

ФЕДЕРАЛЬНАЯ СЛУЖБА ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ

ФЕДЕРАЛЬНОЕ АВТОНОМНОЕ УЧРЕЖДЕНИЕ
«ГОСУДАРСТВЕННЫЙ НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ ИСПЫТАТЕЛЬНЫЙ ИНСТИТУТ
ПРОБЛЕМ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ
ФЕДЕРАЛЬНОЙ СЛУЖБЫ ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ»
(ФАУ «ГНИИИ ПТЗИ ФСТЭК России»)



ИНФОРМАЦИОННО-АНАЛИТИЧЕСКИЙ СБОРНИК

ВЫПУСК 5 (25)



ПРОБЛЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

(по материалам из открытых источников)

ВОРОНЕЖ
2015

к №а - 49409

Федеральная служба по техническому и экспортному контролю

ФЕДЕРАЛЬНОЕ АВТОНОМНОЕ УЧРЕЖДЕНИЕ
«ГОСУДАРСТВЕННЫЙ НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ ИСПЫТАТЕЛЬНЫЙ
ИНСТИТУТ ПРОБЛЕМ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ
ФЕДЕРАЛЬНОЙ СЛУЖБЫ ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ»
(ФАУ «ГНИИИ ПТЗИ ФСТЭК России»)

ГРНТИ 81.93.29
УДК 002:004.056

Экз. № 43

ИНФОРМАЦИОННО-АНАЛИТИЧЕСКИЙ СБОРНИК

ПРОБЛЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

(по материалам из открытых источников)

ВЫПУСК 5 (25)

Воронеж
2015

Сборник подготовлен с использованием открытых публикаций и информационных ресурсов, размещенных в сети Internet

СОДЕРЖАНИЕ

1. Сведения о развитии и реализации новых технологий в сфере ответственности ФСТЭК России	3
1.1. Противодействие техническим разведкам	3
1.2. Техническая защита информации	16
1.3. Обеспечение безопасности информации в ключевых системах информационной инфраструктуры	39
2. Сведения о перспективах развития и достижениях в создании способов и средств защиты информации	44
3. Сведения о новых документах, регламентирующих вопросы в области защиты информации	49
3.1. Нормативные правовые акты федерального уровня	49
3.2. Документы ФСТЭК России	50
3.3. Патентные документы	51
4. Статистические данные по анализу защищенности информационных систем	53
5. Сведения об инцидентах информационной безопасности	60

1. Сведения о развитии и реализации новых технологий в сфере ответственности ФСТЭК России

1.1. Противодействие техническим разведкам

В США стартовала ракета с секретным кораблем «Boeing X-37B»

По информации ряда сайтов, ракетой «Atlas V» на орбиту выведен секретный многоразовый автоматический корабль «Boeing X-37B». О запуске ВВС США «мини-шаттле», его основных целях и продолжительности полета не сообщается. С 2010 г. США осуществили три запуска аппаратов серии X-37B.



Эти аппараты доставляют в космос небольшие по объему и весу грузы, а также осуществляют разведывательные миссии. В настоящее время у ВВС США в наличии есть еще два военных космических беспилотника. Новый аппарат предназначен для функционирования на высотах от 200 до 750 км. Известно, что он способен быстро изменять орбиты и маневрировать.

Источники: <http://lenta.ru/news/2015/05/20/boeing/> (дата размещения материала 20.05.2015); http://www.oreanda.ru/other/V_SSHA_osuschestvlen_zapusk_sekretnogo_korablya_Boeing_X-37/article904339/; <http://www.vesti.ru/doc.html?id=2594775>.

Следующий этап запусков разведывательных спутников оптической разведки США начнется в 2018 г.¹

Как сообщает сайт spaceflightnow.com, очередная программа замены разведывательных космических спутников США начнется в 2018 г. На орбиту будет выведен космический аппарат (КА) для Национального управления космической разведки в рамках миссии NROL-71.

Усовершенствованный аппарат продолжит серию спутников типа «Keyhole», предоставляющих снимки сверхвысокого разрешения в интересах разведывательного сообщества США. Некоторые эксперты полагают, что первое зеркало нового спутника составит 2,4 метра в диаметре. Это соответствует размерам зеркала внутри космического телескопа «Хаббл», который был спроектирован компанией «Lockheed Martin».



Источник: <http://spaceflightnow.com/2015/05/01/next-round-of-u-s-optical-spy-satellites-to-start-launching-in-2018/> (дата размещения материала 01.05.2015).

¹ Перевод с английского выполнен ГНИИИ ПТЗИ ФСТЭК России.

Японский резервный радарный спутник видовой разведки

Согласно информации, опубликованной в журнале «Новости космонавтики», на орбиту успешно выведен секретный КА японской видовой разведки – резервный радиолокационный «спутник сбора информации» IGS-R «Spare».

Национальная система видовой космической разведки IGS предназначена для сбора информации в интересах силовых и дипломатических ведомств страны, а также мониторинга зон чрезвычайных ситуаций в исключительной экономической зоне Японии. В систему входят четыре КА (два радиолокационных IGS-R и два оптических IGS-O), обеспечивающие как минимум однократный ежесуточный обзор любого объекта на Земле. Спутники видовой разведки IGS размещены попарно на круговых солнечно-синхронных орбитах в двух орбитальных плоскостях – утренней и дневной.



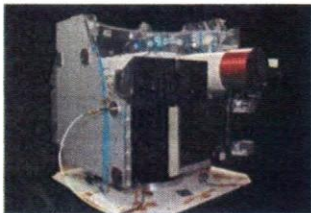
Резервный спутник IGS «Radar Spare» относится к третьему поколению КА видовой разведки и конструктивно аналогичен IGS-R3 и IGS-R4, запущенным в 2011 и 2013 годах. Спутники IGS-R третьего поколения оснащены радиолокатором с синтезированной апертурой с пространственным разрешением менее 1 м. Следующий радарный разведчик IGS-R5 изготавливается по плану для запуска в конце 2016 г.

Впервые в японской практике два радарных спутника (IGS-R3 и IGS-R «Spare») запущены в одну орбитальную плоскость, что позволяет выполнять тандемную интерферометрическую съемку объектов.

Источник: Новости космонавтики, 2015, № 4, с. 17-18.

Канадские космические аппараты контроля космического пространства

В журнале «Зарубежное военное обозрение» опубликованы сведения о проведении в Канаде активных работ по созданию и разворачиванию оптико-электронных средств контроля космического пространства (ККП) космического



базирования в интересах обеспечения безопасности функционирования космических систем. Применение таких средств позволяет осуществлять непрерывное наблюдение за космическими объектами без искажающего влияния земной атмосферы, а также ограничений, связанных с местом дислокации наземных локационных средств и временем суток. В настоящее время на орбитах находятся аппараты «Сапфир» и «НЕОССат» военного и двойного назначения соответственно.

Мини-КА «Сапфир» может функционировать как минимум до 2020 г. в качестве локационного средства, приданного сети ККП США. Эксперимент с аппаратом «НЕОССат» на базе новой универсальной микроплатформы МММБ показал наличие ряда проблем, связанных с недостаточной проработанностью технических решений.

Его эксплуатация продлится, вероятно, до 2016 г., до полного выхода аппарата из строя. Однако опыт, полученный в ходе работы, будет использован при создании в Канаде недорогих перспективных мини- и микро-КА на базе универсальных платформ.

Источник: Зарубежное военное обозрение, 2015, № 4, с. 75-77.

*Украина намерена сформировать собственную
космическую группировку*

По данным сайта vpk.name, Украина намерена сформировать собственную группировку из трех спутников в 2017-2018 годах. Первый аппарат – спутник дистанционного зондирования Земли (ДЗЗ) с невысокой разрешающей способностью «Сич-2-1». Его запуск запланирован на 2017 г. Второй аппарат с высокой разрешающей способностью (не менее 1 м) «Сич-2М» планируется вывести на орбиту в 2018 г.



Сейчас ведутся переговоры с одной из западных стран о возможности покупки такого спутника ДЗЗ для Украины. Информация о третьем аппарате в настоящее время отсутствует. В то же время сотрудничество Государственного космического агентства Украины с Россией в ракетно-космической отрасли свернуто.

Источник: http://vpk.name/news/130930_ukraina_namerena_sformirovat_sobstvennuyu_gruppirovku_iz_treh_sputnikov_v_20172018_gg.html (дата размещения материала 27.04.2015).

*Спутник «Göktürk-1» доставят в Анкару для
выполнения натурных испытаний*

Согласно информации ряда сайтов, турецкий спутник ДЗЗ «Göktürk-1» будет доставлен в испытательный центр в Анкаре, где пройдет натурные испытания. Помимо спутника ДЗЗ, на который будет установлен оптический датчик высокого разрешения, предполагается строительство центра интеграции и испытаний наземного сегмента, который будет контролировать работу спутника на орбите, а также получение и обработку данных.

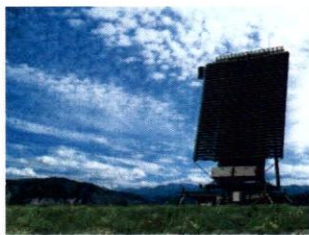


Источники: <http://www.zonebourse.com/THALES-4715/actualite/THALES-Le-satellite-drsquoobservation-Gokturk-1-sur-le-depart-pour-Ankara-ou-debutera-la-campag-20356981/>² (дата размещения материала 12.05.2015); <http://www.infoespacial.com/?noticia=el-satelite-turco-gokturk-1-se-sometera-a-pruebas-ambientales-en-ankara>³.

² Перевод с французского выполнен ГНИИИ ПТЗИ ФСТЭК России.

³ Перевод с испанского выполнен ГНИИИ ПТЗИ ФСТЭК России.

Новая радиолокационная станция НАТО в Латвии



Как сообщает ряд сайтов, вблизи латвийского г. Вентспилс развернута новая американская радиолокационная станция (РЛС) AN/TPS-77. Подобные радиолокационные посты распределены по территории Литвы и Эстонии и включены в структуры «BALNET» и «NATINADS» – системы контроля за воздушным пространством Прибалтики и НАТО на Европейском театре военных действий. Последняя является аналогом североамериканской системы «NORAD» в Европе.

Новая РЛС работает на частотах от 1,22 до 1,4 ГГц.

Источники: <http://armynews.ru/2015/05/pribaltikavooruzhaetsyaradiolokatorom-antps-77/> (дата размещения материала 18.05.2015); <http://vpknews.ru/news/25239>.

Радиолокационный комплекс для системы противовоздушной/ противоракетной обороны Польши «Wisla»

В журнале «Иностранная печать об экономическом, научно-техническом и военном потенциале государств-участников СНГ и технических средствах его выявления» сообщается о намерении Польши закупить средства для наращивания возможностей систем противовоздушной/противоракетной обороны (ПВО/ПРО) страны. Рассматривается вариант модернизации системы на базе зенитно-ракетного комплекса «Patriot PAC-3» компании «Raytheon» за счет включения в его состав нового радиолокационного комплекса.

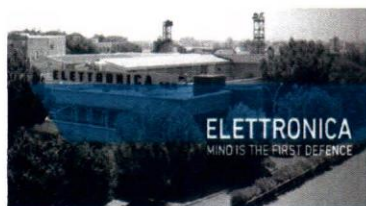


Предлагаемый компанией «Raytheon» радиолокационный комплекс представляет собой набор из трех активных фазированных антенных решеток, использующих наложение полей покрытия. При этом данные, полученные от трех массивов, преобразуются в одну полноценную картину.

Источник: Иностранная печать об экономическом, научно-техническом и военном потенциале государств-участников СНГ и технических средствах его выявления, 2015, № 4, с. 12-13.

Италия помогает КНР в создании центра электронного слежения

Согласно информации сайта bmpd.livejournal.com, итальянская компания «Elettronica», специализирующаяся на производстве электроники для военных нужд (в первую очередь, систем радио- и радиотехнической разведок и радиоэлектронной борьбы), заключила секретный контракт с КНР. Согласно контракту, итальянская фирма будет помогать НОАК в строительстве нового центра радиоэлектронной разведки, который будет находиться в ведении 4-го Управления НОАК.



Источник: <http://bmpd.livejournal.com/1288893.html> (дата размещения материала 03.05.2015).

*Противолодочный самолет GX-6 поступил на
вооружение авиации ВМС НОАК*

Как сообщает сайт vrk.name, новый китайский противолодочный самолет GX-6 недавно начал использоваться в интересах морской авиации ВМС НОАК.

Благодаря своей способности осуществлять контроль больших территорий, GX-6 позволит значительно увеличить морскую безопасность Китая и продвинуть рубежи противолодочной обороны на 1000 км, обеспечивая защиту дальних морских операций. Использование GX-6 может вызывать озабоченность стран, имеющих территориальные споры с Китаем, например, Японии в Восточно-Китайском море, Вьетнама и Филиппин в Южно-Китайском море. Несмотря на то, что самолет отстает от американского противолодочного самолета P-8 по своим боевым возможностям, принятие на вооружение ВМС НОАК GX-6 имеет важное значение, т.к. при его разработке реализован комплекс новых для китайского авиапрома конструктивных и технологических решений.



Источник: http://vrk.name/news/131111_protivolodochnyii_samolet_gx6_postupil_na_vooruzhenie_aviacii_vms_noak.html (дата размещения материала 28.04.2015).

*Тайвань будет патрулировать Южно-Китайское море
самолетами «Орион»*

Сайт vrk.name сообщил, что министерство обороны Тайваня направит на патрулирование районов Южно-Китайского моря противолодочный самолет P-3C «Orion». Тайвань уже получил восемь самолетов этого типа из США, еще четыре будут поставлены до конца этого года. «Орионы» заменят 11 устаревших противолодочных самолетов S-2T ВМС Тайваня, которые уже прослужили более 40 лет.



Источник: http://vrk.name/news/130718_taivan_budet_patrulirovat_yuzhno-kitaiskoe_more_samoletami_orion.html (дата размещения материала 22.04.2015).

*Индия хочет приобрести еще два самолета дальнего
радиолокационного обнаружения A-50Э*

По информации, размещенной на сайте vrk.name, Индия хочет приобрести два дополнительных самолета дальнего радиолокационного обнаружения (ДРЛО) A-50Э на базе транспортника Ил-76 с израильским радиолокационным оборудованием. Этот шаг является ответом Индии на пакистанскую программу приобретения шведских самолетов ДРЛО Saab-2000. Пакистан также получил первый китайский самолет аналогичного класса ZDK-3 из четырех заказанных.



Индийские А-50 будут оснащены израильской РЛС «Phalcon», китайская версия этого самолета имеет обозначение KJ-2000.

Источник: http://vpk.name/news/130780_indiya_zhelaet_priobresti_eshe_dva_samoleta_drlo_a50e.html (дата размещения материала 23.04.2015).

*Беспилотники «Глобал Хоук» могут оснащаться датчиками
разведывательных самолетов U-2*

Согласно данным журнала «Военно-техническое сотрудничество», в ВВС США установили, что интеграция основных бортовых датчиков пилотируемого разведывательного самолета U-2 в бортовую архитектуру беспилотного летательного аппарата (БПЛА) RQ-4 «Глобал Хоук» технически выполнима.



Как показали проведенные исследования, под конструкцию RQ-4В можно адаптировать оптико-электронную разведывательную систему более раннего поколения SYERS-2В/С и камеру слежения ОВС, которыми оснащается U-2.

Источник: Военно-техническое сотрудничество, 2015, № 16, с. 29.

*Разработка беспилотных летательных аппаратов
для ВМС США*

В статье, опубликованной в журнале «Морской сборник», сообщается о создании и применении БПЛА вооруженными силами зарубежных государств. Подробно описываются перспективы создания и применения многофункциональных беспилотных авиационных систем аэродромного и корабельного базирования в интересах ВМС США. Приводятся основные понятия, связанные с БПЛА, в соответствии со стандартами НАТО.

Рассмотрены преимущества беспилотных систем перед пилотируемой авиацией. Проведен анализ основных классов беспилотных аппаратов и решаемых ими задач. Отмечена ведущая роль США в развитии беспилотной морской авиации.



Источник: Морской сборник, 2015, № 4, с. 64-69.

*ВМС США не до конца ясно понимают роль
будущего беспилотника UCLASS*

Как информирует сайт vpk.name, ВМС США все еще не имеют ясного представления, каким должен быть будущий палубный беспилотник UCLASS. Это сдерживает дальнейшую разработку программы. Военные не решили один существенный вопрос – беспилотник должен выполнять разведывательные функции с ограниченным потенциалом нанесения ударов или должен быть ударным БПЛА с ограниченным набором разведывательного оборудования. Разработка ударного БПЛА потребует значительно большего расхода средств.



Источник: http://vpk.name/news/131404_vms_sshi_ne_do_konca_yasno_ponimayut_rol_budushego_bespilotnika_uclass.html (дата размещения материала 05.05.2015).

ВМС США обновляют технологии беспилотного летательного аппарата «Тритон»

Согласно сведениям, опубликованным в журнале «Военно-техническое сотрудничество», ВМС США используют последовательный метод модернизации БПЛА MQ-4C «Тритон» компании «Нортроп Грумман», чтобы минимизировать его устаревание до поступления в войска.

ВМС США планируют в 2018 г. доукомплектовать «Тритон» бортовой РЛС, которая обеспечивает автономное обнаружение других самолетов. Это одно из требований Международной организации гражданской авиации, предъявляемых к полетам военных БПЛА, которое должно выполняться для обеспечения безопасности полетов гражданских самолетов. На данный момент в рамках программы планируется производство 68 летательных аппаратов.



Источник: Военно-техническое сотрудничество, 2015, № 16, с. 29.

Беспилотник «Тритон» с поисковой бортовой РЛС выполнил первый полет

Журнал «Военно-техническое сотрудничество» сообщает, что БПЛА MQ-4C «Тритон» успешно завершил свой первый полет с многофункциональной бортовой РЛС MFAS, которая существенно повысит возможности БПЛА по разведке ситуации на море посредством обеспечения кругового обзора большой площади пространства. Это позволит увеличить скорость обнаружения, классификации, сопровождения и идентификации приоритетных объектов.

Помимо радара MFAS аппарат MQ-4C будет оснащаться: оптико-электронным/ИК датчиком, обеспечивающим формирование в полете статических изображений и полномасштабную видеосъемку движущихся потенциальных угроз; комплексом радиотехнической разведки для идентификации и определения географического положения источников радиолокационных сигналов; системой автоматической идентификации целей AIS, которая будет обнаруживать и сопровождать суда, оснащенные ответчиками AIS.



Аппарат обеспечит круглосуточный мониторинг практически в любой точке мира. Его способность функционирования на большой высоте повысит эффективность сбора разведывательных данных и обеспечит высокий уровень осведомленности о ситуации на морской поверхности.

Источник: Военно-техническое сотрудничество, 2015, № 16, с. 30.

Минобороны Франции приняло беспилотный летательный аппарат «Риппер» на вооружение



Как сообщает сайт vpk.name, генеральная дирекция по вооружению минобороны Франции объявила о принятии на вооружение БПЛА «Риппер» компании «Дженерал атомикс аэронавотикал системз». В ближайшее время комплекс будет развернут в регионе Сахель в Африке. Разведывательная система, состоящая из двух летательных аппаратов, наземной станции управления и вспомогательного оборудования, применяется для ведения разведки в интересах подразделений вооруженных сил Франции.

Источник: http://vpk.name/news/130989_generalnaya_direkciya_po_vooruzheniyu_minoboronyi_francii_prinyala_tretii_bla_riper.html (дата размещения материала 28.04.2015).

В Канаде готовятся к испытаниям беспилотного летательного аппарата, способного обнаруживать субмарины



Согласно информации ряда сайтов, в Канаде планируются испытания новейшего БПЛА, который предназначен для обнаружения кораблей и подводных лодок. Аппарат создан компанией «Brican», специализирующейся на создании аэронавигационного оборудования. Аппарат «Brican TD100» в зависимости от варианта оборудования способен обнаруживать металлические объекты как на воде, так и под водой. Запуск «Brican TD100» может осуществляться с земли или со специальной разгонной полосы. К концу 2015 г. первый такой аппарат может заступить на вооружение одного из кораблей ВМС Канады.

Источники: <http://vpk-news.ru/news/24979> (дата размещения материала 26.04.2015); <http://tass.ru/mezhdunarodnaya-panorama/1927605>.

Проект беспилотного летательного аппарата «Air Strato»

По данным, размещенным на сайте topwar.ru, румынская компания «ARCA Space Corporation» занимается разработкой перспективного БПЛА, предназначенного для участия в научных исследованиях. Не исключается возможность создания военных модификаций.



В первую очередь предполагается поставлять машины с оптико-электронным оборудованием, при помощи которого беспилотник сможет выполнять разведку или наблюдать за определенными территориями. Объявлено о разработке двух модификаций аппарата «Air Strato». Базовой версией является более крупный аппарат «Air Strato Explorer».

Он должен работать на высотах до 18 км. Его максимальная скорость будет достигать 170 км/ч. Одной зарядки аккумуляторов должно хватить на полет продолжительностью до 20 часов. Дальность полета может достигать 840 км.

Уменьшенный беспилотник «Air Strato Pioneer» будет летать на высотах до 8 км с максимальной скоростью 120 км/ч. За счет собственных аккумуляторов аппарат сможет находиться в воздухе до 12 часов, пролетая до 500 км.

Источник: <http://topwar.ru/74192-proekt-bespilotnyh-letatelnyh-apparatov-arca-airstrato-rumyniya-ssha.html> (дата размещения материала 30.04.2015).

Десятимоторный беспилотник GL-10 впервые поднялся в воздух

Согласно информации сайта dailytechinfo.org, специалисты НАСА предложили новую конструкцию летательного аппарата с поворотным крылом, который может взлетать и садиться подобно вертолету, и летать как обычный самолет. Опытный вариант аппарата «Greased Lightning» (GL-10) недавно совершил первый успешный испытательный полет.



Аппарат GL-10 может беспрерывно летать в режиме горизонтального полета в течение 24 часов. Такая длительность позволит ему успешно решать задачи картографирования местности, разведки и наблюдения.

Источник: <http://www.dailytechinfo.org> (дата размещения материала 24.04.2015).

Рекордный полет беспилотного летательного аппарата «Zephyr 7» продолжительностью 14 дней⁴

На сайте ladepeche.fr опубликована информация о новом рекорде БПЛА «Zephyr 7» американской компании «Airbus», который смог пролетать 14 дней без подзарядки на высоте более 22000 м.

«Zephyr 7» представляет собой сверхлегкий дрон. На крыльях установлены солнечные панели, поэтому в дневное время суток солнечные батареи аккумулируют энергию, а в ночное время полет осуществляется благодаря накопленной энергии. В отличие от спутников, «Zephyr 7» может фокусироваться на заданном участке земной поверхности. В состав полезной нагрузки аппарата могут входить фотокамеры и другие разведывательные средства высокого разрешения. Предполагается, что дрон будет вести дистанционное зондирование Земли в военных и гражданских целях.



Источник: <http://www.ladepeche.fr/article/2015/05/08/2101016-notre-drone-a-vole-14-jours-non-stop.html> (дата размещения материала 08.05.2015).

⁴ Перевод с французского выполнен ГНИИИ ПТЗИ ФСТЭК России.

Беспилотник размером с цикаду создали в США

Как сообщает ряд сайтов, инженеры научно-исследовательской лаборатории ВМС США разработали миниатюрный расходуемый БПЛА. Новый беспилотник, получивший название «Cicada», умещается на ладони, выполнен из легкого пластика и не имеет двигателя. После сброса беспилотник способен длительное время планировать на скорости до 74 км/ч, собирая важную разведывательную информацию. На аппарате, в зависимости от выполняемой задачи, могут быть установлены различные типы сенсоров, общим из которых для всех аппаратов является GPS-контроллер.



Источники: http://vpk.name/news/132144_voennyye_inzheneriyi_ssha_sozdali_bespilotnik_razmerom_s_cikadu_ih_mozhno_tyisyachami_sbrasyivat_nad_territoriei_protivnika.html (дата размещения материала 20.05.2015); http://nr2.ru/News/culture_and_science/Voennye-SSHA-predstavili-roy-krohotnyh-bespilotnikov-97078.html; <https://versia.ru/voennye-bespilotniki-ssha-budut-sherstit-ocean-iroitsyanad-nazemnymi-celyami>.

Американский водонепроницаемый дрон с защитой от жесткой посадки

По информации, размещенной на сайте tjournal.ru, основатели стартапа «Lily» представили одноименный БПЛА, который умеет следовать за владельцем благодаря небольшому GPS-трекеру и технологии «компьютерного зрения».



«Lily» не нуждается в ровной поверхности для того, чтобы начать или завершить полет, и благодаря стабилизаторам может приземлиться прямо на ладонь владельца. Встроенная камера способна делать 12-мегапиксельные фотоснимки, снимать видео в качестве 1080p со скоростью 60 кадров в секунду, а также автоматически переключаться при необходимости на режим съемки slo-mo.

Источник: <http://tjournal.ru/p/lily-drone> (дата размещения материала 12.05.2015).

Израиль использует разведывательные аэростаты

На сайте armstrade.org размещена информация о заключении министерством обороны Израиля с компанией «RT LTA системз» контракта на поставку дополнительных тактических привязных разведывательных аэростатов «Скайстар-300».



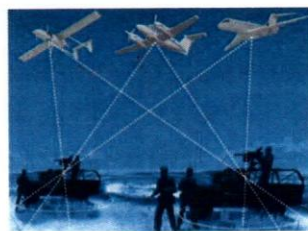
«Скайстар-300» – это тактический аэростат, предназначенный для сбора информации, наблюдения и разведки. Он может использоваться для защиты мест расположения войск, борьбы с самодельными взрывными устройствами, мониторинга обстановки, контроля границ и ретрансляции связи.

Аэростат несет оптическую/ИК полезную нагрузку для ведения круглосуточного наблюдения. Передача данных от средств наблюдения и команд управления, а также питание полезной нагрузки осуществляется по кабелю.

Источник: <http://www.armstrade.org/includes/periodics/news/2015/0514/15> (дата размещения материала 14.05.2015).

Аппаратура радиоразведки компании «QinetiQ»

В статье, опубликованной в журнале «Иностранная печать об экономическом, научно-техническом и военном потенциале государств-участников СНГ и технических средствах его выявления» сообщается, что британская компания «QinetiQ» представила новые образцы бортовой аппаратуры авиационной радиоразведки.



Разработанная на основе систем стратегической радиоразведки, номенклатура аппаратуры ASX предоставляет авиации возможность выполнять задачи разведки сигналов, обнаруживая и определяя местоположение связных передатчиков, излучения которых часто являются признаком деятельности противника. Размещая систему ASX на самолете, пользователь способен осуществлять мониторинг широкой полосы земной или морской поверхности в интересах защиты национальных интересов и охраны границ, а также наблюдения за объектами критической инфраструктуры в отдаленных зонах безопасности.

Источник: Иностранная печать об экономическом, научно-техническом и военном потенциале государств-участников СНГ и технических средствах его выявления, 2015, № 3, с. 3-4.

Наблюдательный полет Норвегии и США над Россией

По данным сайта vpk-news.ru, в рамках реализации международного Договора по открытому небу совместная миссия Норвегии и США выполнит наблюдательный полет над территорией Российской Федерации на румынском самолете наблюдения Ан-30.



В ходе выполнения полета по согласованному маршруту российские специалисты на борту самолета наблюдения будут контролировать соблюдение согласованных параметров полета и применение предусмотренной договором наблюдательной аппаратуры.

Источники: <http://vpk-news.ru/news/25007> (дата размещения материала 25.04.2015).

Наблюдательный полет Румынии и Великобритании над Россией

Как сообщает сайт armsexpo.ru, совместная миссия Румынии и Великобритании в рамках реализации международного Договора по открытому небу планирует выполнить наблюдательный полет над территорией Российской Федерации на румынском самолете наблюдения Ан-30. Самолет и установленная на нем аппаратура наблюдения (аэрофотоаппараты) прошли международное освидетельствование, в котором приняли участие и российские специалисты, что исключает возможность использования технических средств, не предусмотренных Договором по открытому небу.



Источник: http://www.armsexpo.ru/news/vzaimodeystvie/gruppa_nablyudateley_velikobritanii_i_rumynii_vypolnit_nablyudatelnyy_polet_nad_territoriey_rossii (дата размещения материала 12.05.2015).

Представители Дании и США совершат наблюдательный полет над Россией

Согласно информации, размещенной на сайте n-mar.ru, совместная миссия специалистов Дании и США совершит наблюдательный полет над территорией России в соответствии с Договором по открытому небу. Миссия будет использовать американский самолет наблюдения ОС-135В, который взлетит с хабаровского аэродрома. Самолет и установленная на нем аппаратура наблюдения прошли международное освидетельствование, что исключает использование технических средств, не предусмотренных Договором.



Источник: <http://www.n-mar.ru/bussines/17506-predstaviteli-ssha-i-danii-sovershat-nablyudatelnyy-polet-nad-rossiey.html> (дата размещения материала 04.05.2015).

Корабельная радиолокационная станция компании «Raytheon» прошла очередной этап испытаний⁵

На сайте defense-update.com размещена информация о завершении ВМС США и компанией «Raytheon» очередного этапа испытаний новой корабельной РЛС ПВО/ПРО AN/SPY-6(V). В этой РЛС использованы модули S- и X-диапазонов. Данная РЛС будет установлена на ракетные эскадренные миноносцы DDG-51 «Flight III» ВМС США, что позволит повысить их боеспособность и самооборону.



⁵ Перевод с английского выполнен ГНИИИ ПТЗИ ФСТЭК России.

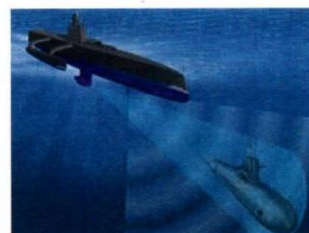
Поскольку в РЛС AN/SPY-6(V) реализован модульный принцип, то в процессе ее функционирования количество задействованных приемо-передающих модулей может варьироваться. Это позволяет формировать апертуру любого размера. Имея антенные решетки большего размера, радар будет по меньшей мере в 30 раз чувствительнее, чем РЛС, установленные на современных эсминцах класса «Орли Берк» DDG 51.

Новая РЛС может одновременно отслеживать в 30 раз больше целей, чем состоящая на вооружении РЛС AN/SPY-1D(V). Использование адаптивных цифровых возможностей формирования диаграммы направленности и программируемой обработки сигналов позволяет быстро адаптировать РЛС для выполнения новых задач и возникающих угроз.

Источник: http://defense-update.com/20150512_amdr_cdr.html#.VVNMpXan11Y (дата размещения материала 12.05.2015).

Беспилотные корабли США в поисках подводных лодок

На сайте versia.ru размещена информация об инициативе Агентства передовых оборонных исследовательских проектов «DARPA» по разработке безэкипажного аппарата для противолодочной борьбы. В настоящее время создан аппарат, который может работать как автономно, так и с использованием дистанционного управления. Он способен непрерывно находиться в море до 80 суток на удалении до 3000 км от базы.



Аппарат будет осуществлять непрерывный поиск вражеских подлодок в заданном районе, а в случае обнаружения субмарины – осуществлять непрерывное слежение за ней. Прототип судна уже запущен в производство.

Источник: <https://versia.ru/voennye-bespilotniki-ssha-budut-sherstit-ocean-i-roitsya-nad-nazemnymi-celyami> (дата размещения материала 12.05.2015).

Исследователи НАТО испытывают подводные дроны в Норвегии⁶

Согласно информации на сайте stripes.com, в Норвегии прошли учения ВМС 10 стран НАТО и Швеции по обнаружению и преследованию подводных лодок. В ходе учений осуществлен очередной этап испытаний подводных дронов, запрограммированных на поиск подводных лодок практически без участия оператора. Специалисты НАТО считают такие аппараты будущим противолодочной обороны.



Исследователи полагают, что адаптировав аппараты к холодным водам региона, можно будет научить их отличать геологические осо-

⁶ Перевод с английского выполнен ГНИИИ ПТЗИ ФСТЭК России.

бенности рельефа дна от таких аномалий, как подводные лодки. На сайте отмечается, что проведение такого рода работ вызвано возросшей активностью российского ВМФ.

Природные особенности вод северного региона – низкие температуры и относительно низкая соленость – в значительной степени влияют на акустические характеристики. Аппараты обрабатывают отраженные от объектов акустические волны путем оценки значений каждого отклика. Затем эта информация используется для слежения за объектом в соответствии с параметрами, заданными операторами. Подводный необитаемый аппарата может отслеживать несколько объектов сразу.

Источник: <http://www.stripes.com/news/nato-researchers-test-underwater-drones-in-norway-1.344499> (дата размещения материала 06.05.2015).

1.2. Техническая защита информации

Мировая карта киберугроз реального времени «Check Point Software Technologies»

Как сообщает ряд сайтов, компания «Check Point Software Technologies» запустила сервис Threat Cloud World Cyber Threat Map – мировую карту киберугроз. Она отображает в режиме реального времени, где в данный момент в мире происходят кибератаки. Информацию для карты предоставляет Check Point Threat Cloud – сеть для совместной борьбы с киберпреступлениями, которая собирает данные об атаках с помощью глобальной сети датчиков угроз.

База данных Threat Cloud содержит более 250 млн. адресов, анализируемых на наличие ботов, более 11 млн. сигнатур вредоносного программного обеспечения (ПО) и более 5,5 млн. адресов зараженных веб-сайтов. Кроме того, карта World Cyber Threat Map предоставляет ежедневную статистику угроз.

Источники: <http://terradv.ru/check-point-predstavila-mirovuyu-kartukiberugroz-realnogo-vremeni/> (дата размещения материала 12.05.2015); <http://www.anti-malware.ru/news/2015-05-12/16102>.



«IID» будет черпать информацию для своей аналитической базы из «Темной паутины»

По информации, размещенной на сайте tavasardze.lv, компания «IID» будет использовать данные скрытого Интернета («Темной паутины») в своей аналитической платформе «ActiveTrust». Благодаря партнерству с «Flashpoint» большая



база «IID» с решениями по работе с данными охватит оперативную информацию, полученную из «теневого сегмента» Интернета, куда не могут проникнуть основные поисковые системы. Информация из «Темной паутины» позволит ИБ-специалистам заглянуть в ранее «непрозрачные»

области Интернета для получения достоверных разведданных. Объединение базы данных «Flashpoint» с «ActiveTrust» поможет крупным компаниям и правительственным организациям, которые полагаются на «IID», быть лучше информированными о текущей ситуации в киберпространстве.

Источник: <http://ru.tavasardze.lv/iid-budet-cherpat-informaciyu-dlya-svoej-analiticheskoy-bazy-iz-temnoj-pautiny> (дата размещения материала 07.05.2015).

В Cisco TelePresence обнаружены уязвимости, которые позволяют удаленно выполнять команды

Как сообщает ряд сайтов, обнаружены уязвимости в программном продукте «TelePresence», позволяющие реализовать удаленное выполнение команд и осуществлять DDoS-атаки. ПО «TelePresence» ТС и ТЕ содержит брешь обхода аутентификации, благодаря которой злоумышленник может получить права суперпользователя на устройствах, где оно установлено. Вторая уязвимость позволяет вызывать перезагрузку систем, посылая специально сформированные пакеты.



Уязвимость присутствует в Cisco TelePresence MX Series, System EX Series, Integrator C Series, Profiles Series, Quick Set Series, System T Series и VX Clinical Assistant. ПО ТЕ уязвимо только в компонентах System EX Series.

Бреши существуют из-за некорректной обработки входных данных и затрагивают различные медиашлюзы «TelePresence», ПО конференц-мостов MCU и MCU MSE, а также аппаратные и виртуальные машины TelePresence Server.

Источники: <http://www.securitylab.ru/news/472923.php> (дата размещения материала 14.05.2015); <http://ru.tavasardze.lv/v-cisco-telepresence-obnaruzheny-uyazvimosti/>.

Уязвимости, позволяющие удаленно вызвать крах ядра Linux

По информации ряда сайтов, в драйвере ozwpan ядра Linux выявлено пять уязвимостей, четыре из которых позволяют инициировать крах или заикливание ядра через отправку специально оформленных пакетов (packet-of-death). Первая и вторая проблемы связаны с выходом за границы буфера из-за некорректной обработки знаковых целых чисел, третья проблема вызвана условиями, при которых выполняется деление на ноль, четвертая проблема приводит к бесконечному заикливанию, пятая вызвана возможностью чтения из областей вне границ выделенного буфера.



Источники: <http://www.opennet.ru/opennews/art.shtml?num=42228> (дата размещения материала 14.05.2015); <http://internetua.com/v-yadre-Linux-obnaruzheni-5-uyazvimostei>.

Катастрофическая уязвимость в iOS 8

На сайте vladtime.ru сообщается, что эксперты компании «Skysecure» обнаружили новую уязвимость в iOS 8. При подключении к Wi-Fi-роутеру устройство, работающее на iOS 8, начинает циклично перезагружаться. Причем «ребут» происходит на первых же этапах включения. Пользователь даже не может зайти в настройки и отключить беспроводную связь.



Специалисты выяснили, что это происходит при определенных настройках роутера, но каких именно не говорят. Такие «баги» могут привести к тому, что злоумышленники с помощью развертывания своей Wi-Fi точки смогут отключить устройства. Собранные данные об уязвимости отосланы в корпорацию «Apple» для ее устранения.

Источник: <http://www.vladtime.ru/computers/427760-specialisty-izskyse-cure-obnaruzhili-katastroficheskuyu-uyazvimost-v-ios-8.html> (дата размещения материала 26.04.2015).

Уязвимость в роутерах D-Link и Trendnet

В соответствии с данными, размещенными на сайте threatpost.ru, уязвимость в популярных домашних маршрутизаторах компаний «D-Link» и «Trendnet» может быть использована для исполнения произвольного кода. Проблема кроется в процессе обработки запросов типа New Internal Client. В этом случае пользовательские данные некорректно saniруются перед вызовом сервиса.



Атакующий может воспользоваться этой уязвимостью для исполнения кода с привилегиями уровня root.

Источник: <https://threatpost.ru/2015/05/05/nezakrytaya-uyazvimost-v-route-rah-privodit-k-ispolneniyu-koda> (дата размещения материала 05.05.2015).

Уязвимость Magic Hash подвергает опасности практически любой сайт

Как сообщает сайт securitylab.ru, эксперты «White Hat Labs» обнаружили уязвимость, которая получила название Magic Hash. Из-за ошибки в PHP при работе с хэшами в некоторых ситуациях злоумышленник может подобрать пароль к учетной записи пользователя, обойти аутентификацию и другие средства обеспечения безопасности, полагающиеся при хэшировании. По мнению экспертов, эта брешь затрагивает миллионы сайтов и может стать действительно проблемой.



Источник: <http://www.securitylab.ru/news/472902.php> (дата размещения материала 12.05.2015).

Защитные механизмы «Apple» легко обойти

По данным экспертов «Synack», размещенным на сайте it-sektor.ru, преступник может обойти традиционные средства защиты операционной системы OS X. Это стало возможным благодаря тому, что защитная технология Gatekeeper позволяет выполнение неподписанного кода. Утилита Gatekeeper используется для проверки кода и является предустановленной на всех Mac под управлением OS X. Она сконструирована так, что по умолчанию позволяет либо выполнение подписанного кода, либо принимает пакеты только от Mac App Store. Ранее обновления безопасности Mac загружались через незащищенное HTTP-соединение, полагаясь на Gatekeeper для верификации кода. Однако после обнаружения способа обхода утилиты злоумышленники имеют возможность осуществить атаку «человек посередине».



Кроме этого десктопная операционная система Apple позволяет работу неподписанных локальных приложений. Таким образом, после того, как машина была скомпрометирована, злоумышленники могут добавлять собственный код в уже подписанные приложения. При этом OS X даже не заметит, что подписанное приложение не является таковым, и позволит ему работать дальше.

Источник: <http://it-sektor.ru/vstroennye-apple-zaschitnye-mexanizmy-legko-oboyiti-i-proekspluatirovat.html> (дата размещения материала 09.05.2015).

Уязвимость в QEMU

На ряде сайтов размещена информации специалистов «Crowd Strike» об обнаружении критической уязвимости нулевого дня в виртуальном гибком диске контроллера гипервизора QEMU с открытым исходным кодом. Уязвимость, получившая название VENOM, позволяет злоумышленнику выходить из виртуальной машины, выполнять код на хост-машине и получать доступ ко всем другим виртуальным машинам на хосте. Некоторые из кодов QEMU, включая и уязвимый бит, используются другими платформами виртуализации, такими как Xen и KVM.

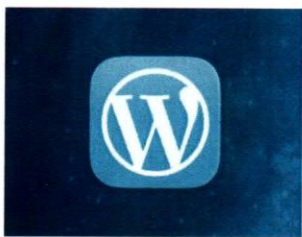


Согласно данным экспертов, сотни, а может и тысячи продуктов, использующих технологии виртуализации, содержат уязвимость VENOM. Поскольку большинство гипервизоров работают с корневым доступом к хост-машине, потенциальный ущерб может быть колоссальным.

Источник: <http://www.securitylab.ru/news/472921.php> (дата размещения материала 14.05.2015); <http://www.opennet.ru/opennews/art.shtml?num=42223>.

В WordPress обнаружены новые уязвимости

По информации, размещенной на сайте threatpost.ru, в двух плагинах для WordPress обнаружены уязвимости. Первая уязвимость присутствует в eShop, плагине для системы управления контентом. Причиной ее существования является недостаточная валидация HTTP-куки, используемых плагином. Входные данные, передаваемые пользователем через куки, могут быть перехвачены атакующим и использованы для перезаписи произвольных PHP-переменных, что приведет к раскрытию полного пути и позволит провести XSS-атаку.

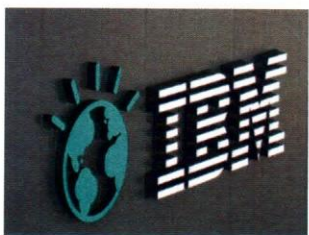


Вторая уязвимость, обнаруженная в плагине, позволяет включить в текущий документ PHP-файл и несколько XSS-уязвимостей. Пакет иконок Genericons, используемый плагином, и тема Twenty Fifteen содержат DOM XSS-уязвимость. Это позволяет пользователям провести кастомизацию, завлечь посетителей и обеспечить безопасность сайта. Имея более 1 млн. установок, он является одним из самых популярных WP-плагинов. Тема Twenty Fifteen также весьма популярна и по умолчанию включена в большинство установок WordPress.

Источник: <https://threatpost.ru/2015/05/08/v-dvuh-plaginah-dlya-wordpress-obnaruzheny-uyazvimosti> (дата размещения материала 08.05.2015).

Уязвимость в IBM SPSS Statistics

Как сообщает сайт securitylab.ru, обнаружена уязвимость, позволяющая выполнение произвольного кода в популярной универсальной системе анализа данных IBM SPSS Statistics. Уязвимость возникла из-за того, что элемент управления ActiveX может быть использован злоумышленниками для передачи вредоносного ПО. В случае, если жертва посетит специально созданную злоумышленником web-страницу, преступник сможет проэксплуатировать уязвимость для произвольного выполнения кода и даже вывести систему из строя.



Уязвимость представляет собой серьезную угрозу, так как многие организации используют IBM SPSS Statistics для обработки интеллектуальной собственности, включая и анализ собственных важных исследований.

Источник: <http://www.securitylab.ru/news/472977.php> (дата размещения материала 14.05.2015).

XSS-уязвимость сайта supermarket.rambler.ru



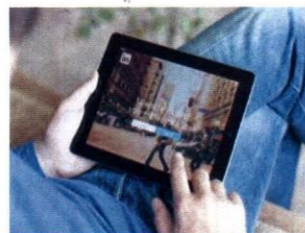
По информации портала securitylab.ru, на сайте «Рамблер.Супермаркет» обнаружена уязвимость, позволяющая осуществить межсайтовый скриптинг. Эксплуатируя брешь, злоумышленник может осуществить XSS-атаку и в результате похитить учетные данные жертвы,

конфиденциальную информацию, файлы cookie, а также историю просмотров в браузере. В настоящее время подобный вид атак применяется в паре с фишингом и социальной инженерией.

Источник: <http://www.securitylab.ru/news/472890.php> (дата размещения материала 05.05.2015).

На сайте linkedin.com обнаружена XSS-уязвимость

Согласно данным экспертов компании «Brute Logic», размещенным на сайте securitylab.ru, на web-сайте linkedin.com. обнаружена XSS-уязвимость, дающая возможность злоумышленникам определенным образом интегрировать в страницу сайта-жертвы скрипт, который будет выполнен при ее посещении. Также XSS-уязвимость на многопосещаемых ресурсах может быть использована для проведения DDoS-атаки. Похищение cookie-файлов, персональной информации, учетных данных, а также просмотр истории браузера – это наименее опасные последствия XSS-атак.



Источник: <http://www.securitylab.ru/news/472872.php> (дата размещения материала 08.05.2015).

Уязвимость в клиентской библиотеке MySQL и MariaDB

По данным сайта anti-malware.ru, в библиотеке libmysqlclient, используемой для подключения к системам управления базами данных (СУБД) MySQL, MariaDB и Percona Server, выявлена уязвимость, позволяющая обойти создание зашифрованного канала связи и организовать MITM-атаку между клиентом и СУБД. При активации в настройках установки соединения с использованием SSL, если такое соединение не удалось установить, канал связи все равно устанавливается, но без применения шифрования.

Подобное поведение является документированным, оно было изменено в ветке MySQL 5.7, но продолжает применяться в ветках MySQL 5.5 и 5.6. Проблема была устранена в кодовой базе MySQL 5.7.3, но не была причислена к категории уязвимостей, поэтому остается неисправленной в ветках MySQL 5.5/5.6, а также во всех выпусках MariaDB и Percona Server. При этом в MariaDB поставляется несколько связующих клиентских библиотек, из которых уязвимы libmysqlclient и Connector/C.



Источник: <http://www.anti-malware.ru/news/2015-05-06/16082> (дата размещения материала 06.05.2015).

Уязвимость в Android позволяет хакерам похищать отпечатки пальцев



На ряде сайтов размещена информация об обнаружении опасной уязвимости, связанной с биометрическими сенсорами Android-смартфонов. Уязвимость существует в системе дактилоскопического сканирования. Суть ее состоит в том, что созданный на телефоне образ отпечатка пальца перед тем как попасть в защищенную зону смартфона может быть похищен хакерами. При этом злоумышленникам даже не нужно полностью взламывать мобильное устройство. Уязвимость обнаружена также в телефонах фирм «HTC», «Samsung» и некоторых других. Уязвимость эффективна в устройствах с операционными системами старше, чем Android 5.0 Lollipop.

Источник: <http://ubr.ua/ukraine-and-world/technology/uiazvimost-v-android-pozvoliaet-hakeram-pohishat-otpechatki-palcev-337486> (дата размещения материала 25.04.2015); <http://www.imena.ua/blog/samsung-galaxy-s5-fingerprint-at-tacks>.

Критическая уязвимость в wpa_supplicant, компоненте для подключения к WI-FI



По данным сайта opennet.ru, в пакете wpa_supplicant выявлена опасная уязвимость, которая потенциально может быть использована для выполнения кода злоумышленника при обработке специально оформленных данных в поле SSID при установке или обновлении информации о P2P-пирах. Пакет wpa_supplicant используется для организации подключения к беспроводной сети во многих дистрибутивах Linux, *BSD и Android. Для эксплуатации уязвимости атакующий должен быть в пределах досягаемости беспроводной сети, чтобы отправить жертве специально оформленный набор кадров, передающих информацию о P2P-связи.

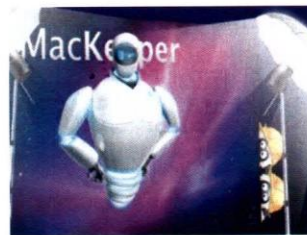
Атака упрощается, если устройство жертвы выполняет активные P2P-операции, такие как поиск узлов в сети (P2P_FIND) или прием запросов на соединение (P2P_LISTEN). Исправление проблемы пока доступно только в виде патча.

Источник: <http://www.opennet.ru/opennews/art.shtml?num=42097> (дата размещения материала 24.04.2015).

Новая уязвимость в утилите MacKeeper для OS X

Согласно информации, размещенной на сайте digitalmetro.us, обнаружена критическая уязвимость в ПО MacKeeper, эксплуатация которой позволяет выполнение произвольных команд с привилегиями суперпользователя без ведома пользователя. Уязвимость, затрагивающая версию MacKeeper 3.4, существует из-за отсутствия проверки входных данных при выполнении команд с использованием схемы URL.

Если пользователь уже однажды ввел пароль в ходе работы с MacKeeper, программа больше не требует повторного введения данных перед выполнением произвольных команд с привилегиями суперпользователя. Если пользователь не был ранее авторизован, система запросит логин и пароль. При этом злоумышленник сможет манипулировать текстом аутентификационного диалога, как частью эксплойта, и применить его к чему угодно. Компания-разработчик приложения уже выпустила исправленную версию MacKeeper 3.4.1.



Источник: <http://digitalmetro.us/technology/34-security/19648-mackeeper-os-x> (дата размещения материала 12.05.2015).

Опасная уязвимость в кросс-платформенном мобильном фреймворке Xamarin

На сайте cnews.ru сообщается об обнаружении компанией «Digital Security» опасной уязвимости во фреймворке для мобильных устройств Xamarin для Android. Xamarin применяется для разработки кросс-платформенных приложений под Android, iOS и Windows Mobile. На нем написаны разные группы приложений, включая программы для «интернета вещей» и банковские клиенты. Обнаруженная уязвимость предоставляет возможность перезаписи динамических библиотек (.dll-файлов) приложений путем создания специальной скрытой директории на карте памяти устройства, доступ к которой можно получить из любого приложения.



Любое вредоносное ПО, обладающее только стандартными правами на доступ к файлам SD карты, может поместить модифицированные библиотеки, которые изменяют логику работы программы, записывают действия пользователя или подменяют данные, в указанную директорию. Примечательно, что модифицированные библиотеки будут иметь приоритет над библиотеками внутри оригинального арк-файла.

Для устранения уязвимости в приложениях необходимо перекомпилировать приложения с использованием новой версии фреймворка.

Источник: <http://safe.cnews.ru/news/line/index.shtml?2015/04/30/595436> (дата размещения материала 30.04.2015).

Обнаружена критическая уязвимость в платформе электронной коммерции Magento

По информации, размещенной на сайте safe.cnews.ru, специалистами компании «Check Point Software Technologies» обнаружена критическая уязвимость категории RCE (удаленное исполнение кода) в платформе онлайн-торговли Magento, которую использует портал «eBay». В результате в зоне риска оказалось около 200 тыс. интернет-магазинов. Уязвимость позволяет скомпрометировать любой онлайн-магазин, работающий с платформой



Check Point
SOFTWARE TECHNOLOGIES LTD.

Magento, и получить доступ к информации о кредитных картах, а также к финансовым и персональным данным покупателей. Уязвимость дает возможность обойти все механизмы безопасности и получить полный контроль над электронным магазином и его базой данных. Таким образом, появляется доступ к учетной записи администратора и возможность кражи информации о банковских картах.

Источник: <http://safe.cnews.ru/news/line/index.shtml?2015/04/24/595222> (дата размещения материала 24.04.2015).

Уязвимость в механизме аутентификации баз данных SAP ASE

Согласно сведениям сайта securitylab.ru, обнаружена уязвимость в продукте Adaptive Server Enterprise (ASE) компании «SAP», позволяющая удаленному пользователю получить доступ к целевому серверу в обход механизма аутентификации. SAP ASE является реляционным решением для управления базами данных, которое предназначено для поддержки высокопроизводительных приложений, обрабатывающих большие объемы данных, поступающих от множества пользователей.

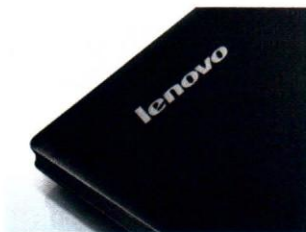
В механизме обработки запросов и ответов для контроля доступа к Adaptive Server в SAP ASE существовал неизменяемый логин «probe», используя который потенциальный злоумышленник мог получить несанкционированный доступ к системе. По данным разработчика, уязвимость устранена.

Источник: <http://www.securitylab.ru/news/472720.php> (дата размещения материала 24.04.2015).

Обнаружена уязвимость в системе безопасности компьютеров «Lenovo»

В соответствии с информацией, размещенной на сайте therussiantimes.com, в системе безопасности компьютеров «Lenovo» обнаружены серьезные уязвимости. Уязвимости могут быть использованы злоумышленниками, чтобы обойти проверку достоверности и заменить уже проверенные приложения на вредоносное ПО. Через одну из уязвимостей злоумышленники могут создать поддельные сертификаты подлинности, что позволяет замаскировать вредоносную программу под официальное ПО «Lenovo». Уязвимость присутствует в Lenovo System Update 5.6.0.27 и более ранних версиях.

Источник: <http://therussiantimes.com/news/15217.html> (дата размещения материала 06.05.2015).



Критическая уязвимость в YubiKey Neo

По данным сайта securitylab.ru, обнаружена уязвимость в реализации OpenPGP в YubiKey NEO – популярном электронном ключе, предназначенном для генерирования одноразовых паролей на любых системах, где есть USB-порт. Исходный код содержит логическую ошибку, связанную с проверкой PIN-кода пользователя. Ошибка позволяет атакующему с локальными привилегиями осуществить операции с ключом без знания PIN-кода. Ошибка содержится в первой строке функций дешифрования, обработки цифровых подписей и внутренней аутентификации.



Целью каждого из этих методов является подтверждение правильности PIN-кода и установка соответствующего режима (режим 81 для цифровой подписи, режим 82 – для всего остального). Производитель пытается преуменьшить серьезность проблемы и избежать необходимости выпуска обновлений. Обновление прошивки на устройствах YubiKey Neo запрещено из соображений безопасности, однако компания обещает заменить уязвимые девайсы всем желающим.

Источник: <http://www.securitylab.ru/news/472725.php> (дата размещения материала 26.04.2015).

Взломаны 4096-битные RSA-ключи

Согласно информации, размещенной на сайте securitylab.ru, хакерам удалось взломать три пары 4096-битных криптографических RSA-ключей при помощи созданного ими инструмента под названием «Phunctor». Принцип работы сервиса «Phunctor» заключается в поиске дублированных модулей на открытых PGP-серверах, поскольку дубликаты указывают на то, что оба ключа были сгенерированы на системе со взломанным источником энтропии или в случае некорректной реализации PGP.



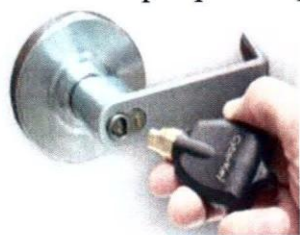
Проблема серверов ключей OpenPGP заключается в том, что пользователь может аннулировать публичный ключ, но не удалить его. Это значит, что помимо старых ненужных ключей на сервере могут скапливаться и «плохие» ключи. Искаженные ключи могут появиться и в результате сетевых ошибок, неисправности жестких дисков или уязвимостей в ПО.

Источник: <http://www.securitylab.ru/news/472954.php> (дата размещения материала 07.05.2015).

Проблемы безопасности в электронных ключах CyberLock

Согласно данным сайта internetua.com, обнаружены проблемы безопасности в электронных замках CyberLock. Электронный ключ оснащен микрочипом, определяющим, подходит ли к замку ключ с батарейным питанием. Ключ может

быть запрограммирован открывать замок в определенное время, а также возможно полное аннулирование действия устройства. Эксперты выяснили, что электронный замок легко скопировать, а новые ключи могут быть созданы из потерянных цилиндров замка и ключей, независимо от разрешения, выданного на них. Кроме этого, определенное время доступа к замку программируется в ключе, а не в цилиндре, позволяя злоумышленнику открывать замок в любую минуту, независимо от конфигурации.



Источник: <http://internetua.com/ekspert-obnarujil-problemi-bezopasnosti-v-elektronnih-kluacsah-CyberLock> (дата размещения материала 12.05.2015).

«Google» устранила clickjacking-брешь в своих продуктах

По сообщению сайта tavasardze.lv, специалистами компании «Google» обнаружена уязвимость, позволяющая атакующему похитить или удалить электронную переписку, а также производить манипуляции с учетными записями пользователей Google Plus и YouTube. Данная уязвимость затрагивает разработчиков, использующих инструмент Google API Explorer.



Clickjacking-атака позволяет злоумышленнику выполнить клик на сайте-жертве от имени посетителя. Уязвимость представляет серьезную угрозу, особенно если учесть, что затронуты все продукты компании, в том числе Gmail, Календари, Google Play, YouTube, AdSense и другие сервисы. Основная идея эксплойта заключается в создании прозрачного фрейма страницы с кнопкой. Злоумышленник может обманом заставить пользователя щелкнуть на специальную кнопку, скрытую за iFrame. При этом жертва будет думать, что регистрируется для получения бесплатного подарка или награды.

Clickjacking-уязвимость в продуктах корпорации «Google» уже устранена.

Источники: <http://ru.tavasardze.lv/google-ustranila-clickjacking-bresh-v-svoix-produktx> (дата размещения материала 06.05.2015).

В Safari устранены серьезные уязвимости

Согласно информации, размещенной на сайте topbrowser.ru, компания «Apple» выпустила очередное серьезное обновление для своего браузера Safari, в котором устранено несколько серьезных уязвимостей. Среди самых серьезных



доработок можно указать устранение трех дыр в браузере, которые при эксплуатации злоумышленниками могли вызывать повреждение памяти. Если жертва мошенников открывала в браузере ссылку на зараженный сайт, то приложение могло моментально закрыться или на компьютере мог выполняться произвольный код. Также исправлен пользовательский интерфейс,

сбои в котором могли использоваться злоумышленниками с целью искажения содержимого гиперссылок.

Источник: <http://topbrowser.ru/34/v-safari-ustranili-sereznyye-uyazvimosti> (дата размещения материала 07.05.2015).

Анализ ботнет сети Win32.Rmnet.12

По данным сайта drweb.ru, специалистами компании «Доктор Веб» завершено исследование бот-сети семейства файловых вирусов Rmnet., распространяющихся без участия пользователя и способных встраивать в просматриваемые пользователями веб-страницы постороннее содержимое. Установлено, что бот-сеть теоретически позволяет злоумышленникам получать доступ к банковской информации жертвы и красть пароли наиболее популярных FTP-клиентов.

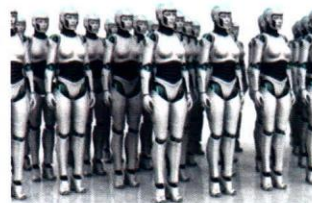


По-прежнему продолжает функционировать бот-сеть, состоящая из компьютеров, инфицированных файловым вирусом Win32.Sector. Количество компьютеров «Apple», инфицированных троянской программой BackDoor. Flashback.39, остается практически неизменным и составляет порядка 25000.

Источники: <http://news.drweb.ru/show/review/?lng=ru&i=9420> (дата размещения материала 30.04.2015).

Выявлен крупный ботнет из незащищенных маршрутизаторов

Согласно информации, размещенной на сайте opennet.ru, при исследовании нескольких DDoS-атак на компанию «Incapsula» было установлено, что они произведены с использованием нового ботнета, включающего более 40 тысяч маршрутизаторов для домашних и небольших офисных сетей. Подавляющее большинство входящих в ботнет маршрутизаторов выпущено компанией «Ubiquiti Networks» и имеет проблемы с безопасностью, позволяющие из внешней сети получить доступ к устройству через HTTP или SSH.



Кроме функций выполнения DDoS-атак, ботнет также включает в себя компонент для самораспространения, выполняющий сканирование сетей для установки на них вредоносного ПО. Координация активности ботнета производится через IRC.

Источник: <http://www.opennet.ru/opennews/art.shtml?num=42220> (дата размещения материала 13.05.2015).

В новой вредоносной кампании используется набор эксплойтов Angler

По информации, размещенной на сайте it-sektor, выявлена вредоносная кампания, в рамках которой злоумышленники увеличивают количество просмотров пропагандистских видеороликов. Для этого они применяют набор

эксплойтов Angler. Вредонос заставляет инфицированную машину посещать сайты для генерирования дохода от размещенной на них рекламы и мошеннического трафика. Встроенный в веб-ресурс фрейм направляет жертву на набор эксплойтов Angler, который определяет наличие антивирусных продуктов, после чего загружает троян Bedep.



Сайты, на которые направляется жертва, зарегистрированы киберпреступниками и скрывают большой объем рекламы, сформированный так, чтобы привлекать максимум трафика. Bedep создает скрытый виртуальный рабочий стол, на котором размещается невидимое окно Internet Explorer COM, функционирующее, как полнофункциональный IE.

Источники: <http://it-sektor.ru/v-novoyi-vredonosnoyi-kampanii-ispolzuet-sya-nabor-eksplotov-angler.html> (дата размещения материала 30.04.2015).

Атаки с использованием имплантированного NFC-чипа

Сайт internetua.com сообщает, что специалистами компании «APA Wireless» продемонстрирована возможность проведения хакерской атаки устройств под управлением операционной системы Android с использованием



NFC-чипа. Подобный чип позволяет проверять при помощи ping-запросов находящийся неподалеку смартфон на базе Android и «попросить» устройство перейти по вредоносной ссылке, которая ведет на вредоносное ПО. Если цель устанавливает и запускает вредоносное приложение, то устройство подключается к удаленному компьютеру. Далее зло-

умышленник может эксплуатировать уязвимость в смартфоне, удаленно устанавливая на него любое вредоносное ПО.

Уязвимость может позволить осуществлять подобные атаки массово. Аналогичный способ может быть использован для эксплуатации брешей в бортовом компьютере самолета. Злоумышленник может имплантировать NFC-чип в тело и пронести его в те места, где запрещены любые виды электронных устройств.

Источник: <http://internetua.com/os-Android-uyazvima-k-atakam-sispolzovaniem-NFC-chipa> (дата размещения материала 02.05.2015).

Набор инструментов, создающий вирусы в автоматическом режиме

Согласно информации экспертов «FireEye», размещенной на сайте internetua.com, ряд вредоносных приложений был разработан при помощи набора инструментов Microsoft Word Intruder.



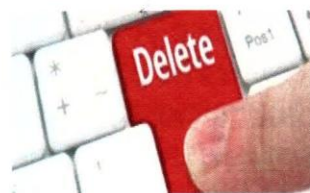
Созданные с его использованием документы Word могут умещать в себе сразу несколько эксплойтов, поочередно

предпринимающих попытки скомпрометировать целевую систему. При этом соответствующие модули и вся работа над формированием вредоноса производится автоматически без вмешательства человека.

Источник: <http://internetua.com/obnaružen-nabor-instrumentov-sozdauasxii-virusi-v-avtomaticheskoi-režime> (дата размещения материала 12.05.2015).

Новый вид вредоносного программного обеспечения выводит из строя компьютер при его сканировании антивирусом

Как сообщается на ряде сайтов, специалисты компании «Cisco» обнаружили новый вид вредоносного ПО, которое при сканировании зараженного компьютера на вирусы выводит его из строя. Программа, получившая название «Rombertik», распространяется с помощью спам-сообщений и фишинговых писем и перехватывает любой незашифрованный текст, вводимый в окне браузера. Этим ПО напоминает банковский троян Dye, однако в отличие от него похищает не только финансовую информацию, но и другие вводимые жертвой данные.

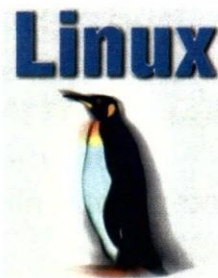


После запуска на компьютере под управлением Windows вредоносное ПО осуществляет несколько проверок для того, чтобы определить, детектируется ли оно антивирусными решениями. Программа «Rombertik» уникальна именно тем, что, обнаружив признаки сканирования системы на вирусы или попытки его удаления, уничтожает главную загрузочную запись.

Источники: <http://freesoft.ru/?news=2624> (дата размещения материала 06.05.2015); <http://www.securitylab.ru/news/472815.php>.

Новые угрозы для Linux

По данным сайта drweb.ru, специалисты компании «Доктор Веб» исследовали новый троянец Linux.BackDoor.Sesox.1, способный заражать операционные системы семейства Linux. Злоумышленники могут управлять этим бэкдором с помощью протокола для обмена текстовыми сообщениями IRC. Бот получает команды от вирусописателей в работающем на принадлежащем им сервере чате.



Троянец распространяется, сканируя удаленные серверы на предмет уязвимости с целью запустить на незащищенном сервере сторонний скрипт, который, в свою очередь, может установить в скомпрометированной системе копию троянца.

Вредоносная программа способна атаковать заданный киберпреступниками веб-узел путем отправки на него повторяющихся GET-запросов.

Источник: <http://news.drweb.ru/show/review/?lng=ru&i=9420> (дата размещения материала 30.04.2015).

Опасный троянец для операционной системы Android

На сайте drweb.ru сообщается, что экспертами «Доктор Веб» обнаружен троянец Android.Toorch.1.origin, предназначенный для незаметной загрузки, установки и удаления приложений, а также способный отображать на экране зараженных мобильных устройств навязчивую рекламу.



Программа распространяется под видом безобидного приложения-фонарика и передает киберпреступникам различную конфиденциальную информацию, включая GPS-координаты зараженного устройства. Троянец способен получить root-доступ и по команде вирусосписателей незаметно выполнять установку и удаление заданных ими приложений, а также помещать в системный каталог дополнительные вредоносные компоненты.

Источник: <http://news.drweb.ru/show/review/?lng=ru&i=9422> (дата размещения материала 30.04.2015).

Троянская программа маскируется под PuTTY

Как сообщает сайт it-sektor.ru, специалистами компании «Symantec» выявлена созданная злоумышленниками вредоносная версия SSH-клиента PuTTY. Обнаруженное вредоносное ПО позволяет получать доступ к компьютеру жертвы и похищать информацию. При помощи основанного на коде PuTTY трояна злоумышленники перенаправляют пользователя со страницы скомпрометированного сайта стороннего разработчика на созданный собственными силами ресурс. Если для связи с другим компьютером или сервером используется вредоносная версия PuTTY, то злоумышленники получают присланные с устройства жертвы конфиденциальные данные, такие как логины и пароли. Обычно PuTTY использует для подключения стандартный SSH URL.

Источник: <http://it-sektor.ru/novaya-troyanskaya-programma-maskiruetsya-pod-putty.html> (дата размещения материала 14.05.2015).



Руткит и кейлоггер для Linux, работающие в видеокарте

Согласно информации экспертов «Team Jellyfish», размещенной на ряде сайтов, ими реализован теоретический метод применения GPU для отслеживания активности пользователей в системе, а также подготовлены рабочие прототипы руткита и кейлоггера, выполняемые на GPU для скрытия своего присутствия в системе. Руткит и кейлоггер примечательны тем, что, получив доступ к GPU, они обходятся без традиционных привязок и изменений кода ядра операционной системы. Отслеживание буфера, содержащего данные о нажатых клавишах, производится непосредственно из



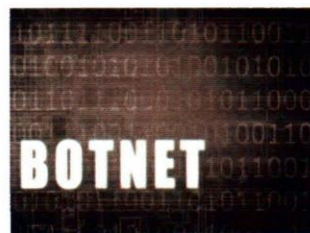
GPU при помощи DMA. На CPU выполняется только инициализация, после чего вся активность руткита ограничивается GPU. После загрузки все данные размещаются в видеопамяти, что затрудняет обнаружение руткита. Перехват содержимого памяти CPU производится через DMA. Выполнение на стороне GPU также позволяет задействовать средства GPU для выполнения сложных вычислений.

Источники: <http://www.anti-malware.ru/news/2015-05-08/16098> (дата размещения материала 08.05.2015); <http://digitalmetro.us/technology/34security/18091-2015-05-08-08-42-40>.

Mumblehard – вредоносное программное обеспечение для Linux и FreeBSD

По данным сайта opennet.ru, компания «ESET» опубликовала отчет с результатами анализа троянского ПО Mumblehard, внедряемого злоумышленниками на серверы под управлением Linux и FreeBSD, и используемого для построения ботнета, специализирующегося на рассылке спама. В настоящее время зафиксировано около 8900 пораженных данным вредоносным ПО хостов.

Для распространения Mumblehard атакующие используют различные уязвимости, незакрытые в web-приложениях. Поражаются в основном web-серверы, на которых ненадлежащим образом организован процесс установки обновлений. Само по себе Mumblehard включает только бэкдор для организации удаленного управления и демон для рассылки спама, сочетающий в себе функции прокси. Mumblehard обычно устанавливается в директории /tmp или /var/tmp и вызывается через cron каждые 15 минут. Необычной особенностью Mumblehard является то, что он написан на языке Perl, но распространяется в форме исполняемого файла в формате ELF с компактным распаковщиком на языке ассемблера. ELF-файл оформлен таким образом, что может запускаться как в Linux, так и на системах BSD.



Источники: <http://www.opennet.ru/opennews/art.shtml?num=42159> (дата размещения материала 04.05.2015).

Обнаружены новые версии Android-троянцев семейства Android.BankBot, атакующие клиентов банков

Сайт news.drweb.ru информирует, что аналитики компании «Доктор Веб» обнаружили несколько Android-троянцев, среди которых – Android.BankBot.43 и Android.BankBot.45. Они распространяются под видом легального ПО, такого как игры, медиаплееры или обновления операционной системы, и благодаря применению злоумышленниками различных методов социальной инженерии опрометчиво устанавливаются на Android-смартфоны и планшеты самими же пользователями.



Запустившись в зараженной системе, троянцы Android.BankBot получают доступ к функциям администратора мобильного устройства, которые дают им

расширенные возможности, включая способность препятствовать их удалению. Основное предназначение троянцев – кража конфиденциальных банковских сведений пользователей и хищение их денежных средств. Для этого вредоносные приложения атакуют установленные на мобильных устройствах пользователей программы типа «Банк-Клиент» ряда кредитных организаций, а также программу Play Маркет.

Источник: <http://news.drweb.ru/show> (дата размещения материала 25.04.2015).

Многокомпонентный банковский троянец Trojan.Dridex.49

Согласно информации сайта drweb.ru, специалисты «Доктор Веб» завершили исследование опасного многокомпонентного банковского троянца, получившего название Trojan.Dridex.49. Характерной особенностью троянца является использование им для связи с управляющим сервером P2P-протокола.



В зависимости от заданных параметров Trojan. Dridex.49 встраивается в процессы Проводника (explorer.exe) или браузеров (chrome.exe, firefox.exe, iexplore.exe). Все сообщения, которыми он обменивается с управляющим сервером, шифруются. Основное предназначение Trojan. Dridex.49 заключается в выполнении веб-инъектов, то есть встраивании постороннего содержимого в просматриваемые пользователем страницы различных финансовых организаций.

Троянец может похищать вводимые пользователем в различные формы конфиденциальные данные и позволяет злоумышленникам получить доступ к банковским счетам жертвы с целью кражи хранящихся там средств.

Источник: <http://news.drweb.ru/show/review/?lng=ru&i=9420> (дата размещения материала 30.04.2015).

Загрузчик Waski распространяет банковский троян Dyreza

В соответствии с данными, размещенными на сайте comss.info, с начала 2015 г. наблюдается значительное увеличение количества обнаружений Win32/TrojanDownloader.Waski. Первые образцы Waski были обнаружены в Германии и Швейцарии, а затем в других регионах, включая Австралию, Новую Зеландию, Ирландию, Великобританию, Канаду и США. Злоумышленники используют фишинговые сообщения электронной почты для распространения Waski. К сообщению прилагается вложение в виде архива с вредоносной программой внутри.



После своего запуска в системе он начинает загружать на компьютер другое вредоносное ПО с заданных URL-адресов. Загрузчик используется для распространения банковской троянской программы Dyreza. Сам исполняемый

файл Waski распространяется в виде исполняемого файла со значком PDF-файла для усыпления бдительности пользователей.

Источник: <http://www.comss.info/page.php?al=Dyreza> (дата размещения материала 06.05.2015).

Еще один троян

В статье, опубликованной в журнале «Хакер», сообщается об обнаружении специалистами «AVG Technologies» банковского трояна Vawtrak. Вирус распространен в США, Великобритании и Чехии. На компьютер жертвы он попадает через drive-by-атаки, эксплойт-паки и загрузчики. Попав в систему, троян получает доступ к банковскому счету жертвы и привлекает модуль Pony для копирования всех возможных учетных данных.



Интерес экспертов Vawtrak заслужил благодаря умению загружать обновления из фавиконов, используя Tor2Web-прокси! Фактически использование стеганографии в малвари не новость, но прятать адреса серверов обновлений в фавиконы ранее не догадывался никто. Разумеется, система не обращает внимания на скачивание фавикона, не подозревая о его содержимом. К тому же доступ к командным серверам осуществляется через Tor2Web без установки дополнительного ПО на компьютер жертвы.

Источник: Хакер, 2015, № 5, с. 7.

Новые троянцы-вымогатели ориентированы на азиатских пользователей

По данным сайта tcinet.ru, специалисты компании «Symantec» обнаружили новую разновидность троянца-вымогателя, получившего название Crypt0l0cker. Подобно всем представителям своего семейства, этот вирус шифрует информацию на инфицированных компьютерах и требует оплаты за восстановление доступа пользователя к его собственной системе.



Главным отличием является то, что Crypt0l0cker адресован пользователям азиатских стран. Он определяет IP-адрес компьютера жертвы и способен выводить на экран требование об оплате на японском и корейском языках. Нынешние атаки Crypt0l0cker – первый случай, когда программы-вымогатели используют японский и корейский языки.

Источник: <http://www.tcinet.ru/press-centre/technology-news/2220> (дата размещения материала 29.04.2015).

Обнаружен очередной клон криптовымогателей TeslaCrypt и Cryptowall 3.0

Согласно информации экспертов «Webroot», размещенной на сайте itsec.ru, обнаружен новый образец в семействе криптовымогателей. ПО, получившее название AlphaCrypt, разработано по аналогии с TeslaCrypt, однако принцип его действия соответствует функционалу Cryptowall 3.0. В него добавлены

некоторые улучшения, в частности, возможность удаления VSS. Как и в предыдущих вариантах, оплата выкупа производится в биткоинах. Таким образом злоумышленники сохраняют свою анонимность и могут без труда «отмыть» деньги через различные Bitcoin-обменники.



Распространение вредоносного ПО происходит через набор эксплойтов Angler. И сам эксплойт, и функциональная часть вируса отличаются чрезвычайно низким уровнем распознавания антивирусными решениями.

Источник: http://www.itsec.ru/newstext.php?news_id=104843 (дата размещения материала 07.05.2015).

WinYahoo изменяет настройки безопасности в Chrome

По информации экспертов «Malwarebytes», размещенной на сайте itsec.ru, потенциально нежелательное ПО WinYahoo изменяет настройки безопасности в Chrome. Программа WinYahoo, несмотря на название и тот факт, что она устанавливает поисковый движок Yahoo! в качестве используемого по умолчанию, не имеет к компании «Yahoo!» никакого отношения. В некоторых случаях WinYahoo могут подвергать компьютер риску быть зараженным.



Источник: http://www.itsec.ru/newstext.php?news_id=104902 (дата размещения материала 14.05.2015).

В Google Play выявлены приложения, содержащие агрессивные рекламные модули

Согласно информации, размещенной на сайте drweb.ru, в каталоге Google Play выявлены приложения, содержащие агрессивный рекламный модуль, в частности, Adware.MobiDash.2.origin. Суммарное число загрузок Adware.MobiDash.2.origin превысило 2500000.



Adware.MobiDash.2.origin используется разработчиками бесплатного ПО для показа разнообразной рекламы. При этом на экране мобильного устройства отображаются различные баннеры, которые размещаются, в том числе и поверх окон других работающих программ.

Источник: <http://news.drweb.ru/show/review/?lng=ru&i=9422> (дата размещения материала 24.04.2015).

Злоумышленники могут повлиять на работу роботов во время телехирургической операции

По информации сайта securitylab.ru, уязвимости к потенциальным киберугрозам роботов в области телехирургии могут повлиять на их работу во время операции. Экстремальные условия, в которых должен работать робот, характеризуются низким качеством связи по сетям общего пользования. Злоумышленник, получив доступ к данным сетям, сможет воспрепятствовать работе медицинского персонала.



Главным способом защиты телехирургии от кибератак является шифрование соединений. Однако даже это не сможет защитить системы от атаки «человек посередине», которая позволяет злоумышленникам перехватывать трафик и манипулировать им.

Источник: <http://www.securitylab.ru/news/472728.php> (дата размещения материала 27.04.2015).

Уязвимость в инфузионном насосе открывает доступ к базе данных лекарств

Согласно данным сайта digitalmetro.us, инфузионный насос, медицинское устройство, предназначенное для вливания лекарственных препаратов пациенту, имеет неаутентифицированный Telnet-порт. Данная брешь является достаточно опасной, так как позволяет злоумышленнику получить доступ к базе данных лекарств больницы.

Производитель отрицает тот факт, что брешь может стать причиной смерти пациента. Инфузионный насос не требует постоянного подключения к Интернету или локальной сети. Кроме того, персонал в большинстве случаев избегает соединения насоса с сетью в случае, если он подключен к пациенту. Кибератака может быть осуществлена только в случае, когда насос функционирует в реальном времени или когда находится на обслуживании для обновления ПО. Обе ситуации предполагают физический контакт устройства со злоумышленником.



Источники: <http://digitalmetro.us/technology/34-security/18073-2015-05-08-07-31-07> (дата размещения материала 08.05.2015).

Новый способ хищения средств с банковских карт россиян

На сайте finrussia.ru размещена информация о новом способе хищения денежных средств с банковских карт. Схема действия интернет-злоумышленников заключается в следующем – сначала они при помощи вредоносных программ собирают информацию о логинах и паролях от интернет-банков россиян и номерах их телефонов, к которым они привязаны. А затем обращаются в салоны сотовой связи, получая

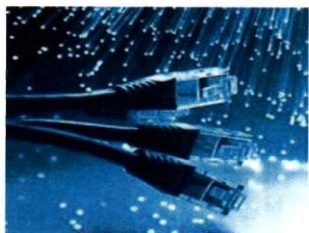


дубликаты SIM-карт по поддельным документам, чтобы на них получать одноразовые пароли, без которых невозможно войти в личный кабинет.

Источник: <http://finrussia.ru/news/show/201505152> (дата размещения материала 15.05.2015).

Создание спецсети связи для госорганов России вынесено на общественное обсуждение

На сайте militarynews.ru размещена информация о поправках в закон «О связи», связанных с планом построения изолированной сети связи для государственных нужд. Оператор сети будет определен Президентом России по представлению Военно-промышленной комиссии. Оператор будет обязан построить и обеспечить функционирование интегрированной сети. На этой сети он будет оказывать услуги госорганам по тарифам, определяемым Правительством России. Требования по безопасности и устойчивости функционирования интегрированной сети будут устанавливаться ФСБ России.



Организационные и технические меры по созданию сети будут выполняться федеральным органом исполнительной власти, определяемым Правительством России. Порядок ввода сети в эксплуатацию будет устанавливаться Минкомсвязи России по согласованию с ФСБ России.

Источник: <http://www.militarynews.ru/story.asp?rid=1&nid=376400> (дата размещения материала 14.05.2015).

Россия намерена сотрудничать с КНР в области обеспечения информационной безопасности

Как информирует сайт stfw.ru, одобрен проект соглашения между Правительством Российской Федерации и Правительством Китайской Народной Республики о сотрудничестве в области обеспечения международной информационной безопасности. Главной целью данного соглашения является создание правовых и организационных основ сотрудничества России и КНР в области обеспечения международной информационной безопасности. Документ констатирует наличие основных угроз, определяет основные направления, принципы, формы и механизмы сотрудничества в данной области.



Источник: <http://stfw.ru/page.php?id=49024> (дата размещения материала 07.05.2015).

США приняли стратегию наступательной кибервойны

Согласно информации ряда сайтов, в США решили проводить хакерские атаки на военную инфраструктуру противников в зоне конфликтов. Это следует из обновленной стратегии министерства обороны в сфере кибербезопасности.

Власти США будут совершать кибератаки на военные вычислительные сети и военную инфраструктуру своих противников в регионах, где США имеют собственные интересы. Решение о применении кибератак будут принимать президент США и министр обороны. За проведение киберопераций будет отвечать Киберкомандование США.



Министр обороны США назвал четыре государства, представляющие для США наибольшую угрозу в киберпространстве – это Китай, Россия, Иран и Северная Корея.

Источники: <http://safe.cnews.ru/news/top/index.shtml?2015/04/24/595227> (дата размещения материала 24.04.2015); http://vpk.name/news/130954_armiya_ssha_pereorientiruetsya_na_razvitie_nastupatelnyih_kibertehnologii.html.

*Программа слежки Агентства национальной безопасности
США под названием «Skynet»*

По информации, размещенной на сайте tjournal.ru, одна из действующих программ слежки АНБ США за людьми носит название «Skynet». Программа собирает информацию о перемещениях и звонках человека с помощью его телефона. Система «Skynet» анализирует путешествия человека, места, которые он регулярно посещает, частоту выключений телефона и смены SIM-карт, визиты в аэропорт, ночные поездки и другие данные.



Источник: <http://tjournal.ru/p/nsa-skynet> (дата размещения материала 11.05.2015).

*Спецслужбы США переходят в единую
информационную среду*

В соответствии с информацией, размещенной на сайте d-russia.ru, разведывательные подразделения различных силовых структур США наладили между собой информационное взаимодействие. В распоряжении каждой службы окажутся данные, которыми обладает другая, и которые представляют ценность в связи с решением конкретных задач.

При этом пользователям не придется преодолевать административные барьеры, возведенные между организациями. Масштабная трансформационная IT-программа для улучшения связи между всеми 17 разведывательными управлениями находится на этапе внедрения. На первом этапе реализации программы к сети будут подключены около 16 тыс. пользователей. Планируется увеличение этого количества до 50 тыс. сотрудников в течение следующего года.



Источник: <http://d-russia.ru/specsluzhby-ssha-nachali-perexod-v-edinuyu-it-sredu.html> (дата размещения материала 14.05.2015).

В США одобрен проект закона о прекращении сбора электронных данных

Как сообщает сайт tass.ru, палата представителей конгресса США одобрила законопроект, предусматривающий прекращение нынешней практики тотального сбора американскими спецслужбами данных электронных коммуникаций. Законопроект нацелен на реформирование ряда методов сбора информации АНБ США, которое занимается радиоэлектронной разведкой.



Одно из ключевых положений законопроекта запрещает массовый сбор данных, лишает АНБ полномочий осуществлять широкомасштабный перехват телефонных разговоров и хранить сведения о них на протяжении по меньшей мере пяти лет. Кроме того, законопроект позволяет телекоммуникационным и технологическим компаниям раз в полгода публично отчитываться о запросах на выдачу информации о клиентах и пользователях со стороны спецслужб.

Источник: <http://tass.ru/mezhdunarodnaya-panorama/1967152> (дата размещения материала 14.05.2015).

Финляндия готовится к информационной войне

По данным ряда сайтов, в Финляндии сформирована рабочая группа из представителей различных министерств и государственных служб, целью которой будет ведение информационной войны против России. Главным в работе новой структуры будет обмен информацией, координация усилий и совместное планирование.



Источники: <http://www.bport.com/news/item/152483.html#ixzz3YVQ34Xiw> (дата размещения материала 26.04.2015); <http://ria.ru/world/20150426/1061039186.html#ixzz3YVQ-KtBW9>.

Эстония набирает гражданских добровольцев в кибервойска

Согласно информации сайта securitylab.ru, Эстония нанимает добровольцев из числа компьютерных специалистов, которые готовы защищать страну от кибератак. В эстонские войска второго эшелона и резерва «Лиги обороны» Эстонии уже входит кибергруппа, состоящая из сотен гражданских волонтеров. Постоянный штат эстонской кибергруппы насчитывает всего три человека. Штаб-квартира находится в Таллине. Почти 1% всех ИБ-специалистов страны уже присоединились к кибервойскам.



Источник: <http://www.securitylab.ru/news/472748.php> (дата размещения материала 28.04.2015).

Совместный семинар минобороны Латвии и Европейского объединенного агентства сетевой и информационной безопасности⁷

По данным информационного портала enisa.europa.eu, в Риге состоялся семинар, посвященный разработке национальной стратегии информационной безопасности. Его целью являлась организация сотрудничества правительственных агентств, промышленных и образовательных учреждений, участвующих в разработке национальных стратегий информационной безопасности Евросоюза.



Среди обсуждаемых были вопросы формирования национальной стратегии информационной безопасности, организации образовательной деятельности и рассмотрение киберинцидентов.

Источник: <http://www.enisa.europa.eu/media/news-items/news-wires> (дата размещения материала 04.05.2015).

КНДР нарастила число специалистов по информационной безопасности

По данным сайта tass.ru, КНДР наращивает свои возможности по ведению кибернетической войны против южного соседа. Численность хакеров составляет 6,8 тыс. человек, из которых 1700 – профессионалы, а 5,1 тыс. – группа поддержки. В Сеуле считают северокорейских хакеров ответственными за осуществленную в декабре 2014 г. кражу данных о южнокорейских АЭС и их публикацию в Интернете. США также обвиняют Пхеньян во взломе корпоративной сети кинокомпании «Sony Pictures».



Источник: <http://tass.ru/mezhdunarodnaya-panorama/1959893> (дата размещения материала 10.05.2015).

1.3. Обеспечение безопасности информации в ключевых системах информационной инфраструктуры

Как увидеть невидимые кибератаки: компания «Positive Technologies» выпустила MaxPatrol SIEM

На сайте ptsecurity.ru компания «Positive Technologies» представила новый продукт – систему MaxPatrol SIEM, предназначенную для мониторинга событий безопасности и выявления хакерских атак. В основе продукта лежит база знаний, полученная в результате 15-летних исследований и экспертного сопровождения таких крупнейших мероприятий, как Универсиада в Казани и Олимпийские игры в Сочи.

В системе аккумулирован многолетний опыт тестирования безопасности бизнес-приложений, банковских, телекоммуникационных систем и АСУ ТП, что

⁷ Перевод с английского выполнен ГНИИИ ПТЗИ ФСТЭК России.

позволяет системе выявлять действительно важную информацию для оценки состояния и поведения активов в любой момент времени.

Система MaxPatrol SIEM в рамках программы импортозамещения целиком спроектирована в России с учетом специфики решаемых задач и требований регуляторов, просто масштабируется и адаптируется к сетям с разной топологией, пропускной способностью и бизнес-направленностью, включая сети АСУ ТП, технологические сети телекомов, биллинговые и банковские системы.

Источник: <http://ptsecurity.ru/about/news/41049/> (дата размещения материала 25.05.2015).

*«Darktrace» запускает новую технологию
обнаружения киберугроз⁸*

Согласно информации, размещенной на сайте businessweekly.co.uk, компания «Darktrace» запустила новое оружие для борьбы с кибертеррористами, нацеленными на автоматизированные системы управления технологическими процессами (АСУ ТП). Компания разработала систему обнаружения киберугроз Industrial Immune System, работающую в режиме реального времени в рамках технологии Enterprise Immune System, в особенности для выявления возникающих киберугроз для АСУ ТП.

Industrial Immune System представляет собой инновацию для поставщиков критической инфраструктуры, поскольку позволяет визуализировать процессы производственной среды и оповещает о потенциальных угрозах прежде чем они перерастут в крупномасштабную кибератаку. Система имеет особую математическую модель, адаптированную для обработки данных АСУ ТП, которая формирует специальную «схему» для машин, сетей и пользователей в заданной рабочей среде. Такая схема используется для обнаружения еще неидентифицированных аномалий в режиме реального времени.

Источник: <http://www.businessweekly.co.uk/news/hi-tech/darktracelaunches-new-cyber-threat-detection-technology> (дата размещения материала 28.04.2015).

*Новосибирская «МСТ» создала промышленный компьютер
с уникальной модульной архитектурой*

Согласно сообщениям ряда сайтов, компания «Модульные Системы Торнадо» (российский производитель АСУ ТП) в интересах реализации программы импортозамещения и перехода на собственную элементную базу запустила в серию производство первого отечественного промышленного компьютера IPC Gridex. Новый компьютер обладает уникальной архитектурой, возможностью

⁸ Перевод с английского выполнен ГНИИИ ПТЗИ ФСТЭК России.

конфигурирования всех составляющих элементов (процессора, памяти и периферии) и уже внедрен в составе полномасштабных АСУ ТП критически важных объектов, таких как Красноярская ТЭЦ, РИТЭЦ Углевик в Республике Сербской и др.

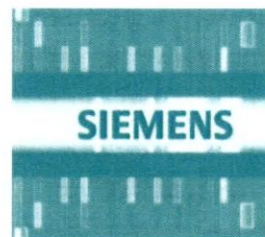
Высокая производительность, защищенность, гибкость и масштабируемость Gridex IPC позволяет использовать процессорные блоки для автоматизации технологических процессов (в том числе на критически важных объектах) в составе систем управления «реального времени», как компьютеры для дата-центров, компьютеры для «жестких» условий эксплуатации, а также специализированные компьютеры со встроенными сигнальными процессорами.



Источники: <http://www.russianelectronics.ru/developer-r/rss-r/news/partners-news/doc/72757/> (дата размещения материала 25.05.2015); <http://corp.cnews.ru/news/line/index.shtml?2015/05/25/595872>.

«Siemens» устранила уязвимость Ghost в своих продуктах

Как сообщает ряд сайтов, разработчики «Siemens» выпустили обновление безопасности для некоторых своих продуктов, подверженных влиянию уязвимости Ghost в библиотеке glibc. Обнаруженная брешь затрагивает приложения Siemens Sinumerik и Simatic HMI Basic, которые применяются во множестве аппаратных решений для промышленных предприятий в химической, энергетической, продовольственной и сельскохозяйственной сферах.



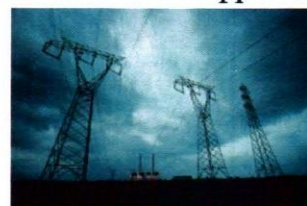
Для эксплуатации бреши атакующему необходимо предварительно получить локальный авторизованный доступ. Более того, для успешного осуществления атаки уязвимые функции должны быть установлены на целевой системе в составе соответствующих компонентов.

Продукты «Siemens» из линейки Simatic HMI все еще остаются уязвимыми к эксплуатации бреши.

Источники: <http://www.securitylab.ru/news/472751.php> (дата размещения материала 28.04.2015); <https://threatpost.ru/2015/04/28/siemens-zakrylauyazvimost-ghost-v-simatic>.

Обнаружена проблема безопасности в Smart Grid

По данным сайта securitylab.ru, исследователи обнаружили уязвимость в используемой в протоколе Smart Grid схемы аутентифицированного шифрования. Схема шифрования открыта для ряда кибератак. Под прицелом находится код подтверждения подлинности сообщения под названием OMA Digest. Недостатки в коде могут быть использованы для определения секретного пароля после нескольких попыток взлома.



Протокол Smart Grid используется в более чем четырех миллионах интеллектуальных счетчиков и аналогичных устройствах по всему миру. Подобные системы широко используются в SCADA-системах для автоматизации распределения электроэнергии.

Источник: <http://www.securitylab.ru/news/472882.php> (дата размещения материала 08.05.2015).

SCADA-системы компании «Rockwell Automation» оказались уязвимыми

Как проинформировал сайт securitylab.ru, специалистам Уральского центра систем безопасности удалось обнаружить критическую брешь в алгоритме шифрования паролей SCADA-системы RSVIEW32, которую разработала американская компания «Rockwell Automation».

RSVIEW32 широко применяется для мониторинга, контроля и управления технологическими процессами. В список сфер, где она применяется, входят объекты критической инфраструктуры, в частности, газовой и нефтяной промышленности.

Брешь позволяет злоумышленнику авторизоваться в SCADA-системах RSVIEW32 версии 7.60.00 (CPR9 SR4) и более поздних. Обход парольной защиты дает возможность вносить любые изменения в технологический процесс, что может привести к созданию аварийной ситуации.

О выявленной бреши сообщено производителю, который уже выпустил обновления для систем RSVIEW32.

Источник: <http://www.securitylab.ru/news/472985.php> (дата размещения материала 20.05.2015).

Серверы на американских судах уязвимы к атакам

По сообщению сайта securitylab.ru, в защите компьютерных сетей береговой охраны США выявлены многочисленные бреши, позволяющие злоумышленникам удалить конфиденциальные данные из системы, подключив к ней съемный накопитель. Также были выявлены незащищенные сети USCG.

Наибольшую угрозу безопасности представляют собой серверы на судах, которые работают под управлением операционной системы от «Microsoft» и на которых не были установлены последние обновления. Несмотря на то, что Microsoft выпустила последнее обновление для своей операционной системы для серверов в апреле текущего года, проведенная экспертами компании «CyberKeel» выборочная проверка показала, что в 37% случаев оно не было установлено.

Многие эксперты в сфере кибербезопасности отмечают, что кибератаки на компьютерные системы портов и кораблей могут иметь катастрофические по-



следствия. Известны случаи, когда системы управления портов, кораблей и буровых установок были повреждены или полностью уничтожены в результате осуществления подобных атак.

Источник: <http://www.securitylab.ru/news/472818.php> (дата размещения материала 05.05.2015).

*В лайнерах «Boeing» обнаружена программная ошибка,
отключающая питание самолета*

На сайте mk.ru размещена информация о наличии в ПО самолета «Boeing 787» ошибок, вызывающих отказ электрооборудования с потенциальной потерей контроля над самолетом. Проблема с электрогенераторами лайнера может возникнуть в том случае, если они проработают без перезагрузки более восьми месяцев.



Компания «Boeing» заявила, что электрооборудование всех самолетов, находящихся на сегодняшний день в эксплуатации, будет регулярно исследоваться для нейтрализации уязвимости и в настоящий момент компания работает над программным патчем, который сможет решить эту проблему.

Источник: <http://www.mk.ru/science/2015/05/12/v-laynerakhboeingobnaruzhen-programmnyy-bag-sposobnyy-otklyuchit-pitanie-samolyota.html> (дата размещения материала 12.05.2015).

*ФБР предупреждает о возможных атаках
хакеров против самолетов*

Как сообщает сайт rbc.ru, ФБР официально предупредило авиакомпания о существовании хакерской угрозы по отношению к пассажирским самолетам. Существует возможность взятия террористами под контроль электронной системы управления полетом при взломе оборудования с пассажирского места. ФБР рекомендовало сообщать о записях в социальных сетях с угрозами взлома беспроводного Интернета на борту, систем слежения и управления движением в воздухе.



Источник: <http://www.rbc.ru/rbcfreenews/553827799a7947331e4747bd> (дата размещения материала 23.04.2015).

2. Сведения о перспективах развития и достижениях в создании способов и средств защиты информации

Обновленная версия средства защиты информации от несанкционированного доступа Secret Net LSP для операционной системы Linux

Согласно информации, размещенной на сайте securitycode.ru, появилась обновленная версия средства защиты информации (СЗИ) от несанкционированного доступа (НСД) Secret Net LSP для операционной системы Linux. В СЗИ Secret Net LSP версии 1.2 расширился список поддерживаемых операционных систем семейства Linux. Теперь Secret Net LSP можно использовать для защиты конфиденциальной информации и персональных данных, обрабатываемых на рабочих станциях и серверах под управлением Red Hat Enterprise Linux 6.2/6.3/6.5, CentOS 6.2/6.5, Альт Линукс СПТ 6.0.0/6.0.2, Alt Linux 6 Centaurus и Debian 6.0.3.



Код безопасности
ГК «Информзащита»

СЗИ от НСД Secret Net LSP соответствует требованиям руководящих документов по 5-му классу защищенности средств вычислительной техники и по 4-му уровню контроля отсутствия недеklarированных возможностей. Таким образом, Secret Net LSP может использоваться для защиты информационных систем персональных данных до 1-го уровня защищенности включительно и государственных информационных систем до 1-го класса защищенности включительно, а также автоматизированных систем до класса защищенности 1Г включительно.

Источник: <http://www.securitycode.ru/company/news/obnovlennaya-versiya-szi-ot-nsd-secret-net-lsp-dlya-os-linux-postupila-v-prodazhu/> (дата размещения материала 12.05.2015).

«Cisco» реализовала интеграцию встроенных средств информационной безопасности инфраструктуры со средствами обнаружения угроз



На сайте корпорации «Cisco» cisco.com размещена информация о полной интеграции встроенных средств информационной безопасности инфраструктуры (ACI) со средствами обнаружения угроз в системе предотвращения вторжений нового поколения FirePOWER Next Generation Intrusion Prevention System (NGIPS). Это сделано в целях автоматизированного отражения угроз и противостояния растущим угрозам безопасности центров обработки данных (ЦОД).

Семейство средств обеспечения информационной безопасности Cisco FirePOWER обеспечивает высокую эффективность противостояния угрозам, качественный контроль и глобальный анализ угроз.

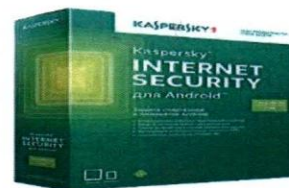
Многопользовательская инфраструктура ACI основана на модели «белых списков», в которой с помощью контроллера Cisco APIC и централизованных

средств автоматизации, контроля и аудита выполняется изоляция и сегментирование физических и виртуальных приложений ЦОД.

Источник: <http://www.cisco.com/web/RU/news/releases/txt/2015/05/07a.html> (дата размещения материала 07.05.2015).

Защитное решение Kaspersky Internet Security для Android

По информации, размещенной на сайте kaspersky.ru, новое решение Kaspersky Internet Security для Android показало отличные результаты в ходе теста, проведенного компанией «AV-TEST». Проверена эффективность выявления вредоносного ПО и практичность самого решения. В рамках исследования на мобильные устройства под управлением операционной системы Android 5.0.1 устанавливались последние версии тестируемых решений с обновленными антивирусными базами. Решениям был предоставлен доступ в Интернет и возможность обращения к собственным облачным сервисам. Для проверки эффективности детектирования защитным продуктам предоставили 3077 образцов нового вредоносного ПО. Продукт успешно определил 100% вредоносных приложений.



С точки зрения практичности решение также показало превосходные результаты – оно корректно определило приложения из Google Play Store и легитимные программы из стороннего источника как неопасные. При проведении нагрузочных тестов не выявлено замедление нормальной работы устройства, увеличение расхода заряда батареи или заметное увеличение интернет-трафика.

Источник: <http://www.kaspersky.ru/about/news/product/2015/Kaspersky-Internet-Security-for-Android-poluchil-nagradu-ot-AV-TEST> (дата размещения материала 08.05.2015).

Kaspersky Security Scan бесплатно подскажет, как устранить выявленные уязвимости

Как сообщает сайт компании «Лаборатория Касперского» kaspersky.ru, представлена новая версия Kaspersky Security Scan – бесплатное решение для компьютеров под управлением операционной системы Windows. Теперь продукт не только поможет выявить вредоносное ПО и уязвимости в настройках операционной системы, но и предоставит советы по решению каждой из найденных проблем.



Источник: <http://www.kaspersky.ru/about/news/product/2015/Kaspersky-Security-Scan-free> (дата размещения материала 18.05.2015).

Антивирусная утилита для сайтов от «Яндекс»

По данным ряда сайтов, компанией «Яндекс» разработано новое корпоративное антивирусное решение для сайтов Manul. Утилита Manul призвана

оперативно устранить заражение и не потерять трафик. Информацию о возможностях программы владельцы сайтов смогут получать вместе с оповещением о заражении, которое рассылает сервис «Яндекс.Вебмастер».

Сканируя, Manul собирает информацию обо всех файлах, расположенных в корневом каталоге и ниже его: об их размере, дате последнего изменения, вычисляет хэш-сумму. Параллельно с этим каждый файл проверяется на вредоносность по приложенной антивирусной базе. Manul не требует доступа к конфиденциальным данным, а все производимые с файлами действия контролирует и подтверждает непосредственно владелец сайта. Утилита имеет собственную защиту, которая заключается в том, что при первом запуске ее необходимо защитить паролем. Это не дает злоумышленникам воспользоваться ею в своих целях.

Яndex

денциальным данным, а все производимые с файлами действия контролирует и подтверждает непосредственно владелец сайта. Утилита имеет собственную защиту, которая заключается в том, что при первом запуске ее необходимо защитить паролем. Это не дает злоумышленникам воспользоваться ею в своих целях.

ключается в том, что при первом запуске ее необходимо защитить паролем. Это не дает злоумышленникам воспользоваться ею в своих целях.

Источники: <http://it-sektor.ru/manul-antivirusnaya-utilita-dlya-sayitov-otyandeks.html> (дата размещения материала 27.04.2015), <https://xakep.ru/2015/04/26/manul/>.

Двойные биометрические пароли

Как сообщает сайт payspacemagazine.com, американский банк «Mountain America Credit Union» объявил о запуске новой системы аутентификации для пользователей смартфонов. Учреждение отказалось использовать уже ставшую привычной биометрическую защиту, основанную на одном биомаркере, например, отпечатке пальца. Руководство решило защитить все финансовые операции в своем мобильном приложении с помощью двойной биометрии.



Пользователю необходимо отсканировать палец или сетчатку глаза. Возможность выбора из двух биомаркеров откроет доступ к услуге для большего количества клиентов. Сканирование и распознавание узора глаза обеспечивает провайдер ПО «EyeVerify». Программа фиксирует переплетение кровеносных сосудов, которое является уникальным для каждого человека.

Источник: <http://payspacemagazine.com/na-smenu-biometricheskimparyam-pridut-dvojnye-biometricheskie-paroli.html> (дата размещения материала 19.05.2015).

Toughbook CF-54: мощный, легкий и защищенный

Согласно сообщению, опубликованному в журнале «Chip», компания «Panasonic» представила новую версию популярной модели полужащенного ноутбука Toughbook CF-54.



Конструкция ноутбука спроектирована так, чтобы ее можно было модифицировать различными модулями, созданными российскими разработчиками, что важно при работе с госзаказчиками в России. Данные модули, изготовленные под конкретного заказчика, возможно встроить в ноутбук,

что составит единое решение для заказчика. В зависимости от решения комплексы могут получить необходимые сертификаты ФСТЭК России и ФСБ России.

Источник: Chip, 2015, № 5, с. 34.

*Определение частотной зависимости коэффициента ослабления
побочных электромагнитных излучений на трассах их распространения
методом импульсного зондирования трасс*

В статье, опубликованной в журнале «Специальная техника», приведены результаты экспериментальных исследований возможности использования сверхкоротких наносекундных видеоимпульсов без несущей в импульсно-временном методе определения частотных зависимостей трассовых коэффициентов ослабления побочных электромагнитных излучений (ПЭМИ) технических средств обработки информации.

На основе полученных результатов сделан вывод, что использование импульсно-временного метода зондирования трасс распространения сигналов ПЭМИ за счет временного стробирования и выделения первого пришедшего импульса позволяет свести определение коэффициента ослабления ПЭМИ к стандартным условиям однолучевости. Это обеспечивает существенное уменьшение негативной (при проведении измерений) изрезанности частотной зависимости. В итоге повышается достоверность сделанного по результатам измерений вывода в отношении защищенности или незащищенности информации, обрабатываемой техническим средством, от утечки по каналу ПЭМИ.



Источник: Специальная техника, 2015, № 2, с. 28-33.

*Разблокировать мобильный телефон с помощью уха вскоре станет
возможным благодаря «Yahoo!»⁹*

Как информирует сайт muysseguridad.net, повышение безопасности мобильных устройств с каждым разом становится все более реальным благодаря биометрической аутентификации, гарантирующей доступ к содержанию только авторизованного пользователя. В настоящее время благодаря встроенному сенсору существует возможность использовать отпечаток пальца для разблокировки мобильного устройства и покупок в магазине приложений.

Проводятся исследования по изучению возможностей разблокировки мобильных телефонов при помощи сетчатки глаза. Недавно была представлена новая концепция, позволяющая идентифицировать пользователя мобильного телефона по отпечатку уха. В частности, в этом направлении работает компания «Yahoo!», представившая систему распознавания формы и отличительных особенности ушной раковины пользователя



⁹ Перевод с испанского выполнен ГНИИИ ПТЗИ ФСТЭК России.

для разблокировки устройства. Помимо прочего она сможет использовать характеристики суставов и ладони пользователя. В рамках небольшого исследования удалось идентифицировать пользователей с точностью 99,52%.

Источник: <http://muysseguridad.net/2015/04/29/desbloquear-movil-oreja> (дата размещения материала 29.04.2015).

*«Мегафон» научился обнаруживать зараженных
вирусами абонентов*

По данным сайта cnews.ru, компания «Мегафон» начала рассылку предупреждающих SMS абонентам, чьи телефоны заражены троянами. «Мегафон» внедрил решение для отслеживания заражений его абонентов вредоносным ПО.



Троянские программы для операционной системы Android, попадая на смартфон абонента, пытаются украсть деньги с его счета у сотового оператора или с привязанной банковской карты. Путем SMS-запросов троян определяет баланс абонента, факт привязки банковских карт и кошельков Qiwi, а затем переводит денежные средства на подконтрольные мошенникам сотовые номера с целью их дальнейшего вывода. В настоящее время около 20% российских пользователей Android-смартфонов могут быть заражены.

Другой признак присутствия в системе такого трояна – это обращения смартфона к центрам управления бот-сетями (C&C). «Мегафон» вместе с антивирусными компаниями выявляет такие центры, а частые обращения к ним со стороны абонентов могут свидетельствовать о факте заражения.

Выявив заражение, «Мегафон» присылает абоненту SMS-сообщение с предупреждением и предложением установить бесплатный антивирус.

Источник: <http://safe.cnews.ru/news/top/index.shtml?2015/04/29/595404> (дата размещения материала 29.04.2015).

3. Сведения о новых документах, регламентирующих вопросы в области защиты информации

3.1. Нормативные правовые акты федерального уровня

*Указ Президента Российской Федерации от 22.05.2015 № 260
«О некоторых вопросах информационной безопасности
Российской Федерации»
(начало действия документа – с момента подписания)*



Утвержден порядок подключения информационных систем и информационно-телекоммуникационных сетей к информационно-телекоммуникационной сети Интернет и размещения (публикации) в ней информации через российский государственный сегмент информационно-телекоммуникационной сети Интернет, поддержание, эксплуатация и развитие которого возложены на ФСО России.

Подключение государственных информационных систем и информационно-телекоммуникационных сетей, находящихся в ведении Администрации Президента Российской Федерации, Аппарата Правительства Российской Федерации, Следственного комитета Российской Федерации, федеральных органов исполнительной власти и органов исполнительной власти субъектов Российской Федерации, должно осуществляться по каналам передачи данных, защищенных с использованием криптографических средств защиты информации, и должно быть завершено до 31 декабря 2017 г.

*Федеральный закон Российской Федерации от 20.04.2015 № 91-ФЗ
«О ратификации Соглашения о порядке защиты конфиденциальной
информации и ответственности за ее разглашение при осуществлении
Евразийской экономической комиссией полномочий по контролю
за соблюдением единых правил конкуренции»*

Ратифицировано Соглашение о порядке защиты конфиденциальной информации и ответственности за ее разглашение при осуществлении Евразийской экономической комиссией полномочий по контролю за соблюдением единых правил конкуренции, подписанное в городе Москве 12 ноября 2014 г.

Источник: система Консультант Плюс.

*Постановление Правительства Российской Федерации от 02.04.2015 № 304
«О внесении изменений в Положение о подготовке к передаче сведений,
составляющих государственную тайну, другим государствам или
международным организациям»*

Внесены редакционные изменения в отдельные пункты Положения о подготовке к передаче сведений, составляющих государственную тайну, другим государствам или международным организациям, утвержденное постановлением

Правительства Российской Федерации от 2 августа 1997 г. № 973 «Об утверждении Положения о подготовке к передаче сведений, составляющих государственную тайну, другим государствам или международным организациям».

Источник: система Консультант Плюс.

*Распоряжение Правительства Российской Федерации
от 02.04.2015 № 583-р*

Утвержден Перечень видов документов, передаваемых при взаимодействии федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, государственных внебюджетных фондов в электронном виде, предусмотренный Правилами обмена документами в электронном виде при организации информационного взаимодействия.

Источник: система Консультант Плюс.

3.2. Документы ФСТЭК России



*Приказ ФСТЭК России от 02.04.2015 № 27
«Об утверждении Порядка уведомления работодателя
о фактах обращения в целях склонения работников
организаций, созданных для выполнения задач, поставленных
перед Федеральной службой по техническому и экспортному
контролю, к совершению коррупционных правонарушений»*

Утвержден Порядок уведомления работодателя о фактах обращения в целях склонения работников организаций, созданных для выполнения задач, поставленных перед ФСТЭК России, к совершению коррупционных правонарушений.

Приведены формы уведомления о факте обращения в целях склонения к совершению коррупционных правонарушений, журнала регистрации уведомлений о фактах обращения в целях склонения работника к совершению коррупционных правонарушений и талона уведомления работодателя.

Источник: система Консультант Плюс.

*Информационное сообщение ФСТЭК России от 07.05.2015
№ 240/22/1792 «О разработке методического документа
ФСТЭК России «Методика определения угроз безопасности
информации в информационных системах»*

Определено, что методический документ устанавливает единый методический подход к определению угроз безопасности информации и разработке моделей угроз безопасности информации в государственных информационных системах, защита информации в которых обеспечивается в соответствии с Требованиями о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденными приказом ФСТЭК России от 11 февраля 2013 г. № 17.

ФСТЭК России предлагает специалистам в области информационной безопасности заинтересованных органов государственной власти и организаций

рассмотреть проект методического документа и направить предложения по указанному проекту на адрес электронной почты methodoubi@fstec.ru.

Источник: система Консультант Плюс.

3.3. Патентные документы



Пат. 2550353 Российская Федерация, МПК H04B17/00 (2015.01). Способ оценки качества маскирующего шума. / Гаврилов И.В., Гребенев Д.В., Басов О.О., Васечкин Е.А., Корнилов А.А.; патентообладатель Государственное казенное образовательное учреждение высшего профессионального образования «Академия Федеральной службы охраны Российской Федерации» (Академия ФСО России). – 2014130567/07, заявл. 22.07.2014, опубл. 10.05.2015.

Изобретение относится к области защиты информации и может быть использовано для оценки качества маскирующего шума. Техническим результатом изобретения является повышение точности оценки качества маскирующего акустического шума.

Пат. 2545516 Российская Федерация, H04L27/00 (2006.01). Устройство обнаружения атак в беспроводных сетях стандарта 802.11g. / Беляков Э.В., Гребенев С.В., Лопатин Д.А., Константинов С.В., Семкин А.В.; патентообладатель Государственное казенное образовательное учреждение высшего профессионального образования «Академия Федеральной службы охраны Российской Федерации» (Академия ФСО России). – 2013134625/07, заявл. 23.07.2013, опубл. 10.04.2015.

Изобретение относится к области электросвязи и может быть использовано для определения состояния беспроводной сети связи, обнаружения в ней атак и повышения достоверности принятия решения системами обнаружения атак в беспроводных сетях. Технический результат, на достижение которого направлено изобретение, заключается в разработке устройства, обеспечивающего обнаружение признаков DDoS-атак, атак типа «человек посередине» и нарушения режимов работы сети.

Пат. 2540838 Российская Федерация, G06F21/00 (2013.01). Устройство обнаружения удаленных компьютерных атак. / Васюков Д.Ю., Коцыняк М.А., Коцыняк М.М., Лаута О.С., Лаута А.С.; патентообладатель Федеральное государственное казенное военное образовательное учреждение высшего профессионального образования «Военная академия связи имени Маршала Советского Союза С.М. Буденного» Министерства обороны Российской Федерации. – 2014108176/08, заявл. 03.03.2014, опубл. 10.02.2015.

Изобретение относится к области электросвязи. Техническим результатом является повышение достоверности обнаружения удаленных компьютерных атак.

Пат. 2543958 Российская Федерация, G08B25/00 (2006.01), G06K9/62 (2006.01). Способ контроля исполнения домашнего ареста с биометрической аутентификацией контролируемого. / Иванов А.И., Фунтиков В.А., Ефи-

мов О.В., Трифонов С.Е., Язов Ю.К., Соловьев С.В.; патентообладатель Российская Федерация, от имени которой выступает Федеральная служба по техническому и экспортному контролю (ФСТЭК России). – 2013122380/08, заявл. 14.05.2013, опубл. 10.03.2015.

Изобретение относится к средствам контроля исполнения домашнего ареста. Техническим результатом является повышение надежности автоматизированного контроля исполнения домашнего ареста, а также отказ от необходимости использования браслетов, носимых на руках или на ногах.

Пат. 2546236 Российская Федерация, МПК H04L1/24 (2006.01), G06F15/16 (2006.01). Способ анализа информационного потока и определения состояния защищенности сети на основе адаптивного прогнозирования и устройство для его осуществления. / Кузькин А.А., Маркин Д.О., Гребенев С.В., Сергеев В.Ю.; патентообладатель Государственное казенное образовательное учреждение высшего профессионального образования «Академия Федеральной службы охраны Российской Федерации» (Академия ФСО России). – 2013136682/08, заявл. 05.08.2013, опубл. 10.04.2015.

Изобретение относится к области передачи цифровой информации. Технический результат – повышенная защита сети за счет использования механизма адаптивного прогнозирования и весовых коэффициентов критических параметров сетевого трафика.

Пат. 2543960 Российская Федерация, G06F17/27 (2006.01), G06F11/00 (2006.01). Способ определения уязвимых функций при автоматизированной проверке веб-приложений на наличие уязвимостей. / Бородакий Ю.В., Нацекин П.А., Букаров Я.Н.; патентообладатель Открытое акционерное общество «КОНЦЕРН «СИСТЕМПРОМ». – 2013140101/08, заявл. 29.08.2013, опубл. 10.03.2015.

Изобретение относится к области выявления программных ошибок и недекларированных возможностей в веб-приложениях на интерпретируемых языках. Техническими результатами являются повышение числа потенциально обнаруживаемых уязвимостей веб-приложений, а также сокращение времени, необходимого для ручного анализа программных ошибок с целью определения их критичности.

Пат. 2538913 Российская Федерация, G06F21/00 (2013.01). Способ деперсонализации персональных данных. / Куракин А.С.; патентообладатель Федеральное государственное автономное образовательное учреждение высшего образования «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики» (Университет ИТМО). – 2012144274/08, заявл. 16.10.2012, опубл. 10.01.2015.

Изобретение относится к области защиты информации, хранимой в информационных системах персональных данных (ИСПДн), от НСД и может быть использовано на стадиях разработки и оптимизации ИСПДн в защищенном исполнении. Техническим результатом является повышение уровня безопасности ИСПДн.

4. Статистические данные по анализу защищенности информационных систем

Главные цели киберпреступников в России

Согласно информации экспертов «Лаборатории Касперского», размещенной на сайте tcinet.ru, хакеров больше всего интересует внутренняя операционная информация российских компаний – она была похищена в 45% случаях. Компании же при этом сильнее всего переживают за клиентские базы и интеллектуальную собственность, несмотря на то, что их утечка была отмечена только в 27% и 29% случаев соответственно.



Владельцы бизнеса также недооценивают интерес к персональным данным сотрудников – о них волнуются всего 5%, в то время как в реальности эти данные были украдены в 25% случаев. Негативный эффект от подобных инцидентов усугубляется не только репутационными потерями, но и возможными штрафами со стороны регуляторов.

Источник: <http://www.tcinet.ru/press-centre/technology-news/2243/> (дата размещения материала 08.05.2015).

Уязвимости онлайн банковских приложений

Ряд сайтов приводит результаты исследования компании «Positive Technologies» по защищенности крупнейших российских банков.

В рамках исследования рассмотрено 28 систем дистанционного банковского обслуживания (ДБО) физических (77%) и юридических лиц (23%). Среди них исследованы и мобильные системы ДБО, представленные серверной и клиентской частью (54%). Две трети систем (67%) являлись собственными разработками банков, остальные были развернуты на базе платформ известных разработчиков.



Половина обнаруженных уязвимостей систем ДБО (44%) имеет высокий уровень риска. Примерно одинаковое количество уязвимостей имеют среднюю и низкую степени риска (26% и 30%). В целом, уязвимости высокого уровня риска выявлены в 78% исследованных систем.

Большая часть уязвимостей (42%) связана с ошибками реализации механизмов защиты систем ДБО, заложенных разработчиками. На втором месте – уязвимости, связанные с ошибками в коде приложений (36%). Остальные уязвимости в основном связаны с недостатками конфигурации (22%).

Источники: <http://www.astera.ru/pr/99739/> (дата размещения материала 19.05.2015); <http://www.rg.ru/2015/05/19/nedocheti.html>.

Безопасность промышленных систем управления в 2014 г.

В отчете компании «Positive Technologies», размещенном на сайте hacker.ru, отмечается, что промышленные системы управления (ICS, АСУ ТП) все чаще становятся мишенью для злоумышленников и киберармий. На смену отдельным червям (Stuxnet и Flame) пришли более изощренные схемы многоступенчатых атак.



Всего в рамках исследования выявлена 691 уязвимость в компонентах АСУ ТП. Основное количество уязвимостей имеет высокую (58%) и среднюю (39%) степени опасности.

Приводится список производителей, лидирующих по количеству уязвимостей в продуктах: «Siemens» – 124 уязвимости, «Schneider Electric» вместе с приобретенной ею компанией «Invensys» – 96, «Advantech» – 51, «General Electric» – 31.

Источник: <https://hacker.ru/2015/05/13/scada-hacks> (дата размещения материала 13.05.2015).

Состояние безопасности автоматизированных систем управления технологическими процессами и SCADA-систем¹⁰

На сайте security-insider.de представлен обзор тенденций развития существующих и появления новых уязвимостей и угроз в отношении АСУ ТП и SCADA-систем. Лаборатория безопасности «QUALYS» сообщила, что по сравнению с прошлым годом количество уязвимых мест в АСУ ТП снизилось на 14%. Несмотря на разнообразие структур SCADA-систем, они все имеют общие компоненты, присутствующие в той или иной форме.

В частности, это устройства сбора и обработки данных. В 2014 г. отмечено всего около 1% от общего числа уязвимостей АСУ ТП/SCADA-систем в компонентах сбора данных. Например, CVE-2014-2378 уязвимость в датчике движения. Что касается устройств обработки, то в 2014 г. в них было обнаружено около 14% уязвимостей. Пример: уязвимость CVE-2014-0769 в программируемых логических контроллерах, используемых для автоматической сборки и производства в таких областях, как выпуск солнечных батарей, автомобильная сборка, где малейшие отклонения критичны для конечного продукта.



Источник: <http://www.security-insider.de/themenbereiche/plattformsicherheit/schwachstellen-management/articles/486515/> (дата размещения материала 24.04.2015).

¹⁰ Перевод с немецкого выполнен ГНИИИ ПТЗИ ФСТЭК России.

Скачок краж персональных данных пациентов

Как сообщает сайт threatpost.ru, с 2010 г. атаки на сферу здравоохранения выросли на 125%. Полученные цифры показывают, что подавляющее большинство медицинских организаций не в состоянии адекватно отвечать на киберугрозы и не обладают достаточными ресурсами, чтобы защитить данные пациентов. При этом в 91% организаций была зафиксирована одна утечка, а в 39% – от двух до пяти, в 40% компаний наблюдалось свыше пяти утечек за последние два года.



Почти половина утечек (45%) вызвана криминальной активностью. Лишь 10% пострадавших отмечают, что по случаю утечки проведена полноценная проверка и инцидент был исчерпан.

Источник: <https://threatpost.ru/2015/05/07/proizoshel-rezkij-skachok-krazh-dannyh-patsientov> (дата размещения материала 07.05.2015).

Менее 23% образовательных учреждений защищены надлежащим образом

Сайт securitylab.ru сообщает, что предметом исследования аналитиков из «BitSight» стала образовательная индустрия. Особое внимание было уделено ботнетам и проблеме утечек данных.

Согласно отчету, в общей сложности проверка затронула 6273 компании. При этом основой для формирования экспертной оценки служила эффективность противостояния компьютерной сети различным типам угроз. Кроме того, исследователи учитывали уже случившиеся в компании инциденты и оценили шаги, предпринятые руководством для предотвращения аналогичных атак в дальнейшем.



По итогам анализа выяснилось, что менее 23% всех исследованных организаций смогли обеспечить надлежащий уровень безопасности для своих компьютерных сетей. Более того, самые неудовлетворительные оценки исследователей получили более 33% всех участников исследования.

Источник: <http://www.securitylab.ru/news/472459.php> (дата размещения материала 10.05.2015).

Специалисты «Лаборатории Касперского» отмечают резкое увеличение количества атак финансового характера

По данным портала ferra.ru, специалистами «Лаборатории Касперского» отмечено резкое увеличение в I квартале 2015 г. количества атак финансового характера. Согласно данным, полученным при помощи облачной инфраструктуры Kaspersky Security Network, по сравнению с предыдущим кварталом число пользователей, столкнувшихся с попытками кражи денег с банковских онлайн-счетов, увеличилось на 50%.



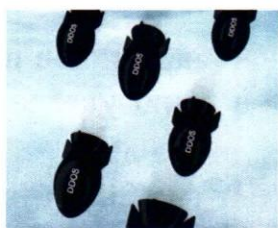
Всего же в период с января по март решения «Лаборатории Касперского» заблокировали более 5 млн. попыток заражения компьютеров пользователей вирусами, предназначенными для кражи денег.

Злоумышленники активно стремятся внедрить функции перехвата конфиденциальной информации для доступа к банковским счетам и платежным системам в любое вредоносное ПО. В I квартале предотвращено более 2 млрд. попыток совершения атак на компьютеры и мобильные устройства пользователей. При этом 40% всех зарегистрированных веб-атак проведены с интернет-ресурсов, размещенных в России.

Источник: http://www.ferra.ru/ru/techlife/news/2015/04/29/kasperskyoho-ta-za-dengami/#.VUH_Wnan11Z (дата размещения материала 29.04.2015).

В I квартале 2015 г. «Arbor» зафиксировала рекордное количество DDoS-атак

По информации сайта threatpost.ru, компанией «Arbor Networks» опубликован отчет о DDoS-атаках по итогам января – марта 2015 г. В этот период зафиксирован новый рекорд по мощности – 334 Гбит/с. Эта атака была проведена



против одного из индийских сетевых операторов, ее продолжительность составила 6 минут. В целом за квартал «Arbor» насчитала 940 тыс. DDoS-инцидентов в сетях пользователей информационно-аналитической платформы ATLAS, которая в настоящее время мониторит до 120 Тб трафика. При этом 17,7% атак по мощности превышали 1 Гб, а 25 показали на пике более 100 Гб. Потолок другого важного показателя мощности DDoS rps (число пакетов в секунду) за квартал снизился почти в два раза, с 112,5 до 65,15 Mpps.

Средняя продолжительность DDoS-инцидентов несколько увеличилась и составила 1 час 14 минут, однако в 90% случаев ресурс подвергался атаке менее 1 часа. Злоумышленники зачастую выбирали «мишень» с американской, китайской или французской пропиской (16,2; 16 и 7,5% атак соответственно). Источники мусорного трафика в 40% случаев определить не удалось, анализ остальных DDoS-атак показал, что злоумышленники предпочитали проводить атаки с территории США (11,3% инцидентов), Южной Кореи (8,5%) и Китая (5,3%).

Источник: https://threatpost.ru/2015/05/06/v_1_kvartale_arbor_zafiksirovala_rekordnuju_ddos (дата размещения материала 09.06.2015).

В I квартале 2015 г. установлен рекорд по количеству совершенных DDoS-атак

Согласно отчету компании «Akamai Technologies», размещенном на сайте comss.info, в I квартале 2015 г. установлен рекорд по количеству совершенных



DDoS-атак. Их число увеличилось практически в два раза по сравнению с этим же периодом 2014 г. Злоумышленники в начале нынешнего года прибегали к DDoS-атакам на 35% чаще, чем в последнем квартале 2014 г.

Мощность типичных DDoS-атак не превышала 10 Гбит/с, а их продолжительность составляла более чем 24 часа. Эксперты также обнаружили восемь «мега-атак», которые превысили 10 Гбит/с.

Больше всего за первые три месяца от DDoS-атак пострадал игровой сектор, на который пришлось более 35% от всех атак. Популярной целью злоумышленников стал протокол SSDP, на долю которого пришлось более 20% от всех векторов атак. На 22,22% увеличилось число DDoS-атак на уровне приложений (уровень 7) и на 36,74% выросло количество атак на уровне инфраструктуры (уровень 3 и 4).

Источник: http://www.comss.info/page.php?al=V_pervom_kvartale_2015_goda_byl_ustanovlen_rekord_po_kolichestvu_overshennyyh_DDoS_atak (дата размещения материала 20.05.2015).

Установлен рекорд по числу вирусов

По данным сайта threatpost.ru, специалистами компании «PandaLabs» опубликован доклад о результатах анализа вирусной активности за 2014 г. В среднем по всему миру появляется 255 тыс. новых угроз ежедневно. Такой показатель отмечен в IV квартале 2014 г.

Большинство вирусов представляют собой ПО, модифицированное хакерами для того, чтобы оно не детектировалось антивирусными средствами. Самое популярное у киберпреступников вредоносное ПО – троянские программы. В числе новых угроз их оказалось 82,18%.



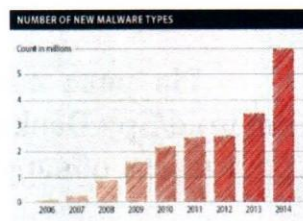
В общей сложности в мире инфицировано 33,21% устройств. Больше всего их расположено в Китае – 47,22%. Затем идут Тайвань (45,92%), Турция (42,33%) и Россия (41,45%).

Самыми атакуемыми областями бизнеса в 2014 г. стали ритейл и сфера услуг. Почти треть всех фишинг-нападений (29,37%) приходилась на эти компании. На втором месте (25,13%) платежные сервисы. В 2014 г. фишинговые атаки зафиксированы практически во всех странах мира. Однако лидером по проценту атакованных пользователей стала Бразилия – 27,47% от всех пользователей.

Источник: <https://threatpost.ru/2015/05/06/chernyj-den-dlya-it-ustanovlen-rekord-po-chislu-zlovredov/> (дата размещения материала 06.05.2015).

Каждые 4 секунды выявляется новое вредоносное программное обеспечение

Как сообщает сайт comss.info, в 2014 г. каждые четыре секунды эксперты выявляли новый вид вредоносного ПО. Во второй половине 2014 г. было обнаружено 4,1 млн. новых вредоносных программ. Темпы роста возникновения вредоносного ПО увеличились за первое полугодие 2014 г. на 125%. В течение всего года выявлено около 6 млн. нового вредоносного ПО – это на 77% больше, чем в 2013 г. Рекламное ПО составило 31,4% от всего обнаруженного ИБ-специалистами вредоносного ПО.



Во второй половине 2014 г. в 18 раз увеличилось количество выявленных рутки-тов. Число кибератак с использованием банковских троянов выросло на 44,5%.

Источник: http://www.comss.info/page.php?al=Kazhdye_4_sekundy_vyjavljaetsja_novoe_vredonosnoe_PO (дата размещения материала 20.05.2015).

Вирус Conficker – основной источник заражений



По данным сайта tcinet.ru, главным источником заражений компьютеров в мире остается вирус Conficker, впервые обнаруженный еще в конце 2008 г. На его долю во втором полугодии 2014 г. пришлось 37% всех заражений, зафиксированных экспертами. Далее следуют вирусы семейств Kilim и Sality – 11% и 10% заражений соответственно.

Источник: <http://www.tcinet.ru/press-centre/technology-news/2215> (дата размещения материала 27.04.2015).

Общее количество используемых при рассылке спама IP-адресов сократилось на 13%

Согласно информации сайта securitylab.ru, общее количество IP-адресов, с которых рассылается спам, сократилось на 13%. Как отмечается в отчете компании «Cloudmark», ситуация со спамом заметно улучшилась в некоторых странах. Однако, в I квартале 2015 г. во многих регионах наблюдалось серьезное сокращение блокируемых по причине рассылки спама IP-адресов. С ноября 2012 г. по апрель 2014 г. «Cloudmark» блокировала от 20 до 25% всех румынских IP-адресов. Сейчас этот показатель упал до 6,2%.



В Панаме, где общее количество IP-адресов достаточно незначительное, более 10% раньше блокировались. Основной причиной такой ситуации был спам с хостинг-сервиса Panamaserver.com. Теперь только 1,5% IP-адресов в Панаме блокируются.

В Саудовской Аравии процент блокируемых адресов вырос и сейчас составляет 6,4%. Среди стран, где число рассылających спам IP-адресов наибольшее, оказались США, Китай, Россия и Румыния.

Источник: <http://www.securitylab.ru/news/472779.php> (дата размещения материала 29.04.2015).

«ESET» предупреждает о росте активности Android/Spy.Banker.F

На ряде сайтов компания «ESET» предупреждает о росте активности Android/Spy.Banker.F. Версия Android/Spy.Banker.F демонстрирует устойчивый рост числа обнаружений с начала 2014 г. с пиком активности в феврале 2015 г.

Данная модификация вредоносного ПО составляет до 68% всех выявленных образцов семейства. Программа ориентирована на русскоговорящих пользователей – до 98% заражений приходится на Россию; 0,76 и 0,21% соответственно – на Украину и Беларусь. При этом некоторые образцы, обнаруженные экспертами, распространялись через колумбийские и чилийские сайты.



Заражение происходит, когда Android-пользователь посещает один из инфицированных сайтов. После установки троян передает на удаленный сервер номер телефона, IMEI зараженного устройства, страну, версию Android и другие данные.

Источники: <https://www.esetnod32.ru/home/products/mobilesecurity/android/> (дата размещения материала 14.05.2015); <http://www.esetnod32.ru/company/press/center/esetraz-oblachayet-russkogosh-piona-dlya-android>.

Межсетевые экраны пропускают вредоносное программное обеспечение

По данным сайта securitylab.ru, межсетевые экраны компаний «Palo Alto Networks», «McAfee» и «Websense» оставляют корпоративные сети открытыми для передачи вредоносного ПО. Экспериментально удалось выяснить, что почти 3 млн. устройств пытались принять исходящее вредоносное соединение, 13% из которых были разрешены межсетевыми экранами. При этом 2% всех устройств были инфицированы и имели возможность обмениваться данными за пределами корпоративной сети. Около 400 тыс. соединений избежали обнаружения межсетевыми экранами.



В результате анализа работы систем управления информацией о безопасности и событиями о безопасности, таких как HP ArcSight, IBM Security QRadar, Splunk, LogRhythm и McAfee Enterprise Security Manager выяснено, что в среднем компаниям требуется около 17 дней для обнаружения проблем безопасности.

Источник: <http://www.securitylab.ru/news/472665.php> (дата размещения материала 22.04.2015).

5. Сведения об инцидентах информационной безопасности

Сайт Следственного комитета России стал жертвой кибератаки

В соответствии с информацией, размещенной на сайте digitalmetro.us, официальный сайт Следственного комитета Российской Федерации подвергся хакерской атаке. Неизвестные разместили на скомпрометированном ресурсе не соответствующую действительности информацию о задержании участников митинга 6 мая на Болотной площади в Москве.

Несмотря на то, что публикация была удалена с сайта практически сразу же, многие средства массовой информации «подхватили» ее, и ложные данные распространились в Сети.

Источник: <http://digitalmetro.us/technology/34-security/18180-2015-05-08-13-41-24> (дата размещения материала 08.05.2015).



Клиенты Сбербанка стали жертвами компьютерного вируса

Как сообщает сайт riafan.ru, число клиентов Сбербанка, пострадавших от нового компьютерного вируса, который списывает средства со счетов через мобильные устройства, уже перевалило за 100 тыс. человек. Вирус типа «Троян» представляет опасность для владельцев смартфонов на платформе Android.

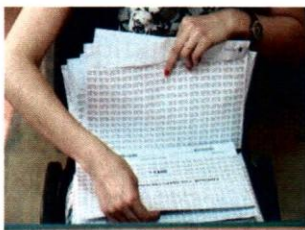


Вредоносная программа самостоятельно переводит средства с привязанной к мобильному устройству банковской карты на счет хакеров. При этом владельцы карт не получают об этом уведомления, поскольку вирус блокирует SMS-сообщения о проведении банковской операции.

Источник: <http://riafan.ru/272443-sto-tyisyach-klientov-sberbanka-stali-zhertvami-kompyuternogo-virusa> (дата размещения материала 12.05.2015).

Атака на сайт Федерального института педагогических измерений

Согласно информации ряда сайтов со ссылкой на главу Рособрнадзора, неизвестными хакерами была совершена атака на сайт Федерального института педагогических измерений, занимающегося исследованиями в области оценки качества образования. Хакерская атака имела целью похищение задания к Единому государственному экзамену. Злоумышленники пытались найти оригинальные экзаменационные материалы. Попытка хищения была предотвращена.



Источники: <http://russian.rt.com/article/93582> (дата размещения материала 25.05.2015); http://www.gazeta.ru/social/news/2015/05/25/n_7225493.shtml.

Взломы платёжных терминалов украли миллионы в России

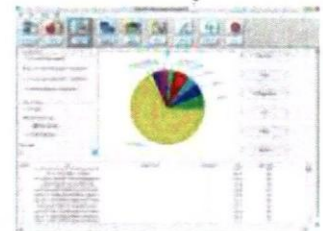
По данным сайта threatpost.ru, платёжные терминалы в Московской, Свердловской, Ивановской, Нижегородской, Тверской и других областях России были заражены вредоносной программой. Ущерб от противозаконной деятельности оценивается в десятки миллионов рублей. По данным следствия, злоумышленники с помощью вредоносной программы удаленно подключались к терминалам экспресс-оплаты, модифицировали их программно-аппаратную часть и начинали осуществлять транзакции внесенных средств на подконтрольные счета.



Источник: <https://threatpost.ru/2015/05/05/vzломshhiki-platezhnyhterminolov-ukrali-millions-v-rossii> (дата размещения материала 05.05.2015).

Вирус под названием «5 рейх» помог хакерам похитить с банковских карт 50 млн. рублей

В соответствии с информацией, размещенной на сайте yarsk.ru, вирус под названием «5 рейх» помог членам кибергруппировки «Фашисты» похищать средства с банковских карт посредством заражения телефонов. Вирус успел заразить 320 тыс. смартфонов. Общий ущерб оценивают в 50 млн. рублей.



Заражались только мобильные устройства, работающие на платформе Android. Вредоносный троян все пострадавшие устанавливали на свои гаджеты сами. При заражении вирус маскировался под приложение Adobe Flash Player.

Источник: <http://www.yarsk.ru/press/?i=100030150> (дата размещения материала 07.05.2015).

Популярный сервис анонимных мнений «Спрашивай.ру» был взломан

По информации, размещенной на сайте internetua.com, в Сети опубликована электронная база с личными данными 6,72 млн. пользователей сервиса «Спрашивай.ру». База записей с пользовательскими данными содержит информацию об электронной почте, имени пользователя, пароле и его IP-адресе. Также в записи может быть указана информация о дате рождения, фамилия, имя, отчество, телефон и ссылки на соцсети пользователя.



Источник: <http://internetua.com/haker-vzlomal-6-72-mln-akkauntov-servisa-anonimnih-mnenii-sprashivai-ru> (дата размещения материала 12.05.2015).

АНБ планировало заразить смартфоны шпионской программой через Google Play

Как сообщил ряд сайтов, АНБ США планировало заражать смартфоны вирусной шпионской программой, перехватывая интернет-трафик онлайн-магазинов Google и Samsung. План взлома смартфонов под кодовым названием «Irritant Horn» был разработан американскими спецслужбами совместно с членами объединения «Five Eyes» («Пять глаз»), в которое, помимо США, входят Великобритания, Новая Зеландия, Канада и Австралия.



Анализ трафика должен был осуществляться через специальный сервер с базой данных XKeyscore, отслеживающий запросы смартфонов к серверам онлайн-магазинов этих компаний, а затем «модифицирующий» их, чтобы отправлять на мобильные устройства шпионские программы под видом полученных от Google и Samsung данных. С помощью этих программ можно было получить полный список контактов, а также установить местонахождение устройства.

Источники: <http://www.pcweek.ru/security/article/detail.php?ID=174681> (дата размещения материала 22.05.2015); <http://informing.ru/2015/05/21/anb-hotelo-zarazit-smartfony-shpionskim-virusom.html>.

Перехват DNS мог привести к утечке данных Федерального резервного банка США

По информации сайта tavasardze.lv, совершена кибератака на сайт Федерального резервного банка США. Злоумышленники осуществили перехват DNS и перенаправили на поддельную web-страницу пользователей, которые пытались перейти на сайт банка. Целью при этом был перехват трафика, в том числе учетных данных.



На официальном сайте Федерального резервного банка представлены, в основном, архивные экономические данные, используемые для исследований. Несмотря на низкую чувствительность подобных данных, руководство банка приняло дополнительные меры безопасности – всем пользователям ресурса предложено сменить пароль своей учетной записи.

Источник: <http://ru.tavasardze.lv/perexvat-dns-mog-privesti-kutechkedanyx-federalnogo-rezervnogo-banka-ssha/> (дата размещения материала 20.05.2015).

Компьютерные сети американских спутниковых и космических программ подвергаются хакерским атакам

Согласно сообщению сайта iksmedia.ru, министерство обороны США распространило данные о проблемах кибербезопасности Космического командования ВВС США. Хакерские атаки организуются из всех уголков мира и за ними стоят самые разные силы: от спонсируемых государствами кибершпионских



подразделений и профессиональных преступников, преследующих корыстные цели, до хакеров-любителей, которым просто интересно попробовать себя. Речь идет о миллионах атак.

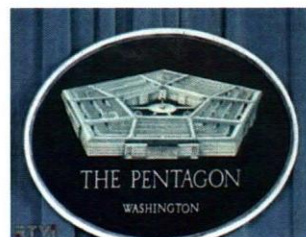
Источник: <http://www.iksmedia.ru/news/5209786-Kompyuternye-seti-amerikanskix-sput.html> (дата размещения материала 30.04.2015).

Атака российских хакеров на сеть Пентагона

Согласно информации сайта Interfax.ru со ссылкой на министра обороны США, российские хакеры проникли в незасекреченную сеть Пентагона. Информация о взломе была рассекречена недавно и ранее не была доступна общественности. Атаку удалось быстро обнаружить.

Сотрудники службы информационной безопасности Пентагона установили, что хакеры действовали с территории России, а затем закрыли им доступ к сети, минимизировав риск повторного вторжения. В начале апреля российских хакеров уже заподозрили во взломе сети Белого дома.

Источник: <http://www.interfax.ru/world/438202> (дата размещения материала 24.04.2015).



Хакеры ИГИЛ готовятся к кибервойне с США и Европой

По данным сайта securitylab.ru, происламистские хакеры из ИГИЛ готовятся к кибервойне с Европой, США и Австралией. По мнению экспертов, среди террористов ИГИЛ достаточно много умелых хакеров, способных взломать компьютерные системы объектов критических инфраструктур по всему миру. В их число входит и группировка под названием «Киберхалифат», которая называет себя «защитниками Исламского государства в Интернете».

Источники: <http://www.securitylab.ru/news/472959.php> (дата размещения материала 19.05.2015).



Хакер из ИГИЛ взломал сайт Министерства миграции, труда и молодежи Кыргызстана

На сайте gambler.ru размещена информация о взломе сайта министерства миграции, труда и молодежи Кыргызстана «mz.gov.kg». Просто взломать пароли хакерам было мало, поэтому они разместили на сайте весьма вызывающий видеоролик. Из содержания послания стало известно, что хакер, взломавший сайт, является членом исламистской террористической группировки Исламское государство. Кроме того, киберпреступник заявил, что готов



взломать еще много сайтов, чтобы сообщить всему миру о важности ислама.

Источники: <http://news.rambler.ru/30133683/> (дата размещения материала 04.05.2015).

Хакерская атака на МИД Саудовской Аравии

По информации ряда сайтов, хакеры «Электронной армии Йемена» проникли в сеть министерства иностранных дел Саудовской Аравии. В руки хакеров попали тысячи секретных документов арабских дипломатов, некоторые из которых уже опубликованы в Интернете.



Преступники выкрали секретные телеграммы, информацию о структуре министерства, досье на десятки сотрудников министерства, а также членов королевской семьи.

Источники: <http://riafan.ru/286697-hakeryi-husityi-vyikrali-sekretnuyu-informatsiyu-mid-saudovskoy-aravii> (дата размещения материала 23.05.2015); http://rian.com.ua/world_news/20150523/367939479.html; <http://russian.rt.com/article/93319>; <http://ru.tavasardze.lv/uchastniki-yemen-cyber-army-pronikli-v-kompyuternye-seti-pravitelstva-saudovskoj-aravii>.

Сирийские хакеры снова атаковали «Washington Post»



Как сообщает портал securitylab.ru, хакеры «Сирийской электронной армии» взломали мобильную версию сайта «Washington Post» с целью размещения антиамериканских лозунгов. Для осуществления атаки на «Washington Post» хакеры вначале взломали системы партнера издания, контент-провайдера «Instart Logic».

Источник: <http://www.securitylab.ru/news/472935.php> (дата размещения материала 14.05.2015).

Зафиксирована шпионская кампания против украинского правительства

На сайте securitylab.ru опубликованы подробности шпионской кампании «Operation Armageddon», организаторы которой похищали конфиденциальную информацию у украинского правительства. При этом нападение, по данным специалистов, длилось не менее двух лет.



Первая активность организаторов «Operation Armageddon» была зафиксирована в середине 2013 г. С тех пор целями злоумышленников становилось как украинское правительство, так и местные правоохранительные органы, а также некоторые высокопоставленные военнослужащие.

Источник: <http://www.securitylab.ru/news/472769.php> (дата размещения материала 29.04.2015).

Взломан сайт министерства финансов Украины

По данным сайта ria.ru, хакеры из группировки «Кибер-Беркут» заявили о том, что им удалось взломать компьютерную сеть департамента внешнего долга министерства финансов Украины. Документы, оказавшиеся в распоряжении хакеров, содержат информацию о структуре государственного долга Украины, стоимости его обслуживания и графики погашения.



Источник: <http://ria.ru/world/20150523/1066118678.html#ixzz3bE84gsYa> (дата размещения материала 23.05.2015).

Азиатские страны пять лет находятся в киберосаде

Как сообщает сайт d-russia.ru, специалисты «Лаборатории Касперского» в ходе изучения одной из самых активных кибершпионских кампаний выяснили, что военные и общественные организации в 11 странах Юго-Восточной Азии уже на протяжении пяти лет страдают от кибершпионажа.

В частности, злоумышленники шпионят за компаниями на Филиппинах, в Малайзии, Камбодже, Индонезии, Вьетнаме, Мьянме, Сингапуре, Непале, Таиланде, Лаосе и Китае.

В арсенале создателей шпионского ПО Naikon – 48 команд для различных удаленных операций, в том числе на проверку данных, находящихся в атакуемой корпоративной сети, выгрузку и загрузку файлов, установку дополнительных модулей.



Киберпреступники сумели создать очень гибкую инфраструктуру, которая может быть легко развернута в любой стране и позволит перенаправлять информацию из систем жертв на сервер злоумышленников. Кроме того, получение необходимых данных упрощается благодаря наличию выделенных операторов, которые «занимаются» определенным кругом пользователей.

Источник: <http://d-russia.ru/odinnadcat-aziatskix-stran-uzhe-5-letnaxodyatsya-v-kiberosade.html> (дата размещения материала 14.05.2015).

Активисты «Anonymous» похитили персональные данные сотрудников Всемирной торговой организации

По данным сайта securitylab.ru, участники движения «Anonymous» осуществили атаку на Всемирную торговую организацию (ВТО) и похитили базу данных, содержащую сведения о тысячах ее сотрудников по всему миру. Для взлома сайта ВТО была применена простая SQL-инъекция. Как оказалось, ресурс содержал большой объем информации – свыше 53 тыс. имен пользователей, номеров телефонов и т.д.

Среди похищенной информации исследователи обнаружили базу данных сайта, а также логины, пароли, полные имена и фамилии, телефонные номера, электронные адреса и заголовки электронных писем 58 пользователей сайта с правами администратора. В другой таблице содержались персональные данные еще 34 администраторов. Хакеры получили большой объем данных руководства и сотрудников организации по всему миру (в общей сложности свыше 2100 человек).



Источник: <http://www.securitylab.ru/news/472809.php> (дата размещения материала 05.05.2015).

Активисты «Anonymous» взломали базу данных online-сервиса по продаже билетов «Best Union»

Как сообщает сайт tavasardze.lv, «Anonymous Italy» продолжают осуществлять кибератаки на компьютерные системы участников выставки «Expo 2015 Universal Exposition». Последней жертвой активистов стал сервис по продаже билетов компании «Best Union».

В ходе атаки на компьютерную сеть компании активисты «Anonymous» похитили базу данных, которая содержалась на сервере, используемом «Best Union». База данных включает информацию о пользователях, которые приобрели билеты online. Судя по всему, пароли пользователей хранились в виде простого текста.



Помимо DDoS-атак, активисты атаковали web-сайт radiglioneitaliaexpo2015 и успешно подменили главную страницу ресурса на свою. В намерение участников «Anonymous» не входило причинение ущерба простым пользователям, но не исключено, что похищенные данные могут попасть в руки мошенников, которые используют их в менее благовидных целях.

Источник: <http://ru.tavasardze.lv/expo-2015-aktivisty-anonymous-vzломали-bazu-dannyx-online-servisa-po-prodazhe-biletov-best-union/> (дата размещения материала 20.05.2015).

Аналитики «ESET» раскрыли крупную атаку на веб-серверы

На сайте anti-malware.ru размещена информация об обнаружении аналитиками компании «ESET» крупной атаки на веб-серверы. Злоумышленники использовали вредоносную программу семейства Linux/Mumblehard. Ее компоненты представляют собой скрипты на языке Perl, зашифрованные и упакованные внутри исполняемого ELF-файла.



Программа предназначена для предоставления атакующим полного доступа к скомпрометированной системе (бэкдор) и рассылки спама. При этом использовались либо набор эксплойтов для

популярных систем управления сайтами Joomla и Wordpress, либо пиратские версии программы DirectMailer для Linux и BSD, устанавливающие бэкдор Mumblehard.

Источник: <http://www.anti-malware.ru/news/2015-05-19/16147> (дата размещения материала 19.05.2015).

Хакерская атака на «SendGrid»

По данным сайта threatpost.ru, совершена хакерская атака на поставщика почтовых веб-услуг компанию «SendGrid». Согласно заявлению руководства компании, злоумышленники скомпрометировали учетную запись одного из сотрудников «SendGrid» и использовали ее для получения доступа к другим системам, в которых хранятся данные клиентских и корпоративных аккаунтов, а также списки электронных адресов, с которыми работают клиенты компании.



Хакерам также удалось получить доступ к базам клиентов почтового сервиса и контактной информации их адресатов. В настоящее время ее почтовый сервис насчитывает 180 тыс. подписчиков, в том числе таких, как «Airbnb», «Foursquare», «Spotify» и «Uber», и ежемесячно отправляет 14 млрд. писем.

Источники: <https://threatpost.ru/2015/04/29> (дата размещения материала 29.04.2015).

Взлом сайта на WordPress с помощью комментария

Согласно информации сайта хакер.ru, финский хакер осуществил взлом платформы WordPress. Для проведения атаки использовалась критическая уязвимость, затрагивающая встроенную систему публикации комментариев WordPress, которая до сих пор широко используется на многих сайтах.

Оказывается, если опубликовать достаточно длинный комментарий (64k символов), то можно вызвать ошибку, которая приводит к исполнению постороннего кода с этой HTML-страницы. Код будет исполнен для каждого, кто зайдет на страницу с таким комментарием, в том числе на компьютере администратора системы, установив в системе бэкдор.



Источники: <https://xakep.ru/2015/04/28/wordpress-comments-bug> (дата размещения материала 28.04.2015).

Хакеры используют набор эксплойтов Fiesta для заражения машин на базе Windows

По данным сайта playground.ru, одна из хакерских группировок вновь использует набор эксплойтов Fiesta для инфицирования компьютеров под управлением операционной системы Windows. На этот раз злоумышленники применяют сложную систему, затрудняющую обнаружение эксплойтов.

В настоящее время группа хакеров использует для инфицирования шлюз, пропускающий трафик со взломанных web-сайтов на вредоносный домен Fiesta. Все доменные шлюзы зарегистрированы китайским регистратором «bizcn» и привязаны к единственному IP-адресу.



По мнению специалистов в области информационной безопасности, пользователям будет нелегко отследить вредоносный трафик со скомпрометированных группировкой интернет-ресурсов.

Чаще всего, HTTP GET-запросы к доменному шлюзу возвращаются с ошибкой 404 Not Found. В некоторых случаях доменный шлюз может вообще не появиться в трафике.

Источник: <http://www.playground.ru/blogs/other> (дата размещения материала 29.04.2015).

Киберпреступники использовали Dropbox для распространения макровирусов

По сообщению сайта comss.info, обнаружена мошенническая кампания на сеть Палаты автоматизированных расчетов США, которая используется многими предприятиями для электронного перевода средств. Злоумышленники использовали облачное хранилище сервиса Dropbox для хранения и распространения макровирусов Bartalex.



Преступники отправляли сообщения, которые содержали ссылку с пометкой «просмотреть полную информацию». При наведении курсора всплывало описание, что это адрес страницы Dropbox с именем файла, имеющим отношение к предполагаемой транзакции АСН. Адрес направлял жертву на страницу «Dropbox» со специальными инструкциями и «очень убедительной» рекомендацией «Microsoft Office» включить выполнение макросов.

При включении макросов вредоносный документ запускал загрузку вредоносного банковского ПО. Атаки хакеров были направлены на ведущие финансовые учреждения США, включая банк «JP Morgan» и «Trend Micro».

Источник: http://www.comss.info/page.php?al=Dropbox_dlja_Rasprostraneniija_makrovirusov (дата размещения материала 30.04.2015).

CareerBuilder используют для рассылки вредоносных резюме

Как информирует сайт itsec.ru, экспертами из «Proofpoint» обнаружена мошенническая кампания, в которой задействован сайт CareerBuilder.com. Злоумышленники рассылают под видом резюме вредоносные документы Microsoft Word.

Когда резюме вносится в список открытых вакансий, сервис «CareerBuilder» автоматически генерирует электронное сообщение работодателю и прикрепляет вредоносный документ, содержащий бэкдор Sheldor. При этом используется вредоносное ПО, эксплуатирующее уязвимость, связанную с повреждением памяти в Microsoft Word RTF. Программа создана при помощи преступного подпольного сервиса Microsoft Word Intruder Service.

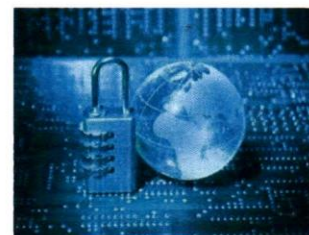


Источник: http://www.itsec.ru/newstext.php?news_id=104842 (дата размещения материала 07.05.2015).

*Группа злоумышленников осуществила атаку
на один из серверов «EllisLab»*

По данным сайта securitylab.ru, группа злоумышленников осуществила атаку на один из серверов компании «EllisLab». Злоумышленники получили доступ к серверу компании, используя похищенные учетные данные администратора, а затем загрузили PHP-бэкдор.

Хостинг-компания «Nexcess» быстро обнаружила и заблокировала атаку, однако хакеры имели доступ к серверу еще в течение трех часов. Злоумышленники могли получить доступ к пользовательской информации – именам, адресам электронной почты, паролям, а также к платежным данным, включая имя, адрес выставления счетов и последние четыре цифры номера кредитной карты. Компания порекомендовала пользователям сменить свои пароли.



Источник: <http://www.securitylab.ru/news/472857.php> (дата размещения материала 07.05.2015).

*Утечка данных карт клиентов
элитного отеля США*

По данным сайта iksmedia.ru, обнаружен факт утечки данных банковских карт клиентов крупного отеля «Hard Rock Hotel», расположенного в г. Лас-Вегасе в США. Под угрозой оказались все, кто побывал в отеле или развлекательном центре в период с 3 сентября 2014 г. по 4 апреля 2015 г.

Источник: <http://www.iksmedia.ru/news/5210807-Obnaruzhena-utechka-dannyx-kart-kli.html> (дата размещения материала 05.05.2015).



*Жертвами утечки конфиденциальных данных стали
более двух миллионов пользователей*



Согласно информации, размещенной на сайте securitylab.ru, сервис mSpy был взломан. Жертвами утечки учетных и других конфиденциальных данных стали более 2 млн. пользователей. Огромный объем данных похищен злоумышленниками с сервера компании.

Доступ хакерами был получен к учетным записям более чем 400000 пользователей, а также их Apple ID, геолокационным данным и деталям около 145000 транзакций.

Источник: <http://www.securitylab.ru/news/472936.php> (дата размещения материала 15.05.2015).