Однако, столь положительные тенденции имеют и обратную сторону. В России, как и во всем мире, нарастает криминальная активность в информационной сфере.

При этом объектами преступных посягательств являются и информация, и информационно - телекоммуникационные ресурсы, и непосредственно финансовые средства, доступ к которым возможен через глобальные компьютерные сети.

В 1997 г. в Российской Федерации была введена уголовная ответственность за преступления в сфере компьютерной информации, а в 1998 г. – в МВД России создано специальное подразделение по борьбе с преступлениями в сфере информационных технологий. В настоящее время задачи по выявлению и пресечению данных преступлений решаются Управлением "К" ГУСТМ МВД России и подразделениями "К" в субъектах Российской Федерации. На настоящий момент данные специализированные подразделения работают в 81 регионе России.

Анализ криминальной обстановки показывает, что ежегодно количество выявленных органами внутренних дел преступлений в сфере информационных технологий увеличивается в 1,8-2 раза. Если в 1997 г. в России было выявлено только 17 преступлений такого рода, то в 2003 г. их число превысило десять тысяч (10920).

В 1-ом полугодии 2004 г. по материалам подразделений "К" возбуждено 1673 уголовных дела, что на 45 % больше, чем за аналогичный период прошлого года. Количество выявленных преступлений возросло почти на 6% и составило – 4295 против 4057 в прошлом году.

Качественный анализ работы территориальных подразделений показывает следующие результаты: из (1673) уголовных дел, возбужденных по материалам наших региональных подразделений за прошедшее полугодие – 55% (935 у/д) составляет неправомерное использование сетевых реквизитов при авторизации в сети Интернет, 10,6% (177 у/д) – компьютерное пиратство (распространение контрафактной программной продукции в том числе с использованием сети Интернет), 8% (137 у/д) – распространение порнографии включая детскую, 4,1% (67 у/д) составляют распространение вредоносных программ как в сети, так и на машинных носителях, включая контроллеры ЭВМ, остальные категории преступлений, такие как фрикинг, телефонное пиратство 3%, кардинг (мошенничества с пластиковыми картами) 1,5%, разглашение сведений ограниченного доступа 2,4%.

Анализ личности выявленных преступников даёт следующие результаты: 16,3% - лица до 18 летнего возраста, 58,9% - от 18 до 25 лет. Таким образом, свыше 75% выявленных преступников составляет молодежь. Следует отметить, что 67% от общего числа преступников имеют высшее или неоконченное высшее образование, что говорит о высоком интеллектуальном уровне противодействующей стороны.

По мнению МВД России в целом сложившаяся ситуация спровоцирована расширением российского сегмента глобальной сети Интернет, существенным увеличением числа пользователей. При желании любой человек имеет возможность получить в сети Интернет готовую вредоносную программу или так называемый "конструктор вирусов", чтобы самостоятельно создать новую. Подобные преступления носят скоротечный, многоэпизодный, а зачастую, и трансграничный характер.

Показателен пример совместной работы Управления "К" с нашими коллегами из Великобритании, которые обратились с просьбой оказать содействие в установлении лиц, причастных к электронным нападениям на сайт одной из британских компаний и последующему вымогательству. Благодаря принятым мерам удалось

установить личности нескольких российских граждан, причастных к данному преступлению, и задержать их. Это уголовное дело послужило также прецедентом в борьбе с так называемыми DDOS-атаками на серверы компаний.

Необходимо отметить, что в России нарастает количество фактов неправомерного доступа к информационным ресурсам государственных и коммерческих организаций в целях копирования (хищения) конфиденциальной информации. В частности, в 2003 г. в 4 раза увеличилось число преступлений, связанных с незаконным получением и разглашением сведений, составляющих коммерческую или банковскую тайну (ст. 183 УК РФ), совершенных с использованием компьютерной техники. В 1-м полугодии текущего года количество таких преступлений возросло более чем в 3 раза.

Так, в период с декабря 2003 г. по январь 2004 г. Управлением "К" МВД России были установлены 2 гражданина, которые незаконно скопировали и пытались сбыть базу данных с пин-кодами, позволяющими осуществлять нелегальные междугородние и международные переговоры. Эта база данных принадлежала одной из московских компаний-операторов связи.

В результате своевременного вмешательства сотрудников милиции противоправная деятельность фигурантов была пресечена. В отношении данных граждан возбуждено 2 уголовных дела.

Следует отметить, что в настоящее время в России отмечается устойчивая тенденция объединения хакеров в группы, в том числе международные, для совершения крупномасштабных преступлений. Причем такие союзы носят ярко выраженные признаки организованных преступных групп. В целях сокрытия своей причастности к совершению преступлений злоумышленниками используются похищенные реквизиты доступа в сеть Интернет, однократные выходы в сеть с присвоением разных динамических IP-адресов и другие способы электронной конспирации.

В качестве примера результатов деятельности в глобальном информационном пространстве организованных преступных групп может быть рассмотрено распространение в феврале 2004 г. в сети Интернет вируса Mydoom. По некоторым данным эпидемия данного вируса была заранее подготовлена злоумышленниками, которые владеют технологиями как создания и применения компьютерных вирусов, так и массовой рассылки информационных сообщений, классифицированных как спам.

С целью оперативного реагирования на совершаемые трансграничные преступления в рамках стран "большой восьмёрки" G8, созданы и активно работают в формате 24/7 (24 часа в сутки, 7 дней в неделю) национальные контактные пункты. Дежурный оперативный сотрудник находится на постоянной связи в режиме реального времени со своими коллегами в национальных контактных пунктах 7 стран. Взаимодействие же со странами не входящими в формат G8 осуществляется по каналам НЦБ Интерпола. Так, только в 1-ом полугодии 2004 г. Национальным контактным пунктом от иностранных правоохранительных органов получено 107 информационных сообщений о фактах распространения в сети Интернет материалов порнографического содержания с участием несовершеннолетних, неправомерного доступа к компьютерной информации и иных правонарушений.

В настоящее время в России стала актуальной проблема так называемого спама - массовой рассылки электронных сообщений, в основном, рекламного характера, не запрошенных получателями. Получение спама ложится на всех пользователей российского сегмента сети Интернет невидимым налогом. По различным оценкам, объемы финансовых потерь колеблются в пределах от 120 до 200 млн. долларов США в год.

Подразделениям "К" также удалось создать прецедент по борьбе и с этим видом преступлений. Так по материалам отдела "К" ГУВД Челябинской области окончено производством уголовное дело в отношении Андросова который, создал программу для ЭВМ sendsms.pl и осуществил массовую рассылку SMS-сообщений нецензурного содержания, порочащих деловую репутацию компании "Мегафон", на телефоны свыше 15 тысяч абонентов Челябинского фрагмента сети "Мегафон" - ЗАО "Уральский Джи Эс Эм".

В целом, можно с уверенность утверждать, что материальный ущерб от преступности в сфере информационных технологий измеряется миллиардами долларов США и увеличивается из года в год. При этом, ожидаемый рост финансовых потерь от преступных посягательств обусловлен не только и не столько увеличением количества электронных атак, сколько растущим масштабом использования сетевых информационных технологий в бизнесе. В условиях жесткой конкуренции компании вынуждены переводить большую часть своих бизнес-коммуникаций в Интернет, что без должного отношения к вопросам защиты информации делает их более уязвимыми для преступников.

В сложившихся условиях эффективное противодействие преступности в сфере информационных технологий возможно только при тесном взаимодействии правоохранительных органов, государственных, общественных и коммерческих структур. Не секрет, что значительная часть преступлений успешно пресекается сотрудниками милиции только благодаря сотрудничеству с компаниями-провайдерами, операторами радиотелефонной связи общего пользования, другими организациями и предприятия, действующими на информационном рынке. Однако многие организации, даже при установлении факта преступного посягательства предпочитают ограничиваться разрешением конфликта своими силами, поскольку их руководители опасаются подрыва своего авторитета в деловых кругах и, в результате, потери большого числа клиентов, раскрытия в ходе судебного разбирательства системы безопасности организации либо выявления собственной незаконной деятельности. Так, за всё время деятельности нашего подразделения поступило лишь одно обращение от российского коммерческого банка о хищении сведений составляющих банковскую тайну. Может сложиться впечатление, что отечественные "преступные таланты" применяют свои способности в основном для нападения на зарубежные информационные системы.

Если же рассматривать распространённость выявляемых информационных преступлений с геополитической точки зрения, то оказывается что их наибольшее число регистрируется далеко не в самых компьютеризированных регионах, что высвечивает ещё одну очень серьёзную проблему. Дело в том, что наше законодательство в области охраны информации настолько не совершенно, что позволяет следователям, прокурорам и судьям трактовать диспозиции статей по своему и порождает такое явление как "местничковое" законодательство. В тех субъектах Российской Федерации, где правоохранительные органы пришли к единому решению – борьба с преступлениями в информационной сфере ведётся активно, там, где не удалось определиться в терминологии и согласовать подходы в квалификации – преступлений данной категории нет.

Как отмечалось ранее, за последние пять лет значительно изменились способы совершения преступлений, при этом уголовное законодательство в данной области с 1996 года не претерпело ни малейших изменений, несмотря на неоднократные попытки Управления "К" ввести, продиктованные практикой, дополнительные составы. Принятые же нормативные акты призванные регулировать деятельность в информационной сфере не только не восполняют имеющиеся пробелы, но и создают новые лазейки для преступных элементов.

Тем не менее, и в настоящее время Министерством внутренних дел, ведется разработка ряда законопроектов, призванных сформировать эффективный нормативно-правовой механизм реализации государственной политики в области обеспечения информационной безопасности в целом и борьбы с информационной преступностью в частности. Регулярно проводятся конференции, совещания и семинары, посвященные данной проблематике. Однако, до сих пор так и не выработана стройная система взаимодействия правоохранительных органов, других государственных структур, а также общественных и коммерческих организаций в данной области. Создание именно такой системы, охватывающей все вопросы, от нормативно-правовых до организационных, позволит эффективно противодействовать любым вызовам и угрозам в информационной сфере.

Управление "К" ГУСТМ МВД России
старший оперуполномоченный Антон Кузнецов

Автор: Артур Скальский © Lenta.Ru ИНТЕРНЕТ , МИР 4023 10.10.2004, 18:41 431
URL: https://babr24.com/?ADE=16491 Bytes: 11556 / 11537 Версия для печати Скачать PDF

Эл.почта: newsbabr@gmail.com

ЗАКАЗАТЬ РАССЛЕДОВАНИЕ:

эл.почта: bratska.net.net@gmail.com

КОНТАКТЫ

Бурятия и Монголия: Станислав Цырь
Телеграм: @bur24_link_bot
эл.почта: bur.babr@gmail.com

Иркутск: Анастасия Суворова
Телеграм: @irk24_link_bot
эл.почта: irkbabr24@gmail.com

Красноярск: Ирина Манская
Телеграм: @kras24_link_bot
эл.почта: krasyar.babr@gmail.com

Новосибирск: Алина Обская
Телеграм: @nsk24_link_bot
эл.почта: nsk.babr@gmail.com

Томск: Николай Ушайкин
Телеграм: @tomsk24_link_bot
эл.почта: tomsk.babr@gmail.com

Прислать свою новость

ЗАКАЗАТЬ РАЗМЕЩЕНИЕ:

Рекламная группа "Экватор"
Телеграм: @babrobot_bot
эл.почта: eqquatoria@gmail.com

СТРАТЕГИЧЕСКОЕ СОТРУДНИЧЕСТВО:

эл.почта: babrmarket@gmail.com

Подробнее о размещении

Отказ от ответственности

Правила перепечаток

Соглашение о франчайзинге

Что такое Бабр24

Вакансии

Статистика сайта

Архив

Календарь

Зеркала сайта