Информационное агентство
«WEB-мониторинг»
Свидетельство ИА № ФС7733219 от 19 сентября 2008 года
Научно-практический электронный журнал

ФИНАНСОВЫЕ ПРАВОНАРУШЕНИЯ И ПРЕСТУПЛЕНИЯ

№ 11 (110) 2015
(выходит с октября 2006 г.)

Киберпреступления стОят меньше, чем борьба с ними
Фото с http://net.compulenta.ru/687454
См. раздел
«Тема номера. Киберпреступность: актуальные проблемы

Издатель
ИП **Фединский Ю.И.**

www.webmonitor.ucoz.ru
www.finprest.ucoz.ru
webmonitor@yandex.ru
тел. 8 985 333 87 59

Москва
2015

Продолжается подписка
на первое полугодие 2016 года
на издания ИА «WEB-мониторинг»

Финансовые правонарушения и преступления

Для тех, кому важно знать закон и формы его нарушения

Объединенный каталог «Пресса России»
подписной индекс **80663**

Валюта: регулирование и контроль

Для тех, кто не знает, какой валюте отдать предпочтение

Объединенный каталог «Пресса России»
подписной индекс **42335**

Налоговые правонарушения и преступления

Для тех, кто стремится грамотно платить налоги

Объединенный каталог «Пресса России»
подписной индекс **41587**

Подписку с любого календарного месяца

можно оформить
по электронному каталогу
ИД «Экономическая газета»

Финансовые правонарушения и преступления

Подписной индекс **80663э**
Инфорция
здесь

Валюта: регулирование и контроль

Подписной индекс **42335э**
Инфорция
здесь

Налоговые правонарушения и преступления

Подписной индекс **41587э**
Информация здесь

ИД "Экономическая газета"
http://www.arpk.org
тел. (499) 152 88 50

Оглавление

Тема номера. Киберпреступность: актуальные проблемы

19.11.2009

Wi-Fi помогает хакерам ломать смартфоны

Большинство популярных моделей смартфонов, подключенных к незащищенным публичным точкам доступа Wi-Fi, могут быть атакованы хакерами. Как передает «Компьюлента», к такому выводу пришли эксперты SMobile Systems.

Тестовым испытаниям подверглись Nokia N95 под управлением Symbian S60, HTC TouchPro 2 (Windows Mobile), HTC Dream (Android) и Apple iPhone (3GS).

Специалисты провели показательные атаки методом перехвата сообщения и подмены ключей, суть которых в незаметном внедрении злоумышленника в сеть передачи данных между смартфоном и Wi-Fi-хот-спотом для прозрачного перехвата любой информации, включая электронные сообщения и банковские транзакции. Эксперты воспользовались набором общедоступных хакерских утилит, позволяющих перенаправлять маршрутизацию пакетов, перехватывать и анализировать HTTP-трафик, прослушивать порты и вести журналирование.

Итоги неутешительны: незащищенное Wi-Fi-соединение может быть легко взломано, а данные перехвачены. В связи с этим авторы отчета рекомендуют пользоваться приложениями, снабженными функционалом шифрования трафика, хотя подобных программ не так много.

Ранее исследователи доказали, что наличие у потенциального злоумышленника необходимых инструментов и навыков может привести к взлому телефона при помощи обычной отправки SMS-сообщения.

Специалисты называют созданный ими метод атак Midnight Raid Attack (Полуночная атака), так как он рассчитан на те моменты, когда рядом с телефоном никого нет, например, ночью, когда владелец аппарата спит. Атакующий отправляет сервисное сообщение, дающее аппарату команду на запуск веб-браузера и отправку его на специальный злонамеренный сайт. Далее сайт предлагает загрузить на телефон хакерское программное обеспечение, предназначенное, например, для кражи контактов или персональных данных.

Напомним, в 2004 году киберпреступность заработала $105 млрд, обойдя по доходности наркоторговлю. Самые популярные киберпреступления – разработка компьютерных вирусов и кража корпоративной информации по заказу конкурентов.

По статистике, 60% киберпреступников – люди в возрасте от 20-ти до 35-ти лет, 24% — до 20 лет.

В 2005 году в сфере высоких технологий в России было зарегистрировано 15 тыс. преступлений, из них свыше 10 тыс. относятся к категории компьютерных. Всего в минувшем году было зафиксировано более 450 случаев компьютерного мошенничества.

http://www.rosbalt.ru
http://all-sbor.net/forum/showthread.php?t=8254

20.01.2011

Защита от киберпреступности: трудности и риски работы

Нир КШЕТРИ

Некоторые эксперты проявляют обеспокоенность по поводу пиратства и безопасности данных, хранящихся в облаке.

Киберпреступления

Как здравоохранение, банковская деятельность и образование, криминальная деятельность в Интернете превратились в киберпреступления. С точки зрения безопасности, облако - это палка о двух концах. Несмотря на потенциальную возможность облака обеспечить безопасность при минимальных затратах, риск, которому подвергаются небольшие компании, может возрасти, если они будут хранить важные данные в облаке.

Криминальные элементы всегда проявляют интерес к источникам ценности, и для хакеров - сети крупных компаний являются более соблазнительной целью, чем мелкие частные сети групп пользователей. Поставщики облачных сервисов чаще становятся объектом атак злоумышленников, и, что еще важнее, именно информация, хранящаяся в облаке, иногда превращается в золотую жилу для киберпреступников.

Чтобы представить уровень рисков безопасности в облаке, обратим внимание на отчет Google за 2009 год, в котором рассказывается об атаке на инфраструктуру компании, причем источник атаки находился в Китае. В Google подчеркивают, что эта атака была частью более крупной операции, которая охватывала инфраструктуру по крайней мере 20 других крупных компаний.

Одно из опасений заключалось в том, что хакеры могли похитить интеллектуальную собственность и другую важную информацию, хранившуюся в облаке. Хуже того, провайдеры облака могли не уведомить своих клиентов о нарушении защиты. Многие компании, как правило,

предпочитают не сообщать о киберпреступлениях из-за опасения, что пользователи усомнятся в их надежности, что негативно отразится на стоимости акций. В отчете одной из инжиниринговых компаний говорится: «Многие из кибератак остаются незамеченными или могут оставаться незамеченными в течение долгого времени».

В развивающихся странах провайдеры облака и пользователи сталкиваются с дополнительными трудностями, вызванными неблагоприятной экономико-правовой средой. Во многих развивающихся странах такие обыденные факторы, как коррупция, непрозрачность и слабая юридическая система, могут увеличить риск нарушения информационной безопасности.

Различные аспекты экономико-правовой среды могут практически свести на нет потенциальные выгоды облака и заставить инвесторов отказаться от подобных проектов. В 2008 году Эрик Шмидт, генеральный директор Google, пообещал, что компания совместно с китайскими университетами, в первую очередь с Университетом Цинху, будет работать над академическими программами, связанными с облаками, однако неблагоприятные политические условия привели к тому, что Google отказалась работать в Китае. Кроме того, возможные перебои в электроснабжении могут также затормозить распространение облачных сервисов - подобные перебои уже не раз приводили к приостановке работы таких популярных облаков, как Gmail, S3, и облаков, принадлежащих Salesforce и Microsoft.

Шпионская машина

В апреле 2010 года американские и канадские исследователи опубликовали отчет, в котором говорилось об обнаружении развернутой сети кибершпионажа, которую они назвали Shadow. Целями этой сети были индийское министерство обороны, Организация Объединенных Наций и представительство Далай-ламы. Облака становятся удобным прикрытием для преступников и шпионских сетей, обеспечивая им многоуровневую защиту, избыточность, дешевый хостинг и традиционно распределенные архитектуры командного управления.

Имеются реальные свидетельства того, что благодаря повышению роли ИТ в сфере национальной безопасности во многих секторах экономики растет протекционизм. Атмосфера подозрительности и недоверия между государствами может способствовать проявлению такого протекционизма. Последствия межгосударственного недоверия хорошо видны на примере взаимоотношений США и Китая. Китайские лидеры опасаются возможных кибератак со стороны США, они уверены в том, что Microsoft и правительство США шпионят за китайскими пользователями, используя для этого тайные «черные ходы» и закладки в продуктах Microsoft. Компьютерное оборудование и программное обеспечение, импортированное в Китай из США и их стран-союзников, придирчиво изучается. Китайские технические специалисты контролируют такой импорт и стараются не допустить, чтобы в установке этих продуктов принимали участие западные эксперты, тщательно контролируя их деятельность.

Несколько лет назад китайские специалисты по шифрованию обнаружили в продуктах Microsoft «ключ АНБ», который они интерпретировали как принадлежащий Агентству национальной безопасности США. Этот ключ, как утверждалось, давал правительству США тайный доступ к Microsoft Windows. Несмотря на то, что Microsoft отвергла эти обвинения и выпустила заплату для того, чтобы устранить проблему, китайские официальные лица это не убедило. Таким образом, руководство Китая, может посчитать неприемлемым хранение данных в облаках, предоставляемых иностранными международными компаниями.

Американские политики в свою очередь обеспокоены интернационализацией китайских технологических компаний, например, некоторые законодатели считают, что приобретение компанией Lenovo подразделения ПК корпорации IBM может привести к передаче передовой технологии китайскому правительству. Когда госдеп США в 2006 году планировал закупить компьютеры Lenovo, политики и эксперты подняли вопрос об угрозе национальной безопасности, утверждая, что тесные связи Lenovo с правительством Китая могут представлять угрозу США.

Есть определенные опасения и относительно внутренней безопасности - властям значительно проще следить за гражданами, когда они работают и общаются в облаках. В отчете Google, опубликованном в апреле 2010 года, упоминается о том, что государственные власти разных стран просят эту компанию предоставить частную информацию и ввести цензуру в приложениях.

Правительства во всем мире по-разному и в разной степени осуществляют цензуру сайтов и используют Web для слежки, но, несмотря на то, что онлайн-среду контролируют около 40 правительств, мало кто делает это более искусно, чем Китай. При определении государственной стратегии Китая в отношении ИТ была предпринята попытка найти баланс между экономической модернизацией и политическим контролем. Китай добился систематического, массового контроля в Интернете - десятки тысяч правительственных агентов участвуют в осуществлении такого киберконтроля. По данным Berkeley China Internet Project, программное обеспечение поддержки цензуры китайского правительства закрывает доступ к сайтам, содержащим такие слова и выражения, как «свобода», «демократия», «либеральный Китай» и «фалунь» («колесо закона» в

китайском буддизме). Также сообщалось, что с санкции китайского правительства проводилось заражение вирусами запрещенных сайтов.

Таким образом, страны, всерьез занимающиеся поддержкой кибершпионажа и организацией кибервойн, такие как Китай, окажутся в более выгодном положении, поскольку смогут использовать уязвимость облака для подобных действий. В случае с Shadow, например, сеть кибершпионажа объединяла платформы социальных сетей и облака от Google, Baidu, Yahoo, Twitter, Blogspot и blog.com с традиционными серверами командного управления.

Негативный эффект страны происхождения

Провайдеры облака из развивающихся стран, таких как Китай и Индия, могут столкнуться с серьезными препятствиями при попытке выйти на международный рынок. Помимо опасений, связанных с безопасностью облаков, одно из таких препятствий заключается в том, что экономико-правовая среда в таких странах сама по себе не может гарантировать безопасность и конфиденциальность клиентских данных.

Перспективы гражданского и уголовного судебного преследования не внушают оптимизма, когда нарушения безопасности и конфиденциальности возникают в стране со слабой властью закона. Аналитики отмечали, что в Индии довольно слабое законодательство в отношении киберпреступлений и обеспечения конфиденциальности, а с другой стороны, европейские и американские законы о защите данных в Индии применены быть не могут.

Репутация китайского правительства не намного лучше и дает основание полагать, что данные, хранимые в облаке, расположенном в Китае, также не могут быть в безопасности. Эти опасения еще больше усиливаются, когда речь заходит о возможности государственного контроля над провайдерами облака, действующими на территории Китая. На долю государства приходится, по крайней мере, 70% экономики этой страны, и ему принадлежит 76% национальных богатств. Например, мобильные операторы на 70% принадлежат государству и тесно аффилированы с государственной властью. В 2001 году в состав советов директоров 70% крупных и средних корпоративных предприятий обязательно входили члены коммунистической партии. Как следствие китайские компании обычно в большей степени, чем западные, ориентированы на государство, а не на потребителей, и для китайских провайдеров облака государственные интересы могут оказаться важнее прибыли акционеров. Частично благодаря реальному и ощутимому государственному контролю китайские провайдеры облака могут считаться в меньшей степени заслуживающими доверия, и, таким образом, им приходится бороться с негативным эффектом образа и стереотипов в отношении страны происхождения.

Облака, контролируемые криминалом

Облако потенциально наиболее уязвимо, когда рассматривается как прикрытие действующим параллельно облакам, контролируемым криминалом. Облако может давать преступникам многие из тех же преимуществ, которые получают добропорядочные компании. Принадлежащие криминальным группам облака могут использоваться для похищения данных, хранящихся в «законопослушных» облаках.

Хорошо известный вирус Conficker, контролирующий 7 млн компьютерных систем в 230 региональных и национальных доменах высшего уровня и поддерживающий пропускную способность 28 Тбит/с, представляет собой, как утверждается, самое большое в мире облако, и, вероятно, это наиболее яркий пример облака, принадлежащего криминалу.

Как и в случае с легитимными производителями облака, ресурсы Conficker можно взять в аренду - киберпреступники могут выбрать место, которое они хотят арендовать в облаке Conficker, оплатить нужную им полосу пропускания и указать предпочтительную операционную систему. Потребители могут выбирать разнообразные виды сервисов для того, чтобы воспользоваться облаком Conficker: организация атаки на отказ в обслуживании, распространение вредоносного программного обеспечения, рассылка спама, скрытое внедрение данных и т. д.

Внутренние риски

Изъяны в безопасности и нарушения конфиденциальности, связанные с утечкой данных и некорректным использованием, вызывают самое большое опасение в офшорной деятельности. Различные истории о краже данных и злоупотреблениях в индийских и пакистанских компаниях, предоставляющих услуги аутсорсинга, свидетельствуют о том, что такие опасения небезосновательны.

Как следствие, офшорные компании приняли соответствующие превентивные меры, такие как биометрическая аутентификация сотрудников, детальный мониторинг и анализ журналов регистрации сотрудников, запрет на использование сотовых телефонов, доступа в Интернет и к электронной почте. У компьютерных терминалов офшорных компаний нет жестких дисков, дисководов для компакт-дисков и других средств хранения, копирования и передачи данных.

В свете этих проблем опасениям относительно конфиденциальности и безопасности придается особое значение, если сотрудники офшорных компаний работают вне выделенных контакт-центров телефонного обслуживания, как многие операторы контакт-центров в Южной Африке.

Риски для индустриальных стран

Для международных компаний, работающих с облаками, заманчиво использовать более дешевые сервисы хостинга в развивающихся странах, однако киберпреступники рассматривают эти сервисы как самые удобные средства проникновения в ресурсы богатых экономик. Например, США - первоочередная цель для кибератак. Поскольку многие развивающиеся страны являются основными источниками киберпреступлений, риски безопасности, связанные с внедрением облаков в этих странах, могут распространиться и на индустриальные страны. Целью и жертвой становились американские федеральные ведомства, в том числе и Пентагон: с сентября 2004-го по апрель 2005 года свыше дюжины версий червя Myfip были использованы для кражи у американских компаний файлов САПР с чертежами конструкций, схемами электронных плат и разводок. Резонно предположить, что облако позволит модернизировать эти виды деятельности до промышленного шпионажа 2.0.

Предстоит еще многое узнать о том, что способствует, а что мешает распространению облаков, и одно из перспективных направлений будущих исследований связано с оценкой того, как облака и социальные сети меняют представления о рисках безопасности и конфиденциальности. Легитимные и нелегитимные организации и люди, движимые разными интересами, применяют облако для получения доступа к информации о пользователях социальной среды с помощью нелегальных, неузаконенных и псевдолегальных средств.

Будущие исследования помогут также оценить, как политические, этические, социальные и культурные факторы связаны с вопросами безопасности при работе в облаке. Например, сейчас не существует четких юридических оснований, позволяющих решать вопросы конфиденциальности и безопасности данных, хранимых в облаке. Однако можно предположить, что юридические институты будут постепенно совершенствоваться, а также что появятся этические и профессиональные стандарты, касающиеся облаков.

Развивающиеся страны могут избежать некоторых проблем, препятствующих реализации всего потенциала облака, за счет более качественного планирования и усилий, предпринимаемых в отношении кадровых ресурсов. Знаний, имеющихся у сотрудников, может оказаться недостаточно для развития индустрии вычислений в облаке.

Правительства должны принять меры для развития навыков, связанных с работой в облаке, а университеты - обеспечить возможность получения практического опыта.

Не менее важно и развитие отраслей, необходимых для поддержки прямой и обратной связи...

Автор Нир Кшетри - адъюнкт-профессор Броуновской школы бизнеса и экономики Университета Северной Каролины (США).

Из статьи «Облака в развивающихся странах».

Журнал «Открытые системы», 2010

http://www.djmeirlan.psj.ru/saver_magazins/detail.php?ID=66115

19.06.2012

Киберпреступления стоят меньше, чем борьба с ними

Александр Березин

Первое систематическое исследование проблемы ущерба от киберпреступлений, проведённое учёными из Кембриджского университета (Великобритания), показало, что стоимость защиты от них может с лихвой перекрыть ваши финансовые потери от самой угрозы. По крайней мере такова сегодняшняя ситуация в мире в целом.

На основании собственных измерений прямых и косвенных убытков от киберпреступлений и стоимости антивирусов и иных видов защиты авторы работы полагают, что мы должны меньше тратить на предупреждения такого рода угроз и больше — на поимку преступников.

Размах киберпреступности в Соединённом Королевстве меркнет на фоне масштабов продаж антивирусов и прочих трат на борьбу с мифическими хакерами. (Иллюстрация jacob.)

Как обнаружили учёные, многие предыдущие оценки стоимости ущерба от киберпреступлений просто не учитывали тех или иных факторов, а значимость других преувеличивали. Так, специализированное изыскание «дочки» BAE Systems компании Detica вывело цифру потерь от киберпреступлений в Великобритании в £27 млрд (за $50 млрд!) ежегодно. При этом методология расчёта является весьма сомнительной, а стоимости затрат на антивирусное обеспечение доклад не учёл вовсе.

В новом исследовании прежде всего была предпринята попытка отделить разные категории киберпреступлений друг от друга. К примеру, хищения в сфере соцобеспечения и

налоговых сборов, всё чаще перемещающиеся (как и сами эти системы) в киберпространство, оцениваются учёными в сотни фунтов в год на гражданина Великобритании; воровство средств с кредитных карточек и при онлайновых банковских операциях — в десятки фунтов. Причём, как отмечают авторы, часто такие хищения невозможны без физического доступа к кредитным картам (персонал гостиниц и магазинов) или непосредственного вовлечения социальных и налоговых органов (сотрудники этих органов). Иными словами, это не столько киберпреступления, сколько использование «нормальными» мошенниками новых форм их вековечного ремесла.

Настоящие киберпреступления — вирусы, руткиты, слежение при помощи троянов за бизнесом и гражданами, даже полумифические логические бомбы — по стоимости оказались равны десяткам пенсов в год на одного гражданина (десятки рублей).

Интересно, что вызванные этими преступлениями непрямые затраты граждан (на покупку антивирусов и другие аспекты борьбы) достигли $1 млрд, из которых $170 млн — стоимость антивирусов. Бóльшую часть таких расходов составили зарплаты работников, отвечающих за компьютерную безопасность, которых доклад решительно отделяет от персонала, ответственного за функционирование собственно компьютеров и сетей.

Итак, средства, направленные на борьбу с киберугрозами, в сотни раз превысили потери от них. При этом лишь $15 млн было потрачено на усилия полиции по выявлению и передаче в суд виновников киберпреступлений — вирусописателей и хакеров (в широком смысле этого слова).

Подготовлено по материалам Кембриджского университета.
http://net.compulenta.ru/687454

20.01.2014

ОРКИ: О российской киберпреступности и работе "киберсыщиков"

"Лаборатория Касперского" известна, прежде всего, своими антивирусными продуктами. Больше года назад в структуре компании появился Отдел расследования компьютерных инцидентов (ОРКИ). Специалисты нового подразделения по заказу клиентов помогают правоохранителям вычислять киберзлоумышленников и при необходимости оказывают информационную и техническую поддержку расследования уголовных дел.

О своей работе в интервью порталу ЮГА.ру рассказал руководитель Отдела расследования компьютерных инцидентов Руслан Стоянов.

ОРКИ – одно из самых наименее известных для обычных пользователей подразделений в "Лаборатории Касперского". Чем именно занимается ваш отдел?

– Наверное, о нас знают меньше, потому что мы самые молодые. Фактически, наша группа реализует тактическое и техническое превосходство над преступниками.
В "Лаборатории Касперского" работают около 1,5 тыс. технических специалистов, которые занимаются разными вещами, связанными с IT-безопасностью. Наше подразделение – это своего рода линза, которая усиливает технические познания специалистов на одну конкретную цель: исследование и противостояние киберпреступности.

А как это воплощается на практике?

– По заказу наших клиентов мы занимаемся расследованием инцидентов, связанных с деятельностью киберпреступников . Уточню: мы не субъекты оперативно-розыскной деятельности, мы не правоохранительные органы и не занимаемся расследованием преступлений. В нашу задачу входит установление технических аспектов произошедшего, выявление стоящей за инцидентом криминальной инфраструктуры, и содействие правоохранителям в установлении личности. Мы работаем для того, чтобы помочь бизнесу и обществу в противодействии киберпреступности.

Количество сотрудников вашего отдела – это закрытые данные?

– У нас небольшое подразделение, но мы пользуемся всей мощью "Лаборатории Касперского" и всеми ресурсами компании.

Какого рода киберпреступления вы расследуете?

– Мы не расследуем киберпреступления, непосредственным расследованием занимаются правоохранительные органы. Мы с технической точки зрения расследуем инциденты – то, что произошло. Наше подразделение занимается поиском, сбором и анализом информации о произошедшем инциденте. Наиболее частые инциденты происходят в банковской сфере. Мы анализируемнарушения доступа в корпоративные сети, DDoS-атаки и вообще все компьютерные инциденты, которые наносят вред и могут принимать различные формы.

Киберпреступники проявляют интерес только к крупному бизнесу? Как обстоят дела у малого и среднего бизнеса, которые гораздо менее защищены?

– Сегодня кибепреступники обращают внимание на всех. Часть из них занимается корпоративным шпионажем, зарабатывая деньги на продаже инсайдерской информации

конкурирующим организациям. Другие заражают компьютеры десятков тысяч людей для атаки на системы ДБО.

Вы работаете только по контракту, когда поступил конкретный заказ?

– Не обязательно. С одной стороны, мы ежедневно занимаемся исследовательской работой, а объектом наших исследований является киберпреступность. Эта работа ведется постоянно. С другой стороны, нас нанимают по контракту, чтобы мы расследовали тот или иной инцидент.

Как быстро с вами заключаются контракт? Ведь такие инциденты, наверное, лучше расследовать по "горячим следам"…

– Подобного рода контракты заключаются долго, потому что они требуют всестороннего анализа юридических служб обоих сторон. Поэтому часто мы продаем подписку – контракт заключается в начале года и проходит долгое согласование, после ничего не требуется. Зато у клиента есть гарантии быстрой реакции на сообщение об инциденте. Обычно это действует для крупного бизнеса, который старается контролировать свои риски и заранее к ним готовится.

Первый этап расследования инцидента происходит очень быстро – за две-три недели. Наши специалисты проводят оперативный анализ, собирают первичную информацию, ищут вредоносное ПО. Следующий за ним этап – само расследование, здесь наша основная цель – определить данные, по которым можно установить вовлеченных в инцидент лиц.
Такое расследование занимает несколько месяцев, а потом начинается этап сопровождения уголовного дела, и это могут быть годы.

Как именно ваш отдел сотрудничает с госструктурами и правоохранительными органами?

– Правоохранительные органы иногда обращаются к нам за помощью в расследовании компьютерных инцидентов и подготовке соответствующей экспертизы. У нас есть специальный экспертно-криминалистический отдел, который как раз занимается проведением подобных экспертиз. Это делается бесплатно. Помимо этого, мы регулярно проводим семинары для представителей правоохранительных органов.

Были ли в вашей практике случаи, когда с конкретной проблемой к вам обращались частные лица, а не бизнесмены?

– Достаточно часто. У нас есть общий почтовый ящик и форма на сайте, которую может заполнить кто угодно. Стоимость наших услуг одинаковая и для физических, и для юридических лиц. Часто организации работают по подписке, а граждане обращаются к нам непосредственно после произошедшего инцидента.

География работы вашего отдела ограничена только Россией? Или вы можете работать по всему миру?

– "Лаборатория Касперского" – международная организация, у нее есть представительства в разных странах и подразделения, которые работают по международным направлениям. Мы же сейчас фокусируемся на русской киберпреступности, так как сегодня она является одной из доминирующих во всем мире. Поэтому пока наш сервис предоставляется только на территории РФ и стран СНГ.

Есть какая-то статистика оказанной вами помощи?

– Мы не ведем статистику. Я вообще не люблю это слово: все, что обычно представляется как статистика относительно киберпреступности – это оценочные суждения отдельных компаний или специалистов.
Посчитать злоумышленников нельзя. Они не участвуют в переписи населения и не ставят галочку: "Да, я ворую деньги у банков или у их клиентов", не объявляют о своем роде деятельности "взломщик сайтов". Это крайне скрытые люди и организации, которые большую часть времени и усилий тратят на обеспечение своей собственной безопасности. Поэтому я не доверяю существующим методикам расчета и их результатам.

Какие устойчивые группировки в сфере киберпреступности вам удалось установить?

– Одно из последних дел, где мы помогли правоохранителям, это раскрытие преступной группировки, которая занималась финансовым фродом (мошеннические действия с целью кражи тех или иных финансовых активов, управление которыми осуществляется с помощью информационных систем). Один из преступников долгое время предоставлял услуги эксплуатации уязвимости с применением пакета вредоносных программ Blackhole. Автор Blackhole был известен в Сети под ником Paunch и помимо сдачи эксплойт-паков в аренду предоставлял киберкриминалу услуги по шифрованию и проверке вредоносного ПО на устойчивость к антивирусам. Отличный пример, но не все понимают, что Paunch не был главным, и в деле присутствуют конечные бенефициарии. Всем им вменили статью 210 УК РФ (организация преступного сообщества или участие в нем), а сделать это очень сложно.

А были случаи международного сотрудничества?

Не так давно мы провели совместную операцию с правоохранителями Украины против группы разработчиков троянского приложения Carberp. Это распространенная среди

киберпреступников троянская программа, известная в разных модификациях с 2009 года. Она собирает информацию о пользователе и системе и отправляет на сервер злоумышленников. Операцию против разработчиков Carberp поддерживали все компании, которые занимаются IT-безопасностью.

В группу Carberp входили программисты, работавшие удаленно в Киеве, Запорожье, Львове, Херсоне и Одессе. Хакеры создали вирус, который проникал в компьютеры при скачивании фотографий или просмотре видео в Интернете. Он получал доступ к данным бухгалтерии, программе 1С, паролям и электронным ключам, после чего передавал их мошенникам. Вредоносная программа постоянно модифицировалась, поэтому антивирусные средства защиты ее не всегда идентифицировали. При заражении компьютерных сетей злоумышленники тратили немало времени на изучение деятельности предприятия и формирование электронных платежей на счета фиктивных предприятий.

Как относятся киберпреступники к вашему отделу?

– Я надеюсь, что они не обращают на нас никакого внимания, чем менее они сфокусированы на параноидальных мыслях: "А не подбирается ли к ним "Лаборатория Касперского", тем лучше. Мы довольно редко широко афишируем результаты своей работы.

Хотя у нас был очень успешный кейс против братьев Евгения и Дмитрия Попелыш из Санкт-Петербурга, которые использовали вредоносную программу и фальшивую копию страницы системы интернет-банкинга ВТБ 24 "Телебанк". Хакеры с помощью вредоносной программы похитили около 13 млн рублей. В итоге они были приговорены к 6 годам лишения свободы условно с испытательным сроком 5 лет и штрафу по 450 тыс. рублей в пользу государства с каждого. Вместе с Попелышами к 4 годам условно и штрафу в 200 тысяч был приговорен помогавший им студент из Калининграда Александр Сарбин.

После этого случая ВТБ 24 стал неким табу для кибепреступников, потому что многие понимают, что выйдет себе дороже.

Если попытаться представить усредненный портрет современной российской киберпреступности, то каким он будет?

– В настоящее время киберпреступность – это массовое явление, куда вовлекается большое количество новых кадров, в большинстве своем это молодые амбициозные люди, стремящиеся получать высокий доход. Они хотят раскидывать вокруг себя доллары и жить, как показывают в видеоклипах на MTV.

Сейчас хакером стать настолько легко, что кибепреступность потеряла свою элитарность. Да, существуют серьезные старые группы, но сейчас ты приходишь на любой IT-форум и можешь прочитать, как заражать компьютеры. На соседней ветке ты скачиваешь примитивную троянскую программу, тут же тебе предлагают защитить свою личность анонимайзером и так далее. Выкладывающие эту информацию в свободный доступ не совершают преступления, их можно судить только по статье "Распространение вредоносного кода", но это другие сроки – не такие высокие у статьи "Мошенничество".

Интернет перестал быть безопасным местом, это опасное место. Здесь множество людей, которые хотят делать деньги из воздуха, не выходя из комнаты, и все это легкодоступно.

Были моменты, когда вам удавалось закрывать места обмена информацией такого рода?

– Это не наша задача контролировать и что-то закрывать. У нас есть Роскомнадзор, который занимается фильтрацией информации в Интернете, оценивать сайты на их безопасность. Мы делимся своими навыками и информацией. Если люди из госструктур не обладают достаточными знаниями в этой области, они могут прийти к нам и обратиться за помощью.

Есть разница между российскими киберпреступниками и зарубежными?

– Безусловно. У каждой страны есть свои особенности, свои лидеры. Основные черты российской киберпреступности – массовость, наглость и агрессивность.

Например, в Англии основной промысел киберзлоумышленников – отмывание денег, в нем участвуют так называемые дропы (дроп – низшее звено мошеннической группировки, занимающейся кражами реквизитов кредитных карточек в Интернете). Например, человеку приходит письмо, такого содержания: "Мы пытаемся оптимизировать наши налоги, примите на свой счет такую-то сумму. Часть оставьте себе, часть перешлите туда-то".

У нас же в стране создаются целые фабрики по созданию вредоносного софта (такого, как Carberp со средой разработки), и это гораздо более серьезная проблема.

Существует определенная тенденция по сращиванию традиционной организованной преступности и киберпреступности, но здесь все не всегда однозначно. Обычным преступникам ведь сначала нужно найти этих молодых амбициозных хакеров, которые, в свою очередь, не горят желанием с кем-то делиться своими доходами. Но когда у этих двух ветвей получается как-то вольно или невольно пересечься, начинается их довольно успешное взаимодействие. Одни занимаются хищением денежных средств, другие – их отмыванием.

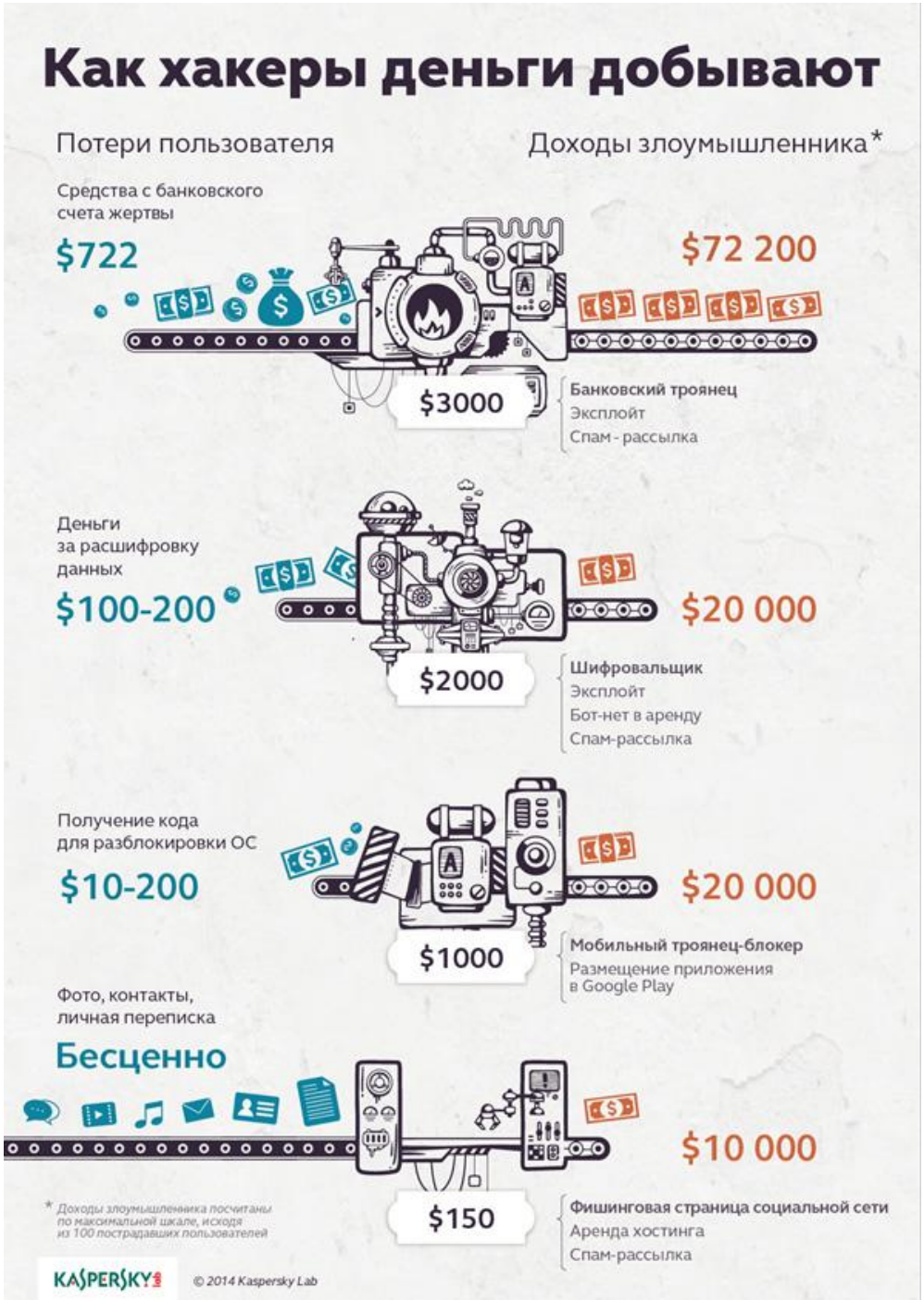
Автор: Антон Смертин

https://www.yuga.ru/articles/sport/6811.html

29.08.2014

Киберпреступления обеспечивают двадцатикратную доходность злоумышленникам

Доходы киберпреступников могут более чем в 20 раз превышать их затраты на организацию атак. Это следует из анализа, выполненного экспертами «Лаборатории Касперского».



По их данным, создание в популярной социальной сети фишинговой страницы для заманивания доверчивых пользователей на мошеннический сайт и организация спам-рассылки с упоминанием этого сайта-подделки обходятся мошенникам сегодня в среднем в 150 долларов. Если же на их удочку «клюнут» хотя бы 100 человек, то злоумышленники смогут заработать до 10 тысяч долларов, продав похищенные таким образом конфиденциальные данные пользователей.

Мобильный троянец, блокирующий экраны гаджетов, обойдется преступникам уже заметно дороже — в среднем в тысячу долларов. Однако и выручка от его использования получается больше. Цены, которые злоумышленники запрашивают со своих жертв за разблокирование экрана смартфона, варьируют от 10 до 200 долларов. Значит, со ста пострадавших можно получить до 20 тысяч долларов.

Немало можно заработать и с помощью программ, зашифровывающих файлы с данными на атакованном компьютере. Однако расходы хакера будут в два раза выше — около двух тысяч долларов.

Наибольшую же доходность мошенникам обеспечивает применение банковских троянцев, которые «охотятся» напрямую за деньгами пользователей. Потратив около трех тысяч долларов на приобретение подобного зловреда в комплекте с эксплойтом (исполняемой программой для его внедрения) и специально организованной для этого спам-рассылкой, киберпреступники имеют

шанс получить до 72 тысяч долларов от ста успешных атак. В этом случае средняя потеря одного пострадавшего пользователя составит 722 доллара.

При этом, по оценке аналитиков, купить вредоносное программное обеспечение сегодня не составляет больших проблем: зловреды легко можно найти на различных хакерских форумах, а довольно низкая стоимость делает их широко доступными.

«Более того, киберпреступникам даже не требуется быть профессионалами в своем незаконном бизнесе — за фиксированную цену они получат уже готовый пакет программ для совершения атак. В такой ситуации пользователям, безусловно, стоит всегда быть начеку, чтобы не потерять деньги и свои ценные данные», — говорит главный антивирусный эксперт «Лаборатории Касперского» Александр Гостев.

http://lenta.ru/news/2014/08/29/income/

27.09.2015

Актуальные проблемы компьютерных преступлений

Автор: Е.С. Шевченко

В условиях совершенствования глобальных информационно-телекоммуникационных технологий, формирования единого мирового информационного пространства, а также вследствие отсутствия единообразного законодательного регулирования общественных отношений, связанных с использованием информационных ресурсов сети Интернет, как на национальном, так и на международном уровне отечественные правоохранительные органы оказались не в полной мере готовы эффективно противостоять новым видам преступных посягательств - киберпреступлениям.

Уголовный кодекс РФ не содержит указания, что именно следует понимать под "киберпреступлениями". Вместе с тем во многих источниках под этими преступлениями понимают: "компьютерные преступления", "преступления в сфере высоких технологий", "информационные преступления", собственно "киберпреступления", "преступления в сфере безопасности обращения компьютерной информации", "преступления в сфере компьютерной информации" и т.д. Независимо от используемой терминологии очевидно, что проблема борьбы с киберпреступлениями, ставшими в последнее время одной из серьезных угроз для личности и государства, является одной из приоритетных задач правоохранительных органов России.

Результаты опроса следователей и дознавателей, проведенного автором статьи, свидетельствуют, что достаточно часто им приходится расследовать следующие киберпреступления, предусмотренные УК РФ: ст. 159.6 "Мошенничество в сфере компьютерной информации", ст. 242.1 "Изготовление и оборот материалов или предметов с порнографическими изображениями несовершеннолетних", ст. 273 "Создание, использование и распространение вредоносных компьютерных программ", ст. 242 "Незаконные изготовление и оборот порнографических материалов или предметов", ст. 274 "Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации информационно-телекоммуникационных сетей", ст. 158 "Кража", ст. 183 "Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну", ст. 138 "Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений", ст. 272 "Неправомерный доступ к компьютерной информации", ст. 137 "Нарушение неприкосновенности частной жизни", ст. 282 "Возбуждение ненависти либо вражды, а равно унижение человеческого достоинства".

Одной из проблем расследования киберпреступлений является недостаточная компетентность лиц, которые занимаются их выявлением и раскрытием.

Так, например, результаты опроса следователей показали, что у 95% респондентов имеется только юридическое образование, другая дополнительная подготовка ими получена не была, что не может не влиять на качество расследования. Только 5% из числа опрошенных имели еще и образование по специальности "Информатика и вычислительная техника". Из числа опрошенных 63% оценивают свой уровень владения персональным компьютером как уровень "среднего пользователя", 37% считают, что они обладают знаниями "продвинутого пользователя". При этом 79% опрошенных следователей назвали источником знаний компьютерных технологий самообразование, 21% - курсы повышения квалификации сотрудников правоохранительных органов, 5% - коммерческие курсы или специальное образование.

Большинство следователей (дознавателей) отметили, что имеющихся знаний дляраследования киберпреступлений недостаточно. Для решения данной проблемы, по мнению опрошенных, необходимо проведение их обучения по расследованию данного вида преступлений, а также организация семинаров, посвященных модификации компьютерных технологий.

Другой проблемой является несвоевременность выявления киберпреступлений. Как показали результаты проведенных исследований, в 53% случаев с момента совершения преступления до поступления информации о совершенном преступлении проходит более 10 дней.

Несвоевременность выявления преступлений отметили 75% опрошенных следователей. Очевидно, что запоздалое начало предварительного расследования может привести к безвозвратной утрате важных доказательств, увеличению сроков предварительного расследования и другим негативным последствиям. Как правило, несвоевременное выявление киберпреступлений влечет за собой опасность уничтожения следов совершенного преступления.

При расследовании киберпреступлений чаще всего проводятся такие следственные действия, как осмотр места происшествия (указали 79% опрошенных), допрос (68%), обыск (63%), выемка (37%) и назначение судебных экспертиз (47%). Наибольшие трудности возникают при проведении осмотра места происшествия (это отметили 42% опрошенных) и назначении судебных экспертиз (37% опрошенных).

Примечательно, что 21% из числа опрошенных нами практических работников не проводили осмотр места происшествия и отметили, что причиной отказа от проведения осмотра места происшествия является отсутствие места происшествия. Это значит, что распознавание места совершения киберпреступления невозможно без установления обстановки совершения преступления, которая определяется системой киберпространства. Иными словами, для расследования преступлений, совершенных в киберпространстве, требуются как технические, так и теоретические знания. Соответственно, возникает необходимость выработки единого понятия киберпространства с точки зрения криминалистики.

Что касается назначения компьютерно-технической экспертизы, то здесь надо отметить, что следователям приходится сталкиваться с загруженностью государственных судебно-экспертных учреждений и, как следствие, несвоевременностью выполнения экспертиз. Однако, коль скоро следователи (дознаватели) вправе выбирать судебно-экспертное учреждение, в 58% случаев проведение экспертизы они поручали государственно-экспертным учреждениям и лишь в 5% - негосударственным. Объясняется это тем, что у негосударственных экспертных учреждений не всегда есть необходимое оборудование и средства для проведения судебной компьютерно-технической экспертизы. На это указали 40% опрошенных.

Другой проблемой при назначении экспертиз является постановка грамотных вопросов эксперту, проводящему компьютерно-техническую экспертизу, что отметили 53% опрошенных. Назначающие экспертизу связывают возникающие трудности с отсутствием у них практики расследования данной категории дел, сложностью технических терминов и отсутствием специальных знаний в этой сфере.

На наш взгляд, решение проблемы лежит в плоскости взаимодействия следователя при назначении экспертизы с экспертом или специалистом, которые могут проконсультировать назначающего экспертизу по всем вопросам научно-методического характера.

Подытоживая изложенное, надо признать, что раскрытие и расследование киберпреступлений остается довольно сложной задачей для большинства сотрудников органов предварительного расследования. Это отчасти обусловлено отсутствием системных обобщений материалов следственной и судебной практики, нехваткой методических рекомендаций по организации расследования данного вида преступлений, небольшим опытом работы конкретных следователей и работников органов дознания со специфическими источниками доказательственной информации, находящейся в электронной цифровой форме в виде электронных сообщений, страниц, сайтов, а также недостаточно высоким уровнем подготовки следователей по соответствующей специализации в высших учебных заведениях.

Как показало исследование научной литературы и опрос следователей (дознавателей), для решения приведенных проблем и повышения эффективности расследования киберпреступлений необходимо: повысить уровень мониторинга данного вида преступлений; разработать программы повышения квалификации следователей (дознавателей) по расследованию данной категории дел; повысить технические возможности экспертов, специализирующихся в области исследования компьютерных технологий; увеличить объем научно-методической литературы, посвященной прикладным аспектам расследования киберпреступлений.

http://stuchilin.ru/services/r/computer-crimes/311/

16.10.2015

За год киберпреступники похитили более 2,6 миллиарда рублей

Хакеры уже умеют перехватывать СМС-подтверждения платежей

Нина Забелина. Независимая газета, 16 октября 2015

Ежедневно в РФ жертвами кибератак на системы интернет-банкинга становятся 16 юридических лиц, теряющих в среднем по 480 тыс. руб. Общая сумма ежегодного ущерба оценивается в 1,9 млрд руб. В феврале 2015 года была проведена первая успешная атака на российского биржевого брокера. За 14 минут банк лишился более 5 млн долл.

Самые умные и опасные хакеры – россияне или выходцы из бывшего СССР

Вчера в Москве прошла конференция «Тенденции развития преступления в области высоких технологий». Открывая мероприятие, глава Минсвязи Николай Никифоров отметил, что преступник в Интернете ничем не отличается от преступника в обычной жизни: «В этой сфере, в виртуальной среде, по сути, необходимо добиться соблюдения базового действующего российского законодательства».

При этом речь идет не только о федеральных законах, но и о различных нормативных актах министерств и ведомств, заметил он. «Важно сделать так, чтобы преступника преследовали, а ответственность была неотвратима», – подчеркнул министр. Он сообщил, что за время его трехлетней работы в министерстве число пользователей Интернета увеличилось в России на 27 млн человек, многие из которых не понимают опасности киберпреступности, включая и прямое хищение денежных средств.

Согласно отчету международной компании Group-IB, представленному на конференции, в РФ за год, с июня 2014 по июнь 2015 года, через системы интернет-банкинга хакеры похитили более 2,6 млрд руб. Физические лица лишились более 99 млн руб., из них 61 млн руб. – с помощью троянских вирусов для операционных систем мобильных устройств. Как рассказал глава компании Илья Сачков, уязвимость мобильных операционных систем привлекает все больше злоумышленников: «Только за последний год выявлено 10 новых преступных групп хакеров, специализирующихся на создании Android-троянов. Ежедневно около 70 пользователей мобильных банков на «андроидах» становятся жертвами преступников».

У юридических лиц хакеры за прошлый год похитили около 1,9 млрд руб. Преступники научились обходить традиционные средства защиты систем дистанционного банковского обслуживания: ни токены (компактное устройство, предназначенное для обеспечения информационной безопасности пользователя), ни дополнительная SMS-аутентификация не спасают юрлиц от «автозаливов» троянов, позволяющих похищать средства со счетов компаний. Руководитель подразделения Bot-Trek Secure Bank Павел Крылов сообщил, что наибольший интерес для хакеров сегодня представляют банки: «За последний год появились две новые преступные группы, в результате их атак российские банки потеряли 638 млн руб. В феврале 2015 года была проведена первая успешная атака на российского биржевого брокера. Она длилась всего 14 минут. Ущерб же составил более 5 млн долл.».

Параллельно с хищениями растет и нелегальный бизнес торговцев данными банковских карт, логинов и паролей разных систем. Выручка зафиксированных семи таких «магазинов» составила за год более 155 млн руб. Расширяется рынок, обслуживающий хищения через устройства считывания банковских карт (так называемые POS-терминалы на рабочем месте кассира). Преступники даже продают устройства обработки банковских карт, которые похищают данные клинентов, по 15–20 тыс. рублей за штуку.

Наиболее опасные банковские бот-сети имеют прямое отношение к русскоговорящим хакерам, утверждает Илья Сачков. Однако нынешний кризис парадоксальным образом повлиял на киберпреступность. «Из-за девальвации рубля злоумышленники из РФ и стран СНГ переориентируются на Запад. Из-за этого масштабы хищений в России за последний год сократились в 3,7 раза», – утверждает Сачков. Кроме того, в прошлом году были задержаны члены одной из крупнейших хакерских команд Anunak, которую составляли выходцы из разгромленной в РФ группировки Carberp.

Всего за неполные два года преступникам удалось похитить около 1 млрд руб. из российских банков, утверждает Илья Сачков. Несмотря на видимое сокращение объема хищений, количество атак растет на сотни процентов. «12 самых популярных троянов разрабатываются русскоговорящими хакерами», – рассказал о сомнительных достижениях наших соотечественников Сачков.

Киберпреступность будет расти, прогнозируют эксперты. Можно ожидать увеличения инцидентов с фишингом (выманиванием паролей) у клиентов банков. Также может увеличиться число инцидентов с программами шифрования для последующего вымогания денег за их расшифровку (криптолокерами).

Вчера на заседании Межведомственной комиссии Совета безопасности РФ также обсуждали вопросы противодействия угрозам в сфере информационной безопасности. «На заседании выработаны меры по противодействию уязвимости коммуникационных технологий в связи с ростом числа попыток несанкционированного доступа в используемое органами госвласти ПО и оборудование», – сообщили в пресс-службе Совбеза.

http://www.aferizm.ru/novost/2015/10/151016-1-ciber-crimes-2015.htm

04.10.2015

В Омске продолжаются аресты членов опг мацелевича. пришла очередь главного финансиста

В Омске задержан шестой член ОПГ Мацелевича. Следственному управлению удалось задержать главного финансиста преступной группы Юлию Аристову, которая непосредственно

давала указания уже арестованным бухгалтерам Екатерине Бунаковой и Елене Зыряновой путем электронных платежей перечислять деньги на расчетные счета конкретных предпринимателей и фирм. В легальном мире она работала членом совета директоров «Единого строительного банка», через который ОПГ осуществляла свои махинации по обналичиванию денежных средств.

Преступный доход «банды Мацелевича» оценивается в 393 млн рублей. Участникам ОПГ грозят разные тюремные сроки до 20 лет лишения свободы. Ранее суд арестовал пять других участников группировки – самого Станислава Мацелевича, бухгалтеров Екатерину Бунакову и Елене Зырянову, юриста Евгения Лузинского и экспедитора Андрея Копейкина. Из них со следствием согласилась работать лишь Бунакова, которая в одиночку воспитывает маленького ребенка.

http://baikal24.ru/text/04-10-2015/opg_macelevicha/

05.10.2015

Забайкальца, подозреваемого в пособничестве хакерской группировке, задержали в Иркутске

Сотрудники правоохранительных органов задержали в Иркутске жителя поселка Чернышевск Забайкальского края, подозреваемого в пособничестве хакерской группировке. По версии следствия, молодой человек помогал похищать денежные средства с банковских счетов граждан. В отношении него возбужденны десятки уголовных дел, сообщили «Забмедиа» 5 октября в прокуратуре Чернышевского района.

- В декабре 2014 года 20-летний подозреваемый в поисках работы наткнулся в Интернете на заманчивое предложение. Суть предложения заключалось в обналичивании денежных средств, которые ему должны были пересылать на банковскую карту новые знакомые. Молодой человек должен был оставлять себе от 20% до 40% суммы, а остальное возвращать на КИВИ-кошелек «работодателей». Подозреваемый сразу согласился на столь прибыльное предложение. При этом он понимал, что участвует в групповом хищении денежных средств, так как «работодатели» не скрывали, что с помощью вируса проникают в телефоны жертв и по услуге «Мобильный банк» переводят с их банковских карт денежные средства на карты своего «работника», - пояснили в пресс-службе.

По данным районной прокуратуры, подозреваемый, находясь в Чернышевске использовал свою пластиковую карту, а также карты своих друзей и родственников. Тем самым, он участвовал в хищении денежных средств.

- После того как банк заблокировал его карты в связи с поступающими жалобами, молодой человек не остановился. Он выехал в Читу, а затем в Иркутск, где расширил поле своей деятельности, - подчеркнули в ведомстве.

В ходе задержания и проведенного обыска у подозреваемого были изъяты сотни банковских карт, а также ноутбук с программным обеспечением и крупные денежные суммы.

http://zabmedia.ru/news/80043/

05.10.2015

Липецкие опера пытались обчистить тысячи заемщиков

Участников преступной группировки задержали с поличным полицейские.

Сотрудники СУ СК России по Липецкой области закончили расследование крупного финансового преступления, участники которого обвиняются по ч. 3 ст. 183 УК РФ (незаконное получение сведений, составляющих коммерческую, банковскую тайну, совершенное из корыстной заинтересованности), ч.3 ст.33 ч.1 ст.30 ч.4 ст. 159.6 УК РФ (организация приготовления к мошенничеству в сфере компьютерной информации, совершенная группой лиц по предварительному сговору в особо крупном размере).

Организатором преступления стал бывший работник одной из липецких кредитных организаций. В период с ноября прошлого года по май текущего он, используя свое служебное положение, скопировал конфиденциальные сведения, содержащие персональную информацию о клиентах банка, а также номера их счетов, кредитных карт, составляющие банковскую тайну.

Злоумышленник склонил на свою сторону двух сотрудников уголовного розыска УМВД России по Липецку, договорившись с ними о похищении денежных средств со счетов клиентов данной организации. Для этих целей обвиняемые нашли соответствующих специалистов, которые передали им базу данных о более чем восьми тысячах клиентах кредитной фирмы, на счетах которых находилось более 430 миллионов рублей.

Похищенные деньги компьютерщики должны были передать им через посредника, не осведомленного об их преступных намерениях. Вечером 1 июня текущего года на трассе Липецк-Данков при передаче муляжей денежных купюр на общую сумму 39 миллионов рублей, якобы списанных со счетов клиентов банка, обвиняемые были задержаны сотрудниками собственной безопасности УМВД России по Липецкой области.

Обвиняемые в период расследования свою вину признали и активно помогали следователям.

http://gorodlip.ru/events/e29081609/

05.10.2015

Возбуждено дело по краже денег у 32 клиентов Сбербанка через страницу-двойник его мобильного сервиса

Фото с сайта ruzaym.ru

В Санкт-Петербурге возбуждено уголовное дело по хищению средств со счетов более 30 клиентов Сбербанка, которые воспользовались услугой "Мобильный банк" с подставной страницы, созданной хакерами, сообщает **пресс-служба прокуратуры северной столицы.**

По данным следствия, с 2014-го по 2015 год неустановленные лица с помощью вредоносного программного обеспечения, позволяющего подменять оригинальную страницу ОАО "Сбербанк России" на страницу-"двойник" при вводе персональных данных в программе "Мобильный банк", перечисляли средства его клиентов на электронные кошельки, а впоследствии обналичивали.

Правоохранителям поступило уже 32 заявления от граждан из разных регионов РФ, у которых похищено в общей сложности 206 773 руб. В результате оперативных мероприятий установлено, что злоумышленники действовали на территории Фрунзенского района Санкт-Петербурга.

В настоящее время по итогам проверок возбуждены два уголовных дела по п. "в" ч. 2 ст. 158 УК РФ (кража, совершенная с причинением значительного ущерба гражданину). Устанавливаются лица, причастные к преступлениям.

http://pravo.ru/news/view/122596/

12.10.2015

В Красноярском крае осужден организатор преступной группы, занимавшейся хищением денежных средств с использованием компьютерных технологий

Железнодорожный районный суд г. Красноярска вынес обвинительный приговор по уголовному делу в отношении жителя г. Санкт-Петербурга. Он признан виновным в совершении преступлений, предусмотренных ч. 4 ст. 159.6 УК РФ (мошенничество в сфере компьютерной информации).

Суд установил, что с апреля по август 2014 года молодой человек с использованием специально разработанной им программы «взламывал» компьютеры туристических агентств и фирм по продаже железнодорожных билетов, расположенных в разных городах России. Затем осуществлял дистанционное оформление железнодорожных билетов от имени указанных фирм на подставных лиц, находящихся с ним в преступном сговоре.

В результате оформления электронного билета он получал цифровой код, с помощью которого подставное лицо в терминалах самообслуживания по продаже билетов, расположенных в зданиях железнодорожных вокзалов, распечатывало билет, который сразу же сдавался в кассу в связи с отказом от поездки для «обналичивания» денежных средств. Половину полученной суммы подставное лицо переводило на банковские карты или электронные кошельки организатора, остальные денежные средства оставляло себе.

Преступная деятельность фигуранта по делу была пресечена на железнодорожном вокзале станции Красноярск. Сумма причиненного потерпевшим ущерба составила более 1,2 млн руб.

По результатам судебного рассмотрения житель г. Санкт-Петербурга признан виновным в совершении 34 преступлений, предусмотренных ч. 4 ст. 159.6 УК РФ. Ему назначено наказание в виде 5 лет лишения свободы с отбыванием в исправительной колонии общего режима.

Государственное обвинение по уголовному делу поддержано Красноярским транспортным прокурором.

http://genproc.gov.ru/smi/news/archive/news-920922/

12.10.2015

Хакера осудили за возврат железнодорожных билетов на 1,2 млн руб.

Фото tkgorod.ru

В Красноярском крае осужден хакер, который взламывал компьютеры турфирм, оформлял через них электронные ж/д-билеты, а затем сдавал их в кассу, сообщает пресс-служба Западно-Сибирской транспортной прокуратуры.

Железнодорожный районный суд Красноярска признал жителя Санкт-Петербурга виновным по ч. 4 ст. 159.6 УК РФ (мошенничество в сфере компьютерной информации – 34 эпизода).

По данным следствия, молодой человек разработал специальную программу для взлома компьютеров турагентств и компаний по продаже железнодорожных билетов. С апреля по август 2014 года он дистационно офомлял билеты на поезда от имени туроператоров на своих сообщников. После оформления электронного билета соучастники получали цифровой код, с помощью которого в терминалах самообслуживания на вокзалах распечатывали проездной документ и сразу же сдавали в кассу.

Половина вырученных с возврата билетов денег переводились на банковские карты или электронные кошельки организатора, остальные шли его сообщникам. Молодой человек был задержан на вокзале в Красноярске. Общая сумма ущерба оценена в 1,2 млн руб.

Суд назначил хакеру пять лет колонии общего режима.

http://pravo.ru/news/view/122811/

14.10.2015

Киберпреступники активно атакуют небольшие компании

Финансовый ущерб от серьезного киберинцидента продолжает расти для компаний среднего и малого бизнеса (СМБ). В 2015 году предприятия СМБ оценили его в 893 тысячи рублей, как свидетельствуют результаты исследования «Лаборатории Касперского»*. В эту сумму входят оплата услуг привлеченных специалистов для устранения последствий, упущенные бизнес-возможности и убытки, вызванные простоем.

Причем если от простоя и упущенных бизнес-возможностей считают себя пострадавшими только около трети компаний, то к услугам специалистов со стороны пришлось прибегнуть подавляющему большинству респондентов (86%). Траты же на эти услуги компании оценили примерно в 282 тысячи рублей. Упущенная прибыль, по мнению опрошенных, достигает 517 тысяч рублей. Кроме того, в результате киберинцидента бизнес несет репутационные потери. Ущерб от удара по имиджу предприятия СМБ оценивают в 188 тысяч рублей. Для сравнения, защита от киберугроз для небольшой компании обходится в менее чем 20 000 рублей в год.

Подобные потери могут грозить каждой компании малого и среднего бизнеса. Исследование показало, что почти все организации (96%) как минимум раз в течение года подвергались внешним угрозам, и 85% испытывали действие внутренних угроз, связанных с уязвимостями в ПО, риском потери устройств и неосторожными действиями сотрудников.

Высокая стоимость одного инцидента кибербезопасности объясняется в частности тем, что злоумышленники в результате успешной атаки получают доступ к важной рабочей информации: в 41% компаний это были внутренние операционные данные.

«СМБ-компании сегодня испытывают трудные времена. Им не только сложно предвидеть, что ждет их в будущем, как будет развиваться макроэкономическая ситуация и смогут ли они рассчитывать на поддержку государства, но и приходится тщательно обдумывать инвестиции и заботиться о каждом аспекте, который может повлиять на прибыль и репутацию. При этом практически каждая небольшая компания регулярно становится жертвой киберинцидентов, которые ведут к серьезным финансовым потрясениям. Мы рекомендуем внимательно относиться к вопросам информационной безопасности, чтобы не потерять прибыль, которая сегодня и так достается с большим трудом, тем более что потенциальные потери в десятки раз превышают стоимость защитных решений», — отметил Сергей Земков, управляющий директор «Лаборатории Касперского» в России, странах Закавказья и Средней Азии.

Для поддержки небольших компаний «Лаборатория Касперского» предлагает решение Kaspersky Small Office Security, специально разработанное для этого сегмента бизнеса. Для средних компаний подойдет решение Kaspersky Security для бизнеса. Отличительной чертой обоих продуктов является сочетание надежной защиты с простотой управления системой безопасности.

**Исследование «Информационная безопасность бизнеса», «Лаборатория Касперского» и B2B International, 2015 год. Опрошено более 5500 IT-специалистов из более чем 25 стран по всему миру, включая Россию.*

15.10.2015

Законодатели стремятся защитить пользователей от киберпреступников

Надежда Арабкина

Более 2,6 миллиарда рублей было похищено хакерами у россиян через системы интернет-банкинга с июня 2014 года по июнь 2015-го. Об этом сегодня на международной конференции «Тенденции развития преступлений в области высоких технологий» рассказал член экспертного совета при Комитете Госдумыпо информационной политике, информационным технологиям и связи, генеральный директор компании «Group-IB» Илья Сачков.

По его словам, кибер-преступник до сих пор воспринимается в обществе, как положительный герой, эдакий виртуальный Робин Гуд, который взламывает электронные кошельки богачей. На самом деле хакеры с одинаковым энтузиазмом крадут деньги со счетов и крупных компаний, и простых пользователей. И похищенные деньги идут отнюдь не на благотворительные цели.

«Виртуальный преступник ничем не отличается от реального, — говорит министр связи и массовых коммуникацийНиколай Никифоров. — И должен преследоваться по закону». По его мнению, законодатели во всём мире сегодня вынуждены переосмысливать правовое регулирование интернет-пространства в связи с новыми угрозами. Российские парламентарии также активно работают над законодательством в этой сфере. И довольно часто подвергаются критике со стороны профессионального сообщества.

«В нашей стране успешно действует механизм общественного обсуждения законопроектов, — подчеркнул министр, — и нужно пользоваться этим инструментом, чтобы донести свою позицию до депутатского корпуса, например, через такие отраслевые организации, как Институт развития Интернета или Российская ассоциация электронных коммуникаций. То есть не просто критиковать, а вносить предложения по решению проблемы».

Каковы же основные тренды высокотехнологичной преступности? Прогнозы экспертов, увы, неутешительны, хакеры активно разрабатывают и используют вирусные программы для краж через смартфоны. А базовый инструментарий для организации такой атаки легко приобрести на хакерском форуме за несколько тысяч долларов.

Виртуальные преступники могут совершить за одну секунду тысячу преступлений по всему миру, при этом они практически неуловимы.

Считается, что преследовать виртуальных воров должны реальные полицейские. С этим не совсем согласен эксперт отдела по борьбе с киберпреступностью национальной полиции Нидерландов Эрик Хэнрикус. Он рассказал о том, что в Голландии полиция все чаще расследует виртуальные преступления в партнёрстве с различными специалистами в сфере информационной безопасности. «Хакеры не работают «под ключ», — пояснил Эрик Хэнрикус. — Одни разрабатывают вредоносное ПО, другие отмывают деньги. И полиция тоже не должна заниматься расследованием киберпреступления «от и до», гораздо эффективнее привлекать экспертов, а также развивать международное сотрудничество, так как виртуальные угрозы универсальны, а преступность не имеет национальности».

http://www.pnp.ru/news/detail/102258

15.10.2015

По статистике киберпреступлений владельцы онлайн-счетов выиграли от девальвации рубля

Несмотря на сокращение размера ущерба, наносимого киберпреступниками, число инцидентов в этом году выросло втрое, в

том числе благодаря вирусам, заточенным под платформу Android,сообщает ТАСС со ссылкой на отчет компании Group IB по расследованию киберпреступлений.

Более половины хищений средств россиян через интернет-банкинг (свыше 60 %) в период с июня 2014-го по июнь этого года было совершено с использованиемоперационной системы Android. При этом более 99 млн руб. похищено у физлиц, а 61 млн из них – с помощью "троянов", заточенных под Android, говорится в отчете. Годом ранее эта сумма достигала 105,8 млн руб., однако при сокращении объемов в денежном выражении, число инцидентов выросло втрое.

По мнению гендиректора Group IB Ильи Сачкова, увеличение активности киберпреступников связано с относительной доступностью базового инструментария для организации таких атак – его можно купить на хакерских форумах за несколько тысяч долларов. Всего мошенники в России с начала года похитили через интернет-банкинг свыше 2,6 млрд руб., что в 3,7 раза меньше, чем за предыдущий аналогичный период. Ощутимее всего от киберпреступников пострадали юрлица, лишившиеся 1,9 млрд руб. (при этом объем хищений снизился более чем в четыре раза). Сами российские банки в результате целевых атак за отчетный период потеряли 638 млн руб., отмечает "Коммерсантъ".

Однако сейчас, согласно исследованию Group IB, российские хакеры переориентируются на западные рынки из-за девальвации рубля. По прогнозам компании, в 2016 году количество атак будет увеличиваться, однако их успешность сократится. При этом наибольшей проблемой будет хищение у простых граждан, использующих смартфоны и планшеты на Android.

http://pravo.ru/news/view/122948/

16.04.2015

Киберпреступления

Компьютер Дмитрия заблокировали хакеры, установив баннер на весь экран. Чтобы убрать баннер, нужно ввести шестизначный код. Естественно сообщают заветные цифры вымогатели только за деньги. Дмитрий заплатил мошенникам, но компьютер так никто и не разблокировал. Пришлось обращаться к экспертам, чтобы переустановить систему.

Ежесуточно хакеры блокируют около двух миллионов компьютеров. На пользователей интернет-сети идет настоящая охота. Зараженные ссылки, баннеры, файлы, письма с вирусами... Способов доставки вредоносного кода много. Общее одно – открывая их человек, сам загружает "червя" на свой компьютер.

Вирусы-вымогатели появились пять лет назад. Первые были весьма примитивны. Продвинутый пользователь мог за полчаса сам удалить их с компьютера. Сейчас появились продвинутые версии "червя", которых называют криптолокерами. Они занимаются шифровкой файлов пользователя. Для разблокировки даже эксперту требуется минимум полгода.

Действия кибермошенников попадают под статьи 272 и 273 уголовного кодекса: неправомерный доступ к информации и распространение вредоносных программ. Наказание - до семи лет лишения свободы. Вот только в России реальных сроков за подобные преступления почти нет. Хотя вычислить куда ушли деньги, несложно. Электронные кошельки прозрачны для правоохранительных органов. Гораздо сложнее, говорят эксперты, доказать, что человек получивший деньги и преступник разместивший баннер – одно лицо. След от баннера к хакеру отследить очень сложно.

Расследование такого дела может длиться годами. Поэтому правоохранительные органы за такие дела берутся неохотно. Рядовым пользователям проще соблюдать правила компьютерной гигиены. Во-первых, устанавливайте только лицензионные программы и пользуйтесь антивирусом. Во-вторых, всегда проверяйте безопасность сайта. В строке браузера при вводе адреса должен появиться "замок". В-третьих, самые важные данные храните на отдельном жестком диске. Тогда в случае блокировки компьютера вы сохраните ценную информацию.

http://www.1tv.ru/sprojects_utro_video/si33/p91757/pg132

16.10.2015

Киберпреступники внедряются в интернет-банкинг

За год с июня 2014 года по июнь 2015 года киберпреступники через системы интернет-банкинга в рунете похитили 2,6 млрд руб., следует из отчета компании Group-IB на конференции "Тенденции развития преступлений в области высоких технологий-2015". За аналогичный период прошлого года сумма была в несколько раз выше - 9,8 млрд руб. "Мы фиксируем снижение ущерба при росте количества атак",- уточнил руководитель сервиса киберразведки Bot-Trek Intelligence Дмитрий Волков.

Наибольший ущерб понесли юридические лица, лишившиеся в результате действий киберпреступников 1,9 млрд руб. Ежедневно жертвами кибератак становятся 16 компаний, теряющих в среднем 480 тыс. руб. Хакеры при этом научились обходить традиционные средства защиты: ни токены, ни дополнительная SMS-аутентификация не спасают от "автозаливов" -

троянов, позволяющих переводить деньги со счетов посредством подмены реквизитов. Подтверждая платеж, клиент, зараженный таким трояном, видит правильные данные получателя, хотя в реальности деньги уходят на счет злоумышленников.

Сами российские банки в результате целевых атак за отчетный период потеряли 638 млн руб. "Даже единичные атаки на клиентов крупных банков приносят большой доход",- говорит руководитель направления Bot-Trek Secure Bank Павел Крылов. Усиливается интерес злоумышленников и к торговым, и к брокерским системам. Так, в феврале была проведена первая в России успешная атака на биржевого брокера, длившаяся всего 14 минут и приведшая к ущербу около 300 млн руб.

Почти 100 млн руб. похищено у физических лиц, причем 61 млн руб.- с помощью троянов, заточенных под платформу Android. Уязвимость Android привлекает все больше злоумышленников, следует из отчета: появилось десять новых преступных групп, работающих с Android-троянами, а количество инцидентов выросло втрое. Ежедневно 70 пользователей мобильных банков на Android становятся жертвами киберпреступников.

По данным Group-IB, продолжается развитие экосистемы, обслуживающей совершение киберпреступлений. Услуги по обналичиванию похищенных денег принесли злоумышленникам 1,92 млрд руб. Растет оборот площадок, торгующих данными о банковских картах, логинах и паролях разных систем: выручка семи таких магазинов превысила 155 млн руб.

Согласно прогнозу, в следующем году разработчики вредоносного софта полностью сосредоточатся на мобильных платформах, число инцидентов и суммы хищений у физических лиц увеличатся за счет перехвата на Android-устройствах данных карт, логинов и паролей для интернет-банкинга. Кроме того, компании столкнутся с еще большим количеством инцидентов с программами, шифрующими данные для последующего вымогания денег за их расшифровку (криптолокерами). Вырастет и количество хищений информации о банковских картах через POS-терминалы: появляется все больше программ для этих целей, а часть из них находится в открытом доступе.

Источник: Коммерсантъ
http://www.astera.ru/news/?id=113194

16.10.2015

За год киберпреступники похитили более 2,6 миллиарда рублей

Хакеры уже умеют перехватывать СМС-подтверждения платежей

Нина Забелина. Независимая газета, 16 октября 2015

Ежедневно в РФ жертвами кибератак на системы интернет-банкинга становятся 16 юридических лиц, теряющих в среднем по 480 тыс. руб. Общая сумма ежегодного ущерба оценивается в 1,9 млрд руб. В феврале 2015 года была проведена первая успешная атака на российского биржевого брокера. За 14 минут банк лишился более 5 млн долл.

Вчера в Москве прошла конференция «Тенденции развития преступления в области высоких технологий». Открывая мероприятие, глава Минсвязи Николай Никифоров отметил, что преступник в Интернете ничем не отличается от преступника в обычной жизни: «В этой сфере, в виртуальной среде, по сути, необходимо добиться соблюдения базового действующего российского законодательства».

При этом речь идет не только о федеральных законах, но и о различных нормативных актах министерств и ведомств, заметил он. «Важно сделать так, чтобы преступника преследовали, а ответственность была неотвратима», – подчеркнул министр. Он сообщил, что за время его трехлетней работы в министерстве число пользователей Интернета увеличилось в России на 27 млн человек, многие из которых не понимают опасности киберпреступности, включая и прямое хищение денежных средств.

Согласно отчету международной компании Group-IB, представленному на конференции, в РФ за год, с июня 2014 по июнь 2015 года, через системы интернет-банкинга хакеры похитили более 2,6 млрд руб. Физические лица лишились более 99 млн руб., из них 61 млн руб. – с помощью троянских вирусов для операционных систем мобильных устройств. Как рассказал глава компании Илья Сачков, уязвимость мобильных операционных систем привлекает все больше злоумышленников: «Только за последний год выявлено 10 новых преступных групп хакеров, специализирующихся на создании Android-троянов. Ежедневно около 70 пользователей мобильных банков на «андроидах» становятся жертвами преступников».

У юридических лиц хакеры за прошлый год похитили около 1,9 млрд руб. Преступники научились обходить традиционные средства защиты систем дистанционного банковского обслуживания: ни токены (компактное устройство, предназначенное для обеспечения информационной безопасности пользователя), ни дополнительная SMS-аутентификация не спасают юрлиц от «автозаливов» троянов, позволяющих похищать средства со счетов компаний. Руководитель подразделения Bot-Trek Secure Bank Павел Крылов сообщил, что наибольший интерес для хакеров сегодня представляют банки: «За последний год появились две новые

преступные группы, в результате их атак российские банки потеряли 638 млн руб. В феврале 2015 года была проведена первая успешная атака на российского биржевого брокера. Она длилась всего 14 минут. Ущерб же составил более 5 млн долл.».

Параллельно с хищениями растет и нелегальный бизнес торговцев данными банковских карт, логинов и паролей разных систем. Выручка зафиксированных семи таких «магазинов» составила за год более 155 млн руб. Расширяется рынок, обслуживающий хищения через устройства считывания банковских карт (так называемые POS-терминалы на рабочем месте кассира). Преступники даже продают устройства обработки банковских карт, которые похищают данные клинентов, по 15–20 тыс. рублей за штуку.

Наиболее опасные банковские бот-сети имеют прямое отношение к русскоговорящим хакерам, утверждает Илья Сачков. Однако нынешний кризис парадоксальным образом повлиял на киберпреступность. «Из-за девальвации рубля злоумышленники из РФ и стран СНГ переориентируются на Запад. Из-за этого масштабы хищений в России за последний год сократились в 3,7 раза», – утверждает Сачков. Кроме того, в прошлом году были задержаны члены одной из крупнейших хакерских команд Anunak, которую составляли выходцы из разгромленной в РФ группировки Carberp.

Всего за неполные два года преступникам удалось похитить около 1 млрд руб. из российских банков, утверждает Илья Сачков. Несмотря на видимое сокращение объема хищений, количество атак растет на сотни процентов. «12 самых популярных троянов разрабатываются русскоговорящими хакерами», – рассказал о сомнительных достижениях наших соотечественников Сачков.

Киберпреступность будет расти, прогнозируют эксперты. Можно ожидать увеличения инцидентов с фишингом (выманиванием паролей) у клиентов банков. Также может увеличиться число инцидентов с программами шифрования для последующего вымогания денег за их расшифровку (криптолокерами).

Вчера на заседании Межведомственной комиссии Совета безопасности РФ также обсуждали вопросы противодействия угрозам в сфере информационной безопасности. «На заседании выработаны меры по противодействию уязвимости коммуникационных технологий в связи с ростом числа попыток несанкционированного доступа в используемое органами госвласти ПО и оборудование», – сообщили в пресс-службе Совбеза.

http://www.aferizm.ru/novost/2015/10/151016-1-ciber-crimes-2015.htm

16.10.2015

Киберпреступность не остановить

Елена Шашенкова

15 октября 2015 г. в Москве прошла конференция «Тенденции развития преступлений в области высоких технологий 2015».

Организатор мероприятия – Group-IB – международная компания, область деятельности которой связана с предотвращением и расследованием киберпреступлений и мошенничества с использованием высоких технологий. Напомним, Group-IB начала свою деятельность в России 12 лет назад. На сегодняшний день компания обладает крупнейшей в Восточной Европе лабораторией компьютерной криминалистики, которая производит экспертизы и исследования в 80% всех резонансных дел в области высокотехнологичных преступлений. Group-IB входит в семёрку мировых компаний, влияющих на информационную безопасность мира.

Министр связи и массовых коммуникаций РФ Николай Никифоров

Министр связи и массовых коммуникаций РФ Николай Никифоров отметил, что технологическая революция, которую переживает весь мир, ставит перед компаниями новые вызовы, на которые нужно отвечать. Этим занимаются российские компании, разрабатывающие решения для обеспечения информационной безопасности. Но и киберпреступники не дремлют. Европейская пресса, по словам Николая Никифорова, всё чаще публикует статьи об угрозах со стороны российских хакеров. И это не пустые слова.

Киберпреступления происходят на фоне изменения геополитической обстановки и экономической нестабильности. Однако представители различных стран понимают необходимость сотрудничества в борьбе с киберпреступниками. «22 октября пройдет встреча министров связи стран БРИКС, на которой, в числе прочего, будет обсуждаться вопрос кибербезопасности», - информировал Николай Никифоров.

Министр отметил, что проникновение услуг широкополосного доступа в Интернет в России постоянно растет. Однако многие новые пользователи не понимают рисков и угроз, которые для них несет виртуальная среда. «В виртуальной среде необходимо добиться соблюдения

российского законодательства, которое уже действует в обычной жизни. Преступник в Интернете ничем не отличается от преступника в реальности, для него должна быть предусмотрена ответственность за совершение противоправных действий», - подчеркнул Николай Никифоров.

Генеральный директор Group-IB Илья Сачков солидарен с тем, что киберпреступность – это серьезная проблема. Чтобы ее решить, нужно понять основу данного явления и подобно медикам, объединить усилия в борьбе с кибер-эпидемией, охватившей мир. «Высокотехнологичная преступность подобна айсбергу», - отметил он.

Глава департамента киберразведки Group-IB Дмитрий Волков представил результаты исследования, проведенной аналитиками компании, о состоянии и динамике развития высокотехнологичных преступлений и актуальных киберугроз за 2014-2015 гг.

Отчет охватывает период с июня 2014 по июнь 2015 года. За этот период, в частности, было похищено через системы Интернет-банкинга более 2,6 миллиардов рублей.

Более 99 миллионов рублей было похищено у физических лиц, из них 61 млн. – с помощью «троянов», внедренных на мобильные устройства под операционной системой Android. По словам Дмитрия Волкова, уязвимость этой платформы привлекает всё больше злоумышленников. В 2012 году в стране действовало шесть групп, занимавшихся хищениями с помощью Android-троянов. Три из них были пойманы и арестованы. Но вместо выбывших появилось 10 новых преступных групп, а количество инцидентов выросло в три раза. Ежедневно 70 пользователей услуги «мобильный банк» становятся жертвами киберпреступников.

Генеральный директор Group-IB Илья Сачков

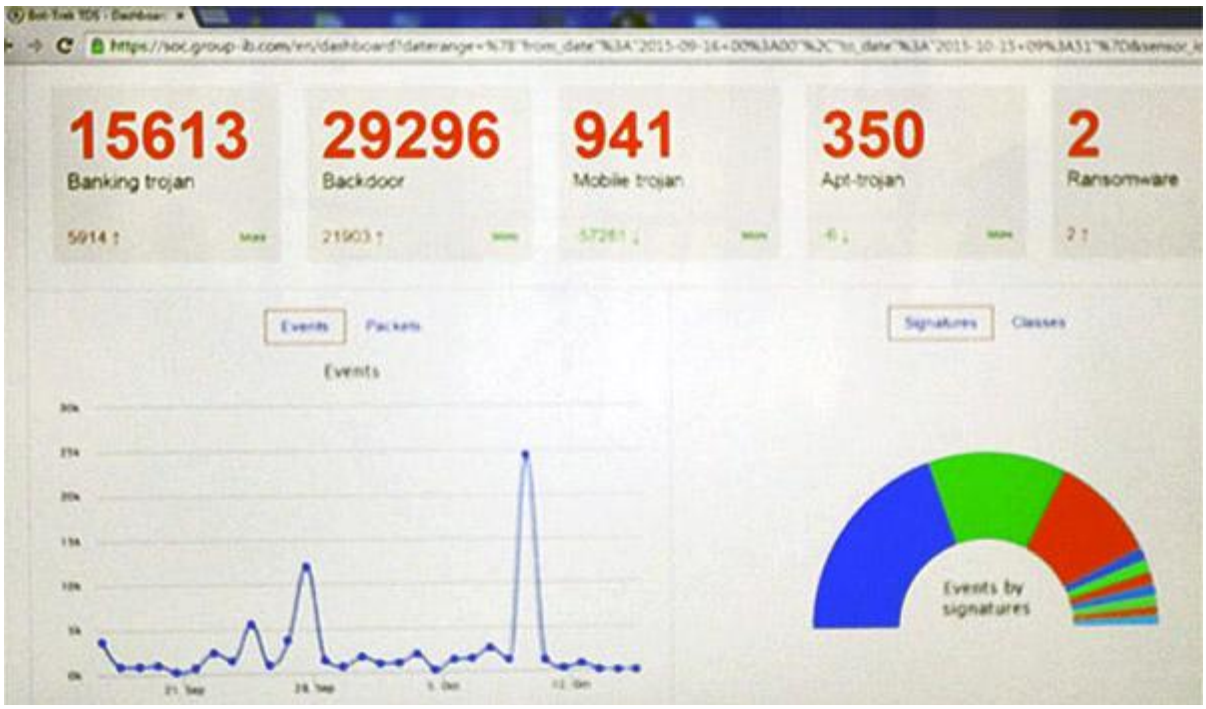
Создатели мобильных троянов продолжают развивать функционал, который позволяет хакерам осуществлять полноценный шпионаж за владельцем телефона: получать историю звонков и SMS, доступ к любым файлам на телефоне и информации в облачном хранилище, следить за местоположением пользователя. При этом отмечается снижение порога входа в преступный бизнес – базовый инструментарий для организации атаки на обычного пользователя можно приобрести на хакерских форумах за несколько тысяч долларов.

Но не только физические лица, но и компании страдают от действий киберпреступников. За год юридические лица лишились таким образом 1,9 миллиардов рублей. Хакеры научились обходить традиционные средства защиты систем дистанционного банковского обслуживания. Сегодня, к сожалению, ни токены, ни дополнительная SMS-аутентификация не спасают компанию от «автозалива» троянов, позволяющих переводить деньги со счетов посредством подмены реквизитов. Подтверждая платеж, клиент, чья система заражена таким трояном, видит правильные данные получателя, хотя в реальности деньги уходят на счет злоумышленников. «Ежедневно жертвами кибератак становятся 16 юридических лиц, теряющих в среднем 480 000 рублей», - говорится в исследовании.

Основной интерес мошеннических групп, специализирующихся на хищениях у юридических лиц – это клиенты крупных банков, даже единичные атаки на которых приносят большой доход. При этом можно прогнозировать, что после укрепления систем защиты крупных банков атаки перекинутся на клиентов более мелких банков, участь которых будет зависеть от способности адаптироваться к новым угрозам.

В исследовании отмечается, что на рынке появились две новые преступные группы, атакующие банки с целью получения доступа к системам, отвечающим за переводы денежных средств. В результате целевых атак российские банки за прошедший год потеряли 638 миллионов рублей.

В феврале 2015 года была проведена первая в России успешная атака на биржевого брокера. В день атаки курс российской валюты колебался от 55 до 66 рублей за доллар. Ущерб брокера составил около 300 миллионов рублей. Усиление интереса к торговым, расчетым и брокерским системам – тренд этого года.



Дмитрий Волков также отметил, что хакеры-профессионалы начали уходить с российского рынка. Причиной этого стала девальвация рубля: свой доход хакеры получали в рублях, а расходы были в долларах. Ушедшие хакерские группы переключились на европейские банки и частично на банки Австралии. Однако вместо ушедших в России стали действовать новые группы. Из-за недостатка опыта, они инициируют большее количество атак, но успешных среди них пока не так много.

В исследовании констатируется продолжение развития экосистемы, обслуживающей совершение киберпреступлений. Услуги по обналичиванию похищенных денег принесли злоумышленникам 1,92 млрд. рублей. Растет оборот площадок, торгующих данными о банковских картах, логинах и паролях разных систем. Выручка семи таких «магазинов» составила более 155 млн. рублей.

Прогнозы Group-IB по России и СНГ на предстоящий год таковы. Во-первых, постепенно прекратятся атаки на физические лица с помощью троянов для ПК, так как разработчики вредоносного ПО полностью сосредоточатся на мобильных платформах. Во-вторых, количество инцидентов и суммы хищений у физических лиц увеличатся за счет перехвата на Android-устройствах данных банковских карт, логинов и паролей для Интернет-банкинга.

Третье, вырастет количество инцидентов с фишингом в отношении клиентов банков в результате появления новых преступных групп и автоматизации процесса хищения денежных средств. В-четвертых, у юридических лиц увеличится количество индицинтов с программами, шифрующими данные для последующего вымогания денег за их расшифровку («криптолокерами»). Далее, эффективность троянов («автозаливов»), подменяющих реквизиты платежей для юридических лиц будет снижена за счет внедрения новых систем защиты крупными банками, а злоумышленники могут переключить свое внимание на хищения с удаленным доступом.

Количество хищений информации о банковских картах через POS-терминалы продолжит расти, так как увеличивается количество программ для этих целей. Напомним, часть таких программ находится в открытом доступе. И, наконец, продолжится рост целевых атак на банки за счет появления новых игроков, но их эффективность в количественном показателе останется невысокой.

Erik Henricus Antonius Van de Sandt – Central Criminal Investigations Division of The Netherlands National Police отметил, что бороться с киберпреступностью нужно объединенными усилиями. Так, в Голландии полиция пришла к выводу и необходимости сотрудничества с частными компаниями, специализирующимися на борьбе с кибермошенниками, а также действительными и потенциальными жертвами. Собранную полицией информацию можно использовать для предотвращения дальнейших киберпреступлений. «Только совместные усилия помогут вытеснить преступные группы с локальных рынков», - полагает Erik Henricus Antonius Van de Sandt.

Представители Microsoft, операторов «большой тройки» рассказали участникам конференции об усилиях, которые они предпринимают для борьбы с кибермошенниками и защиты

своих клиентов от их преступных действий. Свои решения представили РТ-Информ, «Сколково» и других компаний.

http://ict-online.ru/news/n123349/

19.10.2015

Хакеры из России взломали сервера Dow Jones

Александр Абрамов

Американские спецслужбы зафиксировали несанкционированное вмешательство в работу серверов агентства Dow Jones. В похищении инсайдерской информации экономического характера подозревают группу компьютерных взломщиков из России.

СВЕЖЕЕ ПО ТЕМЕ

Госслужба признала уязвимость персональных данных на сайтах госуслуг

Хакерская атака на JD.com завершилась кражей персональных данных россиян

Американские спецслужбы зафиксировали кражу данных из компьютеров компании Dow Jones, занимающейся сбором и распространением важной информации финансового характера. Группой неустановленных злоумышленников были похищены предназначенные для печати данные, могущие представлять ценность для биржевых игроков. По некоторым сведениям, в атаке на сервера Dow Jones подозревают российских компьютерных взломщиков.

Согласно имеющейся информации, проникновение состоялось более года назад, но было ли оно единичным, или имело место регулярное хищение данных, неизвестно. Расследованием происшествия, как обычно, в случаях финансовых преступлений, расследуют ФБР, структуры министерства финансов США и Комиссия по ценным бумагам. Каких-либо официальных сообщений о данной расследовании представители американских властей не обнародовали, но и опровержения появившейся в печати информации тоже не последовало.

Инсайдерская информация, которая может помочь биржевым игрокам достичь успеха, интересует хакеров не впервые. Летом текущего года сообщалось, что группа российских и украинских хакеров сумела наладить хищение конфиденциальных данных о ценных бумагах многих компаний. В результате активной деятельности злоумышленников было украдено около 150 тысяч документов. Информация принесла хакерам и их американским сообщникам, проводившим операции на Нью-Йоркской фондовой бирже, не менее тридцати миллионов долларов заработка. Среди пострадавших оказались и крупные компании, в числе которых Hewlett-Packard, Boeing и Oracle.

http://ict-online.ru/news/n123424/

19.10.2015

Николай Ковалёв: «Началась новая техногенная эпоха – с кибервойнами, кибертерроризмом, киберпреступностью»

По данным Еврокомиссии, минимум 1 млн. пользователей Интернета каждый день подвергаются кибератакам. А совокупный ущерб для бизнеса от деятельности киберпреступников составляет, по разным оценкам, €85-290 млрд. в год. В Сети циркулирует не менее 150 тыс. компьютерных вирусов разной модификации. На вопросы о характеристиках очередной чумы XXI века – кибертерроризме, мерах борьбы с ним ответил экс-директор ФСБ России, председатель Комиссии Государственной Думы, член Комитета по безопасности и противодействию коррупции, член российской делегации в Парламентской Ассамблее ОБСЕ, генерал армии Н.Д. Ковалёв.

– Николай Дмитриевич, как советовали древние, перед вступлением в диалог давайте договоримся о терминах. Странные метаморфозы претерпевают некоторые слова. Так произошло со словом кибер, означавшем на древнегреческом «правительство», «управление». А сегодня, пожалуйста, кибер-почта, кибер-нож, кибер-спорт, кибер-пиратство, даже муниципальные образования с кибер встречаются – деревня Кибер-Спасское в Омской области, в Чувашии – деревня Хоп-Кибер. У вас какие ассоциации в связи со словом «кибер» возникают?

– В полярной экспедиции барона Врангеля в 1820-е годы участвовал врач Август Кибер, не наводит ни на какие размышления?

А если серьёзно, то математик и философ-логик Норберт Винер в 1948 году ввёл понятие кибернетика или – наука об управлении, написал одноимённую книгу. Он исследовал процессы управления с обратной связью, разработал футурологическую по тем временам теорию компьютера, позднее воплотившуюся в реальность. И что поразительно, в книге предупреждал об опасностях кибернетики, способной открыть перед людьми огромные возможности – как для

добра, так и для зла. Получается, кибертерроризмом следует считать разновидность терроризма, управляемого через Сети, Интернет. Давайте в нашей беседе словом «кибер-» именно в таком смысле и будем оперировать.

– Ладно, так тому и быть. У вас первое вузовское образование техническое, в 1972-м завершили учёбу в Московском институте электронного машиностроения. На лекциях вас предупреждали о вероятности применения компьютерной техники в террористических целях?

– В то время – нет, по простой причине, о которой я еще скажу. Фундаментальные работы в области компьютерной техники в нашей стране начались под Киевом на Украине в конце 1940-х. Была успешно создана МЭСМ – малая электронная счётная машина. В начале 1950-х, в Москве тот же учёный – академик Лебедев Сергей Алексеевич собрал БЭСМ – большую электронную счётную машину. БЭСМ – это 10 000 операций в секунду, подобных результатов тогда в Западной Европе ещё не достигли, и с Америкой мы шли почти ноздря в ноздрю. За достижения в вычислительной технике Лебедева удостоили звания Героя Социалистического Труда. Помимо прочего он заложил теоретические основы для создания суперкомпьютера серии «Эльбрус» и выступал категорически против «клонирования» отечественной электроники с импортных прототипов. Параллельно конструировались линии компьютеров «Стрела», М-2, потом «Сетунь», другие модели. Когда я поступал в институт, это было в 1967 году, Лебедевская команда запустила очередную модель БЭСМ со скоростью 1 000 000 операций в секунду! Для того времени – это было нечто! Машину тут же задействовали в системе столичной противоракетной обороны, она успешно прослужила до начала нулевых годов.

– Тогда непонятно, куда эти достижения пропали, отчего в стране прекратилось собственное конструирование компьютерной техники? Мы же сегодня плотно на игле импортной электроники сидим.

– Когда я уже учился в МИЭМ, советское руководство приняло решение: в развитии компьютерной техники ориентироваться на американскую IBM. Повод – множественность электронных разработок разными научными школами: лебедевские эмки, «Урал», «Минск», «Весна», другие. Только вот беда: каждый тип машины – сам по себе. Отличные, добротные модели вне системного взаимодействия и стандартизированной архитектуры. Не было даже внутренней сети типа Интернета. А значит, у аналитиков и прогнозистов не возникало гипотез о вероятности кибертерроризма. Кого атаковать? Приятелей-учёных из кабинета этажом ниже?

В общем, вместо разработки собственной компьютерной сети, введения технической и программной стандартизации у нас поступили иначе: пошли на конструкторскую компиляцию. А в США межкомпьютерной связью плотно занялись в конце 1950-х после запуска советского спутника. Всполошились, что стали уязвимы и приступили к поиску вариантов надёжной системы передачи информации в интересах противоракетной обороны. В итоге создали ARPANET, переросший затем в INTERNET, о чём сегодня каждый школьник знает. Это всё происходило на рубеже конца 1960-х – начала 1970-х. Тогда американцы, углядев коммерческую перспективу, быстро сориентировались и продемонстрировали Алексею Николаевичу Косыгину во время его визита в США возможности компьютерной техники компании IBM. Премьеру презентация приглянулась, кое-кто из советских академиков идею компиляции обосновал, и механизм заработал. Так зарубежные технологии оказались в наших пределах, затирая собственные. Но технологии не передовые, остатки с барского стола, что естественно. Кто станет делиться настоящим ноу-хау? Тем более в условиях «холодной войны». Хотя в союзных нам странах СЭВ, например, в ГДР, разрозненные производства персональных компьютеров объединили в один кулак – ROBOTRON. Мы же пошли своим путём...

– Получается, семидесятые годы стали роковыми для развития независимых отечественных компьютерных технологий?

– Да. Прошло недолгое время, и в 1974-м США против СССР включили поправку Джексона-Вэника. А премьеру А.Н. Косыгину в уши жужжали в 1971-м. За этот недолгий промежуток времени у нас разогнали немало профессиональных коллективов, которые специализировались на оригинальных разработках продвинутых компьютерных технологий сугубо в отечественном исполнении. Податливых обязали заниматься исключительно заокеанским копирайтом. Затем грянул Афганистан, 1979 год, введение дополнительных эмбарго на ввоз высоких технологий… В результате, на излёте перестройки государственная компьютерная политика, а по большому счёту – вся электронная, завершилась тем, что и компилятивные разработки на базе IBM, и собственные технические достижения – «Агат», «Корнет», «букашка» – «БК», всё вместе с разваливающейся экономикой полетело в тартарары. Образовалась пустота и её немедленно заполнили, сами знаете, чьи компьютеры и прочая электронная техника. Включая утюги, тостеры и кофемолки. К этому времени Интернет стал движком сетевых протоколов Всемирной паутины, активнее начал эксплуатироваться как самодеятельными хакерами, так и профессионалами, в том числе работающими на террористические группировки.

– Появление Сети породило новую разновидность терроризма?

– Совершенно верно. В дополнение к уже существовавшим ядерному, химическому, биологическому, другим видам. Этот момент отражён в Концепции противодействия терроризму в Российской Федерации от 2009 года. В ней подчёркивается важность подготовки высокопрофессиональных кадров для противодействия специфическим разновидностям терроризма, в частности, кибертерроризму.

Увы, определённым категориям людей патологически свойственна тяга к насилию. Как только проклюнутся новые технологии и технические продукты, тут же начинается их примерка к использованию в качестве боевого оружия, инструмента политического давления. Организованная преступность, террористические сообщества, даже хакеры-самоучки работают здесь, надо признать, на опережение, порой на годы. Это ли не повод бить в колокола? Теперь оказывается, даже компьютерами социальной инфраструктуры, задействованными в функционировании, например, канализационной системы, можно благодаря Сети управлять извне. И таким образом программировать утилизацию человеческих отходов, так что в случае чего мало не покажется. Началась новая техногенная эпоха – с кибервойнами, кибертерроризмом, киберпреступностью. Вы знаете, сколько людей проживает на нашей планете, сколькими компьютерами они пользуются?

– По Счётчику роста население Земли – свыше 7 млрд. 303 млн. (на 01.09.2014). А персональных компьютеров, если судить по ежегодным мировым продажам, только за последние десять лет, с 2004 по 2014-й было продано и ещё предстоит продать до конца декабря свыше 3 млрд. штук – стационарных, включая промышленные, ноутбуков, планшетников, карманных и прочих. Какая-то доля из них через несколько лет приходит в негодность, но всё равно, предполагаю, в среднем по одному ПК на каждые четыре-пять человек приходится. Это без учёта 5-6-ти, если не больше, миллиардов сотовых телефонов с доступом в Интернет. Из тринадцати лидирующих стран по концентрации компьютерной техники в 2012-м первенствовали американцы, а в текущем году их китайцы, наверное, всё-таки обойдут. Россия пока ближе к концу списка. Надеюсь, ненадолго там задержимся.

– Внятный рапорт. А не вступить ли вам в кибердружинники, в Лигу безопасного Интернета, там народ боевой собрался? Я не напрасно поинтересовался численностью жителей Земли и количеством проданной компьютерной техники. В этих показателях и кроется ответ на вопрос о масштабах потенциальной киберугрозы. Даже одним амбициозным вундеркиндом, решившим поразвлечься в Интернете, может быть нанесен ощутимый вред всему мировому сообществу. Яркий пример – некий школьник, житель немецкого посёлка. Юноша усердно посещал факультативные занятия по информатике, но полученные знания использовал не во благо, а во вред: конструировал вирусы. Лучше б какую-нибудь обучающую игрушку для детей придумал, интернетсайт антихакерский или хотя бы в своей комнате прибрался… Нет, запустил пару «червяков» во Всемирную паутину на своё 18-летие в апреле 2004-го, хотел, как он позднее оправдывался, проверить надёжность мировой компьютерной безопасности. Его быстро вычислили, через неделю. Корпорация Майкрософт, чьи операционные системы дискредитировались, как имеющие «дыры» для проникновения вирусов, объявила о вознаграждении в $250 тысяч за поимку злоумышленника. Юного «гения» тут же приятели «слили» и поделили премию. Опередили мировые спецслужбы, которые к розыску подключились. А к этому времени успели уже, как водится в цивилизованном мире, Россию и Китай обвинить во всех тяжких. Юношу арестовали. Но «червяк», им сконструированный, в последующие месяцы и даже годы наследил здорово, по всему миру заразил десятки миллионов компьютеров. В Финляндии даже банк на некоторое время закрылся вместе со 120-ю офисами. Частично были парализованы службы Еврокомиссии – больше тысячи компьютеров погасли. В Великобритании около двух десятков подразделений Береговой охраны «ослепли». В США авиакомпания на два дня рейсы отменила. И так далее. Так что день рождения школяр отметил глобально. Ущерб ему по суду вменили в 130 тысяч евро, но это мизер в сравнении с совокупным многомиллионным материальным уроном для всех пострадавших от его проделки. И вирусы, повторюсь, «жили» не один год после их запуска в Сеть.

– Это вы о Свене Яшане вспомнили, он из Северной Германии, из-под Бремена. Вот, смотрите, я в Интернет зашёл, видите? Парень до сих пор числится в рейтинговой десятке хакеров мира. Легко отделался, к нему отнеслись как к ребёнку. Пострадавшие представители бизнес-сообщества требовали более сурового наказания, но суд приговорил к 21-му месяцу условно с испытательным трёхгодичным сроком и 30 дням общественных работ. И вот ещё, обратите внимание, школяра тут же наняла на работу немецкая фирма, которая специализируется на компьютерной безопасности... Николай Дмитриевич, по меркам норм права, Яшан, он какой кибер – террористический или криминальный?

– Как следует из приговора, немецкий суд признал его киберпреступником. По российским законам был бы такой же вердикт. Надо проводить водораздел между киберпреступностью и кибертерроризмом, как разновидностью терроризма. В Федеральном законе о противодействии терроризму доходчиво излагается: терроризм есть идеология насилия и практика воздействия на принятие решения органами государственной власти, органами местного самоуправления или

международными организациями, связанные с устрашением населения и (или) иными формами противоправных насильственных действий. Электронные мошенничества, хулиганства хакеров, брошенных семьёй и обществом, а от того не знающих, куда девать свою неуёмную энергию, и прочие компьютерные «шалости», – не из этой оперы.

– И всё-таки. Когда я вникал в правовые акты, регулирующие борьбу с терроризмом, то испытал недоумение. Может быть, вы разъясните и мне, и читателям «Столетия» следующие нестыковки, мною найденные. Зачитываю: 16 января 1997 года была образована Межведомственная антитеррористическая комиссия Российской Федерации, вы были её председателем. В Положении о Комиссии нет и намёка на существование в мире кибертерроризма, ни строчки о компьютерах, электронике, цифровой связи. Допустим, тогда острота кибертеррора не вызывала к себе повышенного внимания. Но этих слов нет и в Федеральном законе «О борьбе с терроризмом» 1998 года, нет в сменившем его Федеральном законе «О противодействии терроризму» 2006 года, нет в Положении о Национальном антитеррористическом комитете, созданном 15 февраля 2006 года. Не нашёл я их в Федеральном законе «О Федеральной службе безопасности», за исключением «выявления электронных устройств, предназначенных для негласного получения информации, в помещениях и технических средствах». Это правовой пробел или чекистская хитрость?

– С вами не соскучишься! На самом деле ни пробела, ни ведомственной уловки здесь не было и нет. Невозможно все возникающие явления, входящие в ведение спецслужб, запихнуть в один закон или в одно положение. Это с одной стороны. С другой стороны, игнорировать с юридической и управленческой точек зрения новые тенденции и проблемы тоже было бы непростительно. Как тогда поступать? Обычно на перспективу в правовые акты про запас, на будущее, закладывают термины, понятия и категории, поглощающие явления частного уровня. Так и в нашем случае. Кибертерроризм – разновидность терроризма. Кибернападения гражданских и военных хакеров, террористов организуются через Сети, Интернет. Сеть – это цифровые потоки, проще – вид информации. Поэтому в Федеральный закон «О противодействии терроризму» включены, в частности, понятия «телекоммуникационные системы», «каналы электронной связи», не говоря уже о фундаментальной категории – «информация», «информационная безопасность». Эти категории поглощают понятие «кибернетическая безопасность», в англоязычном варианте – cybersecurity. Так что в одном вы, безусловно, правы, кибертерроризм вошёл в силу, но эта тенденция российскими спецслужбами была упреждающе отслежена и конкретно, точечно закреплена в нормативных документах. В подтверждение вернёмся к началу нашего разговора: в Концепции противодействия терроризму термин кибертерроризм – есть. Еще раньше, в 2000 году, в Доктрину информационной безопасности Российской Федерации включались фразы, вроде «передача информации по каналам связи», «сети передачи данных» и т.д. В Уголовном кодексе фигурирует квалифицирующий признак – «информационно-телекоммуникационные сети».

– Тогда непонятно, почему по нашему УК «террохакеров» вроде немца Яшана привлечь к строгой ответственности не получится, если кувалда «инфо-теле» в Уголовном кодексе прописана?

– Это другая сторона медали правового регулирования борьбы с кибертерроризмом. И вы правы: пока она отчеканена недостаточно рельефно. В семи из восьми антитеррористических статей УК, где напрямую толкуется о терроризме, квалифицирующий признак «информационно-телекоммуникационные сети» отсутствует. Он охватывает другие деяния, например, статью 171.2 (Незаконные организация и проведение азартных игр), внесён ещё в 11 статей. Из антитеррористических норм близкий нашей беседе квалифицирующий признак отражён только в части 2 статьи 205.2 (Публичные призывы к осуществлению террористической деятельности или публичное оправдание терроризма), он так звучит: «те же деяния, совершенные с использованием средств массовой информации». Но данный признак у́же первого – «информационно-телекоммуникационные сети». Это следует из части второй статьи 1 Закона Российской Федерации «О средствах массовой информации». В ней закреплено: сайт в информационно-телекоммуникационной сети «Интернет», не зарегистрированный в качестве средства массовой информации, средством массовой информации не является. И точка. А вот квалифицирующий признак «информационно-телекоммуникационные сети» подобного уточнения не требует, так как шире понятия «средства массовой информации».

– А к отягчающим обстоятельствам «инфо-теле» относятся? Совершение преступления с особой жестокостью, садизмом, издевательством, мучениями для потерпевшего признаётся отягчающим обстоятельством. Разве кибертеррор – это не жестокость, не издевательство над миллионами людей? «Инфо-теле» – это отягчающее обстоятельство?

– Нет.

– Чудеса! Законодательный парадокс какой-то. Широкие правовые категории, потенциально пригодные для борьбы с кибертерроризмом существуют, но когда речь заходит о противодействии ему конкретными уголовно-правовыми мерами – статьи УК оказываются

безоружными. Кибертерроризм в реальном мире – процветает, а в российском законодательном пространстве – отсутствует. На сайте РИА-Новости перечислены громкие кибератаки за последние 14 лет. Их за три десятка переваливает без учёта помельче. С каждым годом – их больше и с нарастающим ущербом, в том числе политическим. Последний взбудораживший мир случай – кибератака на аккаунт в Твиттере главы российского правительства Дмитрия Медведева. Получается, признать этот факт актом терроризма, осуществлённого через Сеть, при всём желании не удастся?

– При большом желании белое в чёрное и наоборот перекрасить можно. А с точки зрения действующего российского антитеррористического законодательства, повторяю, – нет. Дальнейшее совершенствование правовых конструкций, направленных на предупреждение и борьбу с кибертерроризмом, – дело важное и актуальное. Но, добавлю, еще и непростое.

– На Западе, как известно, нас вместе с китайцами регулярно «мордуют» обвинениями в мировом кибертерроризме. Чуть что – так сразу виноваты Россия и Китай! То якобы «троянов» запускаем, то атакуем энергосети, то водоснабжение и прочие инфраструктуры отключаем в странах, отстоящих от нас на тысячи и тысячи километров. Если в нашем законодательстве пока имеются определенные прорехи, не означает ли это, что отечественным киберслужбам недостает профессионализма? А если так, чего их тогда на Западе боятся?

– У нас бытует поговорка: в чужом глазу соринку замечает, в своём бревна не видит. Вы из Интернета не вышли? Найдите, если не затруднит, мировой рейтинг хакеров… Нашли? Теперь, пожалуйста, перечислите государства, из которых они родом. Фамилии не называйте, ни к чему их рекламировать.

– Вот, первый попавшийся рейтинг 10-ти супер-пупер по версии британской «The Telegraph». Зачитываю страны, где живут хакеры, от десятой – последней, к первой – лидирующей: 10. Германия; 9. США; 8. США; 7. США; 6. Канада; 5. США; 4. США; 3. США; 2. США; 1. США. Итого, восемь американцев и по одному хакеру из Канады и Германии. Здесь сразу статья из The Washington Post на память приходит, где ссылка шла на документы, рассекреченные Эдвардом Сноуденом. Американские спецслужбы только в 2011 году осуществили 231 кибератаку против России, Китая, КНДР и Ирана. На кибервойну в секретном бюджете американских спецслужб, были выделены $652 млн!

– Этот рейтинг, что зачитали, он какого года?

– …2009-го.

– А поближе к нашим дням есть что-нибудь, зайдите, пожалуйста, в Википедию, там, может, поновее найдётся кто-то.

– …Так, набираем: «Хакер Википедия»… Здесь всё те же лица и дополнительно три новых «героя»: США, США, Великобритания.

– Что и требовалось доказать: на воре и шапка горит. Убедились? Нет ни одного россиянина, ни одного китайца в мировом рейтинге хакеров, составленном за рубежом. Ни в Пекине, ни в Москве! Это ответ на вопрос: «Who is who?» Теперь о профессиональной подготовке российских киберструктур и нормативной базе. Коротко.

Разве долголетняя востребованность наших программистов в мире не говорит сама за себя? За рубежом конкуренция между специалистами по киберпространству высочайшая, но выходцы из России её преодолевают. Непосредственно в российские силовые структуры отбор специалистов ещё жёстче. Профессионалами высочайшего класса создаются сценарии кибератак и математические модели их отражения, анализируется международный и зарубежный опыт, отслеживаются глобальные и частные тенденции в этой области. И соответственно разрабатываются проекты нормативных документов национального и международного уровней. Киберподразделения функционируют уверенно, нередко прорывными темпами, и в ФСБ, и в ФСО, и в МВД, в других правоохранительных органах и спецслужбах. Статистику раскрытых киберпреступлений приводить не стану, она успешна. Хотя, конечно, и на старуху бывает проруха.

Наконец, с 2008 года действует Стратегия развития информационного общества в Российской Федерации. Под сотню директивных документов утверждено сроком действия до 2020 года, где рассматриваются проблемы информационной безопасности под разными углами зрения. Около ста! И эта работа координируется. Интенсивно партнёрство ведётся между государствами-участниками СНГ по выявлению и пресечению кибертерроризма. Данная тема на постсоветском пространстве стартовала лет десять назад. Она отслеживается в ОДКБ, кибертерроризм выделен отдельной строкой в Концепции сотрудничества государств-членов ШОС в борьбе с терроризмом, сепаратизмом и экстремизмом от 2005 года. До конца текущего года действует План консультаций между МИД России и Министерством иностранных дел и торговли Новой Зеландии на 2012-2014 годы, где вопросы борьбы с транснациональной организованной преступностью, включая кибертерроризм, обсуждаются на уровне директоров департаментов. Мы добросовестно намеревались развернуть международное сотрудничество против кибертерроризма в глобальном варианте. Представители Китая, России, Таджикистана и Узбекистана в ООН направляли в сентябре 2011 года совместное письмо Генеральному Секретарю этой организации с просьбой

распространить проект Правил поведения в области обеспечения международной информационной безопасности в качестве официального документа на 66-й сессии Генеральной Ассамблеи ООН. Хорошо систематизированный, первый в своём роде документ. В нём предлагались не только принципы и нормы конструктивного и ответственного поведения в мировом информационном пространстве, но также обязательства не использовать информационные технологии для проведения враждебных акций, агрессии. Не распространять информационное оружие (в редакции нашей беседы – кибероружие), не создавать кибероружием угрозы миру и безопасности.

Так что нужная работа нашей страной и союзниками в рамках противодействия кибертерроризму ведётся профессионально, энергично, нормативно выверено и по разным направлениям. Другой вопрос, что работу эту приходится осуществлять в условиях западной практики двойных стандартов, закулисного и открытого вероломства. Эти обстоятельства, конечно, раздражают, но и закаляют одновременно.

– Николай Дмитриевич, в киберпространстве, о котором мы так много сейчас говорим, распространено ваше выступление на антитеррористической конференции ОБСЕ в швейцарском городке Интерлакен. Доклад пользуется спросом не только среди профессионалов в области борьбы с терроризмом, но и среди студенческой молодёжи. Да и представители противного лагеря с ним, не сомневаюсь, ознакомились. Конференция прошла в апреле, а 1 июля на сессии Парламентской Ассамблеи ОБСЕ участники этого международного политического мероприятия согласились с вашими аргументами и поддержали Резолюцию «О борьбе с терроризмом», внесённую российской делегацией. Слух такой, что вы – автор Резолюции. Как проходила процедура её принятия?

– Да нет, конечно, как можно одному столь сложный документ написать? Над текстом не один день трудились вместе, дружно, высококвалифицированные специалисты из разных ведомств. Проект внесли в основную повестку дня в день открытия сессии Ассамблеи. Цель российской резолюции – инициировать приведение разрозненных национальных антитеррористически законодательств в соответствие с международными обязательствами, предусмотренными резолюциями Совета Безопасности ООН и другими антитеррористическими нормативными актами – конвенциям, Глобальной контртеррористической стратегией, международными документами в области прав человека, целым рядом других. Кроме этого, предлагается рассмотреть возможность принятия дополнительных мер по противодействию террористическим угрозам. В частности, реанимировать утраченную практику ежегодных международных антитеррористических конференций ОБСЕ, чтобы они целевым образом финансировались из бюджета Парламентской Ассамблеи. К сожалению, в процессе принятия резолюции не обошлось без эксцессов. Проект дважды пытались заблокировать, звучали провокационные предложения отнести Россию к пособникам терроризма. К счастью, здравомыслящих парламентариев оказалось подавляющее большинство, политически некорректные, неэтичные призывы не нашли поддержки. В результате из 57 представителей государств Европы, Центральной Азии и Северной Америки, входящих в состав Парламентской Ассамблеи ОБСЕ, 44 парламентария проголосовали «за», вдвое меньше – 21 человек – «против», 10 – «воздержались». И резолюция на пользу общему делу борьбы с терроризмом была принята.

– Кто воду-то мутил на сессии?

– К сожалению, наш сосед Латвия при поддержке США и Канады…

–Заключительный вопрос. Тема кибертерроризма в Швейцарии и вообще в Парламентской Ассамблеи ОБСЕ поднималась?

– Постоянно! В швейцарском Интерлакене участникам конференции вручили, на мой взгляд, ценнейшую брошюру, своего рода методическое пособие по мерам противодействия использованию Интернета в террористических целях. Экземпляра три привезли в Россию. Пособие подготовил мощный международный коллектив профессионалов под эгидой Управления ООН по наркотикам и преступности, которым руководит Юрий Викторович Федотов – наш, российский дипломат с богатым опытом зарубежной работы. Одновременно он является заместителем Генерального Секретаря ООН. О содержании пособия распространяться не стану, пусть это содержательное и крайне полезное издание превратится в эффективное оружие противодействия кибертерроризму.

– Николай Дмитриевич, спасибо, что нашли время для встречи. Конечно, хотелось бы затронуть моменты, связанные с кибершпионажем, кибервойнами и энергично создаваемыми за рубежом и в России так называемыми «кибервойсками», коснуться других нюансов развития информационных технологий. Но об этом, наверное, как-нибудь в следующий раз.

- Разумеется. И знаете, что ещё предложу, давайте соблюдём традицию 3 сентября, почтим жертв терроризма минутой молчания…

Автор Борис Калачев,

Источники -

http://www.stoletie.ru/rossiya_i_mir/nikolaj_koval...mom_kiberprestupnostju_477.htm,http://topwar.ru/

http://www.liveinternet.ru/users/dejavu57/post337353085/

19.10.2015

«Киберпреступность по прибыльности обогнала торговлю оружием»

Автор: Александр Третьяков, «Реальное время»

Вредоносное ПО становится все умнее и изворотливее, обходя все известные методы защиты. Об этом эксперты IT-отрасли заявили накануне в Казани в ходе конференции «Код информационной безопасности», в которой приняли участие представители 190 компаний. В частности, обсуждались проблемы резко изменившегося ландшафта угроз, а в качестве одного из главных трендов называлась необходимость сбора улик и уголовного преследования киберпреступников.

Это становится выгоднее, чем заниматься торговлей оружием

Открывалась конференция секцией «Тренды и угрозы в сфере информационной безопасности», модератор которой, консультант по информационной безопасности компании Cisco Алексей Лукацкий, предложил залу путем голосования выбрать тему для дискуссии – из «регуляторики», «импортозамещения» и «угроз». Большинством голосов была выбрана последняя тема.

В своем докладе Лукацкий привел довольно мрачную статистику Cisco. Цифры, касающиеся спама, исчисляются миллионами сообщений в секунду, миллиардами в день. Само вредоносное ПО становится все умнее и изворотливее, обходя все известные методы защиты. Например, еще оптимистично обсуждавшиеся на IT&Secure форуме «песочницы», оказалось, уже в ряде случаев не работают, запускаемые туда «баги» научились плодиться так, что песочница переполняется ими настолько, что ошибки вываливаются наружу и заражают систему.

Пессимизм специалистов по безопасности был ярко проиллюстрирован новой реальностью киберпреступности, фактически она оформилась в успешную индустрию, объем рынка которой оценивается в 1 триллион долларов.

— Ситуация будет только хуже, киберпреступность – это очень хорошая доля рынка. Зачастую это становится выгоднее, чем заниматься торговлей оружием, торговлей алкоголем… Это незаметно для многих, многие судьи до сих пор считают эти действия шалостью, а злоумышленники на этом хорошо зарабатывают. Эта индустрия, копирующая все, что делается в любом бизнесе, это свои платежные системы, адвокаты, компании, которые готовы тестировать вредоносный код, свои инструменты, которые гарантируют возврат денег, если код будет обнаружен.

Идеология поменялась, атака используется не только чтобы украсть деньги

Как рассказал «Реальному времени» ведущий аналитик отдела развития компании Dr. Web Вячеслав Медведев, существуют биржи по продаже вредоносов, на которых можно по частям купить и собрать любую конфигурацию вируса.

Организатор конференции, директор компании «Экспо-Линк» Ольга Поздняк отметила, что выбор тем «Кода ИБ» осуществляется по результатам опроса экспертов: «Интересуют конкретно угрозы, «шифровальщики», о которых сейчас очень много говорят. Не сбавляет популярности тема защиты от внутренних угроз – своих собственных сотрудников. Также эксперты отмечали всплеск, киберрынок растет страшными темпами».

Качественные изменения в структуре киберугроз отмечало большинство экспертов, время хакеров-одиночек, писавших для своего удовольствия, ушло.

— Цель атак абсолютно поменялась, если вы посмотрите последние пять лет, то это промышленные предприятия, ядерные реакторы, про банки вообще не говорю – это каждые день. Идеология поменялась, атака используется не только чтобы украсть деньги, а для информационной, политической, геополитической войны. Для того, чтобы столкнуть два государства, две нации, — рассказал Кирилл Ильганаев, менеджер по работе с ключевыми клиентами компании Fortinet.

Вы скорее всего заплатите, тем более если сумма будет не критическая

Алексей Лукацкий в своем докладе кроме всех прочих негативных факторов отметил и необычайную быстроту, с которой формируется черный киберрынок. Например, уже проведены маркетинговые исследования, сколько люди готовы платить за похищенную у них личную информацию. Например, переписку или фотографии. Сумма выкупа для западных стран составляет $300-500, для России — в несколько раз меньше.

— Сами себя поставьте на место человека, которому зададут вопрос: «Сколько вы готовы заплатить за возврат ваших данных?». Нет гарантий, что данные вам вернут, но попробовать, может, и стоит. Если вы обратитесь в правоохранительные органы – с вероятностью 99% ничего

не произойдет. Вы скорее всего заплатите, тем более если сумма будет не критическая. Это как раз новая тенденция — злоумышленники проводят то, чего зачастую не делают компании, занимающиеся безопасностью: они уточняют, сколько вы готовы платить.

В правоохранительные органы, несмотря на критику, также постепенно приходит понимание того, что интернет – это среда, которая требует присмотра. Робкие шаги в эту сторону делаются, как заявлял в ходе встречи с предпринимателями прокурор РТ Илдус Нафиков, надзорное ведомство давало поручение ориентировать органы МВД на работу в информационной среде. Хотя это пока и довольно далеко от уровня проблем, которые обсуждались на «Коде ИБ», тем не менее хоть какое-то движение в этом направлении уже есть.

Чтобы оборвать деятельность вируса в самом его разгаре и собрать доказательства – вынуть вилку из розетки

Впрочем, не сидят сложа руки и сами представители отрасли. Отдельный доклад о взаимодействии с правоохранительными органами представил ведущий аналитик отдела развития компании Dr.Web Вячеслав Медведев. Чтобы собрать достаточные для суда улики преступления, нужен целый набор грамотных действий. В качестве прогноза Медведев отметил, что вполне возможно, компаниям придется брать в штат не только специалистов по гражданскому праву, но и по уголовному.

С точки зрения технологического процесса в случае «инцидента» безопасности существует целый набор действий, которые должен совершить специалист. Начиная от того, что выдернуть зараженный компьютер из розетки (поскольку при выключении системы вирус может стереть следы своего присутствия).

— Да, возможны проблемы, но если мы хотим оборвать деятельность вируса в самом его разгаре, чтобы собрать доказательства – вилку из розетки!

После этого необходимы довольно далекие от IT-сферы действия, такие как вызов полиции, приглашение понятых и прочие, которые Медведев призвал делать при помощи подготовленных специалистов. При этом уже есть опыт судебных разбирательств, причем не всегда успешных, когда именно невозможность изолировать компьютер не позволила суду принять улики.

— Компания, которая проводила исследования, поменяла даты на образе – все, суд отверг улики. Для снятия, для того, чтобы суд это принял как доказательства, нужна специальная процедура и желательно специальное железо.

Отдельной проблемой Медведев назвал желание IT-специалистов как можно быстрее решить проблему, то есть уничтожить вирус и восстановить работу системы, что не позволяет собрать доказательства против злоумышленников.

Открытый код – головная боль импортозамещения

Еще одной фундаментальной проблемой в ходе конференции было обозначено использование открытого кода подавляющим большинством российских разработчиков. После ряда инцидентов с западными вендорами импортозамещение в российском IT стало вопросом национальной безопасности. Например, на основе открытого кода татарстанскими специалистами написана программа для ЗАГСа, и в настоящий момент создается аналогичная система для минтруда.

Однако время от времени звучавшие на различных отраслевых форумах и конференциях сообщения об уязвимостях открытого кода приобрели системное описание угрозы безопасности настолько, что проблемой занялись в ФСБ и Федеральной службе по техническому и экспортному контролю (ФСТЭК).

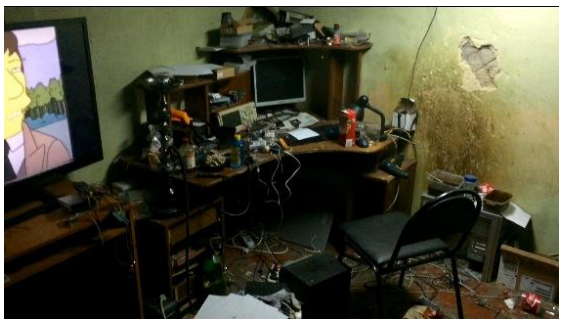
— Отслеживание информации, публикация информации об инцидентах, об уязвимостях — это те тренды, которые задаются уже регуляторами. Регулятор занимается актуальными проблемами и организует свои сервисы по отслеживанию. И ФСТЭК занимается, и ФСБ, — это те тренды, которые внушают оптимизм, — рассказал «Реальному времени» директор по развитию компании «Актив» Владимир Иванов.

Как отмечалось в ходе работы конференции, ФСТЭК активно сертифицирует открытый код. Эксперты в том числе предупредили и о том, что в случае обнаружения уязвимостей сертификаты могут быть и отозваны, что приведет к запрету использования такого ПО государственными структурами.

Источник >>

Фото (с) Роман Хасаев

http://d-russia.ru/kiberprestupnost-po-pribylnosti-obognala-torgovlyu-oruzhiem.html



2015

Киберпреступник-самоучка из сызранского барака

Место преступления, где орудовал сызранский хакер

Непримечательный барак в городе Сызрань: две комнаты и коридор. Никто не догадывался, что под крышей именно этого дома находилась комната обвиняемого в совершении киберпреступления. Она располагалась на чердаке жилого помещения.

Небольшое пространство, где можно было уединиться, выход в интернет и компьютер – этого было достаточно для того, чтобы осуществлять хакерские атаки.

По версии сотрудников уголовного розыска МУ МВД России «Сызранское», в комнате проживал 22-летний молодой человек, имеющий за плечами всего девять классов образования. Про таких, как он, говорят – самоучка. Обвиняемый жил скромно. Родители не смогли дать парню достойное образование. Поэтому он самостоятельно изучал специализированную литературу. Прочел горы книг, начиная от тех, что посвящены возможностям ЭВМ, и заканчивая руководствами по созданию и использованию вредоносных компьютерных программ. По версии следователей, обретя необходимые знания, молодой человек начал их применять на практике и зарабатывать деньги. На заказ разрабатывал сайты и различные программы. За это получал небольшие гонорары. Деньги тратил на еду, технику, помогал родным. Но, вероятно, парню этого было недостаточно. Обвиняемый, как сам потом признался следователям, отправил администраторам сайтов одного банковского учреждения и браузера сети интернет предостережение: мол, получше защитите свои данные от вероятных угроз. А потом и на деле решил доказать свои намерения. За несколько месяцев он, по версии полиции, создал вредоносную программу, которая позволила зарабатывать деньги, правда, обманным путём.

Материальное обогащение было не основным мотивом совершения преступления. По словам молодого человека, он хотел доказать таким образом собственные возможности и, вероятно, беспомощность систем безопасности некоторых крупных компаний.

По данным начальника отдела «К» БСТМ ГУ МВД России по Самарской области подполковника полиции Дениса Илюшина, о том, что на территории Самарского региона может действовать хакер, полицейские узнали от коллег из Тюменской области. К ним за помощью обратилась женщина и рассказала, что лишилась денежных средств, которые находились на ее банковском счете. В марте 2015 года на ее планшет, в который была вставлена сим-карта с абонентским номером, поступило смс-сообщение о запросе кода на номер 900, чтобы перевести денежные средства в сумме 8000 рублей на карту незнакомого ей получателя. Через минуту пришло следующее смс-сообщение о том, что денежные средства в сумме 8000 рублей на карту получателя переведены успешно. Женщина поняла, что кто-то пытается украсть ее денежные средства, и позвонила на «горячую линию» банковского учреждения, попросив заблокировать ее карту. Именно это помогло женщине сохранить оставшуюся часть денежных средств.

Полицейским удалось отследить переводы похищенных денежных средств на другие счета и установить, что они в конечном итоге были обналичены в городе Сызрань Самарской области, информирует пресс-служба облГлавка. Сотрудники полиции сразу поняли, что имеют дело с киберпреступником.

К розыску и задержанию «виртуального» преступника подключились самые опытные оперативники. Установить точное местонахождение злоумышленника и задержать его оказалось под силу сотрудникам отдела «К» БСТМ ГУ МВД России по Самарской области и их коллегам из уголовного розыска МУ МВД России «Сызранское».

В ходе проведения оперативно-разыскных мероприятий с использованием технических ресурсов полицейские установили адрес, по которому находился 22-летний подозреваемый. С целью его задержания оперативники выехали в Сызрань. На момент визита стражей правопорядка молодой человек спал. Когда увидел людей в форме – очень удивился. Явно не предполагал, что будет изобличен. В тот день сотрудники органов внутренних дел работали до пяти утра. Очень было важно ничего не упустить, найти и изъять все улики, опросить свидетелей. Тогда полицейскими были обнаружены компьютерная техника, флеш-носители, банковские карты и другие предметы, которые, предположительно, использовались для совершения преступления.

«За тринадцать лет службы на моей памяти около десятка задержаний виртуальных преступников. Сложность установления таких подозреваемых заключается в том, что они живут, как правило, обособленно. У них очень тесный круг общения. Свидетелей их противоправных деяний – практически не бывает. Впрочем, и преступления подобной квалификации носят латентный характер. Затрудняет процесс расследования преступлений в сфере высоких технологий такое обстоятельство, как сокрытие преступником следов своей деятельности, например, путем стирания данных или путем введения в компьютерную систему вредоносных программ. Очень часто в процессе оперативно-разыскных мероприятий возникает необходимость в тщательном анализе банковских переводов, исследовании носителей оперативной информации т.д. Для того, чтобы идти в ногу со временем, регулярно проходим обучение на базе академии МВД России. Полученных знаний хватает для того, чтобы нейтрализовать хакеров», - комментирует старший оперуполномоченный по особо важным делам отдела «К» БСТМ ГУ МВД России по Самарской области майор полиции Юрий Макавчик.

По словам старшего следователя СУ МУ МВД России «Сызранское» майора юстиции Марины Артамоновой, расследование уголовных дел в сфере компьютерной информации очень специфично. Поэтому необходимы специальные знания в области компьютерных технологий.

«Совместными усилиями с коллегами из отдела «К» собрали достаточную доказательную базу для предъявления обвинения молодому человеку. Большое значение в деле имели результаты проведенных компьютерно-технических экспертиз», - комментирует Марина Артамонова.

Около месяца эксперты изучали обнаруженное программное обеспечение. В результате удалось установить, что на изъятом компьютерном носителе в действительности находится вредоносное программное обеспечение. Оно предназначалось для несанкционированной модификации и копирования компьютерной информации. Именно при помощи этой программы были сняты денежные средства с банковской карты жительницы Тюменской области.

Суть данного нау-хау заключалась в перехватывании смс-сообщений пользователя операционной системы ANDROID, возможности скрывать входящие сообщения от всех отправителей, блокировать информацию на мобильных устройствах (смартфонах, планшетах).

Созданная злоумышленником программа позволяла копировать данные с лицевого счета банковской карты путем отображения сообщения о подтверждении платежных данных для сервиса Google Play. Молодой человек обвиняется в том, что в феврале 2015 года, используя сеть интернет, через пользователя с псевдонимом «Essoni» загрузил созданное вредоносное приложение на сотни устройств с операционной системой ANDROID. Среди них были выявлены телефоны, на которых подключена услуга «Мобильный банк».

Разработанная подозреваемым с нуля программа являлась шлагбаумом для преступной деятельности посредством сети интернет. Оставалось только ее запустить. А именно – разослать среди пользователей виртуальной сети специально подготовленное приложение с вирусом, которое молниеносно поражало операционную систему планшета или смартфона. К примеру, приходит к вам сообщение со ссылкой внутри – достаточно перейти по ней, и ваше устройство уже на «крючке» у хакера. Если к устройству с операционной системой ANDROID подключена услуга «Мобильный банк» - достаточно несколько минут, чтобы остаться без денежных средств. Ранее сотрудникам отдела "К" приходилось сталкиваться с тем, что преступники покупали уже готовое программное обеспечение, при помощи которого осуществлялась рассылка вируса с последующим хищением денежных средств. На криминальном рынке такая программа может стоить по-разному, в зависимости от модификаций, но в руках талантливого хакера она способна нанести ущерб, исчисляемый миллионами. В данном случае, подозреваемый изобрел все сам.

Следователи предполагают, что на счету преступного гения могут быть и другие эпизоды. Есть предположение, что жертвами задержанного стали жители других регионов страны. Сейчас данная версия тщательно проверяется. В настоящее время СУ МУ МВД России «Сызранское» окочено расследование уголовного дела в отношении 22-летнего жителя Сызрани, который обвиняется в совершении преступления, предусмотренного ч. 2 ст. 273, ч. 2 ст. 272, п. «в» ч. 2 ст. 158 УК РФ. Задержанный признал свою вину и в настоящий момент активно сотрудничает с сотрудниками органов внутренних дел. Уголовное дело направлено в суд для рассмотрения по существу.

Сергей Солодовников

«Для раскрытия и расследования киберпреступлений, самарская полиция все шире использует знания и достижения в сфере высоких технологий. Благодаря взаимодействию и слаженной работе следователей и оперативников в короткие сроки удалось раскрыть сложное в техническом плане преступление и нейтрализовать «виртуального» злоумышленника. Значительную роль в расследовании преступления сыграли собранные оперативниками улики и проведенные исследования, подтвердившие причастность задержанного к хищению денег в сети интернет. Кроме этого полицейские собрали достаточное количество доказательств для того, чтобы уголовное дело было направлено в суд и в скором времени злоумышленник понесёт наказание в соответствии с действующим законодательством", - прокомментировал начальник ГУ МВД России по Самарской области генерал-лейтенант полиции Сергей Солодовников.

Несколько советов от сотрудников отдела «К» БСТМ ГУ МВД России по Самарской области, которые помогут защитить Ваши банковские счета от преступников:

Не заполняйте анкеты, полученные по электронной почте. Личную информацию следует вводить только на официальных сайтах. Обычно на таких сайтах в правом нижнем углу есть значок висячего замка.

Никогда не проходите по ссылкам, предложенным в письме. Лучше всего скопировать адрес страницы и ввести его в адресную строку Вашего браузера.

Если Вам письмо кажется подозрительным, то лучше связаться с банком по телефону. Банк вряд ли будет запрашивать Ваши данные через электронную почту.

Обязательно установите на свой компьютер надежную антивирусную программу, которая сможет заблокировать фишинговые сайты.

Подключите к своему телефону смс-уведомления об операциях на Вашем банковском счете. Если это сделать невозможно, то чаще проверяйте баланс Вашего банковского счета, просматривайте все операции на кредитных картах.

Лучше всего подбирать сложный адрес электронной почты, чтобы злоумышленникам было трудно его подобрать. Лучше не использовать своё имя и фамилию.

Если адресат уже не раз присылал Вам подозрительные письма, то лучше внести его в черный список.

Не поддерживайте диалог со спамерами, чтобы злоумышленники не выявили действующий адрес электронной почты.

Часто пользователи сами становятся спамерами, рассылая одинаковые сообщения своим друзьям и знакомым. Будьте уверены, от того, что Вы не пошлете сообщение, беды с Вами и Вашими родными не случится, как это указано в подобных рассылках.

Если спама приходит слишком много, то лучше всего сменить адрес электронной почты. Не публикуйте свой адрес на общедоступных сайтах.

http://tltgorod.ru/reporter/?reporter=58505

20.10.2015

В Ульяновской области перед судом предстанет житель Майнского района, обвиняемый в кибермошенничестве на сумму более 1 млн рублей

Прокурор Майнского района Ульяновской области утвердил обвинительное заключение по уголовному делу в отношении 19-летнего Игоря Серебро. Он обвиняется в совершении преступления, предусмотренного ч. 2 ст. 159.6 УК РФ (мошенничество в сфере компьютерной информации, совершенное с причинением значительного ущерба гражданину).

Как полагает следствие, ранее судимый за кражу Серебро с помощью ноутбука через сеть «Интернет» подключался к сим-картам одной из компаний оператора сотовой связи.

Затем через систему «Мобильный банк» злоумышленник перечислял с лицевых счетов клиентов одного из кредитных учреждений денежные средства, которыми распоряжался по собственному усмотрению.

В результате с ноября 2013 по март 2014 гг. более чем 50 жителям Тамбовской, Костромской, Рязанской, Тульской, Владимирской и Курской областей был причинен ущерб в размере свыше 1 млн рублей.

После утверждения обвинительного заключения данное уголовное дело направлено в Майнский районный суд Ульяновской области для рассмотрения по существу.

http://genproc.gov.ru/smi/news/archive/news-930222/

20.10.2015

Международные эксперты по кибербезопасности обсудили тенденции развития высокотехнологичной преступности на конференции Group-IB

15 октября 2015 года на площадке DI Telegraph состоялась конференция «**Тенденции развития преступности в области высоких технологий 2015»**, организованная одной из ведущих международных компаний по борьбе с киберпреступлениями **Group-IB**. Открыл конференцию «Тенденции развития преступлений в области высоких технологий 2015» министр связи и массовых коммуникаций РФ **Николай Никифоров**.

Технологическая революция, которую переживает весь мир, ставит перед компаниями новые вызовы, на которые нужно отвечать. Этим и занимаются российские компании, разрабатывающие решения для обеспечения информационной безопасности.
Но и киберпреступники не дремлют. Европейская пресса всё чаще публикует статьи об угрозах со стороны российских хакеров, и это не пустые слова.

Николай Никифоров

Министр связи и массовых коммуникаций РФ

Участниками конференции стали более семисот человек, среди которых руководители и специалисты подразделений информационной безопасности государственных и коммерческих организаций, ведущие эксперты по расследованию высокотехнологичных преступлений, государственные деятели, представители профильных министерств и ведомств, международных CERT, а также журналисты. В мероприятии приняли участие гости из США, Австрии и Нидерландов.

Ключевыми темами конференции стали: объемы и прогнозы развития рынка киберпреступности, преступления и мошенничество в корпоративном секторе, современное цифровое пиратство и преступления с использованием известных брендов. Ведущие эксперты отрасли обозначили реальные угрозы киберпреступности, основные тренды кибератак и обсудили методы по уменьшению хищений у юридических и физических лиц.

Генеральный директор Group-IB **Илья Сачков** в своем выступлении подчеркнул, что киберпреступность — серьезная проблема. По его мнению, чтобы ее решить, нужно понять основу данного явления и подобно медикам, объединить усилия в борьбе с киберэпидемией, охватившей мир. «Высокотехнологичная преступность подобна айсбергу», — отметил он.

В рамках конференции эксперты Group-IB представили результаты отчета о тенденциях развития высокотехнологичных преступлений за прошедший год: убытки от действий киберпреступников составили более 2,6 млрд рублей. Отчет Group-IB доступен по ссылке:report2015.group-ib.ru

«Хакеры-профессионалы начали уходить с российского рынка. Причиной этого стала девальвация рубля: свой доход хакеры получали в рублях, а расходы были в долларах. Ушедшие хакерские группы переключились на европейские банки и частично на банки Австралии. Однако в России стали действовать и новые группы. Из-за недостатка опыта, они инициируют большее количество атак, но успешных среди них пока не так много», — рассказал **Дмитрий Волков**, глава департамента кибербразведки Group-IB.

Хуан Хардой, руководитель отдела по борьбе с киберпреступностью в странах Европы, Ближнего Востока и Африки Microsoft отметил, что использование нелицензионного программного обеспечения, в котором все чаще обнаруживается зловредный код, напрямую связано с ростом киберпреступлений. Эксперт рассказал о методах минимизации рисков на основе опыта Microsoft.

Рынок киберпреступности показывает драматические темпы развития. Так, согласно данным Norton, в мире каждые 12 секунд совершается удачная кибератака, жертвами которых становится 400 миллионов пользователей в год, — рассказал Хуан Хардой, руководитель отдела по борьбе с киберпреступностью в странах Европы, Ближнего Востока и Африки Microsoft, — Борьба с киберпреступностью — одно из ключевых направлений Microsoft, и сегодняшняя конференция — это хорошая возможность обсудить с профессиональным сообществом и экспертами рынка основные тенденции развития киберпреступлений и способы борьбы с ними.

Хуан Хардой

Руководитель отдела по борьбе с киберпреступностью в странах Европы, Ближнего Востока и Африки Microsoft

Эрик Ван Де Сандт, специалист Национального центра по борьбе с преступлениями в сфере высоких технологий (NHTCU) Национальной полиции Нидерландов, рассказал, почему государственно-частные расследования — это верный путь борьбы с киберпреступлениями и достижения общих целей с NHTCU.

Глава компании Kroll в России и СНГ **Алекс Волчич** посвятил свое выступление вопросу внутренних угроз утечки конфиденциальной информации.

Представители сферы телекома **Сергей Хренов** (Мегафон) и **Дмитрий Попков** (МТС) обратили внимание аудитории на растущее количество атак на физические лица с помощью вредоносного ПО для смартфонов и поделились механизмами защиты абонентов.

Владимир Кремер, руководитель отдела страхования финансовых рисков AIG в России, в своем докладе рассказал о достаточно новой услуге для российского рынка — страхования киберрисков.

Сергей Ходаков, руководитель направления «Безопасные информационные технологии» IT-кластера Фонда «Сколково», рассказал о новых решениях по обеспечению кибербезопасности в условиях меняющегося ландшафта угроз.

Во время мероприятия были также широко освещены вопросы, связанные с защитой от DDoS-атак (**Александр Лямин**, директор Qrator), социальной инженерии и информационной безопасностью (**Сергей Мартынов**, президент Российского отделения ACFE) и созданием центра

мониторинга и реагирования на компьютерные атаки в организации уровня Госкорпорации (**Андрей Губарев**, директор по безопасности РТ-Информ).

Помимо насыщенной деловой программы, гости мероприятия получили возможность познакомиться с выставочной экспозицией, включающей в себя, в частности, линейку программных продуктов **Bot-Trek**, которые разработаны специалистами Group-IB на основе 12-тилетнего опыта расследования и предотвращения высокотехнологичных преступлений, и уже работают в более чем 200 компаниях в России, США и Европе.

Ознакомиться с презентациями спикеров можно на сайтеreport2015.group-ib.ru

Особую благодарность организаторы конференции выражают концерну Audi Россия, предоставившему для гостей шаттлы Audi A8 - роскошные бизнес-седаны, сочетающие мощную динамику и величественное спокойствие. А так же партнеру по вопросам обеспечения безопасности мероприятия – холдингу Elite Security.

http://www.group-ib.ru/news/20-10-15-post.html

27.10.2015

Самое распространенное киберпреступление в Псковской области - кражи с банковских карт

Кроме того, регион лидирует в России по количеству мошенничеств в социальных сетях, к такому выводу пришли в руководстве УМВД по городу Пскову

По словам **Сергея Титова**, заместителя начальника городского управления, вместе с областной столицей это сомнительное первенство разделяет и второй по значению город региона – Великие Луки. Всего за девять месяцев 2015 года в области зафиксировано 2 545 преступлений в сфере мошенничеств, что на 33,7% больше, чем за аналогичный период прошлого года. Наиболее распространенное преступление в киберпространстве — кражи денежных средств с банковских карт и мошенничества, связанные с интернет-ресурсами.

За девять месяцев этого года по Пскову уже зафиксировано 487 преступлений. При этом — 190 краж средств с банковских карт и 297 мошенничеств в Интернете. Как уточняет «Псковская лента новостей», как правило, киберпреступники не проживают на территории Псковской области.

http://www.glavny.tv/news/9072

28.10.2015

В Московской межрегиональной транспортной прокуратуре утверждено обвинительное заключение по уголовному делу о совершении 16 эпизодов мошенничества в сфере компьютерной информации

Первый заместитель Московского межрегионального транспортного прокурора утвердил обвинительное заключение по уголовному делу в отношении 26-летнего гражданина Российской Федерации Романа Михайлова. Он обвиняется в совершении преступлений, предусмотренных ч. 1 ст. 210 УК РФ (руководство структурным подразделением, входящим в состав преступного сообщества) и ч. 4 ст. 159.6 УК РФ (мошенничество в сфере компьютерной информации, совершенное организованной группой).

По версии следствия, в июле 2013 года обвиняемый и его знакомый разработали преступную схему по хищению денежных средств юридических лиц, осуществляющих деятельность по дистанционному оформлению электронных железнодорожных билетов.

Созданное преступное сообщество представляло собой объединение нескольких групп, состоящих из 29 человек, действовавших на территориях г. Уфы, Республики Башкортостан, г. Москвы, Московской области и г. Санкт-Петербурга.

В соответствии с преступной схемой в организации, осуществляющие продажу железнодорожных билетов, были разосланы электронные письма с вредоносной программой. После открытия адресатом письма программа устанавливалась в операционную систему, и преступники получали полный доступ к информации, логину и паролю личных кабинетов кассиров организаций, незаконно оформляли билеты и обналичивали денежные средства путем их сдачи.

За время существования преступного сообщества его участники незаконно оформили более 500 железнодорожных билетов на общую сумму более 12 миллионов рублей.

С Михайловым заключено досудебное соглашение о сотрудничестве, в рамках которого он предоставил органу следствия информацию о других участниках преступной группы, в отношении которых расследование продолжается.

Материалы уголовного дела направлены в Смольнинский районный суд г. Санкт-Петербурга для рассмотрения по существу.

http://genproc.gov.ru/smi/news/archive/news-940632/

29.10.2015

Киберпреступления: основные проблемы расследований

Источник: Институт судебных экспертиз и криминалистики

Уголовный кодекс РФ не содержит четкого определения, что есть «киберпреступление».

Во многих источниках под киберпреступлениями понимают: «компьютерные преступления», «преступления в сфере высоких технологий», «информационные преступления», собственно «киберпреступления», «преступления в сфере безопасности обращения компьютерной информации», «преступления в сфере компьютерной информации» и т.д.

Независимо от используемой терминологии очевиден целый комплекс сложившихся проблем борьбы с киберпреступлениями.

Следователи и дознаватели констатируют, что им все чаще приходится расследовать следующие киберпреступления, предусмотренные УК РФ:

- ст. 159.6 - «Мошенничество в сфере компьютерной информации»,
- ст. 242.1 - «Изготовление и оборот материалов или предметов с порнографическими изображениями несовершеннолетних»,
- ст. 273 - «Создание, использование и распространение вредоносных компьютерных программ», ст. 242 - «Незаконные изготовление и оборот порнографических материалов или предметов",
- ст. 274 - «Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации информационно-телекоммуникационных сетей»,
- ст. 158 - «Кража»,
- ст. 183 - «Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну»,
- ст. 138 - «Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений»,
- ст. 272 - «Неправомерный доступ к компьютерной информации»,
- ст. 137 «Нарушение неприкосновенности частной жизни»,
- ст. 282 «Возбуждение ненависти либо вражды, а равно унижение человеческого достоинства».

Цифры показывают, что компетентность занимающихся расследованием кибепреступлений недостаточная

Ключевая проблема, которые выделяют исследователи, заключается в недостаточной компетентности лиц, занимающихся выявлением и раскрытием киберпреступлений. Опросы среди следователей показывают, что 95% респондентов получили юридическое образование. И только 5% обладают еще и образованием по специальности «Информатика и вычислительная техника». 63% опрошенных владеют компьютером на уровне «среднего пользователя», 37% - на уровне «продвинутого пользователя». 79% при этом постигают компьютер самостоятельно, курсы для сотрудников правоохранительных органов посещали только 21%, и незначительный процент (5%) - коммерческие курсы.

Кибепреступления на шаг впереди следователей

Другой проблемой является несвоевременность выявления киберпреступлений.

В соответствии с результатами опросов:

- в 53% случаев с момента совершения преступления до поступления информации о совершенном преступлении проходит более 10 дней;
- 73% респондентов отметили запоздалое начало предварительного расследования, когда многие важные доказательства уже утрачены.

Какие действия проводят на месте расследования преступлений?

- осмотр, об этом сказали 79%;
- допрос, об этом сказали 68%;
- обыск, об этом сказали 63%,
- назначение судебных экспертиз, об этом сказали 47%,
- выемка, об этом сказали 37%.

http://www.klerk.ru/law/articles/431376/

Как защищен от киберпреступников официальный интернет-сайт МВД России

Вопрос: «МВД России ведет, в том числе, работу по профилактике и раскрытию преступлений в сфере IT-технологий, борется с интернет-мошенниками. А как защищен от киберпреступников официальный интернет-сайт МВД России?»

- С целью недопущения использования доменного имени mvd.ru в противоправных деяниях официальный интернет-сайт МВД России, состоящий из ряда структурных компонентов: федерального сайта, сайтов подразделений МВД России в субъектах федерации и транспортной полиции, переведен на работу по защищенному протоколу передачи данных (https). Подлинность подключения подтверждается сертификатом публичного центра сертификации в сети Интернет «Thawte».

Поэтому на всех интернет-сайтах МВД России (в доменной зоне mvd.ru) в адресной строке (справа, вверху) есть индикатор безопасности зеленого цвета в виде закрытого замка, а на центральном сайте самого Министерства – рядом с «замочком» располагается наименование ведомства: **Ministry of Internal Affairs RF (RU).** Так что при посещении интернет-сайтов подразделений МВД России всегда обращайте внимание на адресную строку, где должен быть «индикатор безопасности».

Кроме того, помните, что МВД России не рассылает уведомления с предложением оплатить штраф посредством SMS и не блокирует компьютеры граждан.

Получив подобное уведомление, не спешите отправлять SMS-ки с денежными переводами, от кого бы не пришла просьба или требование. Сначала перепроверьте информацию в официальных организациях, обратитесь в компетентные органы, проверьте самостоятельно наличие защищенного протокола у сайта, который вам кажется подозрительным.

Подозрительным интернет-ресурсам и сомнительным смс-рассылкам доверять нельзя.

Скриншоты страниц сайтов МВД России с «индикаторами безопасности».

Пресс-центр МВД России
ДИТСиЗИ МВД России

http://limited.petrovka38.ru/document/2867820

Номер подписан в свет 11.10.2015