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

ФИНАНСОВЫЕ ПРАВОНАРУШЕНИЯ И ПРЕСТУПЛЕНИЯ

№ 7 (118) 2016
(выходит с октября 2006 г.)

Европейский регулятор обращает внимание на киберриски
Фото с сайта
http://www.audit-it.ru/news/finance/868409.html
См. раздел
«Киберпреступления»

Издатель
ИП **Фединский Ю.И.**

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

Москва
2016

Оглавление

+

Киберпреступления

03.06.2016

Медведев: ущерб от киберпреступности – $500 млрд

Фото: Пресс-служба правительства РФ

Премьер-министр РФ Дмитрий Медведев отметил повышенную сложность борьбы с киберпреступностью, а также большой ущерб, который она наносит России, а также мировой экономике в целом.

В рамках совещания об информационной безопасности в кредитно-финансовой сфере Дмитрий Медведев отметил, что ущерб от преступлений в кредитно-финансовой сфере России продолжает расти и, по его мнению, "опыта и сил противостоять этому явлению пока явно недостаточно". Премьер также отметил, что данная угроза носит транснациональный характер и в масштабе мировой экономике ущерб от нее, по ряду оценок, уже достиг $500 млрд.

Добрый день, уважаемые коллеги! Мы давно договаривались собраться и обсудить вопросы информационной безопасности – не просто информационной безопасности, это сейчас максимально широкое понятие, а информационной безопасности именно в кредитно-финансовой сфере, то есть в банках и вообще в финансовом секторе.

Уже довольно давно IT-технологии стали неотъемлемой частью практически всех операций с деньгами – это и многомиллиардные расчеты, и в то же время оплата каких-то достаточно обычных услуг типа коммунальных. Всем понятно, что платить, что называется, одним кликом весьма удобно, но люди, бизнес должны быть уверены, что транзакция состоится, деньги не украдут, поэтому защита средств является ключевым вопросом современного кредитно-финансового оборота, особенно при переходе от наличных расчетов к электронным платежам. Мы живем в эпоху, когда этот переход происходит очень масштабно и никакой альтернативы в этом смысле, по всей вероятности, не существует, и сегодняшняя тема информационной безопасности, вообще безопасности в кредитно-финансовой сфере, касается любого человека и в нашей стране, и за рубежом.

Мошенники, которые занимаются киберпреступлениями, атакуют не только электронные кошельки конкретных владельцев, но и вообще элементы всей кредитно-финансовой системы, счета банков, финансовых компаний, государства. Они хорошо изучили уязвимость программного продукта, тем более что каждый программный продукт пишется людьми и всегда есть те или иные бреши, которые могут быть пробиты в этих продуктах, даже несмотря на то, что технологии меняются, усложняются, становятся более защищенными. Есть и просто использование доверчивости обычных людей. Активность таких преступников и количество таких преступлений растет повсеместно. Есть факты установления таких преступных групп, и совсем недавно такая информация прошла. Но очевидно, что проблема не решается просто путем задержаний, хотя это и результат совместной работы специалистов в сфере безопасности, правоохранительных органов.

Хакеры часто атакуют дистанционные услуги, те услуги, которые идут через интернет, через операторов мобильной связи, причем сегодня ограбления банков часто происходят не так,

как это было на протяжении веков, не с оружием в руках, а с использованием экрана планшета или компьютера. Очень часто, что особенно опасно, атаки хакеров направлены не только на то, чтобы деньги украсть, что тоже печально, но часто смысл этих атак и в том, чтобы подорвать доверие, сорвать какие-то значимые мероприятия или программы, проще говоря, навредить всем. Поэтому эта угроза носит транснациональный характер. По некоторым оценкам, мировые потери от киберпреступности составляют около полутриллиона долларов. Посчитать их очень сложно, потому что далеко не все потери фиксируются, не обо всех потерях заявляется.

В России ущерб от такого рода преступлений тоже растет. Опыта и сил противостоять этому явлению пока явно недостаточно. Большинство взломов выявляются постфактум, после потери средств или после блокирования той или иной системы, фиксируются десятки тысяч несанкционированных операций через системы дистанционного банковского обслуживания. Бороться в одиночку с такими преступлениями практически невозможно.

Киберзащита – дорогое удовольствие, и, самое главное, ее невозможно сделать, что называется, в один канал. Для снижения рисков и киберугроз нужны совместные усилия по борьбе с электронной преступностью. Необходимо к этой проблеме отнестись системно, создать и отладить механизм противодействия как на уровне технической оснащенности, так и формирования необходимой инфраструктуры в целом и, конечно, законодательной базы, что тоже весьма непросто, потому что даже описать все современные технологии и явления юридически безупречным языком – крайне трудная задача.

Ряд шагов был сделан и правительством, и Банком России, в частности созданы специальные центры мониторинга и реагирования на компьютерные атаки, разработан проект отраслевого стандарта. Уверен, что у делового сообщества, у банковского сообщества, у государственных структур есть и другие идеи, которые могут способствовать укреплению борьбы с киберугрозами и предотвращению таких угроз в будущем. Накоплен довольно успешный опыт, который можно было бы переносить и на систему в целом.

http://www.vestifinance.ru/articles/71538

04.05.2016

С корсчета в ЦБ хакеры похитили свыше полумиллиарда рублей

В результате несанкционированного доступа 21 января 2016 года с корсчета Русского международного банка (РМБ) в ЦБ РФ были списаны 508,67 млн рублей, говорится в отчете банка по МСФО.

Ранее банк уже сообщал, что из-за хакерской атаки руководство кредитной организации попросило регулятора отключить ее от системы БЭСП (Банковские электронные срочные платежи). РМБ стал первым российским банком, который публично сообщил о том, что хакеры смогли похитить средства с его счета в ЦБ.

Как говорится в отчете РМБ, 25 марта по факту несанкционированного списания было заведено уголовное дело по статье "мошенничество". "В результате активной работы с Банком России и банками-контрагентами сумма возвращенных средств составила 336 млн рублей", - указано в документе. Как поясняет банк, остаток суммы равен 131,88 млн рублей, или двум процентам от капитала, работа по возврату средств продолжается.

В отчете говорится, что после хакерской атаки РМБ изменил внутренние документы, в том числе план ОНИВД (обеспечения непрерывности и восстановления деятельности). Также были проведены мероприятия по усилению информационной безопасности, приобретено специализированное программное обеспечение для выявления аномальной сетевой активности.

В 2015 году РМБ увеличил чистую прибыль по МСФО на 46,8% - до 551,75 млн рублей. Аудитор - "ФБК Грант Торнтон" - в своем заключении к отчету указывает, что прошедшая уже в январе 2016 года хакерская атака говорит о недостатках в системе обеспечения информационной безопасности банка. Также аудитор отмечает, что у РМБ несовершенная система оценки рисков по заемщикам-нерезидентам.

По итогам первого квартала 2016 года Русский международный банк занимает 128-е место по размеру активов в рэнкинге "Интерфакс-100".

Источник: Интерфакс

http://www.audit-it.ru/news/finance/865609.html

04.05.2016

Практически любой банкомат в мире уязвим к кибератакам

В основном причина заключается в использовании устаревшего программного обеспечения и отсутствии защиты многих компонентов системы.

Практически любой банкомат в мире уязвим к атакам – как с помощью вредоносного ПО, так и без него, показалоновое исследование компании «Лаборатория Касперского». В основном причина заключается в использовании устаревшего программного обеспечения, наличии ошибок в

конфигурации сети, а также отсутствии защиты многих компонентов системы от проникновения извне.

К примеру, в большинстве банкоматов нередко используется операционная система Windows XP, с апреля 2014 года не поддерживаемая Microsoft. К тому же, программное обеспечение, предназначенное для взаимодействия системного блока банкомата с инфраструктурой банка и аппаратными модулями обработки транзакций, базируется на устаревшем незащищенном стандарте XFS. В XFS отсутствует авторизация команд, благодаря чему преступники могут инфицировать ОС банкомата и отправить свою команду в кардридер или диспенсер банкнот, а затем просто забрать все деньги, хранящиеся в устройстве.

Как показало исследование, злоумышленникам вовсе не обязательно использовать вредоносы для заражения ПО банкомата или сеть банка, к которой он подключен. Очень часто в банкоматах отсутствует адекватная физическая защита, что позволяет преступникам получить доступ к блоку, где располагается компьютер, или к интернет-кабелю. Имея даже частичный физический доступ к устройству, злоумышленник может установить управляемый удаленно микрокомпьютер. Это позволит мошеннику перенаправить трафик с банкомата на поддельный процессинговый центр, с которого могут поступать любые команды.

Соединение между банкоматом и процессинговым центром можно защитить различными методами, в частности, при помощи реализации VPN, SSL/TLS, межсетевого экрана или MAC-аутентификации. Однако в действительности банки часто пренебрегают подобными мерами безопасности.

Источник: SecurityLab
http://www.audit-it.ru/news/finance/865398.html

04.05.2016

Хакеры Anonymous пообещали атаковать сайты центробанков по всему миру

© zastavki.com

Участники хакерской группы Anonymous пообещали в течение ближайших 30 дней атаковать сайты центробанков по всему миру, сообщает Reuters со ссылкой на видеообращение, размещенное группой хакеров на YouTube.

В сообщении Anonymous, которое цитирует агентство, говорится, что хакеры совершили атаку на сайт Банка Греции, и этот шаг знаменует собой начало 30-дневной кампании, направленной против сайтов центральных банков по всему миру.

О том, что во вторник, 3 мая, Anonymous атаковали сайт Центробанка Греции, Reuters также сообщил неназванный представитель банка. По словам собеседника агентства, кибератака привела к непродолжительному сбою в работе сайта Банка Греции.

«Атака длилась несколько минут, с ней успешно справилась система безопасности банка. DDoS-атака затронула только наш веб-сайт», — сказал представитель регулятора.

Anonymous была создана в 2003 году. Жертвами их DDoS-атак становились PayPal, MasterCard, церковь сайентологии, сайты Интерпола, Европарламента и Ватикана. В ноябре 2015 года Anonymous объявила войну запрещенной в России организации «Исламское государство» и начала публиковать персональные данные предполагаемых террористов. По заявлению самой группы, с их помощью были заблокированы 5,5 тыс. Twitter-аккаунтов террористов.

В начале марта этого года Anonymous объявила «тотальную войну» миллиардеру Дональду Трампу, борющемуся за право выдвигаться от Республиканской партии на президентских выборах в США. Группа хакеров пригрозила «разрушить его компанию». Anonymous сообщила о намерении нарушить работу сайтов, связанных с миллиардером, и обнародовать компрометирующую его информацию.

Источник: РБК
http://www.audit-it.ru/news/soft/865631.html

05.05.2016

СМИ: хакеры из России взломали 272,3 млн почтовых аккаунтов

Сотни миллионов почтовых аккаунтов крупнейших почтовых сервисов попали в руки хакеру из России, пишет Reuters со ссылкой на старшего эксперта по безопасности Hold Security Алекса Холдена.

По его словам, хакер был замечен на тематических форумах, предлагая взломанную базу на 1,17 млрд аккаунтов. После проверки и отсева дубликатов Hold Security выяснила, что

база имеет 272,3 млн уникальных аккаунтов, среди которых 57 миллионов - сервиса Mail.ru, 40 млн - в Yahoo, 33 млн - в Microsoft Hotmail, 24 млн - в Google.

За всю базу хакер просил лишь 50 рублей, но так как политика фирмы исключает плату за украденную информацию, неизвестный согласился передать базу бесплатно в обмен на положительные отзывы от сотрудников на хакерских форумах.

Источник: ПРАЙМ
http://www.audit-it.ru/news/soft/865650.html

05.05.2016

Целью хакеров все чаще становятся банки

Как сообщили "Российской газете" в ЦБ, в последнее время у киберпреступлений в сфере финансов сменились жертвы. Если раньше основными целями хакеров были клиенты банков, то сейчас ими стали сами кредитные организации.

"В последнее время вектор хакерских атак сместился с клиентов кредитных организаций на сами банки", - заявили в пресс-службе регулятора.

Там сообщили, что за 4-й квартал 2015 года и 1-й квартал этого года потери банков от хакерских атак превысили 2 млрд рублей. За этот период хакеры покушались еще примерно на 1,5 млрд рублей, но эти атаки удалось отразить.

"Банк России предпринимает все необходимые усилия для противодействия преступности в данной сфере, стимулирует банки повышать уровень защиты от хакеров", - подчеркивают в пресс-службе ведомства.

Недавно в России произошел первый случай кражи средств с корреспондентского счета банка в ЦБ, ставший достоянием общественности. Жертвой хакерской атаки стал Русский международный банк (РМБ). В своем отчете организация сообщила, что 21 января 2016 года с ее счета в ЦБ было списано 508 миллионов рублей. Это примерно равняется всей прибыли кредитной организации за последний год работы.

Часть денег удалось вернуть. "В результате активной работы с Банком России и банками-контрагентами сумма возвращенных средств составила 336 млн рублей", - говорится в отчете РМБ. Сейчас ведется работа по возврату остальных средств.

В банке подчеркивают, что сразу после атаки внутренняя система безопасности была усилена. В том числе приобретено программное обеспечение для выявления хакерских атак в будущем.

В ЦБ подтвердили факт хищения средств с корреспондентского счета.

В последнее время ведомство активно работает над укреплением информационной безопасности российских банков. Так, с 1 мая в России действуют рекомендации для кредитных организаций. Сообщалось, что после 1 мая российские банки должны будут отчитываться в единый реестр данных о совершенных на них кибератаках.

Вместе с тем в ЦБ отмечают, что следить за собственной безопасностью должны сами банки.

"Специалисты ЦБ могут проверить правильность заполнения бумаг для сертификации. Но компетенции для проверки эффективности конкретного маршрутизатора или межсетевого экрана в ЦБ нет. Эту функцию можно передать частным организациям, которые получили лицензии от ФСТЭК и ФСБ. Такова международная практика", - говорил ранее заместитель начальника главного управления безопасности и защиты информации Банка России Артем Сычев.

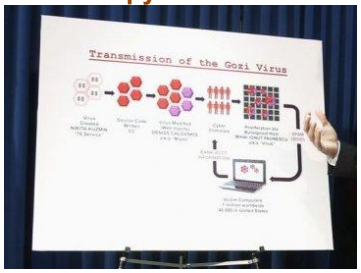
Специалисты отмечают, что в последнее время активным кибератакам все чаще подвергаются банки средних размеров, которые не так активно занимаются вопросами защиты от хакеров, как их более крупные конкуренты. Сейчас темпы роста количества кибератак в России вдвое превышают прирост в объемах оборота электронных денег. И этот факт серьезно беспокоит регулятора.

Вместе с тем недобросовестных участников рынка подозревают в том, что под прикрытием кибератак они могут заниматься нелегальным выводом капитала.

Источник: Российская газета
http://www.audit-it.ru/news/finance/865748.html

05.05.2016

Автору банковского вируса Gozi присудили штраф в 6,9 млн долларов в США



© golos-ameriki.ru

Автора банковского вируса Gozi, которым оказался российский программист Никита Кузьмин, в США признали виновным в создании данного вируса и приговорили к 37 месяцам тюремного заключения.

Однако Кузьмин был освобожден в зале суда, так как уже отбыл этот срок в ожидании суда. При этом обвинители

запрашивали 84 месяца тюрьмы, но суд при вынесении приговора учел сотрудничество молодого человека со следствием и признание вины, передает BBC.

Также программисту, которого обвиняли в том числе в продаже созданного им вируса другим хакерам, назначили штраф в размере 6,9 млн долларов в качестве возмещения потерь пострадавших от вируса клиентов банков.

От вируса Gozi пострадали более миллиона компьютеров в США, Германии, Великобритании, Польше, Франции, Финляндии, Италии, Турции и других странах. На своем вирусе Кузьмин предположительно заработал 25 млн долларов.

Источник: Banks.eu
http://www.audit-it.ru/news/finance/865750.html

13.05.2016

ЕЦБ обяжет европейские банки сообщать о значительных кибератаках

Банки еврозоны будут обязаны информировать регуляторов о «значительных» кибератаках при помощи новой службы оповещения в режиме реального времени, сообщает Financial Times.

ЕЦБ сообщил изданию, что он собирает данные о значительных кибератаках в 18 крупнейших банках еврозоны с февраля. Сейчас проект находится в пилотной стадии, к следующему году к системе должны присоединиться 130 банков.

Регулятор, по словам заместителя генерального директора ЕЦБ по наблюдению за банками Франсуа Луи Мишо, не будет собирать данные по всем инцидентам с кибербезопасностью, он сосредоточится на «значительных событиях», таких как атаки, повлекшие за собой серьезные финансовые потери или серьезный вред репутации.

«Мы хотим выявить тенденции и сообщать банкам, когда мы видим, что что-то происходит в одном из банков: «Вам надо что-то с этим сделать», — сказал он.

ЕЦБ намерен делиться данными с другими центробанками, например ФРС и Банком Англии.

Такое решение ЕЦБ принимает на фоне сообщений о кибератаке на ЦБ Бангладеш. Ранее Reuters сообщило о вероятной атаке на SWIFT группы хакеров, которая, предположительно, ранее похитила 81 млн долларов из Центрального банка Бангладеш. Для атаки на платежную систему использовалось вредоносное ПО под названием Alliance Access, атакующее клиентское программное обеспечение SWIFT.

Источник: Banki.ru
http://www.audit-it.ru/news/finance/866598.html

16.05.2016

Вьетнамский банк приостановил подозрительный перевод на миллион евро

Вьетнамский банк Tien Phong (TPBank) прервал подозрительную операцию, участники которой попытались передать через систему обмена банковской информацией SWIFT средства на сумму в один миллион евро, передает агентство Рейтер.

По данным агентства, представители SWIFT сообщили сотрудникам банка, что программное обеспечение, использовавшееся производителем банковских карт, с которым ранее сотрудничал банк, могло быть заражено компьютерным вирусом. Сейчас банк использует более безопасную систему, которая позволяет выходить на прямую связь с системой SWIFT.

Инцидент произошел в первом квартале 2015 года. Банк известил заинтересованные стороны сделки о прекращении операции. В результате финансовых убытков удалось избежать, отмечает агентство со ссылкой на заявление банка.

В пятницу система обмена банковской информацией SWIFT сообщила о втором случае кибератаки, аналогичной краже хакерами более 80 миллионов долларов со счета бангладешского центробанка. Представитель SWIFT заявила, что объектом второй атаки стал коммерческий банк, не уточнив его название. Она также не сообщила, оказалась ли попытка взлома успешной.

Группа хакеров взломала систему бангладешского ЦБ в начале февраля. Получив данные о счетах банка, хакеры попросили федеральный резервный банк в Нью-Йорке (важнейший из 12 резервных банков, входящих в Федеральную резервную систему США), где хранятся золотовалютные резервы Бангладеш, осуществить денежный перевод со счетов ЦБ на счета некоммерческой организации Shalika Foundation на Шри-Ланке и Филиппинах.

Источник: РИА Новости
http://www.audit-it.ru/news/finance/866749.html

27.05.2016

Европейский регулятор рекомендует стресс-тесты банков на предмет кибер-рисков

Банковским регуляторам стран ЕС следует проводить стресс-тестирование своих финансовых институтов на предмет кибер-рисков, сообщает Reuters со ссылкой на заявление председателя Европейского банковского регулятора (European Banking Authority, EBA) Андреа Энриа. Он предупредил, что банкам может потребоваться выделение дополнительного капитала в качестве буфера против данной угрозы.

«Я не буду обкатывать масштабный сценарий кибер-атаки для 28 стран-членов в одно и то же время, — сказал Энриа. — Но если вы спросите у меня, рекомендую ли я соответствующим национальным властям задуматься об этом и изучить возможность проведения такого типа стресс-тестов, я отвечу утвердительно».

Энриа сообщил, что EBA разрабатывает ориентиры для работы с IT-рисками — как их оценивать, как реализовывать контрмеры, какими должны быть действия регуляторов (вплоть до введения дополнительных требований по капиталу).

Эти ориентиры будут опубликованы EBA для консультаций позднее в текущем году.

Источник: RNS

http://www.audit-it.ru/news/finance/868409.html

01.06.2016

Группировка из 50 хакеров задержана за хищение 1,7 млрд рублей

Группа хакеров похитила со счетов российских банков более 1,7 миллиарда рублей. По данному делу задержаны 50 киберпреступников, 18 из них предъявлены обвинения. Возбуждены уголовные дела. Подозреваемые уже доставлены в Москву.

Хакеры при помощи вредоносной программы похитили более 1,7 млрд рублей со счетов российских банков. Как сообщили во вторник в силовых структурах, задержаны 50 киберпреступников. Они действовали по всей стране. В рамках операции по задержанию хакеров проведены более 80 обысков в 15 регионах страны.

"МВД России совместно с ФСБ России задержаны 50 подозреваемых в совершении многочисленных хищений денежных средств с расчетных счетов юридических лиц, а также с корреспондентских счетов кредитно-финансовых учреждений с использованием вредоносного программного обеспечения", - сообщила официальный представитель МВД России Ирина Волк.

Она добавила, что в результате оперативных мероприятий заблокированы фиктивные платежные поручения на 2,2 миллиарда рублей. По данным полиции, 18 участникам хакерской группы предъявлены обвинения. Они уже арестованы, пишет ТАСС.

В Центре общественных связей ФСБ рассказали агентству "Интерфакс", что в результате обысков были изъяты компьютерная техника, средства связи, банковские карты, оформленные на подставных лиц, а также финансовые документы и значительные суммы наличных.

Возбуждено уголовное дело по статьям "Организация преступного сообщества и участие в нем" и "Мошенничество в сфере компьютерной информации". Фигуранты уже доставлены в Москву.

http://www.tvc.ru/news/show/id/93473

02.06.2016

Хакеры похитили 3 млрд рублей с помощью уникального вируса

В течение нескольких лет хакерам с помощью вирусной программы "троян" удавалось похищать денежные средства со счетов пользователей, проживающих на территории России и стран СНГ.

За все время стражи порядка произвели арест порядка 50 хакеров, укравших 3 млрд рублей. Сотрудникам, работающим в компании "Лаборатория Касперского" удалось установить, что для осуществления своих планов злоумышленники пользовались вирусной программой Lurk (разновидность "трояна"). Основными целями преступников являлись банковские и кредиторные учреждения, а также их клиентура.

Использование Lurk для хищения денежных средств с банковских организаций началось приблизительно 1,5 года назад, так как до этого атаки в основном производились на корпоративные и домашние компьютерные сети.

Как рассказывают эксперты, хищение средств происходило следующим образом: программа посредством рассылки или иных способов распространения попадала в компьютерную сеть банковской организации, заражала ее, а после получала контроль над компьютером интересующего хакера клиента организации и производила списание денежных средств.

Максим Матюшин - Корреспондент РИА VistaNews

http://vistanews.ru/computers/security/59318

02.06.2016

Троян вскрыли на Урале

В России задержаны участники преступного сообщества хакеров

Хакеры атакуют

Вчера стало известно об арестах организаторов и активных участников преступного сообщества хакеров, которое базировалось в Екатеринбурге, но имело сообщников в 15 регионах России. По версии следственного департамента МВД, злоумышленники с помощью троянской программы Lurk на протяжении пяти лет выводили деньги со счетов клиентов российских и зарубежных банков. Общий ущерб, по подсчетам следствия, составляет более 1,7 млрд руб. Хищение 2,2 млрд руб. удалось предотвратить.

О проведении масштабной операции по задержанию 50 членов межрегиональной группировки хакеров вчера сообщила официальный представитель МВД России Ирина Волк. "Сотрудниками МВД России совместно с ФСБ России задержаны подозреваемые в совершении многочисленных хищений денежных средств с расчетных счетов юридических лиц, а также с корреспондентских счетов кредитно-финансовых учреждений с использованием вредоносного программного обеспечения. В рамках уголовного дела проведено 86 обысков на территории 15 субъектов",— рассказала госпожа Волк. В отношении задержанных следственный департамент МВД РФ расследует уголовное дело по факту организации преступного сообщества (ст. 210 УК РФ) и мошенничества в сфере компьютерной информации (ст. 159.6 УК РФ).

По сведениям "Ъ", масштабная операция началась в мае в Екатеринбурге, где проживали предполагаемые организаторы ОПС и его наиболее активные участники. Для этого МВД России привлекло сотрудников регионального УФСБ, а также бойцов СОБРа и ОМОНа нацгвардии. Как отмечают в региональном УФСБ, в ходе обысков у членов группировки было изъято около 12 млн руб. в рублях и валюте, более 1 тыс. сим-карт, около 100 единиц компьютерной техники и свыше 200 средств связи (телефоны и смартфоны различных моделей).

Киберпреступники нанесли России урон на $3 млрд

Ущерб экономике России от киберпреступности в 2015 году составил 203,3 млрд руб., или 0,25% от ВВП. Более 92% крупных коммерческих компаний, госструктур, а также предприятий малого и среднего бизнеса столкнулись с киберинцидентами

По сведениям "Ъ", следствие считает, что группировкой руководили екатеринбуржцы Константин Козловский и Александр Еремин. Вместе с рядовыми участниками ОПС они были арестованы решениями Кировского райсуда Екатеринбурга и этапированы на двух спецрейсах нацгвардии в Москву, где ведется расследование уголовного дела. По такой же схеме были проведены задержания в других городах.

Согласно материалам уголовного дела, участники преступной группировки — в основном разработчики и тестировщики программного обеспечения. Их работа заключалась в совершенствовании и распространении кода троянской программы Lurk. Данный вид вирусного программного обеспечения появился в России в июле 2011 года. Эта программа изначально создавалась под атаки на системы дистанционного банковского обслуживания iBank для неправомерного доступа в систему интернет-банкинга и совершения со счетов жертвы мошеннических платежей. Кроме того, следователи установили причастность хакеров к другим способам хищения денег банков — от установки скимминговых устройств до осуществления целевых атак на процессинговые центры кредитно-финансовых учреждений и межбанковские системы обмена информацией. По подсчетам следствия, на данный момент ущерб от деятельности хакеров составляет около 1,7 млрд руб., а примерно 2,2 млрд руб. подозреваемым вывести не удалось: подозрительные операции были заблокированы при содействии правоохранительных органов.

Русские хакеры дошли до Берлина

Германия в мае обвинила хакеров из России в кибератаках на партийные органы и информационные серверы властей ФРГ. Представители спецслужб сообщили, что с российской стороны могла исходить и другая серьезная опасность — возможные диверсии на объектах промышленной и энергетической инфраструктуры

Под хакерские атаки попали десятки банков, в том числе такие крупные, как ВТБ и Сбербанк. Руководитель департамента информационных технологий, старший вице-президент ВТБ Дмитрий Назипов сообщил, что самая крупная DDoS-атака на банки, входящие в группу ВТБ, была проведена осенью прошлого года, и ее удалось успешно отразить. Такой же версии придерживаются в банке "Метрополь". Его представитель рассказал "Ъ", что хакеры активно атаковали финансовые учреждения с ноября прошлого года и в "Метрополе" к этому успели подготовиться. Поэтому, когда в январе 2016 года злоумышленники пытались списать деньги, сработала система безопасности, и хищения были предотвращены. Сейчас банк активно сотрудничает с правоохранительными органами по этому делу, хотя потерпевшей стороной по нему себя не считает. В свою очередь, зампред правления Металлинвестбанка Михаил Окунев рассказал "Ъ", что из финансовой структуры хакеры пытались похитить 680 млн руб.— 240 млн банку удалось вернуть, около 200 млн блокировано на корсчетах других банков, а остальные средства разыскиваются.

Как пояснили в "Лаборатории Касперского", специалисты которой вместе с работниками отдела информационной безопасности Сбербанка делали экспертизу по данному вирусу для МВД и ФСБ, программа Lurk была технически хорошо проработана, что затрудняло ее выявление. К примеру, ее вредоносный код не сохранялся на жестком диске зараженного компьютера, а функционировал исключительно в операционной памяти устройства. Как отмечают в "Лаборатории Касперского", заражение обычно происходило через взломанные сайты, программы-эксплойты либо после проникновения в наименее защищенный компьютер внутри корпоративной сети организации.

Представители банков сообщили, что выйти на группировку создателей Lurk удалось за счет консолидации банковского программного обеспечения. "Центробанк в последнее время наладил взаимосвязи между банками по вопросам кибербезопасности. Как правило, преступники, похищающие деньги со счетов с помощью вирусных программ, сразу выводят их через цепочку из нескольких банков. Благодаря тому, что сейчас банки плотно взаимодействуют друг с другом, они научились быстро выявлять такие операции, блокировать их и находить их источник",— рассказал "Ъ" собеседник в одном из уральских банков.

Вчера связаться с адвокатами фигурантов уголовного дела не удалось. Однако, по сведениям "Ъ", ни один из лидеров группировки на сделку со следствием не пошел, и все отказываются признавать свою вину.

Игорь Лесовских, Дмитрий Комаров, Алена Тронина, Екатеринбург; Алексей Соковнин

Газета "Коммерсантъ" №96 от 02.06.2016, стр. 4
http://www.kommersant.ru/doc/3002230

02.06.2016

Троян на миллиарды

© РИА Новости. Владимир Астапкович

Interfax-Russia.ru – *ФСБ и МВД при поддержке Нацгвардии задержали в 15 российских регионах около 50 хакеров, причастных к хищениям в финансовых учреждениях.*

Сотрудники ФСБ России совместно с МВД пресекли деятельность хакерской группы, причастной к созданию, распространению и использованию вредоносной компьютерной программы. Как сообщили "Интерфаксу" в ЦОС ФСБ России, с ее помощью злоумышленники похитили более 1,7 млрд рублей со счетов российских финансовых учреждений.

В ходе следственных действий, проведенных одновременно в 15 регионах РФ, сотрудники ФСБ и МВД при силовой поддержке Федеральной службы войск Нацгвардии РФ задержали около 50 человек. С помощью авиации Национальной гвардии фигурантов уголовного дела доставили в следственные изоляторы Москвы.

На основании оперативных материалов ФСБ России Следственный департамент МВД РФ возбудил уголовное дело по признакам преступлений, предусмотренных частями 1, 2 ст.210 УК РФ (организация преступного сообщества и участие в нем) и ч.4 ст.159.6 УК РФ (мошенничество в сфере компьютерной информации).

Членам преступной группы уже предъявлено обвинение: 18 из них были заключены под стражу, трем избрали меру пресечения в виде подписки о невыезде.

В ходе обысков сотрудники правоохранительных органов изъяли большое количество компьютерной техники, средств связи, банковских карт, оформленных на подставных лиц, а также финансовые документы и значительные суммы наличных денежных средств, подтверждающие противоправный характер их деятельности.

В свою очередь, официальный представитель МВД России Ирина Волк сообщила "Интерфаксу", что в результате оперативных мероприятий были заблокированы фиктивные платежные поручения на 2 млрд 273 млн рублей.

По ее словам, в ходе обысков были получены материалы, подтверждающие причастность подозреваемых к созданию бот-сетей зараженных компьютеров, организации целевых атак на инфраструктуру кредитно-финансовых и государственных учреждений и совершение хищения денежных средств.

Волк рассказала, что с середины 2015 года по настоящее время по всей стране было зафиксировано 18 целевых атак на автоматизированные рабочие места клиентов банков, ущерб от которых превысил 3 млрд рублей. При этом полиция смогла предотвратить возможный ущерб на сумму 2 млрд 273 млн рублей.

Как оказалось, выйти на след преступников помогло участие в операции специалистов "Лаборатории Касперского" - они провели тщательный анализ вредоносного программного обеспечения, в результате чего была выявлена сетевая инфраструктура группы атакующих, установлены их личности и собраны доказательства их причастности к киберпреступлениям.

По информации "Лаборатории Касперского", атаки с участием троянца Lurk начали фиксировать с июля 2011 года. Как поясняют эксперты, конечная цель "зловреда" – доступ к системе дистанционного банковского обслуживания для непосредственной кражи денег.

Однако помимо клиентов банков и самих финансовых организаций, злоумышленники, использовавшие вирус, интересовались также веб-ресурсами СМИ и новостных агрегаторов, поскольку размещение троянца на таких популярных страницах открывало им возможность широкого распространения зловреда. Заражение жертв обычно происходило либо через взломанные сайты, либо через программы-эксплойты, либо через проникновение в наименее защищенный компьютер внутри корпоративной сети организации.

По информации экспертов, данный троянец отличается хорошей технической проработкой – на протяжении пяти лет вирусописатели постоянно совершенствовали его, используя современные технологии. К примеру, он оказался одним из чрезвычайно редких "зловредов", чей вредоносный код не сохраняется на жестком диске зараженного компьютера, а функционирует исключительно в оперативной памяти.

Помимо этого, разработчики всеми возможными средствами старались минимизировать риск детектирования троянца антивирусными программами. Киберпреступники использовали различные VPN-сервисы, анонимную сеть Tor, скомпрометированные или беспроводные точки доступа сторонних пользователей и даже серверы атакованных IT-организаций.

Как отмечает руководитель отдела расследования компьютерных инцидентов "Лаборатории Касперского" Руслан Стоянов, авторы Lurk всегда делали все возможное для того чтобы заразить максимальное количество интересных им жертв, не привлекая при этом внимания аналитиков и правоохранительных органов.

"В ходе анализа нам удалось выяснить, что за троянцем все-таки стояла одна группировка, и, по всей видимости, в нее входили профессиональные разработчики и тестировщики. Наши продукты всегда распознавали и успешно блокировали деятельность зловреда, а арест его создателей, надеемся, приведет к окончательному закату Lurk", - говорит Стоянов.

Проблема информационной безопасности в России, в том числе кредитных учреждений, не первый год стоит на повестке дня. Не случайно особое внимание на это обращал и Центробанк, заявляя, что за низкий уровень информационной безопасности будет применять меры воздействия к банкам.

"Речь идет о том, что информационная безопасность напрямую влияет на финансовые показатели. В тех атаках, которые были совершены, банки иногда теряли весь дневной остаток корреспондентского счета, а с одной организацией мы столкнулись с вопиющим фактом - она фактически за один раз потеряла весь свой капитал. Одна атака - и банк в состоянии, когда ЦБ обязан отобрать у него лицензию. Мы наказываем не за отсутствие или присутствие тех или иных методик и средств обеспечения информационной безопасности - это дело банков, а мы наказываем за то, как банк думает о своей финансовой устойчивости, и это правильно", - пояснял позицию ЦБ заместитель начальника главного управления безопасности и защиты информации Банка России Артем Сычев.

На Уральском форуме "Информационная безопасность финансовой сферы" он подробно рассказал о том, как злоумышленники проводят хакерские атаки на банки. В частности, по его словам, атака идет на инфраструктуру кредитной организации, причем вброс идет от любого источника - это может быть фишинговое письмо или письмо с трояном. Дальше происходит захват управления всей инфраструктуры, особое внимание уделяется АРМКБР (автоматизированные рабочее место клиента Банка России), подкладывается фиктивный платежный документ, он отправляется в платежную систему Банка России, для которого документ является легитимным, и он принимается к исполнению.

"Интересно то, что те, кто сидит и смотрит за АРМКБР на стороне злоумышленников, как только начинают видеть, что от нас приходит отбой в проведении транзакции или сообщение, что на счету не хватает денег и операция не будет проведена, не только "гасят" АРМКБР, что вполне нормально, а они "валят" всю сеть кредитной организации, потому что под их управлением помимо АРМКБР еще и домен, почтовые серверы и все остальное. Информатизация (информационная служба банка - ИФ-АФИ), естественно, бросается сражаться за выживание кредитной организации. Это приводит к тому, что, во-первых, деньги, которые надо было бы спасать, уже улетели, а во-вторых, в сеть, которая не вычищена после атаки вредоноса, ставится еще одно средство, и оно тут же оказывается под контролем злоумышленников", - рассказал Сычев.

ЦБ РФ совместно с МВД провел экономический анализ хакерских атак. Оказалось, что часто организатор атаки, который должен получать основную часть похищенных средств, получает в лучшем случае 30%. Этот факт дает основания предполагать, что такие атаки используются прежде всего для сокрытия ранее совершенных финансовых преступлений.

"Выводить деньги, чтобы получить 30% - это не очень выгодно, а вот организовать атаку на себя и сказать "вот у меня украли столько денег, и я не могу обслуживать счета своих клиентов", а

при этом эти деньги уже давно были выведены с помощью других технологий - вполне возможно", - сказал Сычев, отметив, что три банка в прошлом году лишились лицензии из-за таких атак.

По словам замначальника главного управления ЦБ РФ, в настоящее время внимание злоумышленников сосредоточено на трех вещах - поиск и вербовка инсайдеров, проработка схем монетизации атак, а также поиск уязвимости систем мобильных операторов, их интересуют новые информационные технологии и они готовы вкладывать в это свои средства.

С целью минимизировать риски утечки информации Банк России разработал и предложил кредитным организациям комплекс мер по выстраиванию эффективной системы мониторинга и контроля информационных потоков.

Особое внимание в рекомендациях по обеспечению информационной безопасности организаций банковской системы РФ, уделяется вопросам выявления и предотвращения утечек информации в результате действий самих работников кредитных организаций или лиц, обладающих легальным доступом к внутрибанковской информации.

Рекомендации также касаются вопросов работы банков с конфиденциальной информацией. Кроме того, в документе подробно изложены подходы к организации бесперебойного мониторинга процессов, которые могут представлять угрозу информационной безопасности кредитных организаций.

Одной из основных причин, тормозящих развитие сферы информационной безопасности в банках, эксперты не первый год называют кадровый голод. На эту проблему эксперты указывали еще в 2008 году. Спустя пять лет эта проблема также была отмечена специалистами аналитического центра российского разработчика DLP-систем Zecurion.

Исследования показали, что почти две трети (62,7%) российских банков терпят кадровый голод в области информационной безопасности. В числе основных причин сложившейся ситуации называли недостаток или слабую квалификацию соответствующих специалистов.

В целом, констатируют в Zecurion, на данный момент банковская отрасль стала более зрелой в вопросах информационной безопасности, в том числе и благодаря деятельности ЦБ, изменениям в законодательстве, касающемся защиты персональных данных граждан и, наконец, интересам бизнеса.

Как рассказали Interfax-Russia.ru в компании, учащающиеся инциденты в сфере информационной безопасности приводят к большим потерям вплоть до прекращения деятельности. Поэтому кредитные организации и без кнута со стороны регулятора активно работают над повышением безопасности своих ИТ-систем и сервисов.

Проблема безопасности стала особенно острой с широким распространением сетевых сервисов вроде интернет- или мобильного банкинга. Доступ к сервисам получили многие клиенты, слабо знакомые с компьютером и последними технологиями. Именно они попадают в категорию наиболее вероятных жертв хакеров и других злоумышленников.

Основными направлениями работы специалистов по безопасности в банках в Zecurion называют: организационные меры, повышение осведомленности о существующих угрозах среди сотрудников кредитной организации, а также информирование о рисках клиентов, держателей пластиковых карт, пользователей интернет-банка.

Второе важное направление — это своевременное реагирование на новые угрозы и применение технических средств защиты информации от утечки (DLP-системы). Работа в данных направлениях, считают специалисты российского разработчика DLP-систем, позволит российским кредитным организациям минимизировать риски утечки информации и успех хакеров при реализации направленных атак.

Обозреватель *Анастасия Николаева*

http://www.interfax-russia.ru/view.asp?id=731830

02.06.2016

Серверы Teamviewer ушли в оффлайн, пользователи пострадали от массового взлома

автор: Мария Нефёдова

Настоящая паника поднялась в стане пользователей TeamViewer в ночь с первого на второе июня. Серверы компании и официальный сайт были недоступны на протяжении нескольких часов, и одновременно с этим Reddit и социальные сети начали стремительно наполняться сообщениями от пользователей, которые писали о взломах и хищении денежных средств. Официальные представители TeamViewer уверяют, что компанию не ломали, а недоступность своих сервисов объясняют проблемами с DNS.

Достаточно зайти на r/teamviewer, чтобы оценить размах происходящего. Несколько первых страниц сабреддита полностью оккупированы темами формата «Меня взломали!», рядом с которыми идет бурное обсуждение случившегося.

Нечто странное начало происходить около 24 часов назад, 1 июня 2016 года. Пользователи ПК, Mac и даже владельцы серверов, которых объединяло разве что использование продуктов TeamViewer, стали сообщать о том, что их машины взломаны, и некто неизвестный полностью захватил контроль над системой. Некоторые пострадавшие пишут, что использовали надежные пароли и двухфакторную аутентификацию, но даже это не уберегло их от взлома.

Неизвестные хакеры, предположительно, сумели перехватить управление веб-аккаунтами TeamViewer, которые и использовали для получения контроля над машинами жертв. По сообщениям пострадавших, хакеры опустошали PayPal аккаунты, заходили в чужую почту и заказывали товары с eBay и Amazon.

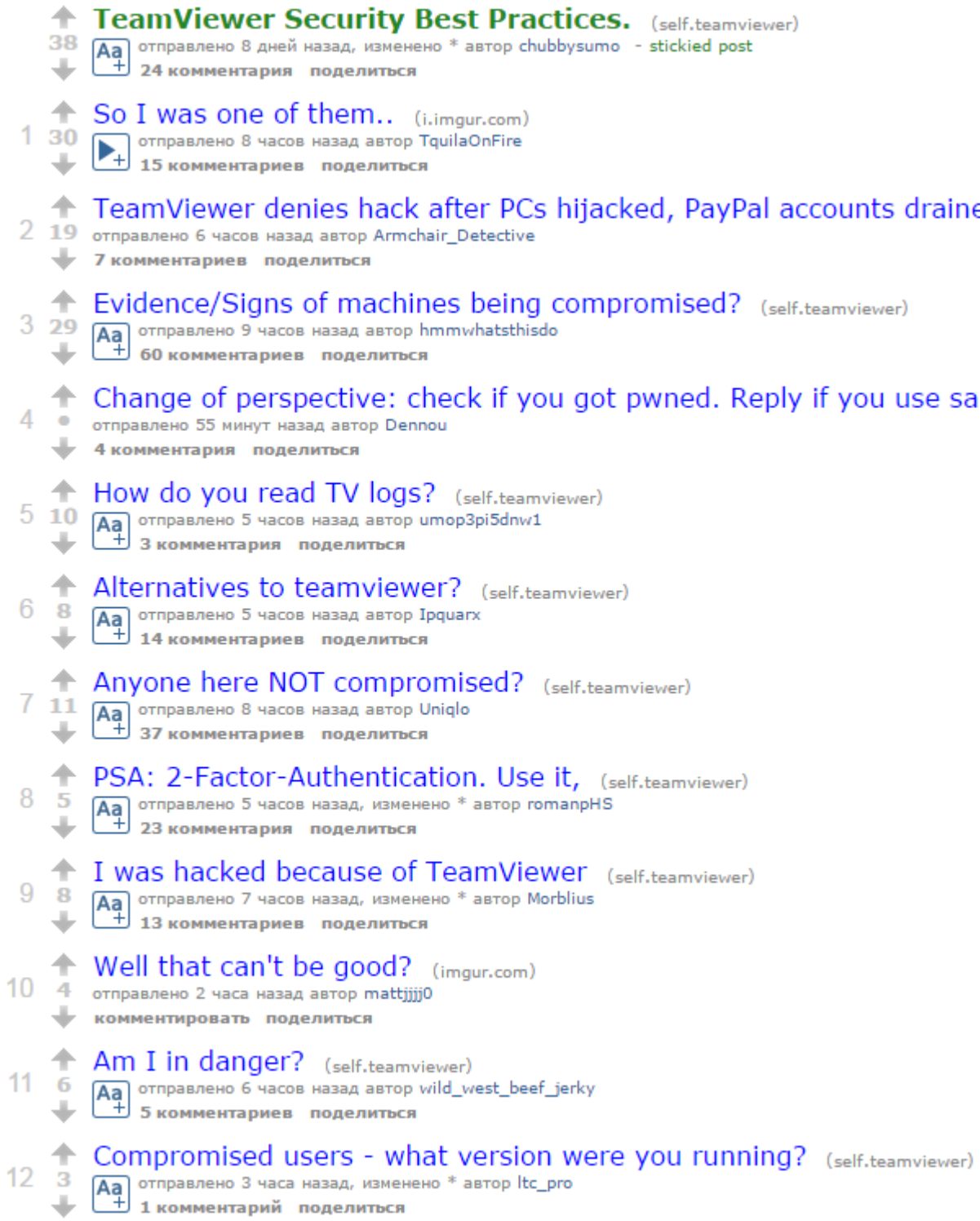
«Хакеры забрали у меня все. Они удаленно подключились в пять утра, зашли в мой Chrome и использовали PayPal, чтобы заказать подарочных карт на сумму $3000. И, да, у меня включена двухфакторная аутентификация», — рассказал один из пострадавших журналистам издания The Register.

«Я сидел на стуле [за компьютером] и увидел, как курсор начал самостоятельно двигаться по экрану. Конечно, я тут же отключил удаленный контроль и спросил [хакера], кто он такой», — пишет другой пострадавший на Reddit. — «Он тут же отключился, но попытался войти на мой сервер Ubuntu, где я храню все свои бекапы. Хорошо, что я вошел на сервер сразу же, как только он отключился от компьютера. Я отключил его прежде, чем он успел запустить Firefox. Поле этого я начал паниковать и подумал, что он только что похитил все мои пароли».

«Со мной сегодня произошло то же самое. Хорошо, что я играл в Rocket League. Я прибил соединение меньше чем через десять секунд. Как только в моем мозгу щелкнуло, и я понял, что только что случилось, я залогинился на свой сервер и выключил TeamViewer, собираясь разобраться с ним позже», — пишет еще одна жертва.

Официальные представители TeamViewer уверяют в Твиттере, что проблема не на их стороне: компанию никто не взламывал, и злоумышленники не получали доступ к информации пользователей. Проблемы с серверами и недоступность официального сайта разработчики объяснили неполадками с DNS. Сейчас все сервисы компании уже работают в штатном режиме.

Также на сайте компании недавно был опубликован пресс-релиз, в котором факт взлома TeamViewer или наличие какой-либо уязвимости тоже опровергается. Тогда компания сообщала, что пострадавшие пользователи, очевидно, недобросовестно относятся к созданию паролей (то есть пароли либо были слишком простыми, либо использовались для нескольких сервисов сразу). Однако этот текст датирован 23 мая 2016 года и, по всей видимости, относился к инцидентам с трояном BackDoor.TeamViewer.49.



Можно предположить, что массовый взлом пользователей TeamViewer — это действительно результат использования ненадежных паролей, или последствия недавнихмасштабных утечек данных. Также можно предположить, что ситуацию осложняет троян BackDoor.TeamViewer.49, использующий абсолютно легитимные версии TeamViewer для осуществления атак. Тем не менее, многие пострадавшие от рук хакеров пользователи пишут, что для TeamViewer у них были уникальные пароли, а никакой малвари на машине точно нет.

По данным The Register, представители TeamViewer дали вторичный комментарий о происходящем, где немного подробнее объяснили, что произошло :

«Проблемы, возникшие с сетью, были обусловлены DoS-атакой, направленной на инфраструктуру DNS-сервера TeamViewer. Команда TeamViewer оперативно отреагировала на происходящее и устранила проблему, вернув все сервисы в строй».

UPD. 02.06.2016, 22:30.

Компания TeamViewer выпустила пресс-релиз об инциденте и еще раз опровергла все обвинения:

«Некоторые сетевые СМИ ошибочно связывали перебои в обслуживании с заявлениями пользователей о взломе аккаунтов и теориями о возможном наличии уязвимостей в системе TeamViewer. У нас нет никаких доказательств, подтверждающих связь между этими инцидентами.

На самом деле произошло вот что:

Сервис TeamViewer был прерван из-за проблем с сетью, вызванных DoS-атакой на DNS-сервера компании. На данный момент все эти проблемы устранены.

В TeamViewer уязвимостей нет.

Невзирая на случившееся, команда TeamViewer делает все возможное для защиты пользователей и их данных.

Несмотря на то, что перебои в обслуживании никак не связаны с советом ниже, команда TeamViewer напоминает:

Большинство проблем с любыми веб-сервисами вызвано небрежным отношением к защите учетной записи пользователя. К этому, в частности, относится использование одинаковых паролей для разных учетных записей пользователей для различных сервисов.

Также никто не застрахован от случайной загрузки и установки вредоносного ПО. Как только система заражена, злоумышленники могут сделать с ней практически все что угодно, в зависимости от изощренности своего ПО — подчинить себе всю систему, завладеть и управлять данными в ней и т. д.».

https://xakep.ru/2016/06/02/teamviewer-panic/

02.06.2016

В Курганской области передано в суд уголовное дело о незаконном получении сведений, составляющих банковскую тайну

В июне 2015 года Следственным управлением УМВД России по г. Кургану было возбуждено уголовное дело по признакам состава преступления, предусмотренного частью 3 статьи 183 УК Российской Федерации «Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну».

Поводом для возбуждения уголовного дела послужили обращения граждан о том, что с их банковских счетов стали незаконно списываться денежные средства.

В ходе расследования было установлено, что злоумышленник установил на один из банкоматов Кургана скимминговое устройство, предназначенное для негласного сбора сведений, составляющих банковскую тайну. Используя устройство, он получал сведения о пин-кодах и магнитных лентах банковских карт. Эта информация дала злоумышленнику возможность снимать денежные средства с расчетных счетов граждан.

Обвиняемый изготовил дубликаты карт с известными ему банковскими данными и, используя полученные пин-коды, провёл семь операций по снятию денежных средств на общую сумму более 160 тысяч рублей.

Сотрудниками полиции совместно со службой безопасности банка были изучены записи с камер видеонаблюдения, а также проведён ряд других оперативно-разыскных мероприятий, позволивших задержать злоумышленника.

Им оказался 50-летний уроженец города Челябинска, временно проживающий в Кетовском районе Курганской области. В отношении обвиняемого избрана мера пресечения в виде заключения под стражу. 30 мая этого года уголовное дело передано в Курганский городской суд.

https://мвд.рф/news/item/7892093/

03.06.2016

Сколько денежных средств хакеры украли с карт граждан России в начале 2016

Сурнин Михаил Захарович

***Кибермошенники** взяли на вооружение новый метод социальной инженерии, пишут «Известия», ссылаясь на данные компании Zecurion.*

Общий объем хищений достиг 270 млн руб. Хакеры программируют и внешние интерактивные голосовые ответы (IVR) для звонков клиентам. Либо высылают на электронную почту клиентам банков письма со ссылками и файлами, ориентированными на их запросы, интересы. Открывая эти приложения, клиенты загружают вирус. В данной схеме потенциальный покупатель предлагает сразу внести задаток за автомобиль на банковскую карту клиента. При этом мнимый клиент просит назвать код авторизации, который приходит собственнику автомобиля на мобильный телефон, на самом деле являющийся доказательством перевода средств с карты продавца. С конца 2015 на похожие уловки попались уже 300 человек.

Согласно экспертной оценке, продавцы авто в последнее время стали более острожными, чаще обращаются к посредникам, чтобы исключить варианты мошенничества. — При использовании таких площадок возможности для маневра у правонарушителей уменьшаются.

Как отмечает Дмитрий Кузнецов, возглавляющий департамент методологии и стандартизации Positive Technologies, около 4% всех атак, которые осуществляются

в киберпространстве, приходится на «социальную инженерию». Для сектора машин до 300-500 тыс. руб. данного вполне достаточно. Практически четверть (24%) случаев кибермошенничества — результат прямого взлома банковских систем, а 72% - атаки на юридических лиц.

По утверждению гендиректора компании «Источник» Роберта Багратуни, все усилия служб, специализирующихся на сопротивлению киберхищений, были нивелированы развитием технологий «социальной инженерии».

По предположениям профессионала, вред от действий хакеров, активно использующих социальный инженеринг, будет стремительно расти, так как этот метод менее затратный и дает возможность не оставлять следов в web-сети.

http://tvoygorodpskov.ru/2016/06/160150-skolko-denezhnih-sredstv-hakeri-ukrali-s-kart-grazhdan.html

06.06.2016

«Нажмите Enter - это ограбление!»

Анна Королева «Expert Online» 06 jun 2016

По оценкам Дмитрия Медведева, потери от киберпреступности только в банковской сфере в мире оцениваются в 0,5 трлн долларов. Рост потерь от этого вида криминала заставил правительство собраться на специальное совещание. Фоном для обсуждения его итогов оказался ставший сегодня известным инцидент не финансовый, но все равно характерный - кража данных 100 млн пользователей сети "Вконтакте"

ГрабIТели наступают

Уже довольно давно IT-технологии стали неотъемлемой частью практически всех операций с деньгами – это и многомиллиардные расчёты, и оплата обычных услуг типа коммунальных, отметил Дмитрий Медведев. Всем понятно, что платить "одним кликом" весьма удобно, но люди и бизнес должны быть уверены, что транзакция состоится, деньги не украдут. Поэтому защита средств является ключевым вопросом современного кредитно-финансового оборота, особенно при переходе от наличных расчётов к электронным платежам.

Мошенники, которые занимаются киберпреступлениями, атакуют не только электронные кошельки конкретных владельцев, но и вообще элементы всей кредитно-финансовой системы, счета банков, финансовых компаний, государства, отметил премьер. Они хорошо изучили уязвимость программного продукта, тем более что каждый программный продукт пишется людьми и там есть "бреши". Есть и просто использование доверчивости обычных людей. Активность таких преступников и количество преступлений растёт повсеместно. Есть факты установления преступных групп, но очевидно, что проблема не решается просто путём задержаний.

Хакеры часто атакуют дистанционные услуги. Ограбления банков теперь происходят не так, как это было на протяжении веков, а с использованием экрана планшета или компьютера.

Очень часто атаки хакеров направлены на причинение общего вреда, отметил премьер, и действительно, совещание совпало с новостью о том, что данные чуть более 100 млн пользователей российской социальной сети "ВКонтакте" украдены и выставлены на продажу. Об этом сообщил американский онлайн-портал Motherboard. Другой портал под названием LeakedSource, проверил выставленные на продажу данные и выяснил, что 92 из случайно выбранных 100 аккаунтов оказались действующими. Советник президента РФ по вопросам развития интернета Герман Клименко в ответ на новость предложил рассмотреть возможность создания международного центра деанонимизации для борьбы с киберпреступностью, заявив: "Первопричина киберугроз - это сохранение странами анонимности пользователей в интернете".

Те еще защитники информации

В принципе российское законодательство в сфере защиты персональных данных и борьбы с киберпреступлениями является одним из самых развитых и современных в мире, что, впрочем, не является гарантией обеспечения высокого уровня защиты интересов граждан и государства, - говорит партнер юридического бюро Замоскворечье Дмитрий Шевченко. Он напоминает, что впервые само понятие преступлений в сфере компьютерной информации появилось в законодательной базе аж в 1996 году, когда в УК РФ была включена 28 глава, предусматривающая внушительные штрафы и даже лишение свободы для нарушителей.

Уголовная ответственность предусмотрена в случае кражи данных и их незаконного использование в большинстве стран, однако, как показывает практика, до сих пор это не позволяет эффективно бороться с киберпреступниками, число которых по мере развития технологического оснащения и развития сети, постоянно растет вместе с масштабами совершаемых преступлений. Главной причиной низкой эффективности борьбы с преступниками является крайне низкий уровень международного взаимодействия.

К примеру, рассказывает эксперт, едва ли не единственным международным соглашением в этой сфере является открытая Конвенция Совета Европы ETS 185, содержание которой вызывает массу нареканий и противоречий, которые в частности приводят к тому, что ряд стран, включая Россию, не являются ее участниками, что в свою очередь негативно сказывается на

эффективности борьбы с преступниками. Опять же, учитывая, что киберпреступность носит интернациональный характер, а ее целью почти всегда является конфиденциальная информация, касающаяся деятельности крупного бизнеса, государства и больших групп физических лиц - то есть, представляющая большой интерес в том числе и для спецслужб, занимающихся, помимо борьбы с киберпреступниками, практически аналогичной деятельностью в интересах государства - обмен данными и взаимодействие с этой сфере крайне ограничены.

Деанонимизация, по мнению Шевченко, не позволит искоренить киберпреступность - такие меры позволяют отслеживать деятельность рядовых пользователей, в то время как хакеры обычно используют достаточно совершенные системы, позволяющие им действовать анонимно и скрываться от правосудия, чему в частности способствует развитие неиндексируемой "глубокой паутины" и криптовалют. Бороться с утечками данных можно исключительно развитием международного сотрудничества, но, учитывая, что борьбой с киберпреступниками в основном занимаются спецслужбы, и это весьма затруднительно.

Готовимся к настоящим кибервойнам

На сегодняшний день информационные технологии стали определять национальную безопасность и суверенитет страны, отмечает, в свою очередь, заслуженный юрист России, профессор Академии МВД России Иван Соловьев. При этом, если говорить в целом о ситуации в глобальном информационном пространстве, то она имеет тенденцию к ухудшению. Эксперты в сфере кибербезопасности говорят, что геополитическое состояние современного мира - в силу специфики революции в сфере информационно-коммуникационных технологий и методов их использования - можно было бы назвать «войной в условиях мира».

С этим вполне можно согласиться, говорит юрист, хотя бы потому, что в среднем в год количество вредоносных воздействий на российские государственные интернет-ресурсы превышает 70 млн. Киберпреступность наносит огромный совокупный ущерб: ежегодно от 500 млрд до 2–3 трлн долларов.

Нельзя забывать и о таком новом и одновременно опасном явлении как кибертерроризм. Так, «Исламское государство» (запрещенная в РФ террористическая группировка) уже влезло в информационное пространство и занимается кибертерроризмом. Сегодня тема информационной безопасности объединяет весь спектр угроз для современного государства: военно-политическое использование контента, терроризм и киберпреступность. В связи с этим государства активизировали подготовку к возможным кибервойнам. Есть официальные данные, по которым 12 из 15 крупнейших стран мира разрабатывают киберстратегии на уровне своих военных ведомств.

И здесь, полагает Соловьев, становится непринципиально важным, на кого будет направлен кибеудар: на госсектор или корпорации. Ведь удар по информационным системам нескольких крупных банков или промышленных корпораций может быть не менее болезненным, чем удар по ФОИВам или госучреждениям. В зависимости от специфики кибератаки, ее результатом может стать обычный взлом без особых последствий, просто для демонстрации силы. А может произойти полный паралич важнейшего объекта - системы освещения или безопасности целого города.

Кроме того, имея в своем распоряжении персональные данные, хакеры получают еще больший простор для различного рода противоправных действий. По украденным паспортным данным можно оформить поддельный договор, сведения, составляющие врачебную тайну могут как дисредитировать человека, так и стать причиной вымогательства, а данные налоговой службы - поводом для ограбления, если злоумышленникам станет известно, что человек задекларировал большой объем полученного дохода или имущества. Можно также смоделировать неоплаченный штраф или налог. С учетом стремительного развития электронных порталов государственных услуг, включающих массу информации о гражданах, а также сопровождающегося созданием различных электронных баз данных, реестров и кадастров, актуальность киберугроз стремительно возрастает.

Раньше отдельные ведомства сами создавали системы защиты от киберугроз, при этом многое дублировалось, что приводило к неэффективным тратам госсредств. В таких условиях логичным было бы создать единый центр и уполномоченных орган исполнительной власти, который имел бы все компетенции и полномочия в этой сфере. Не случайно в 2013 году президент Владимир Путин поручил ФСБ разработать систему противодействия кибератакам на информационные ресурсы страны.

Но нельзя оставлять в стороне такой фактов как слабую подготовку непосредственно сотрудников государственных ведомств и коммерческих структур. Специалисты говорят, что в 90 процентах случаев утечка данных происходит именно по их вине. Речь идет даже не о злом умысле. Люди просто не умеют обращаться с информацией: используют слишком простые пароли, скачивают сведения на флешки, которые потом теряют, забывают гаджеты в общественных местах и т.д.

Говоря о мерах, направленных на минимизацию киберугроз отметим создание упомянутой нами государственной системы обнаружения, предупреждения и ликвидации последствий

компьютерных атак на информационные ресурсы страны. Правовой основой для этого послужил указ президента РФ. Система ориентирована, прежде всего, на защитукритической информационной инфраструктуры Российской Федерации, но и владельцы иных информационных систем получат возможность использовать ее потенциал, в том числе методику обнаружения компьютерных атак, для защиты своих информационных ресурсов.

Создание государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации это важный шаг в совершенствовании системы управления информационной безопасностью в стране и не последний. Уже назрела необходимость разработки новых доктринальных подходов к обеспечению информационной безопасности с учетом масштабов применения информационно-коммуникационных технологий (ИКТ), появления новых угроз, в том числе угроз военного применения таких технологий. Также необходимо сформировать современную эффективную институциональную структуру управления информационной безопасностью в государстве.

Также Иван Соловьев полагает, что парадигма отношения к информационной безопасности как к комплексу технических проблем защиты информации и систем связи в последние годы принципиально изменилась. С развитием информационно-телекоммуникационных сетей, прежде всего, Интернета, стало очевидно, что не менее важно содержание размещаемой в сети информации, контент. Поэтому понятно стремление общества очистить Интернет от информации, которая может нанести ущерб правам и законным интересам людей, даже не являющихся пользователями Сети. В этих целях принимаются международные акты и национальные законы, предусматривающие запреты на использование Интернета для торговли детьми, их эксплуатации, детской проституции, а также деятельности, связанной с изготовлением и оборотом материалов или предметов с порнографическими изображениями несовершеннолетних, незаконным оборотом наркотиков, распространением экстремистских материалов.

Еще одним важным моментом является сохраняющаяся пока довольно опасная для страны технологическая зависимость в сфере связи и информации. Используемые повсеместно программные комплексы и программно-технические средства, разработанные за рубежом, не могут с достаточной надежностью обеспечить информационную безопасность, особенно при применении их в критически важных информационных инфраструктурах. (Имеется в виду потенциальное наличие в иностранном программном обеспечении так называемых «недекларируемых возможностей» (НДВ), способных переключать управление, блокировать и разрушать информационные системы и т.п.). Устранить такие риски можно, развивая отечественное производство, конечно, не по всему спектру программных средств и систем, но хотя бы по приоритетным направлениям. Кроме того, программное обеспечение иностранного производства должно передаваться со всеми исходными кодами, чтобы была возможность провести экспертизу на наличие НДВ.

Масштабы киберпреступлений, распространение негативной информации посредством Интернета, а также желание максимально эффективно использовать возможности этой технологии для удовлетворения разнообразных потребностей граждан, побуждает законодателей искать механизмы правовой защиты их интересов при использовании интернета. Последние 13 лет практически в каждом созыве Государственной думы рождаются предложения о разработке закона об интернете. Общее законодательство, безусловно, распространяется на общественные отношения, осуществляемые с использованием интернета.

Однако иногда оно труднопременимо, например, поиск и идентификация киберпреступника. Кроме того, появились новые субъекты (хостинг-провайдеры, контент-провайдеры, сервис-провайдеры и др.) и объекты (сайт, доменное имя и др.) общественных отношений. Очевидно, что в законе об Интернете речь должна идти об особенностях регулирования правоотношений, осуществляемых с его использованием. Необходимо также оценивать реализуемость предлагаемых правовых процедур в условиях глобальных коммуникаций. И, конечно же, учитывая быстрорастущую аудиторию российского интернета, концепция такого закона должна пройти широкое общественное обсуждение. При этом Россия стоит во главе перечня стран - лидеров по агрессивности интернет-среды: более 58% пользователей подвергались атакам в интернете. В целом по миру частота столкновения пользователей с киберугрозами выросла на два процента и теперь составляет 34,7%.

Что касается простых граждан, то здесь интересны результаты опроса, проведенного Национальным агентством финансовых исследований (НАФИ). Согласно его положениям, надежность и безопасность при передаче персональных данных – наиболее важные для россиян факторы выбора канала онлайн платежей. Ради них потребители готовы пожертвовать удобством и функциональностью. Техническая надежность и отсутствие мошенничества в переводе денежных средств - лидирующая характеристика в рейтинге критериев выбора способа для осуществления платежей и переводов, по оценкам пользователей дистанционных каналов

обслуживания. Все это, заключает профессор, ярко свидетельствует о том, на что в первую очередь стоит обращать внимание при купировании киберугроз.

http://expert.ru/2016/06/6/ispolzovanie-doverchivosti/?ny

08 06 2016

Киберпреступность: «Мы отстаём от хакеров на милю»

Хакерские атаки ежегодно обходятся немецким компаниям в миллионы евро. В интервью с немецким изданием DW, консультант Сандро Гайкен рассказал о преступниках и жертвах, и одном из крупнейших ограблений банка в истории, которое едва удалось предотвратить.

На фото: Символическое изображение хакерской атаки

В Берлине происходит ежегодный форум частного колледжа "Европейской школы менеджмента и технологий" (ESMT). Главной темой в этом году является преобразование данных в цифровую форму и компьютеризация систем. Сандро Гайкен является директором "Института цифрового общества" в ESMT и является выдающимся экспертом в вопросе киберпреступности.

Господин Гайкен где, по Вашему мнению, в интернет-преступности затаилась самая большая проблема для бизнеса?

Мы наблюдаем целый ряд новых моделей атак. В настоящее время очень сильно распространяется так называемая "программа вымогатель". Такие атаки шифруют данные компании. Получить доступ обратно к данным можно только при условии уплаты выкупа. Такие атаки поражают и большой, и средний и малый бизнес.

В банковском деле и финансовом секторе мы наблюдаем увеличение числа атак, которые имеют дело с манипулированием на биржевом рынке и с перехватом трансакций. Совсем недавно была предпринята попытка в банке Бангладеш в Нью-Йорке незаконно провести транзакцию на сумму в миллиард долларов. По факту злоумышленники успели перевести 80 миллионов. Если бы они успели украсть миллиард, это было бы самым большим ограблением банка в истории.

Вы консультируете различные компании. О каких видах нападений они чаще всего сообщают?

Чаще всего мы сталкиваемся с обычными преступниками. Они работают в основном с программным обеспечением, написанном для вымогательства. Затем существуют также и организованные преступники. Последнее время они питают сильный интерес к киберпреступности, особенно в области банковского дела и финансов. Они стоят немного в стороне от традиционных бизнес-моделей, они больше склонны к инновационным подходам. Также есть и государственные злоумышленники, которые орудуют в сферах стратегического и промышленного шпионажа.

Сандро Гайкен: "Борьба требует новых подходов". Сандро Гайкен является директором Института цифрового общества в ESMT. Он ведёт исследования в сфере киберпреступности и консультирует компании, организации и немецкое государство. Он, например, участвует в соглашении "No-Spy" между Китаем и Германией.

Кто в предприятии представляет собой наибольший риск для безопасности: человек или машина?

Риск для безопасности существует на обоих уровнях. Часто многие обобщают и утверждают, что человек представляет собой наибольший риск. На людей легко можно надавить и заставить их помочь с вторжением в информационно технологическую составляющую предприятия. Но если на людей повлиять не получается, то сама аппаратная часть также может предоставить возможность для атаки. Таким образом, обе составляющие в равной степени несут в себе долю риска.

У крупных компаний есть преимущество перед мелкими и средними компаниями, когда речь идет о кибер-безопасности?

У малого и среднего бизнеса проблема заключается в том, что они не могут так хорошо вооружиться, как крупные корпорации. Таким образом, конечно, они более уязвимы перед атаками. Малые предприятия часто не имеют достаточного опыта и средств, чтобы купить нужную защиту. Они часто не знают точно, где именно кроются их риски и проблемы, и что именно они должны лучше защищать. Многие из рекомендованных технологий безопасности также являются слишком дорогими для малого и среднего бизнеса. Злоумышленники знают об этом и поэтому нацеливаются именно на них.

Поговорим о четвертой промышленной революции, то есть о машинах, которые взаимодействуют друг с другом и приобретают все большее значение для отрасли. Неужели это следующий открытый фланг для потенциальных кибер-атак?

Конечно! Было уже много таких атак. Недавно, например, по недосмотру произошло нападение на немецкий ядерный реактор. Грузовой кран для ядерного материала был заражен вирусом. В Швеции нападению подверглась система воздушной безопасности, и на несколько часов её перевели в автономный режим. Это также очень высокий риск. У управляющих критической инфраструктуры это вызывает все больше и больше беспокойства.

Как вы думаете, киберпреступность будет иметь влияние на развитие процесса компьютеризации?

Я надеюсь, что люди извлекут положительные уроки и будут строить более безопасные и эффективные системы. Но, пока ИТ-индустрия не сильно к этому стремится, так как процессы постройки новых и более безопасных систем, являются очень сложными и дорогостоящими.

Компании могут также отказаться от процесса дальнейшей компьютеризации.

Уже есть много компания, которые говорят: нам достаточно и этого. Я дойду до этой точки, и пока что мне хватит. Это особенно заметно в сфере промышленности 4.0, где многие машиностроители говорят, что им это не нужно, и они не видят в этом большой пользы.

Индустрия безопасности сильно выросла в последние годы. По уровню развития она идёт вровень с "агрессором"?

Нет! Индустрия безопасности обязана развивать новые идеи. Но с 90-х годов в течение многих лет уже почти ничего не меняется. Все делают вид, что они изобрели что-то новое, но, в конце концов, компании продают старьё под новыми этикетками. Им необходимо срочно разжиться какими-никакими деньгами и разрабатывать новые подходы. Основная проблема заключается в том, что в этой сфере существует много мелких и средних компаний, у которых нет большого бюджета для развития всей отрасли. Таким образом, индустрия безопасности отстаёт от злоумышленников на целую милю.

Интервью вёл Николас Мартин.

http://obzor.press/press/23963-kiberprestupnost-myi-otstayom-ot-xakerov-na-milyu

09.06.2016

В Горно-Алтайске зарегистрирован очередной факт хищения денежных средств, при помощи вирусной программы

В дежурную часть отдела МВД России по г. Горно-Алтайску с заявлением обратилась местная жительница 1981 года рождения, которая сообщила о краже денежных средств с банковской карты.

В ходе разбирательства установлено, что у потерпевшей к смартфону, с которого она выходила в интернет, была подключена услуга "мобильный банк". Являясь пользователем одной из социальных сетей и скачивая различные приложения, женщина установила вредоносную программу. В результате с ее банковского счета были списаны денежные средства в сумме 16000 рублей. Известно, что в смартфоне потерпевшей отсутствовала антивирусная программа. В настоящее время аппарат изъят и направлен на экспертизу.

По данному факту возбуждено уголовное дело по признакам состава преступления предусмотренного ч. 2 статьи 158 Уголовного кодекса Российской Федерации "кража, совершенная с причинением значительного ущерба". Санкция данной статьи предусматривает наказание в виде лишения свободы на срок до 5 лет.

Пресс-служба МВД по Республике Алтай

http://www.mngz.ru/russia-world-sensation/1983930-v-gorno-altayske-zaregistrirovan-ocherednoy-fakt-hischeniya-denezhnyh-sredstv-pri-pomoschi-virusnoy-programmy.html

10.06.2016

Сбербанк: хакеры крадут больше всех

Вопросам кибербезопасности на различных уровнях необходимо уделять особое внимание. Заместитель председателя правления Сбербанка Станислав Кузнецов рассказал о состоянии дел в сфере борьбы с киберпреступностью.

Он отметил, что в 2015-2016 гг. в мире зафиксировано резкое увеличение крупномасштабных хакерских атак на дистанционные банковские сервисы и услуги, предоставляемые через интернет и операторами мобильной связи. Мировые потери от киберпреступности в 2015 г. составили $500 млрд и к 2018 г. могут увеличиться в 4 раза.

Россия не является исключением. По словам Кузнецова, 2015 г. в России зарегистрировано 43 тыс. киберпреступлений. При этом ущерб составил 400 млрд руб., что в два раза превышает потери от всех экономических преступлений.

"Мы понимаем остроту проблемы и предпринимаем исчерпывающие меры, для того чтобы защитить средства наших клиентов от посягательств криминалитета, — заявил Кузнецов. — В Сбербанке направление по кибербезопасности вошло в топ-10 важнейших направлений развития. Мы ведем эту работу с учетом передового международного опыта, используя наработки ведущих мировых операционных центров по информационной безопасности (SOC)".

Согласно сообщению компании в Сбербанке открыта программа "Кибербезопасность 2018". Банк активно совершенствует собственный SOC. Центр функционирует в режиме 24 х 7 и расположен на пяти площадках в Санкт-Петербурге, Самаре, Екатеринбурге, Новосибирске с головным отделением в Москве. Подключено около 18 тыс. устройств безопасности, что позволяет отслеживать в режиме онлайн функционирование порядка 300 тыс. элементов инфраструктуры.

Как отметил Станислав Кузнецов, в день регистрируется и расследуется порядка 200 событий информационной безопасности. В ближайшее время центр перейдет на новую технологию работы с использованием BigData и Machine Learning.

Планируется обеспечение мониторинга защиты не только российских подразделений банка, но и зарубежных дочерних обществ и банков. В ближайшие месяцы к системе фрод-мониторинга будет подключен первый дочерний банк в Хорватии.

Недавно ФСБ и МВД России удалось задержать группу хакеров, похитивших более 3 млрд руб. у отечественных банков и крупного бизнеса. Помощь в поимке злоумышленников оказали "Лаборатория Касперского" и Сбербанк.

"Мы наладили систему эффективного взаимодействия с правоохранительными органами и планируем еще теснее развивать это сотрудничество, обмениваясь данными об атаках с Государственная системой обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА), а также с Центром мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Банка России. Кроме этого, будет запущена интеграция систем мониторинга для получения информации от провайдеров, операторов связи, крупных российских и международных поставщиков услуг", — заявил Кузнецов.

Напомним, что в начале месяца что сотрудниками МВД России совместно с ФСБ России во взаимодействии с ПАО Сбербанк задержаны 50 подозреваемых в совершении многочисленных хищений денежных средств с расчетных счетов юридических лиц, а также с корреспондентских счетов кредитно-финансовых учреждений с использованием вредоносного программного обеспечения (ПО). Об этом рассказала официальный представитель МВД России Ирина Волк.

В рамках уголовного дела проведено 86 обысков на территории 15 субъектов Российской Федерации. В ходе обысков получены материалы, подтверждающие причастность подозреваемых к созданию бот-сетей зараженных компьютеров, организации целевых атак на инфраструктуру кредитно-финансовых и государственных учреждений и совершению хищения денежных средств. Изъято большое количество компьютерной техники, электронных носителей, сим-карт, банковских карт, печатей и документов юридических лиц, оформленных на подставных граждан.

В период с середины 2015 г. по настоящее время по всей стране зафиксировано 18 целевых атак на автоматизированные рабочие места клиентов банков, ущерб от которых превысил 3 млрд руб. При этом полиция смогла предотвратить возможный ущерб на сумму 2 млрд 273 млн руб.

http://www.vestifinance.ru/articles/71772

11.06.2016

Сбербанк России создал новую программу для борьбы с хакерами

По данным Сбербанка количество кибер преступлений за последние два года выросло в 12 раз

Руководство Сбербанка России объявило о старте компании, которая будет эффективно бороться с кибератаками. Первым делом, созданная программа протестирует системы онлайн-безопасности.

По данным банка, сегодня 98% всех финансовых преступлений совершают именно в интернете. Для противодействия хакерам запустили специальный операционный центр. Компьютерная программа последнего поколения в режиме реального времени отслеживает отражение хакерских атак и наглядно демонстрирует, сколько денег удалось уберечь от кибер преступников. Шестизначная сумма на мониторе средств, которые могли похитить злоумышленники всего за один день, составляет более 35 млн. рублей.

«В день мы имеем, примерно, 1-2 млн. событий, которые в ту или иную степень могут иметь отношения к различного рода нарушениям работы технологических систем. Такого рода количества информации событий необходимо анализировать, выявлять, конечно, же, критические

события, для того, чтобы ими управлять», — рассказал Станислав Кузнецов, заместитель председателя правления Сбербанка.

По данным Сбербанка количество кибер преступлений за последние два года выросло в 12 раз. А ущерб в российской экономике только за прошлый год составил более 600 млрд. рублей.

http://www.pravda-tv.ru/2016/06/11/234907/sberbank-rossii-sozdal-novuyu-programmu-dlya-borby-s-xakerami

14.06.2016

Новые возможности мошенников: КАК защитить свою собственность

В Украине набирает обороты "нотариальный скандал". Речь идет о том, что у мошенников появилась возможность от имени практически любого нотариуса страны совершать действия в Реестре недвижимости и ряде других реестров. Коротко говоря, после внесения определенных изменений в Реестр собственность любого украинца или фирмы может… поменять владельца! Причем когда истинный хозяин об этом узнает, может быть поздно.

Минюст же заявляет, что все базы реестров хорошо защищены. Как ни парадоксально, утверждают специалисты, реестры Минюста и в самом деле под защитой. Но жулики нашли другие пути, без взлома самих реестров. Почему так случилось и каким образом собственность меняет владельцев, разбиралась газета "Сегодня".

ПЕРЕМЕНЫ. Как известно, в конце прошлого года Кабмин расширил полномочия нотариусов, но одновременно лишил их возможности ставить подпись и печать на извлечениях из Реестра. Теперь нотариус выдает лишь информационную справку о принадлежности собственности, зафиксированной в Реестре. Расширен и перечень структур, имеющих доступ к реестрам: не только нотариат, но и ряд других субъектов, — банки, исполнительная служба, другие структуры, уполномоченные Минюстом, которым переданы ключи доступа к реестрам. Если ранее конкретный нотариус совершил какое-то действие в Реестре (скажем, наложил запрет на имущество), то только он мог совершить обратное действие (снять запрет). Это доставляло определенные неудобства клиентам, даже чисто географически. Теперь обратное действие может совершить любой из уполномоченных лиц.

Нотариусы считают, что Украина к такому повороту была не готова по техническим причинам. И, судя по жалобам нотариусов и оценкам специалистов, число мошенничеств с действиями в Реестре после изменений законодательства резко увеличилось, однако официально это пытаются скрыть, чтобы не создавать панику.

ТРЕВОГУ ЗАБИЛ СЪЕЗД. Ситуация с мошенничествами в реестрах стала столь острой, что в конце апреля 2016 года нотариусы страны собрались на свой внеочередной съезд. Было заявлено в резолюции съезда, что лишь за последнее время произошло свыше 300 несанкционированных, посторонних вмешательств в Госреестр вещевых прав, в результате чего пострадали более 20 нотариусов. Хотя, отметил съезд, на деле таких вмешательств гораздо больше. Причем в сфере незаконных действий оказались не только частные владения, типа квартиры или дома, но и крупный банк, кондитерская фабрика и пр.

Правоохранители, по словам участников съезда, не очень-то хотят реагировать на заявления пострадавших нотариусов. Например, один из нотариусов трижды (!) обращался с заявлением о несанкционированном вмешательстве в Реестр от его имени, но безрезультатно. И только судебное решение заставило правоохранителей наконец открыть уголовное производство по этому поводу. Но даже в таких случаях при расследовании уклон обычно делается в сторону… виновности самого нотариуса!

"Я с дрожью включаю каждое утро свой рабочий компьютер и, зайдя в Реестр, запрашиваю отчет о… собственных действиях за последние сутки, — рассказал "Сегодня" на условиях анонимности столичный нотариус. — Боюсь того, что увижу — от моего имени кто-то изменил право собственности, наложил или снял запрет на что-то, и т. д. Ведь отвечать в случае чего мне. Дошло до того, что на нервной почве у меня развилась аллергия, а врач сказал, что если не перестану так волноваться, то стану пациентом психиатра…"

Расценки. Жулики вовсю рекламируют себя на закрытых сайтах.

СХЕМА. О подробностях мошеннических действий с реестрами и о возможности от этого защититься мы поговорили со специалистом в области компьютерной криминалистики, директором лаборатории Сергеем Прокопенко.

— Сегодня любая собственность является, образно говоря, просто записью в базе Реестра (например, недвижимости), — говорит специалист. — А держателем ряда баз является Минюст. Примерно с конца 2014 года появились случаи несанкционированного доступа к базам и реестрам с помощью хакерского взлома. Заявления Минюста, что их базы хорошо защищены, скорее всего, соответствуют действительности. Но дело в том, что хакеры ее и не пытаются ломать! Есть путь гораздо проще: хакеры проникают в компьютеры нотариусов, завладевают их паролями и ключами доступа, а затем как бы от имени конкретного нотариуса производят в реестрах определенные действия, конечно, не бесплатно, а по заказу.

Схема, как правило, такова... В адрес нотариуса присылается электронное письмо с подделанным обратным адресом якобы от Минюста. Озаглавлено обычно очень строго, типа: "Срочно!", "К исполнению" и пр. А в письме содержится некое вложение, то есть шпионская программа. Как только нотариус откроет письмо, программа запускается и начинает действовать. То есть скачивает пароль и ключ доступа к Реестру от конкретного нотариуса.

Причем хакеры получают также все контакты этого нотариуса. И как только он обратится к коллеге — тот тоже получает "шпиона". И так далее, заразиться могут десятки компьютеров, откуда тоже будут скачаны пароли и ключи доступа. А затем от имени любого из нотариусов производятся различные незаконные действия в Реестре, например, по переводу собственности от настоящего хозяина к другому лицу.

ОТ РЕКЛАМЫ — К МАССОВЫМ ВЗЛОМАМ. Ранее такие нападения были скорее рекламно-хакерскими. То есть взламывали компьютеры 1—2 нотариусов и рекламировали себя: мол, вот что можем сделать, разумеется, не бесплатно. Самих же действий от имени нотариуса было мало. Потом появились заказы, и число нападений резко увеличилось. Особенно оно возросло с осени прошлого года — видно, хакеры поняли, что появился настоящий спрос, и стали массово заражать компьютеры нотариусов.

Преступная группа, скорее всего, выглядит так: есть очень профессиональный хакер, либо несколько, с ними связан человек или люди, знающие всю юридическую кухню, потому что действовать от имени нотариуса, не зная, что к чему в том или ином документе, нереально. Теперь, когда можно анализировать уже прошедшие вмешательства в реестры, можно сделать вывод, что орудует скорее не бывший нотариус, а экс-работник исполнительной службы. Это видно по "почерку" заполнения документов, если без технических подробностей. Бывший работник — потому что порой не в курсе некоторых нововведений, например, касательно суммы оплаты за те или иные действия.

Далее идет группа людей, занимающихся распространением "продукта", в каком-то смысле пиарщиков. Они ищут клиентов и рекламируют "товар". Например, находят человека с проблемной ипотекой, с которого банк требует возврат кредита, угрожая забрать недвижимость. Ему предлагают: платите нам куда меньшую сумму, мы снимаем в Реестре запрет на действия с вашим жильем, вы продаете квартиру, отдаете долг банку и живете спокойно. Цена за такие действия в последнее время здорово выросла. Вначале хакер просил примерно 300 долларов, и проблемы в Реестре решались. Но сейчас стоимость услуги для конечного потребителя (в нашем примере владельца недвижимости) выросла до 3—5 тысяч долларов.

В этой связи к нам стали обращаться нотариусы, пострадавшие от подобных действий. Впервые это произошло в начале 2015 года. Нотариус принесла к нам компьютер, потому что заподозрила неладное — она действий не совершала, а на деле они от ее имени произведены. Мы разобрались, нашли следы взлома и выяснили, каким образом машина была заражена, куда отправлялись сведения, и пр.

Когда дело приобрело массовый характер, Минюст разослал нотариусам электронное письмо, в котором рекомендовал, входя в базу, проверять, какие от его, нотариуса, имени были совершены действия, и какие из них сделаны не им. Если заметил неладное, надо позвонить в НАИС ("Национальные информационные системы", подразделение Минюста. — Авт.) — орган, который осуществляет техническое обслуживание баз реестров и выдает ключи и коды доступа к базам.

Попросить заблокировать ключи, попавшие в чужие руки, параллельно написать заявление в полицию, и ждать решения Минюста. Правда, написав заявление в полицию, есть шанс, что тебя же и заподозрят в мошенничестве, мол, ты — черный нотариус, а пытаешься снять с себя ответственность, сделав вид, что твои ключи украли. Ведь, пока нет официального подтверждения, что был взлом компьютера, получается, что к Реестру обращался именно данный нотариус. Действия-то совершались от его имени…

В ДЕЛЕ — РОССИЙСКИЕ СЕРВЕРЫ. "Вернемся к первому случаю обращения к нам, — продолжает специалист в области компьютерной криминалистики, директор лаборатории Сергей Прокопенко.

— Мы тогда провели полноценное расследование и многое сумели определить. Нашли программу, которая позволяла удаленно подключаться к компьютеру нотариуса и параллельно ему выполнять от его имени любые действия на виртуальном рабочем столе. Обнаружили и сервер, куда отправляла программа-шпион все данные (в основном хакеры Украины пользуются сейчас российскими серверами, потому что с началом АТО нет полноценного обмена информацией между двумя странами). Получили мы и доступ к этому серверу, и увидели всю преступную цепочку. Нашли в том числе почтовые ящики, с которых делались рассылки фальшивых писем от имени Минюста, а также список пострадавших нотариусов.

Правда, наши попытки связаться с ними, кое-что уточнить в основном успехом не увенчались, потому что нотариусы решили, будто это мы сами и взломали их машины, а теперь пытаемся шантажировать… Что делать, люди у нас подозрительные… Обратившемуся к нам

нотариусу мы выдали заключение, с которым он, хотя бы на стадии досудебного следствия, мог доказать, что компьютер был взломан, и такие-то действия от его имени совершал не он. Тут есть нюанс.

По многим экспертизам есть четко выписанный порядок аттестации экспертов, допущенных к работе. Но несколько экспертиз, в том числе та, о которой мы говорим выше, такого порядка не имеют, поэтому, принять ли наше заключение, зависит от доброй воли следователя или судьи. Пройти аттестацию могут только сотрудники государственных экспертных учреждений. Насколько знаю, в упомянутом выше случае наше заключение было принято во внимание, и нотариус уголовного наказания за несовершенное им преступление не понес".

ОФИЦИАЛЬНО. На сайте Минюста сказано, что существующий режим доступа к реестрам, которые находятся в ведении этого ведомства, отвечает мировым аналогам, а в ряде случаев превышает их. Благодаря этому достигается беспрецедентно высокий уровень защиты информации. И хотя, мол, в СМИ появились сообщения о возможности постороннего вмешательства в деятельность Реестра недвижимости, по данным НАИС, никаких фактов нарушения технологии режима доступа к реестрам не зафиксировано.

При этом, подчеркивается в сообщении, именно на самих нотариусов возложена обязанность хранить ключи, идентификаторы и пароли доступа к реестрам в тайне, не допускать использования их другими лицами. Но если в отношении помощников нотариусов и других работников офиса в этом плане все понятно, то как быть с хакерскими атаками? Об этом ведомство ничего не говорит...

Съезд обратился к Минюсту с рядом предложений, а также о правовой защите самих нотариусов, пострадавших от действий мошенников. Надеются, что ведомство поможет решить возникшую проблему.

РЕАЛИИ: НИКТО ИЗ НАС НЕ ЗАЩИЩЕН ОТ МОШЕННИКОВ

— На сегодня мы уже расследовали около десятка подобных случаев, — продолжает Сергей Прокопенко. — Но это, судя по всему, очень небольшой процент от реального количества хакерских атак и взломов компьютеров нотариусов. К тому же от имени каждого нотариуса совершаются десятки действий (например, в одном из последних случаев таких действий было более пятидесяти!). Объектами может служить недвижимость, в том числе и коммерческая (например, как-то нелегально завладели заправкой), или вообще "снятие ареста со всего имущества".

Скажу, что это касалось даже очень больших, известных компаний, проигравших некий спор в суде, после чего имущество было арестовано… Можно снять арест по любому, в том числе уголовному делу, наложенному судом, ибо все равно запрет в конечном итоге исполнительной службой зафиксирован в реестре, куда получают доступ жулики. Бывали случаи, когда объект недвижимости за день-два мошенниками перепродавался несколько раз, попадая в итоге к добросовестному покупателю. В таком варианте вернуть собственность владельцу весьма сложно…

Хакеры совершенствуют свои методы, меняют кое-что в программах, хотя общая схема остается прежней. Мы же свои наработки отдаем в антивирусные компании, и их программы начинают отлавливать "шпионов", уже понимая, что это вирус. Впрочем, сейчас применяется технология, когда сам вирус лежит на файлообменнике и ждет, когда зараженный маленьким файлом-кодом компьютер к нему обратится. Техническую сторону особо объяснять не буду, это для специалистов.

Но суть в том, что, по нашим прикидкам, уже свыше 500 компьютеров, находящихся у нотариусов, заражены, от их имени могут совершаться тысячи незаконных операций. В конечном итоге получается, что никто из украинцев не защищен от того, что его собственность не уйдет путем, который описан выше. Ведь собственность человека — это запись в соответствующем реестре. Там написано, скажем, что квартира такая-то принадлежит Иванову, с таким-то идентификационным номером. Стоит эти сведения в реестре изменить — и жилье уже принадлежит другому человеку, который может, например, тут же его продать…

ЗАШИТА: СМС, ОСОБЫЕ ФЛЕШКИ ИЛИ "СЕРВЕР-СТЕНА"

— Среди объектов атаки хакеров может быть и государственная или коммунальная собственность, ее реально переписать на конкретную личность или фирму, — говорит специалист по компьютерной криминалистике Сергей Прокопенко. — Это касается не только реестра недвижимости, но и, скажем, земельного кадастра, к которому тоже имеют доступ нотариусы, а значит, путем взлома их компьютеров, и жулики. Такие случаи уже были, нас даже приглашали в определенную структуру для консультации, как это могло случиться. Мы объяснили. А сейчас передается регистрация и перерегистрация предприятий в ведение нотариусов. Это серьезная предпосылка для рейдерских захватов. Схемы их проведения — как и описанные выше мошеннические операции с недвижимостью.

Проблема в том, что, на наш взгляд, украинские власти не очень понимают, как с этим бороться. Сейчас мелькнули сообщения о том, чтобы использовать СМС, как в банкинге, когда на

ваш телефон придет некий код, без которого не войдешь в реестр. Либо предлагают использовать специальные флешки, с которых нельзя скачать ключи (эти ключи и сейчас у нотариусов в основном на флешках, но обычных).

Но на самом деле это совершенно не решит проблему, потому что программа удаленного доступа, о которой мы говорили выше, позволяет создать виртуальный рабочий стол, который будет работать параллельно с обычным, открытым у нотариуса на компьютере. И защищенная флешка или СМС не помогут, — на виртуальном столе хакер все видит и может выполнять любые действия, ибо нотариус вошел в реестр (а с ним и хакер). Например, нотариус выполняет определенные, совершенно законные действия, не подозревая, что в то же время хакер от его имени снимает арест с какой-то квартиры или переписывает имя владельца собственности…

Может быть другой путь (см. инфографику). Как только компьютер нотариуса станет подключаться к необычному для себя серверу, с которым работает хакер, возникнет предупреждение, машина нотариуса перестает быть доверенной и к реестру подключиться не может. Соответственно, не подключится и виртуальный рабочий стол хакера. То есть ставится промежуточный сервер, и все нотариусы обращаются к нему, а уже он связывается с реестром. Если же кто-то пытается связаться с базой данных Минюста без промежуточного сервера, напрямую, это точно хакер. Потом зараженный компьютер нотариуса лечится, получаются новые ключи, и работа продолжается.

От себя добавим: предложение специалистов может быть не единственным выходом, важно, чтобы власти обратили внимание на проблему и предложили действенное решение.

Автор: Корчинский Александр, «Сегодня»

http://stopotkat.net/articles/view/51572

16.06.2016

Грабившие банки свердловские хакеры предстанут перед судом

Злоумышленникам удалось похитить со счетов банков более 2,6 млн рублей

В Свердловской области для рассмотрения по существу в суд передано уголовное дело, возбуждённое в отношении жителей Кировграда Вадима Шарапова и Евгения Томилова. Их обвиняют в создании вредоносных компьютерных программ, с помощью которых они осуществляли хищения денежных средств со счетов кредитных организаций. Об этом сообщили в пресс-службе прокуратуры Свердловской области корреспонденту **ИА REGNUM.**

По версии следствия в период с ноября 2014 года по март 2015 года Вадим Шарапов разработал вирусную программу, с помощью которой получил доступ к счетам расположенных в Татарии, Туве и Хакассии банков. Деньги переводились на банковскую карту которую обналичивал Евгений Томилов в Екатеринбурге и Кировграде. Всего за указанное время злоумышленникам удалось обналичить свыше 2,6 млн рублей.

Как сообщил начальник управления информации Главного управления МВД России по региону Валерий Горелых, группировка была обезврежена в мае 2015 года сотрудниками Управления «К» МВД России, отдела «К» ГУ МВД России по Свердловской области совместно с отделом «К» МВД России по Республике Хакасия. В марте 2015 года в одном из коммерческих банков Хакасии были зафиксированы хищения денежных средств с банковских карт клиентов. В ходе оперативно-розыскных мероприятий были задержаны жители Екатеринбурга и Кировграда. У них изъяли 200 сим-карт, использовавшиеся в хищении денежных средств, 100 банковских карт, носители информации, денежные средства в сумме более 600 тыс. рублей, и т.д.

Как сообщало ранее **ИА REGNUM**, в начале июня текущего года на Среднем Урале было задержано девять хакеров. Они являлись участниками преступной группы осуществлявшей деятельность в 15 регионах Российской Федерации. В ходе совместных мероприятий сотрудников ФСБ и МВД в регионах России всего было задержано 50 человек, из них 18 участников группы было отправлено в следственные изоляторы города Москвы, а трое отпущены под подписку о невыезде. За время преступной деятельности злоумышленникам при помощи вирусных программ удалось похитить со счетов российских банков более 1,7 млрд рублей.

Все девять фигурантов дела задержанных в Свердловской области были доставлены самолётами в Москву, причём троим предъявлено обвинение в организации преступной группы.

https://regnum.ru/news/accidents/2145623.html

25.06.2015

С банковской карты украли деньги?! ТОП-6 способов обчистить вас!

Случаи кражи денег со счетов клиентов банков при помощи кредитки – едва ли не один из самых излюбленных способов мошенников. Как правило, такие кражи совершаются в ночное время, пока владелец карты спит и не сразу заметит пропажу, а злоумышленники успеют «замести следы».

Банковские карточки есть в бумажнике практически каждого взрослого человека. Бесспорное удобство в использовании, возможность избежать в путешествиях необходимость носить с собой «кэш», доступность оплаты таким путем почти в любой стране мира – неоспоримое преимущество карт перед наличными.

Но что делать, если Вы живете, скажем, в Европе и являетесь держателем счета, а соответственно, и карты европейского банка? Какими способами мошенники могут обчистить вас, и возможно ли вернуть пропавшие с карты деньги – в материале Banks.eu.

Киберпреступность в Европе становится все популярней?

В начале года были опубликованы результаты работы Европейского центра борьбы с киберпреступностью. Ведомство поддержало 18-месячный проект, финансируемый ЕС, направленный против мошенничества с платежными картами.

Новый проект осуществлялся под кодовым названием Skynet, он фокусировался на международном сотрудничестве в борьбе с онлайновым мошенничеством. Шесть государств-членов ЕС участвовали в данном проекте. Программу разработали по инициативе властей Великобритании. В результате ее осуществления всего за несколько месяцев были арестованы 59 лиц, возбуждено 32 уголовных дела и вынесено 17 обвинительных приговоров, а также к ответственности было привлечено 5 организованных преступных групп, занимающихся кражей с помощью электронных платежей.

По данным центра борьбы с киберпреступностью, в общей сложности мошенники на территории ЕС взломали **52 812 номеров карт.** Пострадавшие потеряли около **23 миллионов фунтов стерлингов**.

Примечательно, что активность кибер-мошенников различается в зависимости от страны: по-разному себя вели преступники в Европе, Канаде и США. По данным Европейского Центробанка за 2013 год (результаты 2014-го все еще обрабатываются), потери держателей банковских карт от рук мошенников в отчетном периоде варьировались от 2,8 базисных пунктов в Нидерландах до 7,1 базисных пунктов во Франции и 5,9 – в Великобритании. Для примера: в США эта цифра составила в тот же период 10,4 базисных пункта, а в Канаде – 8,7.

Итак, ТОП-6 самых распространенных вариантов кражи:

1. Скимминг

Смысл способа в том, что к банкомату крепится «фальшивая» клавиатура, пользуясь которой владелец банковской карты (сам того не зная) передает в чужие руки ПИН-код карты. Кроме этого, в кардридер банкомата (отверстие для карт) вставляется устройство (скиммер), с помощью которого злоумышленник считывает данные с магнитной полосы.

2. Кража карточки

Кража – самый банальный способ заполучить Вашу карту, и по статистике именно он является одним из самых популярных. Чтобы украсть карту другого человека злоумышленнику не нужно обладать какими-либо необычными знаниями. Нужно просто уметь воровать. Опытные мошенники воруют карту уже после того, как был подсмотрен ПИН-код (они обычно следят за человеком). А особо продвинутые воры крепят мини-камеры на банкоматы и подсматривают ПИН-коды.

3. Кража банкомата

Злоумышленники получают не только деньги из банкомата, но и имеют возможность считать информацию обо всех картах, которые проходили через кардридер. Стоит отметить, что сегодня воровство банкоматов – явление крайне редкое, но еще совсем недавно этим промышляли многие злоумышленники.

4. Атака на POS-терминал

Кража персональных данных осуществляется посредством установки вредоносной программы или специального дополнительного устройства. Вредоносный код с успехом находит лазейку в защите системы и передает необходимую информацию злоумышленнику о тысячах карт, прошедших через данный терминал.

5. Фальшивые банкоматы

Не редкость в наше время — поддельные банкоматы, они по внешнему виду никак не отличаются от настоящих. Такие устройства представляют собой, на самом деле, полую коробку с вмонтированным в ней скиммером. Пользователь вставляет карту в кардридер и видит сообщение о невозможности проведения операции с деньгами (предлог может быть различным). Он, конечно, забирает карту и идет искать следующий банкомат. На самом же деле все данные с карты уже считаны мошенниками. Остается ими воспользоваться в корыстных целях.

6. Перехват данных с банкомата

Довольно сложно воплощаемый в жизнь способ, но умельцы находятся. Злоумышленник подключается непосредственно к кабелю банкомата, через который передаются данные в банк. Сложность заключается в том, что осуществить подключение необходимо без разрыва проводов.

С чьей карты могут украсть деньги в Европе?

В группе риска все держатели карт, особенно те, кто активно пользуется платежами через интернет, банкоматами и бесконтактными платежами в магазинах. Преступники каждый день выдумывают новые способы получения ваших данных, а банки, со своей стороны, работают над усилением степени защиты своих карт от воров.

Одна ситуация, если Вы не заметили, как кассир дважды провел карту через терминал по ошибке, и подписали чек, не глядя. Тут все просто: пишете в банк-эмитент заявление о несогласии с трансакцией, предоставляете кассовый чек, даете объяснения менеджеру банка. Деньги Вам вернут в довольно короткое время.

Деньги с карты украли: что делать?

Другое дело, если без Вашего ведома с карты была списана некая сумма денег, а Вы — ни сном, ни духом, как говорится... Чтобы увеличить шанс вернуть свои деньги, одним заявлением в банк не обойтись. Как только Вы обнаружили пропажу денег, где бы Вы ни были, немедленно обратитесь в банк для блокировки карты. Круглосуточный телефон службы поддержки написан практически на всех картах европейских банков с задней стороны. Если вы за границей в путешествии, позаботьтесь заранее и возьмите в своем банке все данные для экстренной связи, сегодня в Европе большинство банков предоставляют клиентам услугу связи по скайпу, к примеру.

После того, как Вы заблокировали карту, необходимо прийти в свое отделение банка, лучше туда, где Вы получали карту, вызвать полицию и написать заявление о краже.

И тут начинается бюрократическая волокита... Если речь о маленькой сумме, полицейские честно с глазу на глаз скажут, про деньги забыть. По опыту пострадавших от мелких мошенников сумма, которую не стоит и пробовать вернуть – себе дороже – до 50 евро.

Однако, если же существует прямой путь до ваших денег, то есть: злоумышленники оплатили какой-то товар, на продавца можно выйти, можно отследить адрес доставки товара и т.д. – в этом случае Вы – счастливчик!

Если же следов никаких нет, то расследование может занять несколько месяцев, а с учетом загруженности европейской полиции – и до нескольких лет.

Перед тем, как поднимать шум, вспомните, не задолжали ли Вы каким-то службам, судебным приставам, быть может, на карте включен автоплатёж или только сейчас снялись деньги за ранее произведённую покупку, и т.д. Если эти варианты не про вас, то, обратившись в банк и полицию одновременно, ждете развязки.

Если Ваши деньги украли через интернет и в выписке банка Вы видите такие сервисы, как: Яндекс-деньги, webmoney, pokerstars, qiwi-кошелёк – то, по опыту таких ситуаций, вероятность 80%, что с этих сервисов деньги Вам возвратят. Обычно мошенники не списывают деньги на один кошелёк, они раскидывают все деньги по частям в разные системы. Если же деньги ушли на сотовые операторы, то удастся вычислить только номера, и если SIM-карты зарегистрированы на мошенников, то выйти на них удастся. Кстати, мошенники уже отходят от перечисления денег на SIM-карты, так как вывод с них денег довольно трудоемкий.

Мнение:

Саня (Sanja), зампред крупного сербского банка: *«Наш народ еще не привык к безналичным платежам, предпочитают за живые деньги покупать товар и оплачивать услуги, поэтому держатели карт сербских банков крайне редко сталкиваются с кражами. Все больше это происходит по собственной оплошности. Могу сказать однозначно, наша страна, впрочем, как и рядомлежащие балканские земли — еще далеки от объемов кибер-мошенничества по сравнению с центральными соседями».*

Как не стать жертвой кибер-мошенников?

Во-первых, и это самое важное, не давайте даже мельком свою банковскую карту никому чужому, не допускайте, чтобы кто-нибудь, кроме вас, знал реквизиты вашей карты. Для того, чтобы обчистить вас, мошеннику не нужна сама карта, достаточно знать её основные параметры и CVV код на обратной стороне.

Во-вторых, не подтверждайте по СМС операций, которых вы не совершали.

В-третьих, если Вы заподозрили что-то неладное с вашим личным кабинетом, проводимая операция может прерваться, Вас может вдруг «выбросить» из кабинета и нужно снова вводить пароли для входа в свой кабинет, можете быть уверены — Вы подхватили хакерский вирус, который ворует Ваши данные.

Ваш антивирус должен всегда иметь актуальные базы – постоянно обновляйте их, если Вы – активный пользователь интернет-магазинов.

Не верьте сомнительным СМС уведомлением от, якобы, банка. Мошенники часто застают врасплох клиентов банков, сообщая им, к примеру, о победе в розыгрыше. Клиент перезванивает по указанному номеру, ему предлагают перевести выигрыш на карту и просят сообщить цифры с обратной стороны. И... Прощайте денежки!

Большие суммы денег лучше хранить в депозитах. Или установить лимит по доступной сумме на карте, которую Вы можете потратить.

В заключении, хотелось бы еще раз предостеречь держателей карт, в частности, европейских банков, и посоветовать не давать свою карту в руки чужим людям, даже работникам вашего банка и регулярно проверять остаток на счете. Ведь большинство банков Европе не оповещает по СМС своих клиентов о списании малых сумм со счета.

Яна Куанбекова, Banks.eu

Источник**:** Banks.eu

http://banks.eu/news/info/810

29.06.2016

Московская межрегиональная транспортная прокуратура утвердила обвинительное заключение по уголовному делу о мошенничестве в сфере компьютерной информации на сумму более 17 млн рублей

Московская межрегиональная транспортная прокуратура утвердила обвинительное заключение по уголовному делу о мошенничестве в сфере компьютерной информации на сумму более 17 млн рублей

Первый заместитель Московского межрегионального транспортного прокурора утвердил обвинительное заключение по уголовному делу в отношении 24 лиц, 5 из которых обвиняются в совершении преступления, предусмотренного ч. 1 ст. 210 УК РФ (создание преступного сообщества) и 19 – по ч. 2 ст. 210 УК РФ (участие в преступном сообществе). Указанные лица, объединившись в преступное сообщество, совершили от 3 до 63 эпизодов мошенничества в сфере компьютерной информации (ч. 4 ст. 159.6 УК РФ).

По версии следствия, один из создателей преступного сообщества Максим Матюшев разработал схему хищения денежных средств юридических лиц, осуществляющих дистанционное оформление электронных железнодорожных билетов.

В соответствии с ней он разослал в организации, осуществляющие продажу билетов, электронные письма с вложенной в них вредоносной программой. После открытия адресатом письма она самостоятельно устанавливалась в операционную систему и Матюшев получал полный доступ к информации, логину и паролю личных кабинетов кассиров организаций.

После входа в интерфейс кассира Матюшев вводил информацию о пассажирах, данные которых передавали другие создатели сообщества, в электронную квитанцию, и от имени организации, за счет ее денежных средств производил электронный платеж.

Номера незаконно оформленных квитанций передавались через других сообщников лицам, на чьи паспортные данные оформлялись билеты, для последующего обналичивания денежных средств путем их сдачи в кассы.

Преступное сообщество, состоящее из 29 человек, представляло собой объединение нескольких территориально обособленных групп, действовавших на территориях городов Москва, Санкт-Петербург, Уфа и Новосибирск, Алтайского края и Московской области.

За время существования сообщества по октябрь 2014 года его участники незаконно оформили свыше 5 тыс. электронных маршрутных квитанций на общую сумму более 17 млн рублей.

В ходе расследования уголовного дела выполнен значительный объем следственных действий: допрошено 167 свидетелей, проведено более 100 экспертиз, объем обвинительного заключения составляет 624 тома.

После вручения обвиняемым копий обвинительного заключения уголовное дело будет направлено в суд для рассмотрения по существу.

http://genproc.gov.ru/smi/news/archive/news-1098045/

Номер подписан в свет 11.07.2016