СОЦІАЛЬНІ МЕРЕЖІ ЯК ЧИННИК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Огляд інтернет-ресурсів
(16.09–2.10)

2016 № 11

Соціальні мережі
як чинник інформаційної безпеки

Інформаційно-аналітичний бюлетень
Додаток до журналу «Україна: події, факти, коментарі»
Огляд інтернет-ресурсів
(16.09–2.10)
№ 11

Засновники:
Національна бібліотека України імені В. І. Вернадського
Служба інформаційно-аналітичного забезпечення
органів державної влади (СІАЗ)

Відповідальний редактор
Л. Чуприна, канд. наук із соц. комунікацій

Упорядник
І. Терещенко

Заснований у 2011 році
Виходить двічі на місяць

Київ 2016

ЗМІСТ

РОЗВИТОК І ПЕРСПЕКТИВИ СОЦІАЛЬНИХ МЕРЕЖ

18.09.2016
Viber теперь умеет звонить и отправлять сообщения с помощью Siri

Мессенджер Viber обновил свое приложения для iOS, добавив в него несколько интересных функций. В списке изменений версии 6.3.1 значится поддержка голосового ассистента Siri, оптимизация расхода памяти, интеграция с функциями iOS 10, а также обновление пользовательского интерфейса (IGate).

Теперь сервисом Viber на iPhone или iPad можно будет управлять при помощи виртуального помощника. Это означает, что для отправки сообщений достаточно будет продиктовать Siri нужный текст и сказать, кому именно его отправить. Кроме того, отвечать на звонки можно даже без разблокировки устройства.

Из других изменений стоит отметить, интеграцию мессенджера с приложением Телефон. Теперь звонки внутри сервиса будут отображаться на экране Apple-устройств как обычный звонок в привычном интерфейсе платформы. История звонков Viber также будет интегрирована с интерфейсом iOS 10.

***

16.09.2016
В «ВКонтакте» исчезли аудиозаписи пользователей

Одни пользователи жалуются на исчезновение всех аудиозаписей, у других сохранилась часть треков. Из мобильных приложений также исчезли все добавленные аудиозаписи, а из сообществ пропали разделы с музыкой (Экономические известия).

Проблемы с доступом к аудиозаписям наблюдались вечером 15 сентября в социальной сети «ВКонтакте». На это указывают многочисленные жалобы пользователей.

Трудности появляются при попытке захода на страницу с помощью компьютера, при этом через мобильное приложение на базе Android плей-листы доступны. Кроме того, музыку можно было послушать в записях личных страниц и сообществ.

Одни пользователи жалуются на исчезновение всех аудиозаписей, у других сохранилась часть треков. Из мобильных приложений также исчезли все добавленные аудиозаписи, а из сообществ пропали разделы с музыкой.

Проблема вызвала волну негативных комментариев по этому поводу.

Представитель «ВКонтакте» подтвердил, что компания в курсе сбоя и работает над его устранением.

12 сентября «ВКонтакте» вернула раздел с музыкой в обновленной версии приложения для iOS. Это стало возможным благодаря подписанию соглашения о лицензировании контента с крупнейшими мировыми звукозаписывающими компаниями – Universal Music Group, Warner Music Group и Sony Music Entertainment.

***

20.09.2016

Twitter перестав враховувати картинки та посилання в ліміті довжини повідомлень

Сервіс мікроблогів Twitter з 19 вересня перестав враховувати фотографії, відео, gif-файли та посилання при підрахунку символів у повідомленнях (Espreso.tv).

Про це повідомили в компанії Twitter.

Також обмеження більше не стосуються цитат і опитувань.

«Таким чином у користувачів з'явиться ще більше можливостей для самовираження та спілкування один з одним», – зазначили в компанії.

***

21.09.2016

«ВКонтакте» запустила сервис игровых видеотрансляций

Социальная сеть «ВКонтакте» объявила о запуске собственной платформы для стриминга видеоигр. Пользователи получат возможность прямо на сайте наблюдать за игровым процессом, обсуждать его с друзьями и подписчиками в режиме реального времени, а авторы трансляции – зарабатывать на пожертвования и показах рекламы (InternetUA).

«Трансляция "ВКонтакте" выглядит как обычная видеозапись: её можно отправить личным сообщением, добавить к себе на страницу или в сообщество, поделиться с друзьями и подписчиками, а также встроить на внешний сайт», – сказали разработчики. Пользователям, подписавшимся на страницу трансляции, придет уведомление сразу после ее начала.

Киберспортсменам и поклонникам видеоигр «ВКонтакте» предлагает два способа заработка: путем приема пожертвований от зрителей (стимера можно финансово поддержать, нажав на соответствующую кнопку под плеером) и показа рекламы перед началом видео.

***

21.09.2016

У Viber 800 млн пользователей

Viber – одно из ведущих приложений для общения – продолжает глобальное развитие. Количество зарегистрированных пользователей мессенджера в мире уже преодолело отметку в 800 млн (ITnews).

«Сегодня мы наблюдаем стремительное развитие мессенджеров и активный рост спроса на них. Причем связать это можно как с распространением мобильного Интернета по всему миру и увеличением количества пользователей смартфонов, так и с расширением функционала самих приложений, – отметил Е. Рощупкин, глава Viber в России и странах СНГ. – Как один из лидеров рынка Viber учитывает эту глобальную тенденцию. Россия и страны СНГ являются для нас ключевыми рынками и приоритетными площадками для запуска стратегически важных проектов. Постоянно улучшая наш сервис, сегодня мы готовим к выходу на рынок новые, интересные и полезные функции для наших пользователей, в том числе, – для корпоративных».

***

21.09.2016
Microsoft удалит старые версии Skype

Компания Microsoft закрыла лондонское подразделение Skype, в результате чего 200 сотрудников остались без работы (U-News).

Как сообщает источник издания, это сделано из-за того, что цифровой гигант из Редмонда работает над новым приложением Skype for Life, которое заменит все ныне существующие разновидности мессенджера. И все работы по этому приложению Microsoft собирается сосредоточить в штаб-квартире в Редмонде.

Сегодня существует огромное количество версий мессенджера для разных ОС для использования на ПК и смартфонах, а также веб-версия. Но новый Skype for Life станет унифицированным приложением, которое заменит весь этот «разнобой».

Утилита разрабатывается наряду с Skype Team (аналог Slack) и Skype for Business. Но после создания станет основным клиентом для Microsoft, поэтому остальным приложениям будет уделяться минимум внимания.

К сожалению, эти данные пока что не подтверждены официально Microsoft, поэтому сказать точно, насколько они правдивы, нельзя.

***

22.09.2016
В личной переписке «ВКонтакте» появились голосовые сообщения

Социальная сеть «ВКонтакте» добавила возможность отправки аудиосообщений в личной переписке пользователей. В официальном блоге компании отмечается, что новый способ общения, в первую очередь, будет

удобен тем, кто любит живые разговоры и хочет сэкономить время на переписке (IGate).

Для отправки аудиосообщения в нижнем правом углу мобильных приложений и прямо в поле ввода сообщений в веб-версии соцсети появилась кнопка в виде микрофона, которую нужно зажать, чтобы записать послание.

Сделать запись можно на любом устройстве: новая функция была реализована как для настольных компьютеров, так и в мобильных приложениях VK App для Android, Windows Phone, а в ближайшее время выйдет и для iOS.

***

21.09.2016

Ольга Карпенко

Google представил конкурента WhatsApp и Telegram – мессенджер Allo

Компания Google запустила мессенджер Allo – его уже можно скачать в Google Play и App Store. Как и большинство современных мессенджеров, он умеет пересылать картинки и стикеры, работает с групповыми чатами и т. д. Одно из его основных отличий – интегрированный Google Assistant, с которым можно общаться в виде чатбота. Чтобы начать говорить с ним, достаточно ввести @google (AIN.UA).

С его помощью можно строить планы с друзьями – достаточно добавить бота в групповой чат, и он подскажет данные о близлежащих ресторанах, времени сеансов кино, проложит маршрут, подскажет погоду, найдет смешное видео или картинку и т. д.

Еще одна из функций мессенджера – Smart Reply. Она призвана сэкономить время и работает на том, что приложение анализирует ответы пользователя и затем выдает подсказки, базируясь на том, какие выражения пользователь употребляет чаще. Эта функция на русском пока недоступна.

В мессенджере по умолчанию сообщения не шифруются (как в WhatsApp), но можно включить режим инкогнито. Это защитит чат с помощью сквозного шифрования, даст возможность использовать скрытые оповещения и выбирать срок хранения сообщений.

Как и во многих мессенджерах сегодня, в Allo можно пересылать картинки, добавляя на них свои рисунки или текст. А еще здесь упростили возможность поорать на собеседника капсом: увеличить шрифт сообщения можно одним движением пальца.

Отзывы на приложение в основном пока что нейтральные и положительные, но есть и немного дегтя. Первые пользователи жалуются на то, что приложение в отличие от конкурентов не поддерживает видеочаты, в нем нет встроенной поддержки GIF и т. д. Также, судя по всему, мессенджер не очень любит синхронизацию.

Компания анонсировала мессенджер еще в мае этого года, на конференции для разработчиков Google I/O. Мессенджер вышел как раз перед

следующим большим релизом от Google – новой линейкой смартфонов, которую покажут 4 октября.

***

26.09.2016

Google собирается стереть границы между мессенджерами

Главным неудобством современных мессенджеров является тот факт, что их чрезвычайно много, и собрать всех друзей и родственников в одном сервисе просто невозможно. Так получается, что большинство владельцев смартфонов используют сразу несколько мессенджеров для поддержания связи со всеми людьми из своего круга общения. Компания Google же решила исправить эту ситуацию, предложив глобальное решение (IGate).

Поисковый гигант разработал функцию App Preview Messaging, которая позволяет отправлять сообщения абонентам в любой мессенджер, который бы они не использовали.

К примеру, если вы отправили владельцу Android-устройства сообщение через WhatsApp, а у него он не установлен, то человек все равно получит ваше сообщение и сможет на него ответить при помощи App Preview Messaging, а вы получите сообщение обратно в WhatsApp. В уведомлении ему также будет предложено установить сервис, который вы использовали.

App Preview Messaging будет входить в пакет сервисов Google Play, в связи с чем работать функция будет в полной мере только между Android-устройствами, тогда как с iOS можно будет лишь отправлять сообщения.

***

26.09. 2016

Базиленко Анна

Facebook Messenger додав опитування та пришвидшив доступ до грошових переказів

Facebook запустив опитування в групових обговореннях у Messenger. Як пише VentureBeat, випробувати на собі нововведення поки що зможуть лише користувачі додатку в США (Watcher).

У компанії обіцяють, що часових обмежень щодо тривалості опитувань не буде. Створити нове опитування зможе кожен учасник обговорення. Для цього потрібно натиснути на кнопку «Poll» у вікні повідомлення або ж натиснути на «More» і обрати «Poll». Користувачі, які проживають за межами США, будуть бачити опитування, але взяти участь у них не зможуть.

Компанія також презентувала ще одне нововведення в Messenger – це швидкий доступ до грошових переказів. Відтепер технологія машинного навчання Facebook аналізуватиме зміст і значення слів у повідомленнях у межах додатку. Якщо система «побачить», що користувач хоче перевести кошти, вона активує відповідну функцію.

***

28.09.2016
YouTube можно будет смотреть в оффлайн

Компания Google решила прислушаться к многочисленным просьбам пользователей мобильных устройств, жаловавшихся на недоступность видеоконтента с YouTube в оффлайн-режиме. Новое приложение под названием YouTube Go даст возможноть сохранять видео для отложенного просмотра, даже если в тот момент вы не будете находится в сети. К сожалению, пока что сервис доступен только жителям Индии (IGate).

«YouTube Go спроектирован и вырос с оглядкой на Индию. Для того чтобы донести жителем этой страны всю прелесть нашего сервиса, были учтены местные особенности интернет-покрытия и работы сети», – говорится в официальном заявлении компании.

Приложение позволяет выбирать качество ролика при скачивании, а также при необходимости быстро передать его на другой телефон при помощи Bluetooth.

В настоящее время Google набирает участников для тестирования приложения. Точная дата релиза в Индии, а также в других странах мира пока не оглашалась.

***

28.09.2016
В WhatsApp появилась возможность делиться ссылками на группы

Если вы являетесь активным пользователем WhatsApp и для общения часто используете группы, то знаете, как проблематично бывает пригласить нового участника, когда вы не являетесь администратором, или как сложно собрать большое количество людей вместе, не зная контактов каждого. Новая функция должна решить эти проблемы раз и навсегда. В последней бета-версии WhatsApp появилась возможность делиться ссылками на группы. Это значит, что вы можете разослать необходимым контактам ссылку, нажав на которую, они автоматически присоединятся к группе (InternetUA).

Если вам нужно собрать большое количество людей, контактов которых у вас нет, то ссылку можно представить в виде QR-кода и распечатать его. Также имеется возможность создать NFC-метку, при контакте с которой пользователи смогут вступить в группу.

Подобное нововведение может быть полезно при организации мероприятий. Например, если вы хотите устроить вечеринку с привлечением незнакомых людей, то можно напечатать и расклеить QR-коды по городу, а затем обсудить все детали в группе в WhatsApp.

На сегодня новая функция доступна только в бета-версии WhatsApp.

***

29.09.2016

Facebook представит собственный аналог YouTube

Facebook опубликовала вакансию директора по лицензированию музыки. В его задачи будет входить ведение переговоров с музыкальными лейблами и издателями. Также он будет участвовать в создании собственного сервиса компании. Кандидат должен обладать хорошими знаниями в области ведения бизнеса в Интернете (InternetUA).

По мнению источников «Ведомостей» компания планирует создать не музыкальный сервис, а аналог YouTube. Последнее время социальная сеть делает упор на видео, в частности, была введена возможность онлайн-трансляций для пользователей. Также организации могут размещать проморолики в Facebook и Instagram.

Объем рынка видеорекламы в США по данным за 2015 г. составил 9,6 млрд долл. При этом 72 % рекламодателей, опрошенных eMarketer в 2015 г., планировали продвигать свой бренд через YouTube, а размещать рекламу в Facebook хотели только 46 % компаний.

СОЦІАЛЬНІ МЕРЕЖІ ЯК ВИЯВ ФОРМУВАННЯ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА

20.09.2016

Користувачі соцмереж висміяли у фотожабах А. Садового

Мера Львова А. Садового висміюють у соціальних мережах через неспроможність владнати проблему із вивозом сміття зі Львова (ІНФОРМАЦІЙНА АГЕНЦІЯ «ВГОЛОС»).

Про це повідомляє кореспондент «Вголосу».

«Коли Україна ввійде до ЄС, сміття з Львова везтимуть у Париж», – пише на своїй сторінці у Facebook Н. Березовська.

***

22.09.2016

Сепаратисты-живодеры поглумились над Героями Майдана: в сети вспыхнул скандал

Появившееся в сети селфи молодой пары со значками фейковой «Новороссии» на Аллее Героев Небесной сотни в Киеве вызвало гнев пользователей (Обозреватель).

Соответствующую информацию опубликовал на своей странице в Facebook Kostiantyn Bilokha.

Отмечается, что сепаратисты по имени Юра и Люба проживают в Луцке.

«Неужели нам такие нужны?» – задал риторический вопрос автор поста.

Также он опубликовал ссылку на видео, где сепаратисты хвастаются своим жестоким отношением к животным.

Комментаторы гневно отреагировали на наглую выходку молодой пары.

В сообществе «Файний-паблік #FP» на Facebook утверждают, что молодые люди прибыли в Луцк из Луганска.

***

28.09.2016

Аваков про фейкові публікації на своєму Facebook: Ці повідомлення йдуть із російських сайтів

Міністр внутрішніх справ А. Аваков прокоментував фейкові публікації на своєму Facebook. Про це він заявив на брифінгу (112ua).

«Я дуже хочу, щоб мене правильно зрозуміли, а не піддавали професійному тролінгу, тому що я людина доволі стійка до тролінга, і стійкіший за мене до тролінга тільки Луценко. Мені смішно бачити публікацію фотографій з власного Facebook, записів, яких там не існувало. У нас є кіберполіція, яка дивиться, як це з'являється. Ці всі головні меседжі йдуть з російських спеціальних сайтів. Ми дамо цю інформацію у найближчі дні, щоб просто було об'єктивно», – заявив він.

Він додав, що в питанні щодо презумпції правоти поліцейського, про яке він повідомляв раніше, питання не тільки в законодавстві, але і в загальному усвідомленні суспільства.

«Презумпція правоти поліцейського наступна, якщо поліцейський зупинив машину і каже руки на кермо або пред'явіть документи, у відповідь він чує не пішов ти..., а він підпорядковується, а якщо не підпорядковується, поліцейський до нього вживає адекватні заходи із законом, у тому числі застосування електрошокера, вогнепальної зброї... Якщо ми витрачаємо гроші на поліцію, якщо ми даємо їм повноваження, ставимо їм виконувати завдання, давайте кожен зробить своє маленьке обмеження заради ще великої свободи, яка є. Це не обмежує свободи громадян», – пояснив він.

БІЗНЕС І СОЦІАЛЬНІ МЕРЕЖІ

19.09.2016

Акционер Twitter подала в суд на компанию из-за отсутствия обещанного роста популярности сервиса

Владеющая акциями Twitter Д. Шенвик подала судебный иск, в котором обвинила компанию в обмане акционеров. По мнению Д. Шенвик, руководство сервиса не выполнило обещаний по основным показателям роста. Об этом пишет Bloomberg (IGate).

Истец утверждает, что компания не выполнила обещания довести количество пользователей Twitter до 550 млн человек в краткосрочный перспективе, а также до одного миллиарда в долгосрочной, данное в ноябре 2014 г.

У руководства не было никаких оснований для таких расчетов, однако оно предпочло умолчать этот факт, указывается в иске.

Отметим, что на 30 июня текущего года активная аудитория Twitter составляла 313 млн пользователей в месяц.

Д. Шенвик намерена добиться для своего заявления группового статуса. В этом случае истцами по делу станут все акционеры компании, которые приобрели акции Twitter в период с 6 февраля по 28 июля 2015 г.

***

20.09.2016
«ВКонтакте» запустила послугу грошових переказів

Найбільша російська соціальна мережа «ВКонтакте» запустила послугу грошових переказів (Forbes).

Нова послуга буде здійснюватися через особисті повідомлення. Користувачі можуть перевести суму від 100 до 75 тис. рублів зі своїх банківських карт.

Як повідомляє компанія, технічна сторона грошових переказів забезпечується банком ВТБ24, процессингом Mail.Ru Group і «Мультикарта».

«Популярність банківських карт серед користувачів “ВКонтакте” неухильно зростає. На частку цього способу оплати припадає вже половина платежів. Кількість прив’язаних до сторінок банківських карт теж продовжує зростати. У цих умовах “ВКонтакте” як комунікаційна платформа може допомогти користувачам вирішити важливе повсякденне завдання – як передати один одному гроші. Тим більше що ми пропонуємо одні з найкращих умов здійснення грошових переказів з картки на картку в Росії», – заявив директор з електронної комерції соціальної мережі Ю. Іванов.

***

22.09.2016
Facebook купила разработчика электроники Nascent Objects

Facebook приобрела Nascent Objects – компанию по разработке электроники, целью которой является упрощение процесса перехода от простого концепта к полноценному продукту в считанные недели. Финансовые детали сделки не разглашаются, однако Nascent Objects сообщила, что станет

частью экспериментальной программы Building 8, запущенной Facebook в апреле (InternetUA).

«Мы восхищены возможностью создавать продукты, которые могут открыть мир каждому, и творить в том масштабе, которого раньше мы даже представить не могли», – пишет исполнительный директор купленного стартапа Б. Эльмиех (Baback Elmieh). «Люди привыкли к тому, что с помощью программного обеспечения можно получить что угодно и когда угодно. Мы хотим сделать то же самое с аппаратным обеспечением – и мы думаем, что Facebook является лучшим местом для реализации этого».

Nascent Objects, основаная в 2014 г., создала платформу, состоящую из десятков электронных модулей – сенсоров, камер, мини-компьютеров и т. д. Всё это объединяется и превращается в единое целое с помощью 3D-принтеров. Во многом проект напоминает закрытую недавно модульную инициативу Project Ara от Google.

Выгода такого приобретения может быть неочевидна: Facebook в первую очередь известна благодаря своему программному обеспечению, а не аппаратному. Однако тот факт, что Nascent Objects вошла в Building 8, может означать, что компания работает над новым инструментарием для разработчиков Oculus Rift, Open Computer Project или инициатив по обеспечению доступом к Интернету как можно большего количества людей – например, Aquila. К тому же, Building 8 – подразделение под управлением Р. Дуган (Regina Dugan), бывшего директора DARPA и топ-менеджера Google.

Конечно, Nascent Objects может быть полезна и в разработке различного рода прототипов и проведении внутренних тестов. Напомним, что недавно Facebook представила Area 404 – пространство для совместной работы инженеров из различных команд, в котором они могут помогать друг другу в ускорении разработки своих проектов.

***

21.09.2016

Facebook представил динамическую рекламу для ретейлеров

Динамические объявления будут рекламировать товары, которые есть в наличии в ближайших магазинах, и отображать цены товаров в этих магазинах, отмечает likeni.ru. Если товара больше нет в наличии в определенном регионе, объявление перестанет показываться пользователям этого региона. В динамических рекламных объявлениях будет содержаться следующая информация: наличие товара в ближайших магазинах и их расположение; описание товара и вся необходимая информация о нем; действия, которые можно предпринять (связаться с магазином, приобрести товар онлайн); похожие продукты, доступные в ближайших магазинах. Сейчас Facebook тестирует новый рекламный формат, в ближайшие недели он будет доступен более широкому числу рекламодателей (Marketing Media Review).

***

26.09.2016

Издатели газет обвинили Google и Facebook в получении дохода от рекламы в чужом контенте

Британские издатели газет обвинили интернет-гиганта Google и социальную сеть Facebook в получении прибыли от рекламы, которая сопровождает контент изданий, сообщает Adindex.ru (Телекритика).

Так, британская новостная ассоциация News Media Association (NMA) направили письмо британскому правительству, в котором пожаловались на Google и Facebook за то, что они собирают контент газет, переупаковывают его, линкуют и монетизируют.

В Google данные обвинения отвергают, заявив, что сервис Google News не имеет рекламы, а, напротив, помогает изданиям увеличить прибыль за счет дополнительного количества переходов с новостного агрегатора. В Facebook же от комментариев отказались.

***

26.09.2016

Базиленко Анна

Facebook упродовж двох років обдурював рекламодавців щодо тривалості перегляду їхніх рекламних роликів

Останні два роки Facebook завищував ключовий для рекламодавців показник – середню тривалість перегляду рекламних роликів користувачами соцмережі. Ідеться про відхилення від реального показника на 60–80 %, передає The Wall Street Journal (Watcher).

Як з'ясувалось, кілька тижнів тому Facebook повідомив у довідковому центрі для рекламодавців, що показник середньої тривалості перегляду відеореклами компанія штучно завищувала у роликах тривалістю більше трьох секунд. Щоб вирішити цю проблему, компанія ввела нову метрику – «Середня тривалість перегляду». Вона враховує всі перегляди відео, незалежно від їхньої тривалості.

Дізнавшись про це, рекламні агентства звернулися в компанію за поясненнями. Рекламно-комунікаційна компанія Publicis Media розіслала своїм клієнтам лист з поясненнями від Facebook, у якому повідомлялось про те, що попередній метод підрахунку спричинив завищення показників тривалості пергляду відео на 60–80 %. У Facebook вибачились і заявили, що помилку вже виправили, пообіцявши, що на оплату реклами це ніяк не вплине.

Як відомо, влітку 2013 р. Facebook презентував рекламні відео із автозапуском, які з'являтимуться за межами стрічки новин у десктопній версії соціальної мережі. Тоді у компанії планували продати перші «абонементи» на таку рекламу за більш ніж 1 млн дол. кожен.

***

26.09.2016
Сергей Хухаркин
Bloomberg оценил стоимость Twitter в 16,7 млрд долл.

Аналитическое финансовое агентство Bloomberg Intelligence оценило текущую рыночную стоимость Twitter Inc. в 16,7 млрд долл., исключая наличные средства. Как возможные покупатели выступает корпорация Google Inc. и Salesforce.com (HiTech-News.ru).

В публикации агентства указано, что помимо ценных данных Twitter Inc., потенциальному покупателю придется решить вопрос конфликта между руководством и провести оздоровление копании в связи с медленным ростом экономических показателей. Установлено, что текущий исполнительный директор и соучредитель Twitter Inc. Дж. Дорси занимает руководящую должность в Square Inc. и от перехода к новому руководству вполне может отказаться. Согласно прогнозу Bloomberg Intelligence, глобальные стратегические изменения в компании могут повлечь за собой отток кадров.

***

27.09.2016
Google и Disney заинтересовались покупкой Twitter

Один из крупнейших финансовых конгломератов индустрии развлечений в мире компания Disney начала вести консультации по вопросу покупки сервиса микроблогов Twitter, сообщает Bloomberg со ссылкой на источники (Блог Imena.UA).

Ожидается, что сделка позволит увеличить присутствие Disney на рынке цифровых медиа и рекламы. Однако официально в компаниях эту информацию пока не комментируют.

Кроме того, по данным источников CNBC, в списке потенциальных покупателей Twitter находится и интернет-гигант Google. Он также заинтересован в контенте, генерируемом сервисом. В Google эту информации не комментируют.

***

29.09.2016
Технологические гиганты объединились, чтобы создать искусственный интеллект

Amazon, Google, Facebook, IBM и Microsoft объединились, чтобы вместе рассматривать проблемы, связанные с правом на частную жизнь, безопасности и взаимодействия людей и искусственного интеллекта (Источник).

Инициатива называется «Партнерство по искусственному интеллекту». «За весьма короткий промежуток времени произошло очень быстрое развитие

ИИ», – сообщил профессор Й. Банджио из Монреальского университета. «Сотрудничество всех основных компаний, занимающихся развитием ИИ, – лучший способ добиться того, чтобы мы разделяли одни и те же ценности и стремились достичь одних и тех же целей для всеобщего блага», – добавил он.

При этом, в «Партнерстве по искусственному интеллекту» пока не принимает участие Apple, хотя некоторые говорят, что компания, возможно, присоединится к проекту в ближайшем будущем. Партнерство также подчеркивает, что оно не намерено лоббировать никакие правительства или законодательные органы.

***

28.09.2016

Google, Facebook и Apple затеяли дружбу против Amazon и PayPal

Международный интернет-консорциум W3C вместе с Google, Facebook, Apple и другими интернет-гигантами разработал единый глобальный стандарт онлайновых платежей (InternetUA).

Международный индустриальный интернет-консорциум World Wide Web Consortium (W3C) близок к анонсу нового глобального стандарта для проведения онлайновых платежей, сообщает The New York Times. Для разработки единых правил консорциум собрал вместе ведущих интернет-гигантов, таких как Google, Facebook и Apple.

По мнению обозревателей The New York Times, новый платежный стандарт стандарт W3C «столкнется с противостоянием Amazon и PayPal во всем мире, равно как и с мировыми кредитными платежными системами, каждая из которых предпочла бы видеть себя в качестве основного, а не запасного платежного средства в Сети».

Суть нового стандарта интернет-платежей сводится к тому, чтобы обеспечить любому пользователю единый способ ввода данных кредитной карты или платежной системы в любой веб-браузер для совершения любой покупки в Интернете. После однократного ввода данных карты, они автоматически будут вызываться в качестве одного из вариантов совершения онлайновых транзакций. С технической точки зрения это напоминает функцию автозаполнения полей, широко распространенную во многих браузерах, однако по нормам нового стандарта, все поля будут заполняться скрытыми данными по единому клику.

Нынешние гиганты отрасли онлайновых платежей, компании Amazon и PayPal, отказались принимать участие в разработке платежной системы W3C. Помимо отказа от работы с форматом W3C, Amazon и PayPal также намерены «предоставлять альтернативу тем потребителям, которые не хотят вводить платежные детали в свои браузеры».

Безопасность платежей по платежному стандарту W3C будет обеспечиваться тем, что браузер вместо пересылки данных кредитной карты будет отправлять одноразовый маркер оплаты, сгенерированной специально

для этой транзакции. Таким образом предполагается избежать оседания данных кредитных карт в многочисленных базах данных по всему миру.

Конкуренты и недоброжелатели

Как и множество других универсальных платежных интернет-проектов, разработка W3C может потерпеть фиаско в случае отсутствия поддержки со стороны онлайн-продавцов, производителей веб-браузеров и даже потребителей, если им что-то не приглянется в новой платежном стандарте.

Платежный стандарт W3C

Аналитики высказывают определенный оптимизм в отношении нового платежного стандарта W3C – хотя бы потому, что ему не потребуется одобрение со стороны потребителей или онлайн-продавцов. Стандарт заведомо предполагает использование любого существующего способа оплаты с помощью карты или платежного приложения, но через единую площадку, которую большинство покупателей используют и без того: веб-браузер.

Несмотря на возможное противодействие PayPal и Amazon при внедрении альтернатив своим платежным системам, на стороне W3C – мощная команда из более чем 40 крупных международных игроков рынка онлайновой коммерции, включая Apple, Microsoft, Facebook, American Express, и даже китайские онлайновые гиганты Alibaba и Tencent.

Как это работает

В настоящее время разработка нового стандарта интернет-платежей близка к завершению. Так, один из авторов проекта – Google, уже представила соответствующую версию своего браузера Chrome, другие компании также близки к анонсу соответствующих обновлений.

В версии, представленной Google, при нажатии кнопки для совершения онлайновой покупки, открывается дополнительное меню с сохраненными адресами доставки и способами оплаты. Пользователь выбирает адрес и платежную карту, вводит трехзначный секретный код защиты и нажимает кнопку «оплатить сейчас». Другие компании для идентификации могут использовать вместо кода защиты отпечаток пальца.

Сборы от проведения транзакций по-прежнему будут отчисляться соответствующим финансовым институтам – эмитентам кредитных карт и банкам, кроме тех случаев, когда пользователь выбирает в качестве метода платежа Apple Pay или Samsung Pay.

Стандарт платежей W3C также будет востребован по мере развития VR-магазинов, платежей в мессенджерах и платежей между компьютерами (например, когда автономный автомобиль без водителя будет оплачивать стоянку). Новый стандарт также подразумевает легкую интеграцию новых методов совершения платежей – таких как биткойны или китайский провайдер платежей Tencent.

Одним из наиболее заинтересованных в адаптации платежного стандарта W3C игроков рынка является Apple, которая подготавливает для этих целей как новую версию браузера Safari, так и собственную систему Apple Pay. В представленной недавно новой версии операционной системы Apple впервые

поддерживается онлайновый шоппинг с помощью браузера Safari и Apple Pay. Для завершения транзакции через Apple Pay покупателю достаточно пройти идентификацию отпечатка пальца на своем смартфоне.

***

28.09.2016

Kantar: каждый четвертый пользователь активно игнорирует бренды в онлайне

Несмотря на популярность Snapchat и Instagram вместе с длительным успехом Facebook, 26 % респондентов отметили, что игнорируют посты в сетях или рекламу от брендов. Исследование Kantar TNS Connected Life обнаружило, что бренды атакуют многих в социальных сетях, а 34 % чувствуют, что за ними «постоянно следит» онлайн-реклама. Больше всего скептично настроенных пользователей в скандинавских странах, 57 % отметили, что активно игнорируют контент брендов. 15 % в Саудовской Аравии и 19 % в Бразилии также избегают контента брендов. 24 % пользователей в Китае и 26 % в Южной Африке игнорируют бренды в сетях, как в целом в мире. Исследование обнаружило, что блокировка рекламы широко распространена в Польше (51 %), что намного выше среднего показателя в мире – 18 %. По мнению глобального директора Kantar TNS «Instagram и Snapchat умело используют желание пользователей к мгновенному, развлекательному контенту от друзей и лидеров мнений, часто улучшенное смешными фильтрами и редактированием. Это настоящая возможность для брендов приобщиться к этому тренду, создавая персонализированный контент, такой как видео и истории. Сложность состоит в том, как сфокусироваться на правильном контенте для правильных людей, на правильных платформах и в нужный момент. Некоторые бренды, такие как Disney, Starbucks попадают в цель. Они использовали фильтры Snapchat таким образом, чтобы не надоедать пользователям. В этом ключ, как преодолеть негативное восприятие активности бренда в онлайне». В настоящее время почти четверть (23 %) интернет-юзеров сейчас в Snapchat, по сравнению с 12 % два года назад. Instagram также увеличил аудиторию – до 42 % с 24 % в 2014 г. (Marketing Media Review).

***

28.09.2016

Базиленко Анна

Кількість рекламодавців у Facebook перевищила 4 млн

Кількість компаній, які активно купують рекламу у Facebook, перевищила 4 млн. Про це повідомляє MarketingLand. Як пише видання, у березні ця цифра становила 3 млн активних рекламодавців (Watcher).

Лише минулого місяця 20 % рекламодавців розмістили у Facebook відеорекламу, 40 % створили рекламне оголошення за допомогою телефона або планшета.

Більше 70 % компаній, які розміщують рекламу у Facebook, знаходяться за межами США. За останній рік найбільший приріст кількості рекламодавців зафіксований в таких країнах, як США, Бразилія, Мексика, Великобританія та В'єтнам.

Минулого тижня Instagram оприлюднив власні відомості. З'ясувалось, що 500 тис. активних рекламодавців щомісяця розміщують рекламу в Instagram. Натомість, як зазначає MarketingLand, головний конкурент Facebook – Google – уже давно нічого не повідомляв про рекламодавців, які купують рекламу в компанії.

***

29.09.2016

Facebook и Всемирный банк объединились для сбора и анализа данных

Компания Facebook объединилась со Всемирным банком и Организацией экономического сотрудничества и развития (ОЭСР) для выработки нового способа сбора и анализа данных, который позволит быстрее узнать настроение рынка. Кроме того, новая технология будет дешевле той, что есть на сегодняшний день (InternetUA).

28 сентября, благодаря усилиям представителей всех трех организаций, была запущена новая технология аналитики рынка. Для сбора данных используются страницы организаций, зарегистрированных в Facebook, пишет The Wall Street Journal.

Технологию тестировали с февраля этого года, информацию по 15 различным запросам предоставляли 90 тыс. представителей малого и среднего бизнеса из 22 стран. С помощью опросов представители организаций пытались выяснить, какие факторы влияют на развитие мелких предпринимателей. Ранее это требовало большого количества времени и денег, а также множества личных встреч с экспертами рынка.

Благодаря Facebook Всемирный банк и ОЭСР получили доступ к подробной информации об экономической ситуации в различных странах.

***

1.10.2016

Корпоративная соцсеть Facebook at Work может быть запущена в ближайшее время

Ещё в январе 2015 г. Facebook начала бета-тестирование бизнес-ориентированной социальной сети Facebook at Work. И вот, согласно данным

источников изданий The Information и TechCrunch, компания, наконец, довела свой проект до ума и приготовилась к запуску соцсети (InternetUA).

Сообщается, что доступ к Facebook at Work для всех желающих будет открыт уже в ближайшие недели. Примечательно, что Facebook решила отказаться от фиксированной платы для компаний, желающих внедрить социальную сеть в рабочий процесс. Вместо этого организациям будет предложено платить за каждого активного пользователя. Facebook остановилась на такой модели потому, что она верит в то, что ей удастся заинтересовать отдельных пользователей, при этом организациям не придётся переплачивать за использование соцсети в том случае, если, к примеру, в каких-то отделах она не приживётся.

СОЦІАЛЬНІ МЕРЕЖІ І ПРОБЛЕМИ СУСПІЛЬНОЇ БЕЗПЕКИ

Інформаційно-психологічний вплив мережевого спілкування на особистість

18.09.2016
Соцмережі помітно погіршують якість роботи персоналу – вчені

Норвезькі вчені поставили перед собою завдання вивчити, як впливають соцмережі на якість роботи офісних працівників. Виявилося, що дуже негативно (Голос українською).

Причиною зниження продуктивності служить те, що більшість конторських працівників значну кількість часу проводить у соцмережах у своїх особистих цілях. Для того, щоб прийти до такого висновку, психологами було опитано близько 11 тис. респондентів, які займають різні посади в різних офісах. Виявилося, що з кожних п’яти учасників четверо використовують службовий Інтернет для власних потреб.

При цьому співробітники молодого віку роблять це набагато частіше за своїх старших колег, а ті, що мають більш високий рівень освіти витрачають на особисті потреби в Інтернеті більше часу, ніж менш освічені. Особливо відрізняються інтернет-активністю «для себе» холостяки та керівники високого рангу, вони бояться втратити через це свою роботу менш ніж інші.

Керівний склад прекрасно знайомий з такими діями своїх підлеглих і намагається з цим боротися. Як один із заходів є збільшення інтенсивності праці та кількості завдань, які ставляться перед працівником.

***

27.09.2016

Ученые рассказали, как «лайки» в соцсетях влияют на человека

Некоторые пользователи готовы на все, чтобы собрать как можно больше «лайков» (отметок «Мне нравится») в социальных сетях. Судя по всему, это говорит о серьезной проблеме. Новое исследование показало: у людей, считавших «лайки», часто отсутствовала цель в жизни (GoGoNetNews).

Специалисты проанализировали данные 250 пользователей Facebook. Участники ответили на вопросы о самооценке и смысле жизни. Исследователи обнаружили, что многие добровольцы, у которых самооценка зависела от их популярности на Facebook, не имели цели в жизни. Такие люди очень расстраивались, когда собирали мало «лайков».

Ученые добавляют: попытки сделать селфи, которое понравится другим, могут привести к несчастному случаю. Кстати, когда подростки видят большое количество «лайков» под своими фотографиями или фото сверстников, в их мозге активируются те же нервные цепи, что и при употреблении шоколада. Это выяснили исследователи из Калифорнийского университета.

***

30.09.2016

Психологи выяснили что у большинства пользователей Facebook низкая самооценка

Психологи выяснили, почему некоторые пары используют сайты социальных сетей как платформу, с которой заявляют всему миру о своей вечной любви к друг дружке. Многих такое слащавое проявление любовных чувств раздражает. Этот вопрос заинтересовал исследователей Олбрайт-колледжа (PerCare).

Первоначальной версией ученых было предположение, что так неуверенные в своих отношениях пары компенсируют свои страхи быть отвергнутым.

По результатам исследования ученые смогли подтвердить и доказать свою версию: пользователи Facebook с нездоровой самооценкой своих отношений при помощи выкладывания фотографий и своих историй любви пытаются обезопасить себя от разрыва отношений. Результаты исследования были представлены на конференции по психологии в городе Остине (Техас), а также в Сан-Франциско (Калифорния).

Доцент Г. Сейдман, опрашивая тех пользователей Facebook, которые были в романтических отношениях и утверждали, что были счастливы в своих отношениях, выяснил, что те использовали платформу и как милое средство «шпионажа» за своим партнером. Больше всего к этому предрасположены интроверты. Экстраверты же, хотя отличаются большей эмоциональностью, намного прохладнее относятся к признаниям в любви через Facebook.

19.09.2016

В соцсети появилась «Сумская народная республика»

На днях некий С. Кривец переименовал одну из групп Facebook в «Сумскую Народную Республику» (Данкор онлайн).

Вражеский двуглавый орел с гербом Сум на теле, лозунги типа «стыдно быть украинцем!» – прихлебатель Кремля размещает в соцсети сепаратистские посты. А среди участников группы, которых больше семисот, остаются городские чиновники, депутаты и журналисты. И это при том, что нашу область СБУ отнесла к регионам с высоким уровнем угрозы террористических вторжений. А нардеп от Сумщины О. Медуница публично заявляет об активизации так называемой «пятой колонны»:

– Российская пятая колонна внутри Украины – не меньшая угроза, чем военное вторжение на Донбассе. Соцсети – это только одно из направлений деятельности вражеских спецслужб, – уверен нардеп. – Москва создала и финансирует целую сеть медиа-ресурсов для дестабилизации ситуации в Украине и «раскрутки» контролируемых нею политиков-популистов. Каплин со своей «Партией простых людей», Добродомов с типа «Народным контролем», Борислав Береза с «рішучими громадянами» – все это одна команда, пляшущая под балалайки Кремля. Как и Опоблок, ДНР и ЛНР.

Недавний поджог здания телеканала «Интер» был также спланирован российскими спецслужбами, говорит О. Медуница. Его фракция «Народный фронт» еще полтора года назад официально обращалась в СБУ и Нацсовет по вопросам телевиденья и радиовещания относительно информационной политики «Интера».

***

22.09.2016

Посол України просить Британію припинити діяльність пропагандиста Г. Філліпса в Україні

Посол України у Великій Британії Н. Галібаренко просить Британію припинити в Україні проросійську пропагандистську діяльність блогера та журналіста Г. Філліпса (Інформаційна агенція «Вголос»).

Про це йдеться у її відкритому листі, оприлюдненому на сайті посольства України в Об'єднаному королівстві Великої Британії та Північної Ірландії, передає УНН.

«Я хотіла б попросити британську сторону вжити всіх можливих заходів, у тому числі щодо його документів, щоб зупинити пропагандистську роботу пана Філліпса на російську окупаційну владу в Україні, щоб він покинув нашу країну назавжди», – йдеться у зверненні.

Також посол звернула увагу британської сторони на те, що британець Г. Філліпс у 2014–2015 рр. на Сході України працював в інтересах проросійських бойовиків, його депортували з України в липні 2014 р. Йому заборонили в'їзд до України на три роки через загрозу нацбезпеці. Називаючи себе британським журналістом, він руйнує стандарти британської журналістики, додала вона.

«Оскільки Г. Філліпс гордо називає себе британським журналістом, а його дії є ганебними й обурливими, він псує імідж Великобританії як країни, яка послідовно підтримує Україну в протидії російській агресії… Г. Філліпс руйнує високі стандарти британської журналістики», – наголосила посол.

Як повідомлялося раніше, Г. Філліпс, російський пропагандист, вдерся до редакції німецького видання Correctiv у Берліні.

***

21.09.2016

Федеральна служба безпеки Росії моніторить електронне листування депутатів Чернігівської міської ради?

Окремі депутати, голови постійних комісій та фракцій Чернігівської міської ради використовують для офіційного електронного листування поштові скриньки, які зареєстровані на російських сайтах. Спецслужби якої країни можуть читати – фактично, без жодних перешкод, в «автоматичному» режимі – все листування, яке проходить через ці e-mail, – питання риторичне (Чернігівщина: події і коментарі).

Громадська організація «Чернігівська правозахисна спілка» та «Антикорупційний дайджест» звернулися до Чернігівської міської ради з проханням надати контактні дані депутатів, постійних комісій та фракцій міської ради, щоби мати можливість направляти звернення безпосередньо адресатам як звичайною, так і електронною поштою, і ось деякі депутатські електронні адреси викликали деяке здивування.

З отриманої відповіді міської ради випливає, що до цього часу «народні обранці» чернігівського органу місцевого самоврядування використовують для виконання своїх депутатських обов'язків поштові скриньки електронної пошти, які зареєстровані на російських сайтах типу mail.ru, yandex.ru.

«У нас не було і не має жодного бажання розкручувати шпигуноманію або антиросійську істерію, але і залишати без реагування ситуацію з використанням місцевими депутатами електронних ресурсів, які підконтрольні РФ, вважаємо неправильним під час проведення, фактично, військових дій на території України.

Можна згадати події навколо соціальної мережі «ВКонтакті», засновник якої був вимушений відмовитися від своєї частки акцій, по одній з версій внаслідок його (П. Дурова) відмови надавати «компетентним органам» персональні дані українських користувачів.

Українське законодавство Постановою КМУ від 21 жовтня 2015 р. № 851 «Деякі питання використання доменних імен державними органами в українському сегменті Інтернету» зобов'язує державні органи влади та їхні посадові особи використовувати для здійснення службового листування виключно електронних поштових скриньок, розміщених на серверах, які перебувають у доменній зоні GOV.UA або .УКР.

Щодо органів місцевого самоврядування, суб'єктів господарювання державного та комунального секторів економіки є лише рекомендація дотримуватися вимог цієї Постанови. Чернігівська міська рада врахувала ці рекомендації, а частина депутатів вирішила для своєї представницької діяльності використовувати, як розуміємо, свої особисті поштові скриньки на російських інтернет-ресурсах, що на сьогодні навряд чи є доцільним з точки зору хоча би інформаційної безпеки», – зазначив керівник ГО «Чернігівська правозахисна спілка» та «Антикорупційного дайджесту» Є. Малецький.

Зарубіжні спецслужби і технології «соціального контролю»

19.09.2016

Поклонська хоче порушити справу проти Полозова за пости в соцмережах

Прокремлівська прокуратура окупованого Криму просить порушити кримінальну справу стосовно адвоката М. Полозова (Українська правда).

Про це він сам розповів ТАСС.

«Щойно мені зателефонували з Головного слідчого Управління СК по республіці Крим і запросили для надання пояснень у рамках дослідчої перевірки за заявою прокуратури», – сказав він.

М. Полозов пояснив, що в заяві прокуратура просить порушити кримінальну справу проти адвоката за образу ним у своїх постах у соцмережах сторони звинувачення у справі заступника голови меджлісу кримських татар А. Чийгоза.

«Нібито на моїй сторінці в Facebook міститься якась характеристика державного обвинувача у справі А. Чийгоза прокурора Домбровського А. А., імовірно виражена словами "дрібний, нездалий"», – розповів адвокат.

Він уточнив, що рішення йти в СК для надання пояснень він прийме тільки після консультації з керівництвом Адвокатської палати Москви.

Разом з тим М. Полозов підкреслив, що розцінює дії прокуратури окупованого Криму як спробу політичного тиску на нього.

Адвокат М. Полозов брав участь у захисті фігурантів гучних судових процесів, у тому числі над учасницями Pussy Riot, а також нардепом ВР Н. Савченко.

***

21.09.2016

ЗМІ повідомили про плани влади Росії розшифровувати весь інтернет-трафік росіян

ФСБ, Мінкомзв'язку та Мінпромторг Росії обговорюють набір рішень, які дадуть змогу дешифрувати весь інтернет-трафік росіян (LB.ua).

Про це пише «Коммерсантъ» з посиланням на джерела в IT-галузі та адміністрації президента.

Для виконання положень «закону Ярової» ФСБ спільно з Мінкомзв'язку і Мінпромторгу обговорює не лише питання зняття даних та їхнє зберігання, а й розшифровки та аналізу всього інтернет-трафіку, розповів газеті топ-менеджер одного з виробників обладнання та підтвердили співрозмовник в адміністрації президента і джерело в IT-компанії.

ФСБ виступає за те, щоб розшифровувати весь трафік у режимі real-time і аналізувати його за ключовими параметрами, умовно кажучи, за словом «бомба», а міністерства наполягають на розшифровці трафіку лише тих абонентів, які привернуть увагу правоохоронних органів, розповів співрозмовник газети в АП. У Мінпромторгу від коментарів відмовилися, в ФСБ і Мінкомзв'язку на запит «Коммерсанта» не відповіли.

Згідно з «законом Ярової», організатори поширення інформації, тобто власники інтернет-майданчиків, що дозволяють передавати електронні повідомлення, такі як Google, «Яндекс», Mail.ru Group, WhatsApp, Telegram, Viber, Facebook, «ВКонтакте» та ін., зобов'язані вже з 20 липня здавати ключі шифрування на вимогу ФСБ. Про те, що рішення для дешифрування інтернет-трафіку знадобиться, йдеться і в технічних вимогах для виконання «закону Ярової», які в серпні надсилав до профільних міністерств «Ростелеком». У «Ростелекомі», «Вимпелкомі», «Мегафоні» відмовилися від коментарів, у МТС повідомили, що їм нічого не відомо про дискусії на тему дешифрування трафіку.

Двоє співрозмовників газети стверджують, що один з обговорюваних варіантів дешифрування – установка на мережах операторів обладнання, здатного виконувати MITM-атаку (Man in the Middle). Це атака, при якій для користувача устаткування прикидається запитаним сайтом, а для сайту – користувачем. Виходить, що користувач буде встановлювати SSL-з'єднання з цим обладнанням, а вже воно – з сервером, до якого звертався користувач. Устаткування розшифрує перехоплений від сервера трафік, а перед відправленням користувачеві заново зашифрує його SSL-сертифікатом, виданим російським підтверджуючим центром (ПЦ). Щоб браузер користувача не видавав йому сповіщень про небезпечне з'єднання, російський ПЦ повинен бути доданий у довірені кореневі центри сертифікації на комп'ютері користувача, пояснює співрозмовник «Коммерсанта».

Для аналізу нешифрованих і вже розшифрованого трафіку планують використовувати DPI-системи (Deep Packet Inspection), які і зараз застосовують

багато операторів, наприклад для URL-фільтрації за списками заборонених сайтів, стверджують троє співрозмовників «Коммерсанта», знайомих з обговоренням між відомствами.

***

20.09.2016

Герман Ким

Google в Индии заблокирует файлы о способах определения пола ребенка

Всемирным ресурсам Google, Yahoo и Bing, принадлежащих компании Microsoft, вскоре заблокируют информацию о способах по определению пола ребенка в Индии, соответствующее постановление вынесено Верховный судом страны. Таким образом в Индостане решили повлиять на проблему демографии. Речь идёт об отмене продвижения в поисковиках всего контента, связанного с определением пола (HiTech-News.ru).

По сообщениям пресс-представителя холдинга Alphabet, в который входит Google, Yahoo! и Microsoft, дело было рассмотрено судом 19 сентября. По информации телевизионного канала NDTV, будет заблокирована реклама индийских специализированных служб, которые помогают будущим родителям определить пол ребенка до его рождения. Речь идёт о мерах, связанных с местным законодательством, законодательные акты которого направлены на решение проблемы гендерного неравенства в стране.

В связи с этим агентство Bloomberg пишет, что ранее Верховный суд Индии небезосновательно обвинял мировые поисковые системы в нарушении местных законов. Власти страны вынуждены были предупредить интернет-корпорации, что в случае отказа высших менеджеров работать по правилам индийского рынка, деятельность этих брендов в интернет-пространстве страны может быть прекращена полностью.

***

21.09.2016

Кримчанина оштрафували за «екстремістський» пост у соцмережі шестирічної давності

Сімферопольський залізничний суд Криму 20 вересня оштрафував активіста О. Шостаковича на 1 тис. рублів за пост у соціальній мережі, зроблений у 2010 р., і за «спробу провести мітинг» (LB.ua).

Про це повідомляється на сайті Кримської правозахисної групи.

Як розповів адвокат О. Попков, у 2010 р. О. Шостакович розмістив у соціальній мережі «ВКонтакте» відеоролик «Останній відеозапис хлопців із Приморських партизанів», визнаний в Росії «екстремістським матеріалом».

Ініціювали справу про адміністративне правопорушення співробітники так званого Центру «Е», які 17 вересня зупинили О. Шостаковича біля його

будинку, оскільки їм здалося, що він перебував у стані наркотичного сп'яніння. 18 вересня О. Шостаковича офіційно запросили на допит. 20 вересня відбувся суд, на якому співробітник Центру заявив, що О. Шостакович «причетний до праворадикального руху та розміщення на стінах міста трафаретних написів про бойкот виборів».

На засіданні О. Шостакович оголосив себе «громадянином світу» у відповідь на запитання судді про громадянство. У кримчанина, як виявилося, є тільки український паспорт, російського він не отримував.

Адвокат О. Попков заявив, що справа О. Шостаковича політично вмотивована, оскільки той проводив акції на підтримку політв'язнів українців у РФ, зокрема кримчанина О. Кольченка.

Суддя відмовилася переносити розгляд справи, не давши можливості захисту підготуватися, відхиливши також заявлені клопотання, зокрема про проведення фото- та відеозйомки.

***

22.09.2016

Великобританія збільшить кількість шпигунів для боротьби з тероризмом

Служба розвідки MI6 набере на роботу майже тисячу шпигунів (Корреспондент.net).

Служба зовнішньої розвідки Великобританії MI6 намір збільшити штат майже на тисячу осіб для боротьби зі світовим тероризмом, пише газета Times.

Розширення MI6 відбудеться згідно з планом уряду від 2015 р. зі збільшення на 15 %, або на 1900 осіб, співробітників британських спецслужб.

Таким чином, кількість співробітників служби зовнішньої розвідки збільшиться до початку 2020 р. з 2,5 тис. осіб до майже 3,5 тис.

Такий захід необхідний для переробки великого обсягу цифрових даних, що використовуються MI6 для визначення посередників і загроз. Очікується, що аналітики займуться встановленням «цифрових відбитків», які залишають користувачі Інтернету, мобільних телефонів і ноутбуків.

***

22.09.2016

Российский интернет-омбудсмен назвал недопустимой расшифровку трафика россиян по закону Яровой

По словам уполномоченного по защите прав предпринимателей в Интернете Д. Мариничева, на сегодня в России не существует технологических возможностей для дешифровки всего интернет-трафика, предусмотренной антитеррористическими поправками председателя думского комитета по безопасности и противодействию коррупции РФ И. Яровой (Сайт «ПолитТех»).

Расшифровка информации, которой российские пользователи обмениваются в Интернете, нарушит приватность передачи данных, заявил уполномоченный по защите прав предпринимателей в интернете Д. Мариничев в интервью радиостанции «Говорит Москва».

«Это недопустимая вещь, потому что дискредитирует цифровые технологии и, соответственно, дискредитирует платежные системы, онлайн-банкинг и приватность передачи информации», – пояснил собеседник радиостанции.

По его мнению, такую практику стоит применять только для лиц, в отношении которых ведутся расследования или уголовные дела.

«Делать это по всем россиянам просто недопустимо», – уверен омбусдмен.

По словам Д. Мариничева, на сегодняшний день в России не существует технологических возможностей для дешифровки всего интернет-трафика.

«Я не верю, что это технологически возможно. Я пока не владею информацией, что существует система, способная дешифровать налету все и вся», – отметил омбудсмен.

***

22.09.2016

У Росії заборонять критикувати владу в Інтернеті

Вибори в Державну Думу показали, що альтернативи та конкуренції в політиці не існує, тому вони взялися за останній оплот свободи в Росії – Інтернет (Інформаційна агенція «Вголос»).

Про це повідомляє російський публіцист Л. Радзіховський, передає «Апостроф».

«Кремлівська влада має намір організувати розшифровку всього трафіку. Для цього планується реалізувати цілий набір технічних рішень. Один з варіантів – встановити на мережах операторів спеціальні пристрої для дешифрування. Це дасть можливість спецслужбам РФ відстежувати в режимі real-time увесь контент, який запитують користувачі», – повідомляє експерт у блозі.

Водночас, повідомляє Л. Радзіховський, вибори показали, що опозиційна активність у російському сегменті Інтернету не конвертується в голоси виборців. Експерт відзначає, що в Росії також можуть застосувати китайську модель регулювання Інтернету.

***

22.09.2016

У Росії під'єднання до Wi-fi – за паспортом

Російських користувачів бездротової мережі пропонують ідентифікувати за паспортом (Інформаційна агенція «Вголос»).

З такою пропозицією виступив Роскомнагляд, передає «Знай», посилаючись на російські ЗМІ.

За ідентифікацією стежитиме спеціальне програмне забезпечення. Крім того, планується ввести адміністративну відповідальність для власників Wi-Fi-точок.

Роскомнагляд перевірив понад 18 тис. бездротових терміналів доступу в публічних місцях по всій країні. Результати показали, що більш ніж 5,5 тис. користувачі виходили в мережу без будь-якої ідентифікації.

Роскомнагляд вважає, що така ситуація є неприпустимою. Відомство введе правила регулювання для приватних Wi-Fi-мереж, які надають безкоштовний вихід в Інтернет.

***

23.09.2016
Базиленко Анна
Українська влада поки що не цікавиться українцями в Twitter

У більшості країн світу кількість запитів на розкриття даних користувачів соціальної мережі Twitter продовжує зростати. Натомість, українська влада поки що не цікавиться українцями в соцмережі. Згідно зі звітом компанії, упродовж січня – червня 2016 р. Twitter отримав на 2 % більше запитів порівняно зі звітним періодом за липень – грудень 2015 р. Даних щодо України компанія не надала (Watcher).

Найбільшу кількість запитів на розкриття даних направили державні органи США – 44 % (2520 запитів) від загальної кількості запитів у світі за звітний період. 82 % запитів від держорганів США Twitter усе ж задовольнив. Японія надіслала 732 запити, Twitter задовольнив 61 % з них. Велика Британія надіслала 631 запит (щодо 76 % запитів інформація надана Twitter), Франція – 572 запити (також щодо 76 % запитів інформація надана Twitter), Індія – 139 запитів (щодо 31 % запитів інформація надана Twitter), Німеччина – 111 запитів (щодо 58 % запитів інформація надана Twitter), Канада – 65 запитів (щодо 91 % запитів інформація надана Twitter).

У першому півріччі 2016 р. Туреччина зробила на 13 % більше запитів на видалення твітів та екаунтів користувачів Twitter – 280 запитів. Соціальна мережа не задовольнила жоден з них.

***

28.09.2016
В Германии Facebook запретили собирать данные пользователей WhatsApp

Социальную сеть Facebook суд обязал прекратить сбор данных пользователей мессенджера WhatsApp в Германии, сообщает Deutche Welle (InternetUA).

«Пользователи WhatsApp сами должны принимать решение, хотят ли они связывать свой аккаунт с Facebook. Соответственно, Facebook должен заранее просить у них на это разрешение. Однако этого не произошло», – сообщили специальный представитель Гамбурга по защите персональных данных и свободе информации Й. Каспар.

Отмечается, что действия Facebook квалифицируются как «нарушение национального закона о защите персональных данных».

***

30.09.2016

Посадовців РФ звільнятимуть за користування WhatsApp, Viber та Telegram

В адміністрації президента Росії відбулася нарада стосовно використання державними службовцями несертифікованих програм для обговорення робочих питань (Інформаційна агенція «Вголос»).

Про це пише ТСН.

Як повідомляють російські ЗМІ, до дискусії залучили представників ФСБ, уряду та галузевих підприємств. В обговоренні брав участь секретар ради безпеки РФ М. Патрушев.

За словами учасників засідання, він кілька разів порушував питання про неприпустимість використання чиновниками WhatsApp, Viber, Telegram та інших месенджерів для обговорення робочої інформації. У підсумку ФСБ отримала доручення підготувати відповідну нормативно-правову базу.

Аргументи на користь жорстких рішень у цьому питанні наводилися різні. Так, одні переповідали, що йшлося про легкість витоку інформації з подібних переписок і потрапляння її у розпорядження третіх осіб. Разом із тим інші говорили, що спецслужбам важко моніторити переписку в подібних програмах.

Учасники обговорення зійшлися на тому, що забороняти користування месенджерами для приватних потреб немає сенсу, однак при обговоренні службових питань необхідно користуватися лише сертифікованими каналами зв’язку та засобами шифрування. Передбачається, що за порушення цього посадовців каратимуть аж до звільнення з посади.

***

1.10.2016

Apple отслеживает, с кем общаются пользователи iMessage, и может выдать эти данные по запросу полиции

iMessage обеспечивает надежное шифрование данных, поэтому получить доступ к содержанию переписки не может ни один сторонний пользователь. Несмотря на это, компания Apple сохраняет данные о том, когда и с кем общаются пользователи мессенджера (InternetUA).

iMessage позиционируется Apple как конфиденциальный способ общения с друзьями и близкими, однако, по данным The Intercept, приложение не такое приватное, как можно было бы подумать. Когда пользователь пытается связаться с кем-нибудь через фирменный сервис «яблочной» компании, приложение автоматически отправляет запрос на серверы Apple, чтобы проверить, есть ли у предполагаемого получателя сообщения аккаунт в сервисе. В этот момент компания получает возможность увидеть, с кем человек пытается связаться – вне зависимости от того, есть у получателя аккаунт в iMessage или нет.

Более того, Apple записывает время и дату запроса, а также IP-адрес, с которого делается этот запрос, что может позволить определить местоположение пользователя.

Вся эта информация хранится на серверах Apple в течение 30 дней. Однако iMessage и другие стандартные приложения на iOS время от времени отправляют запросы к компании, генерируя новые записи о том, с кем пытается связаться пользователь. В записях хранится лишь информация об имеющихся на телефоне контактах, но даже это для некоторых может иметь последствия.

Проблема захисту даних. DDOS та вірусні атаки

19.09.2016

В Украине запустили вирусы, которые воруют данные с банковских карт в магазинах

В Украине фиксируют небольшое уменьшение случаев воровства денег с банковских карточек, но при этом отмечен рост преступлений с использованием вредоносного ПО (вирусов) (Украинские реалии).

Как рассказал UBR.ua замначальника департамента киберполиции Нацполиции Украины В. Чубаевский все чаще фиксируются факты заражения АТМ-терминалов (банкоматов) и POS-терминалов больших сетевых магазинов вредоносным программным обеспечением (вирусами) для воровства технической информации и ПИН-кодов банковских карточек клиентов, которые воспользовались услугами терминала, передают «Украинские реалии» ссылаясь на strana.ua.

По данным В. Чубаевского такие схемы широко распространены во многих странах ЕС, но в Украине раньше встречались редко.

Получив данные по банковским картам, злоумышленники передают их для изготовления поддельных карточек и снимают средства за пределами Украины, в том числе, в странах Азии, что делает невозможным быстрое задержание преступников и их привлечение к уголовной ответственности.

В департаменте киберполиции на таких преступлениях ловили граждан Беларуси, Румынии, Молдовы, Болгарии. Все задержанные лица за совершение

данного вида правонарушений привлекаются к уголовной ответственности, предусмотренной ст. 200 и ст. 361 УК Украины. Злоумышленникам грозит наказание в виде штрафа от 500 до 1000 необлагаемых налогом минимальных доходов граждан или лишение свободы на срок от двух до пяти лет.

***

19.09.2016

Взломавший ФБР хакер Л. Лав будет экстрадирован в США

Британско-финский хакер Л. Лав (Lauri Love) будет экстрадирован в США, где ему предъявлены обвинения во взломе компьютерных систем американского правительства. Соответствующее решение было вынесено Судом Вестминстерского магистрата в Лондоне 16 сентября (InternetUA).

В настоящее время 31-летнему Л. Лаву грозит наказание в виде 99 лет лишения свободы за взлом в 2012–2013 гг. сетей ФБР, Армии США, Агентства по противоракетной обороне, NASA и Федерального резервного банка Нью-Йорка. По данным британской прокуратуры, обвиняемый принимал участие в операции #OpLastResort, проводимой Anonymous в ответ на смерть активиста А. Шварца (Aaron Swartz).

Как пояснила окружной судья Н. Темпия (Nina Tempia), после экстрадиции Л. Лава его дело будет передано в Госдепартамент США. В настоящее время обвиняемый выпущен под залог и имеет право подать апелляцию. По словам судьи, медицинское обслуживание в тюрьмах США в полной мере сможет обеспечить Л. Лаву, страдающему от синдрома Аспергера, надлежащие условия.

Хакер был арестован в своем доме в Стрединшелле (Великобритания) в октябре 2013 г., и британская полиция изъяла его ноутбук и жесткие диски. Позже Национальное агентство по борьбе с преступностью Великобритании (National Crime Agency, NCA) через суд пыталось добиться выдачи Л. Лавом ключей шифрования для расшифровки содержимого жестких дисков. Тем не менее, в прошлом месяце британец выиграл дело против NCA.

***

16.09.2016

Глава ФБР рекомендовал в целях безопасности заклеивать веб-камеры

С развитием технологий слежения все больше пользователей заклеивают свои веб-камеры изолентой. К примеру, по данным «Лаборатории Касперского», подобной меры предосторожности придерживаются 23 % россиян.

Однако заклеивают камеру не только рядовые пользователи. Как известно, так поступают глава Facebook М. Цукерберг и даже директор ФБР Дж. Коми.

14 сентября на конференции в Центре стратегических и международных исследований (Center for Strategic and International Studies) Дж. Коми заявил, что такая мера предосторожности продиктована здравым смыслом и рекомендовал всем поступить так же. «Есть важные вещи, которые нужно сделать, и эта – одна из них. Если вы зайдете в любое правительственное учреждение, то увидите, что у всех нас есть эти крошечные камеры, и они закрыты маленькими крышками. Если вы сделаете так же, то люди, не имеющие на это прав, не смогут наблюдать за вами», – цитирует The Hill слова Дж. Коми.

Об использовании директором ФБР изоленты как меры безопасности впервые стало известно весной текущего года. Новость вызвала большой резонанс, особенно учитывая специфику работы возглавляемого Дж. Коми ведомства.

Как отметил глава ФБР во время своего выступления на конференции, за изоленту на камере его «много дразнили». Тем не менее, Дж. Коми продолжает заклеивать «вебку» и рекомендует остальным поступить так же.

***

21.09.2016

Хакери Росії атакують партію Клінтон – розвідка США

Кібератаки на Демократичну партію США вчинила Росія. Так вважає директор Національної розвідки США Дж. Клеппер. За його словами, для Москви вже стало традицією втручатися у вибори як усередині своєї країни, так і у волевиявлення інших держав (podrobnosti.ua).

Водночас Дж. Клеппер наголосив, як саме використає Росія отриману інформацію, і чи вплине насправді це на хід президентських виборів у США – поки що не зрозуміло. У результаті ряду кібератак на сервери демократів у мережу потрапив ряд внутрішньопартійних документів.

Представники Демократичної партії назвали напади спробою втручання у волевиявлення американців – мовляв, Росія хоче перемоги для лояльного до неї кандидату, республіканця Д. Трампа.

***

21.09.2016

Эксперты обвинили хакеров из России во взломе компьютеров немецких политиков

В деле о кибератаках с возможным участием российских хакеров появился очередной эпизод. Политики и члены ряда немецких партий подверглись массированной атаке киберпреступников, которые, предположительно, могут входить в группировку, поддерживаемую государственными органами России или действующую по заданию российских спецслужб, передает DW (InternetUA).

Атаки преступников произошли летом, однако известно о них стало только сейчас. Как сообщается, 15 и 24 августа немецкие политики – члены фракций бундестага, представители молодежной организации Христианско-демократического союза (ХДС), канцелярии Левой партии и отделения ХДС в федеральной земле Саар – получили письма по электронной почте, в которых утверждалось, что они якобы отправлены из штаб-квартиры НАТО в Брюсселе. Однако в них находилась ссылка, при переходе по которой компьютер становился уязвимым для шпионского программного оборудования. В итоге преступники заполучили доступ к секретной информации.

Издание отмечает, что эта же группа хакеров совершила серию атак в 2015 г. Тогда она проходила под названием APT28 (или Sofacy Group). Позднее, в мае текущего года, штаб-квартира ХДС, лидером которого является канцлер ФРГ А. Меркель, также подвергалась атаке, организованной группировкой Sofacy Group. Эксперты из ФРГ подозревают, что киберпреступники действовали по заданию российских спецслужб.

***

22.09.2016

Бурмас Роман

Эксперты обнаружили в сети данные сотрудников мировых корпораций

Британские специалисты по кибербезопасности нашли в свободном доступе в сети личные данные 5,5 млн работников из тысячи крупных мировых компаний. Об этом сообщает авторитетное британское издание (HiTech-News.ru).

В Интернете размещены пароли пользователей сервисов Linkedln, Dropbox и MySpace. Неизвестно, сотрудники каких именно компаний пострадали. Также эксперты сообщают, что 90 % данных появились в сети совсем недавно. По мнению британских специалистов, проблема в том, что некоторые используют одни и те же пароли на разных интернет-ресурсах, в том числе и на своей электронной почте.

Особенно большое количество персональных данных было украдено из сайтов знакомств, таких как Adult Friend Finder и Ashley Madison. По результатам проверки, около 290 тыс. корпоративных сотрудников пострадало подобным образом.

***

21.09.2016

«Доктор Веб»: троянцы Android.Xiny научились внедряться в системные процессы

Вирусные аналитики компании «Доктор Веб» обнаружили новые версии троянцев семейства Android.Xiny, которые предназначены для незаметной загрузки и удаления программ (ITnews).

Теперь эти троянцы могут внедряться в процессы системных приложений и загружать в атакуемые программы различные вредоносные плагины.

Троянцы семейства Android.Xiny известны с марта 2015 г. Вирусописатели активно распространяют их через различные сайты – сборники ПО для мобильных устройств и даже через официальные каталоги приложений, такие как Google Play, о чем компания «Доктор Веб» сообщала ранее.

Попадая на Android-смартфоны и планшеты, троянцы Android.Xiny пытаются получить root-доступ, чтобы незаметно загружать и устанавливать различное ПО. Кроме того, они могут показывать надоедливую рекламу. Одной из особенностей этих вредоносных приложений является впервые использованный механизм защиты от удаления. Он основан на том, что троянским apk-файлам присваивается атрибут «неизменяемый» (immutable). Однако злоумышленники продолжили совершенствовать троянцев Xiny и добавили в них возможность внедряться (выполнять инжект) в процессы системных программ, чтобы запускать от их имени различные вредоносные плагины.

Один из таких обновленных троянцев, исследованный вирусными аналитиками «Доктор Веб», получил имя Android.Xiny.60. Он устанавливается в системный каталог мобильных устройств другими представителями семейства Android.Xiny. После запуска Android.Xiny.60 извлекает из своих файловых ресурсов несколько вспомогательных троянских компонентов и копирует их в системные каталоги:

/system/xbin/igpi;

/system/lib/igpld.so;

/system/lib/igpfix.so;

/system/framework/igpi.jar.

Далее при помощи модуля igpi (добавлен в вирусную базу Dr.Web как Android.Xiny.61) троянец выполняет инжект библиотеки igpld.so (детектируется Dr.Web как Android.Xiny.62) в процессы системных приложений Google Play (com.android.vending) и Сервисы Google Play (com.google.android.gms, co.google.android.gms.persistent). Кроме того, внедрение этого вредоносного модуля может выполняться и в системный процесс zygote, однако в текущей версии троянца эта функция не используется.

При заражении процесса zygote Android.Xiny.62 начинает отслеживать запуск новых приложений. В результате, если троянец обнаруживает вновь запущенный процесс, он внедряет в него вредоносный модуль igpi.jar (Android.Xiny.60). Этот же модуль внедряется и после заражения процессов системных приложений Google Play и Сервисы Google Play.

Основная задача модуля igpi.jar – загрузка заданных злоумышленниками вредоносных плагинов и их запуск в контексте зараженных программ. Он отслеживает состояние мобильного устройства и при наступлении

определенных системных событий (например, включение или выключение экрана, изменение состояния подключения к сети, подключение или отключение зарядного устройства и ряд других) соединяется с управляющим сервером, куда отправляет следующую информацию об инфицированном смартфоне или планшете:

IMEI-идентификатор;
IMSI-идентификатор;
MAC-адрес сетевого адаптера;
версию ОС;
название модели мобильного устройства;
язык системы;
имя программного пакета, внутри процесса которого работает троянец.

В ответ Android.Xiny.60 может загрузить и запустить вредоносные плагины, которые после скачивания будут работать как часть того или иного атакованного приложения. Вирусные аналитики пока не зафиксировали распространение таких вредоносных модулей, однако если злоумышленники их создадут, Android.Xiny.60 будет способен атаковать пользователей многих программ. Например, если троянец внедрится в процесс Google Play, он сможет загрузить в него модуль для установки ПО. Если будет заражен процесс какого-либо мессенджера, Android.Xiny.60 получит возможность перехватывать и отправлять сообщения. А если троянец внедрится в процесс банковской программы, после запуска необходимого плагина он сможет красть конфиденциальные данные (логины, пароли, номера кредитных карт и т. п.) и даже незаметно переводить деньги на счета злоумышленников.

Специалисты компании «Доктор Веб» продолжают отслеживать активность троянцев семейства Android.Xiny. Для защиты мобильных устройств от заражения рекомендуется установить антивирусные продукты Dr.Web для Android, которые успешно детектируют все известные модификации этих вредоносных программ.

***

21.09.2016
Новый вымогатель блокирует главную загрузочную запись

Специалисты обнаружили новое семейство приложений-вымогателей, которое нацелено на главную загрузочную запись жёсткого диска (MBR) и не позволяет компьютерам загружаться, зашифровывая их файлы. Приложение HDDCryptor (другое название – Mamba) функционирует с нынешнего января, о чём сказано на форуме компании Bleeping Computer (InternetUA).

Вымогатель HDDCryptor появился раньше более известных вымогателей Petya и Satana, работая примерно так же. Недавняя кампания по распространению вымогателя пользователям по всему миру доставляла новую версию программы. Первым её заметил исследователь Р. Мариньо из Morphus

Labs, зафиксировав случаи распространения в США, Бразилии и Индии. Далее сходный технический анализ выпустила компания Trend Micro.

В отчётах сказано, что пользователи заходят на определённый веб-сайт и скачивают содержащий вредоносный код файлы. Файлы содержат HDDCryptor или промежуточное ПО, которое скачает вымогатель позднее. Когда запускается основной исполняемый файл, на компьютер устанавливается ряд других файлов и запускаются в определённом порядке.

Для начала HDDCryptor сканирует локальную сеть на наличие сетевых дисков. Затем бесплатный инструмент Network Password Recovery ищет и собирает данные общих папок. Ещё один бесплатный инструмент (DiskCryptor) шифрует пользовательские файлы на жёстком диске и на сетевых дисках. Напоследок HDDCrypter перезаписывает MBR и перезапускает компьютер, показывая записку с требованием выкупа. Выкуп составляет 1 биткоин (около 610 долл.).

***

21.09.2016

22 сентября разработчики OpenSSL выпустят патчи сразу для нескольких уязвимостей

Представители OpenSSL сообщили, что 22 сентября 2016 г. будут выпущены OpenSSL 1.1.0a, 1.0.2i и 1.0.1u (InternetUA).

Проект OpenSSL анонсировал скорый выход новых релизов, и разработчики пояснили, что в новых версиях будет устранен ряд проблем, включая уязвимость, получившую высокий приоритет (high). Также среди исправлений будет представлен патч для одной умеренной угрозы (moderate) и ряд патчей для низкоуровневых уязвимостей.

До выхода обновлений никакая информация о найденных багах традиционно не раскрывается. Можно предположить, что злоумышленники с меньшей вероятностью будут эксплуатировать уязвимость, получившую статус high, в противном случае баг имел бы статус критического.

Также в конце анонса разработчики OpenSSL еще раз напомнили пользователям, что 31 декабря 2016 г. будет прекращена поддержка OpenSSL 1.0.1.

***

23.09.2016

Epoch Times повідомила про причетність російських хакерів до атак на 85 компаній

Серія кібератак до яких, ймовірно, мають відношення російські хакери, була спрямована щонайменше на 85 великих компаній та корпорацій (Західна інформаційна корпорація).

Про це інформувала в четвер у своїй електронній версії газета the Epoch Times, – повідомляє ТАРС.

Як зазначає видання, яке посилається на відомості, одержані від приватної компанії, що пропонує послуги із забезпечення безпеки в Інтернеті, кібернападів зазнали, зокрема, інтернет-магазин Amazon, платіжна система Apple Pay, онлайн-аукціон Ebay, мережа ресторанів Mcdonald's, авіаперевізник American Airlines, компанія з онлайн-викликом таксі Über. У неповному списку, який надає Epoch Times, фігурують виключно компанії, які базуються в США.

«Дані, що стосуються осіб, які стоять за атаками, поки що не є повними, однак вони, ймовірніше всього, є звичайними кіберзлочинцями, не пов'язаними з урядом», – пише газета. З відома Epoch Times, хакери використовували під час кібернападів російські комп'ютерні сервери, а також спілкувалися в інтернет-чатах російською мовою, координуючи свої дії.

Як зазначив представник каліфорнійської компанії щодо забезпечення кібербезпеки DBI E. Александер, зловмисники, зокрема, здійснювали атаки з метою викрадення номерів кредитних карт і особисту інформацію користувачів платіжної системи Apple Pay.

***

23.09.2016

Yahoo оголосила про крадіжку 500 млн акаунтів

Компанія Yahoo заявила, що в 2014 р. хакери викрали дані, пов'язані з 500 млн акаунтів (Західна інформаційна корпорація).

Метою зломщиків були імена користувачів, адреси електронної пошти, номери телефонів, зашифровані паролі, а також контрольні запитання та відповіді. Дані, пов'язані з банківськими картами і рахунками, викрадені не були.

За зломом, за припущенням Yahoo, стоять хакери, яких «підтримує держава», – повідомляє Медуза.

Про яку саме державу йде мова, не уточнюється. Компанія співпрацює з правоохоронними органами в розслідуванні атаки.

У Yahoo заявили, що інформує можливих жертв злому про необхідні кроки щодо захисту облікових записів. Компанія рекомендує змінити паролі тим, хто не робив цього з 2014 р., а також поміняти паролі та контрольні питання на інших сайтах, якщо вони збігаються з аккаунтом на Yahoo.

***

26.09.2016

В Україні кіберзлочинці завдали шкоди на 27 млн грн

За вісім місяців цього року в нашій країні збитки від злочинів з використанням інформаційних технологій (ІТ) сягнули 27 млн грн (Інформаційна агенція «Вголос»).

Про це в інтерв'ю газеті «Сегодня» заявив керівники кіберполіції С. Демедюк. Він зазначив, що вказаний показник за попередні 2014–2015 рр. становив, відповідно, 39 і 10 млн грн.

За його словами, понад половину від суми збитків правоохоронцям вдалося повернути жертвам. Крім того, працівники кіберполіції виявили групу осіб, які обікрали іноземні банки на суму 7–8 млн дол. Однак ця сума не ввійшла в офіційну статистику, бо розслідування справ ведеться за кордоном, пояснив С. Демедюк. Він зазначив, що кіберполіція виявляє в середньому лише 50 % злочинів з використанням ІТ, бо не завжди жертви звертаються до правоохоронців.

Найбільше шкоди зловмисники завдають довірливим громадянам, обіцяючи їм крупні виграші та обманом виманюючи гроші.

***

26.09.2016

Вредоносное ПО можно получить и по обычной почте

Получить вирус или троян на свой компьютер или мобильное устройство по электронной почте очень просто – такие письма рассылаются сотнями тысяч ежедневно. Теперь же появилась возможность заразить свой компьютер вредоносным ПО при помощи самой обычной почты, не имеющей отношения к глобальной сети (InternetUA).

По сообщению портала Slash Gear, в мире зафиксирован ряд случаев доставки вирусов по почте в белых конвертах без опознавательных знаков. Владельцы почтовых ящиков находили в них конверты с USB-накопителем внутри. Очевидно, те, кто занимается подобной рассылкой, пытаются играть на одном из самых сильных человеческих чувств – любопытстве.

И это у злоумышленников неплохо получается, поскольку получателю посылки очень интересно, что же скрывается на носителе, и он, забывая обо всех предосторожностях, подключает опасную флешку к своему ПК. Последствия, в зависимости от типа malware, могут быть самыми разными, вплоть до кражи персональных данных, требования денег или удаления всей информации с жесткого диска. Подобные случаи уже зафиксированы в США, Британии и Австралии.

Конечно, опытных пользователей или недоверчивых граждан, не верящих в бесплатный сыр (и тем более в бесплатные USB-драйвы), на простом любопытстве не возьмешь, и на этот случай у преступников тоже есть план: вместе с флешкой в конверте обнаруживается листовка, рассказывающая о полезном содержимом накопителя – это может быть пробная версия нового антивируса, какая-либо интересная база данных и многое другое. Конечно, в результате там все равно вирус, но подобный обман все равно работает.

Разработчики антивирусных систем настоятельно не рекомендуют проверять содержимое присланных по почте накопителей на своих компьютерах или же делать это под ОС, практически не подверженных

вирусам, например, под Linux. Но в конверте может оказаться не просто флешка – а USB Killer: устройство, замаскированное под накопитель, но на деле являющееся буквально убийцей компьютеров, накапливающим заряд в 220 вольт и посылающим его на системную плату несколько раз в секунду, пока та не выйдет из строя. В результате ремонт ПК затребует крупных финансовых вложений.

***

23.09.2016
Базиленко Анна
Нацполіція та медіаспільнота спільно боротимуться з піратством

Національна поліція України та представники медіабізнесу підписали меморандум про співробітництво у боротьбі з інтернет-піратством (Watcher).

Сторони будуть обмінюватися інформацією, для поліцейських будуть проводити тренінги та надаватимуть технічну підтримку. Також обіцяють доопрацьовувати існуючу законодавчу базу.

«Треба знайти законодавчу "золоту середину", коли поліція не буде порушувати інтереси бізнесу, водночас забезпечуючи правопорядок у сфері дотримання авторських прав. Підписання Меморандуму виведе роботу з нашими партнерами на вищий рівень», – зазначила голова Нацполіції Х. Деканоідзе.

Вона додала, що питаннями боротьби з піратством займається Департамент кіберполіції, який вже отримує багато звернень щодо порушення авторських прав. У свою чергу, завдання представників медіа-простору – допомогти Нацполіції розібратись, що відбувається на цьому ринку, які є правопорушення та як їх можна виявити.

***

20.09.2016
Евгений Опанасенко
Флешка-киллер уничтожает компьютер за секунды

Изобретатель под псевдонимом Dark_Purple создал уникальное USB-устройство, способное за секунды уничтожить любой девайс с USB-портом. Прототип получил название USB Killer 2.0 (podrobnosti.ua).

Принцип работы гаджета-убийцы выглядит следующим образом: при подключении к USB порту запускается инвертирующий DC/DC преобразователь и заряжает конденсаторы до напряжения -110в, при достижении этого напряжения DC/DC отключается и одновременно открывается полевой транзистор, через который -110в прикладываются к сигнальным линиям USB интерфейса.

Затем при падении увеличении напряжения на конденсаторах до -7в транзистор закрывается и запускается DC/DC. И так в цикле пока не «поджарит» электронику.

***

22.09.2016

Сегодня хакеры намерены атаковать крупные мировые СМИ

Участники группировки под названием Powerful Greek Army пообещали 22 сентября нынешнего года запустить DDoS-кампанию, нацеленную на крупнейшие мировые новостные агентства и медиа-ресурсы. Как пояснили хакеры, таким образом Powerful Greek Army намерена выступить против некорректного освещения событий информагентствами и проправительственной позиции, которую они занимают (InternetUA).

В списке целей группировки фигурируют ресурсы BBC, The Daily Mail, The Independent, Reuters, телеканал «Первый канал» (Россия), The Huffington Post, FOX и др. По словам участников группировки, кампания под названием #OpClosedMedia продлится месяц.

***

21.09.2016

НБУ презентував проект створення центру реагування на інциденти кібернетичної безпеки в банківській системі

Національний банк України (НБУ) презентував проект створення центру реагування на інциденти кібернетичної безпеки в банківській системі. Про це повідомив представник Управління безпеки інформації Департаменту безпеки Національного банку України Р. Проскуровський на засіданні Комітету з питань банківської інфраструктури та платіжних систем НАБУ – Конференція «Захист інформації та персональних даних. Анти: -вірус, -фрод, -DDOS» (InternetUA).

Учасникам Комітету було презентовано проект створення «Центру реагування на інциденти кібернетичної безпеки в банківській системі та платіжному просторі України (CERT-NBU)», метою якого є допомога в розв’язанні проблем боротьби із кіберзагрозами та сприяння розвитку фінансової системи України.

У своєму виступі Р. Проскуровський неодноразово звертав увагу на бажанні Національного банку України йти на зустріч банкам у розв’язанні проблем кіберзагроз і налагодженні відкритого та прозорого діалогу в процесі створення та діяльності CERT-NBU.

Також, ряд компаній, зокрема, Check PointSoftware, Symantec, Netwell, ISSP та ESET запропонували банківській аудиторії сучасні рішення та методи боротьби із інформаційними загрозами, що виникають перед фінансовими установами.

***

26.09.2016

Технология распознавания по радужной оболочке глаз станет популярной

Технология распознавания по радужной оболочке глаз является одним из самых надежных и безопасных методов идентификации пользователя, которая в ближайшем будущем получит широкое внедрение на глобальном рынке коммуникаторов, прогнозируют аналитики ABI Research. По оценкам экспертов, в 2021 г. мировые поставки смартфонов со сканерами радужной оболочки достигнут почти 300 млн штук (InternetUA).

«Поскольку рисунок радужной оболочки является неизменной и совершенно уникальной характеристикой человеческого тела, все больше производителей смартфонов стремятся внедрять в своих продуктах системы биометрической идентификации, основанные на сканировании радужки, с помощью которых пользователи могут разблокировать устройства и совершать мобильные платежи», – комментирует прогноз старший аналитик ABI М. Лю (Marina Lu).

Специалист полагает, что такая технология поможет преодолеть существующую у многих пользователей боязнь перехода на мобильные платежи из-за опасений, связанных с безопасностью.

Говоря о достоинствах технологии, в ABI отметили, что для сканирования рисунка радужки не требуется прямого физического контакта, что делает процедуру аутентификации более удобной и легкой, чем в случае с другими методами, такими как введение цифрового ПИН-кода или считывание отпечатка пальца. Кроме того, сканеры радужной оболочки, которыми оснащаются мобильные устройства, используют камеру и инфракрасный светодиод для освещения глаз, что позволяет распознавать пользователя даже в полумраке.

В 2015 г. японская компания Fujitsu первой внедрила сканирование радужки в своих смартфонах. Затем эта функция появилась в аппаратах Microsoft Lumia 950 и 950 XL, ZTE Nubia Prague S, а также в планшете HP Elite x3.

Технология нашла применение и в новейшем фаблете Samsung Galaxy Note 7. Эксперты полагают, что вскоре этому примеру последуют многие другие производители. Что касается Apple, то она пока не решилась использовать сканирование «радужки» в iPhone. Специалисты полагают, что пройдет еще как минимум год, прежде чем технология распространится и на смартфоны Apple.

В заключении аналитики отметили, что хотя на сегодняшний день сканирование радужной оболочки менее распространено по сравнению с другой, более зрелой технологией распознавания по отпечатку пальца, в дальнейшем новый метод идентификации станет популярнее благодаря более

высокой стабильности работы и меньшей чувствительности к внешним факторам. Также в ABI считают, что в будущем эту технологию получат не только высококлассные смартфоны, но и более доступные по цене модели.

***

26.09.2016

Из-за ботнета Necurs количество почтового спама вернулось на уровень 2010 г.

Специалисты компании Cisco обнародовали отчет, согласно которому уровень почтового спама, постепенно снижавшийся в последние пять лет, вновь начал расти. В 2016 г. спам вновь вышел на уровень, которого аналитики не видели уже давно (InternetUA).

В качестве иллюстрации специалисты Cisco предлагают график Composite Block List, в котором собраны данные об уровне спама с 2009 г. Как можно заметить, нынешняя ситуация сравнима с ситуацией 2010 г.

Еще один график, составленный SpamCop, показывает динамику общемирового уровня спама в текущем 2016 г. Если до 2016 г. в среднем наблюдалось порядка 200 000 IP-адресов, распространяющих мусорную корреспонденцию, в августе 2016 г. сейчас этот показатель успешно преодолел отметку в 450 000.

Почему возник такой прирост? Специалисты Cisco полагают, что в этом виноват ботнет Necurs. По данным экспертов, многие IP, рассылающие Necurs спам, заражены уже более двух лет. При этом операторы ботнета стараются действовать осторожно, к примеру, хосты задействуются для рассылки писем на два-три дня, а затем не используются на протяжении двух-трех недель. Это здорово осложняет работу аналитиков, которые успевают предположить, что зараженный хост был обнаружен и очищен, но спустя время рассылка спама возобновляется.

Летом 2016 г. Necurs на некоторое время пропадал с радаров, что тогда связали с арестом авторов трояна Lurk. Однако спустя несколько недель ботнет возобновил свою деятельность в полном объеме и, что гораздо хуже, сменил тактику. Если раньше Necurs рассылал обычный спам, то теперь ботнет переключился на сообщения, содержащие вредоносные вложения. К примеру, Necurs уже был замечен за распространением банковского трояна Dridex и вымогателя Locky.

***

27.09.2016

Герман Ким

«Лаборатория Касперского»: Хакеры могут отключать камеры ГИБДД

По мнению инженеров «Лаборатории Касперского», злоумышленники могут получать свободный доступ к камерам фиксации скорости, которые установлены на дорогах России. Речь идёт о возможности подключаться к ним, а затем манипулировать полученной информацией. Об этом сообщается в итогах исследования «Лаборатории». Как оказалось, найти IP-адреса видеокамер и узнать их местонахождение не составляет никакого труда (HiTech-News.ru).

В ходе продолжительного исследования группе сотрудников отечественной «Лаборатории Касперского» удалось выяснить, что камеры видеофиксации дорожных нарушений, которые установлены специалистами КИП на российских дорогах, становятся объектом атак интернет-злоумышленников. Как заявляют эксперты, в ряде городов Российской Федерации к камерам видеофиксации теретически может иметь доступ любой хакер.

Это происходит потому, что данные с комплексов не шифруются, что является потенциалом для просмотра «живого» видео, а также получать оперативный контроль над аппаратурой. Эксперты «Лаборатории» заявляют, что устройства нужно немедленно защитить от доступа к ним из Интернета. Ранее на пригородном шоссе Кинешма – Иваново хакерам удалось установить незаконные дорожные камеры и начать рассылку о штрафах местным водителям.

***

27.09.2016

На Кіровоградщині кіберзлочинці відмивали гроші для проросійських сепаратистів

Служба безпеки України у містах Києві та Кропивницькому викрила злочинну групу, що відмивала гроші, викрадені міжнародними хакерами проросійського угруповання «кіберберкут». Через спеціально створені інтернет-ресурси зловмисники отримували дані викрадених банківських карток. Гроші з них виводились через веб-сервіс з використанням так званого «білого пластику» (підроблених платіжних карток), криптовалюти «Біткойн» та ресурсів кількох небанківських платіжних систем (Олександрійські новини).

Як повідомляє прес-центр СБУ, клієнтами нелегального бізнесу були юридичні та фізичні особи з тимчасово окупованих терористами територій України.

Під час обшуків у рамках кримінального провадження щодо фінансування тероризму правоохоронці вилучили понад 27 тис. дол. США, 450 тис. російських рублів, 340 тис. грн, 10 тис. польських злотих і золоті вироби.

Співробітники СБ України також виявили «чорну бухгалтерію», комп'ютерну техніку, спеціальне обладнання для зчитування та запису підроблених пластикових карток і банківські картки, що підтверджують здійснення фінансових оборудок. Наразі тривають оперативно-слідчі дії,

встановлюються причетні до протиправної діяльності та обсяги нелегальних фінансових оборудок.

***

27.09.2016

Ливийские хакеры используют Каддафи для одурачивания пользователей

В свежем докладе антивирусной компании ESET приводятся сведения о серии кибератак, направленных против пользователей Ливии. Злоумышленники используют троянское ПО для кражи данных и осуществляют взлом правительственных сайтов – причём, по информации аналитиков, делают это весьма успешно (InternetUA).

Согласно данным облачной системы ESET LiveGrid, «ливийский» троян распространяется с 2012 г. и предназначен для сбора данных. Зловред способен перехватывать нажатия клавиш, осуществлять запись звука с микрофона, делать скриншоты рабочего стола и снимки веб-камерой, а также собирать информацию об операционной системе и антивирусном ПО на компьютере жертвы.

***

28.09.2016

Российских хакеров подозревают в создании трояна, позволяющего получить полный доступ к компьютерам Mac

Эксперты обнаружили вредоносное приложение, которое распространяется через PDF-документ, содержащий подробности о Федеральной космической программе России. Они полагают, что за этим вредоносом стоят кибервзломщики из РФ (InternetUA).

Специалисты компании Palo Alto Networks сообщили о появлении нового трояна, используемого в атаках на компьютеры Mac. В настоящее время известно о существовании трех разновидностей вредоноса. Две из них предназначены для архитектур x86 и x64, третья – универсальная.

По данным Securitylab, троян Komplex связан непосредственно с возросшей активностью хакерской группировки Fancy Bear, также известной под названиями APT28, Sednit, Pawn Storm, Strontium и Sofacy. Она специализируется на кибершпионаже в особо крупных масштабах, но также нередко крадет персональные данные с компьютеров-жертв для дальнейшей спекуляции ими.

Заражение целевого компьютера осуществляется посредством эксплуатации уязвимости в приложении MacKeeper. Вредонос распространяется через PDF-документ, якобы содержащий подробности о Федеральной космической программе России на 2016–2025 гг. Оказавшись на компьютере, Komplex собирает данные о системе. Троян ожидает, пока

пользователь подключится к Интернету, и только тогда связывается с управляющим сервером злоумышленников и отправляет информацию.

На основе полученных данных операторы вредоноса принимают решение об отправке дополнительных модулей. Исследователям удалось идентифицировать модули, используемые злоумышленниками для загрузки файлов на целевой компьютер, хищения данных, выполнения команд.

По мнению специалистов, Komplex является версией для Mac OS X банковского трояна Carberp, который ранее взяла на вооружение группировка Fancy Bear. Предполагается, что именно эта команда стоит за атаками на серверы Национального комитета Демократической партии США и Всемирного антидопингового агентства.

***

28.09.2016
«Брэд Питт умер»: Facebook атаковал новый вирус

В соцсети Facebook распространяется вирус под видом новости с заголовком «Брэд Питт умер». Киберпреступники решили использовать одну из главных новостей шоу-бизнеса в мире, которая вызвала общественный резонанс по всему миру – развод Джоли и Питта (podrobnosti.ua).

В соцсети уже появилось предупреждение об опасности нового поста. Если пользователь попался на удочку мошенников, то ему предложат поменять пароли, а компьютер проверить антивирусной программой.

***

28.09.2016
Константин Семенов
Хакеры Fancy Bears атаковали Apple «космическим вирусом»

Команда российских хакеров Fancy Bears создала новый вирус для Mac OS. Троянская программа получила название Komplex. При заражении системы она может скачивать и удалять файлы, а также запускать программы, сообщает PCWorld (podrobnosti.ua).

Примечательно, что троян сохраняет на компьютер файл с описанием российской космической программы на 2016–2025 гг.

Этот файл служит для отвлечения внимания при загрузке самой троянской программы, которая начинается при переходе по ссылке, распространяемой по электронной почте. По словам Palo Alto Networks, при этом используется уже известная уязвимость в антивирусной программе MacKeeper.+

Fancy Bears обвиняют в ряде крупных хакерских атак на политические структуры США. Специалисты считают, что код троянских программ, при помощи которых были совершены атаки на американское правительство, использовался и для создания Komplex.

***

29.09.2016

Операция «Пираты» против киберпреступлений

Проблема пиратства в Украине в последнее время особенно актуальна. Речь идет об использовании нелицензионного программного обеспечения, незаконном распространении аудио- и видеопродукции или использовании изобретений без разрешения авторов. Чтобы предотвратить подобные преступления на Сумщине, отдел противодействия киберпреступности в Сумской области Департамента киберполиции проводит целевую оперативно-профилактическую операцию «Пираты» (Ваш шанс).

Эта операция направлена на охрану авторских прав, выявление и пресечение противоправной деятельности как отдельных граждан, так и организованных преступных групп, которые изготавливают, воспроизводят, продают или распространяют контрафактную продукцию, используя для этого Интернет или другие телекоммуникационные сети.

Подразделения киберполиции НПУ собирают информацию, детально анализируют печатные издания, публикации в Интернете, сетевые информационные ресурсы, находящиеся в открытом доступе, интернет-хостинг провайдеров, контент-провайдеров, регистраторов доменных имен.

Согласно Уголовному кодексу Украины, лица, нарушающие авторские права или незаконно использующие товарные знаки или фирменные наименования, несут ответственность в виде штрафа, исправительных работ или даже лишения свободы.

***

28.09.2016

Bellingcat піддалися кібератакам через розслідування катастрофи рейсу MH17

На сайт розслідувачів Bellingcat здійснювалися хакерські атаки з метою дискредитувати результати їх дослідження, більшість з яких підтвердила в звіті міжнародна слідча група в Нідерландах. З цією ж метою російськими ЗМІ була запущена пропагандистська кампанія (LB.ua).

Про це заявив помічник президента аналітичного центру Atlantic Council М. Чуперський, повідомляє Громадське.

«Ми стали свідками наполегливих спроб дискредитувати команду Bellingcat. Не тільки через кібератаки, що тривають останні два тижні, а й через прицільну та продуману пропаганду. Два тижні тому, коли міжнародна слідча група оголосила про плани оприлюднити звіт, майже синхронно з ними Russia Today, Sputnik та інші російські новинні агентства почали дискредитувати та писати відверту брехню про розслідувачів Bellingcat і будь-що причетне до розслідування», – сказав він.

За його словами, оприлюднення нових результатів міжнародної комісії призведе до більшого тиску на російську владу.

«Це складна ситуація для Кремля та російського МЗС, які постійно заперечують, що “Бук” доставлено російськими військовими, хоча всі докази вказують на це. Тому чекайте збільшення дипломатичного тиску на Кремль і спроби Москви відвернути або спотворити реальність», – додав М. Чуперський.

***

28.09.2016

Zillya! запускает сертификацию специалистов по антивирусной защите

Украинская компания объявляет о старте программы сертификации «Zillya! Laboratory: специалист по антивирусной защите» (AIN.UA).

Программа ориентирована на IT-специалистов, системных администраторов, а также руководителей IT-проектов, для которых обеспечение информационной безопасности является одной из сфер деятельности. Участники смогут получить более широкие знания в области антивирусной защиты с дальнейшим применением их в своей профессиональной и коммерческой деятельности.

***

28.09.2016

В 2016 г. компрометации подверглись более 15 тыс. сайтов на WordPress

С начала 2016 г. по меньшей мере 15 769 сайтов на WordPress стали жертвами взлома. Такие данные приводят специалисты компании Sucuri в отчете за II квартал 2016 г. В указанный период эксперты проанализировали более 9 тыс. инфицированных ресурсов под управлением WordPress (78 %), Joomla! (14 %), Magento (5 %) и Drupal (2 %) (InternetUA).

Как показало исследование, 55 % сайтов на WordPress использовали устаревшие версии ПО, однако лидирующие позиции в этом аспекте занимают сайты на платформах Magento (96 %), Joomla! (86 %) и Drupal (84 %). Как отмечают эксперты, во II квартале число случаев использования устаревших версий Magento, Drupal и Joomla! в среднем возросло на 2 %.

На почти 75 % всех инфицированных сайтов были обнаружены бэкдоры, позволяющие злоумышленникам загружать различное вредоносное ПО и использовать скомпрометированные ресурсы для дальнейших атак. В настоящее время точно не известно, с какой целью хакеры взламывают ресурсы, однако многие из них служат в качестве промежуточных сайтов в инфраструктуре C&C-сети или используются для хостинга вредоносного ПО. В кодах 38 % порталов были обнаружены спам-инъекции.

Согласно отчету, взлом 22 % сайтов на WordPress стал возможен из-за использования уязвимых плагинов, в частности RevSlider (46 %), Gravity Forms (27 %) и TimThumb (27 %). Как отмечается, для всех трех плагинов обновления не выпускались уже больше года, а для TimThumb последний патч вышел еще в 2011 г.

***

28.09.2016

Уязвимость в принтерах Epson 1999 г. выпуска позволяет получить доступ к неподключенным к Интернету сетям

Уязвимость в прошивке многофункциональных принтеров Epson 1999 г. выпуска позволяет получить доступ к сетям, не подключенным к Интернету. Для успешного осуществления атаки необходимо соблюсти два условия: жертва должна установить вредоносную прошивку и использовать факсимильную функцию принтера (InternetUA).

Прошивка устройств представляет собой кастомизированную версию Linux, обеспечивающую злоумышленникам знакомую сетевую среду. Попав в эту среду, они могут получить доступ к сети, к которой подключен принтер.

Проблему обнаружили исследователи безопасности И.-Н. Вевелер (Yves-Noel Weweler), Р. Спеннеберг (Ralf Spenneberg) и Х. Швартке (Hendrik Schwartke). По их словам, уязвимость существует из-за того, что многофункциональные принтеры Epson WorkForce не требуют подписанного образа прошивки. Исследователи протестировали свой эксплоит на модели Epson WF-2540 MFP, однако, скорее всего, проблема затрагивает все устройства линеек WorkForce и Stylus.

Экспертам удалось создать и инсталлировать образ вредоносной прошивки, устанавливающий бэкдор с помощью встроенного модема. Этот бэкдор позволяет получить доступ к сети, даже если она не подключена к Интернету.

***

28.09.2016

Какие опасности таит в себе умный город

Многие элементы умного города вроде банкоматов или платёжных терминалов облегчают гражданам получение различных услуг, и все к ним уже настолько привыкли, что зачастую забывают о потенциальных опасностях, которые таит в себе использование подобных устройств. «Лаборатория Касперского» предупреждает, что все они содержат уязвимости, которые позволяют раскрыть личные данные, следить за пользователями или распространять вредоносный код (InternetUA).

Дело в том, что все платёжные и информационные терминалы работают под управлением Windows или Android. Подобные устройства снабжены

интерактивной графической оболочкой, которая перекрывает пользователю доступ к привычным функциям этих операционных систем. Но хакеры могут запросто воспользоваться ими в корыстных целях благодаря уязвимостям, которые имеются почти в любом подобном устройстве. К примеру, в интерфейсе некоторых терминалов содержатся ссылки на внешние сайты, которые позволяют злоумышленникам получить доступ к ОС устройства и запустить виртуальную клавиатуру.

Ещё один тип уязвимости был найден в терминале для печати квитанций: после ввода необходимых реквизитов и подтверждения действия терминал на некоторое время открывает стандартное окно печати. Подгадав момент, мошенники могут успеть изменить параметры печати и выйти в справочный раздел, а оттуда перейти в панель управления и открыть экранную клавиатуру. Таким образом, они способны запустить вредоносный код, а также получить информацию о распечатанных файлах и пароль администратора.

Бреши в системах конфигурации, которыми могут воспользоваться преступники, присущи даже камерам регистрации скорости. Эксперты утверждают, что злоумышленники могут без проблем подключиться к ним и манипулировать собранными данными. С помощью поискового механизма Shodan хакеру не составит труда отыскать IP-адреса этих устройств, а для доступа к ним даже не нужен пароль.

***

29.09.2016

Новый вымогатель даёт четыре дня на выплату выкупа

Новое семейство приложений-вымогателей нацелено на государственные учреждения и образовательные заведения США, распространяясь в спаме по электронной почте. Программа MarsJoke найдена специалистами компании Proofpoint в письмах якобы от авиакомпании. Название MarsJoke было взято из строки кода HelloWorldItsJokeFromMars (InternetUA).

В письме говорится об «отслеживании посылки» и для этого нужно перейти по ссылке. Скачивается исполняемый файл file_6.exe, при его запуске активируется вымогатель MarsJoke. Когда шифрование пользовательских файлов завершается, создаются файлы !!! For Decrypt !!!.bat, !!! Readme For Decrypt !!!.txt и ReadMeFilesDecrypt!!!.txt, которые сохраняются в нескольких папках. Размер выкупа составляет 0,7 биткоинов (320 долл.).

Потом меняются обои, говоря о том, что файлы зашифрованы. Таймер показывает обратный отсчёт 96 часов, после чего файлы останутся зашифрованными навсегда. Для примера возможности расшифровки дешифруются два файла. Также выдаётся инструкция по покупке биткоинов.

Государственные и образовательные учреждения становятся любимой целью вымогателей, разглядевших слабости их систем безопасности. Например, частое отсутствие резервных копий повышает вероятность того, что хакеры получат выкуп за файлы.

***

29.09.2016

Уязвимости в космических аппаратах могут привести к разгоранию «звездных войн»

Как считалось до недавнего времени, звездные войны – это чистой воды фантастика, что-то, что может произойти в далекой-далекой галактике, но не в реальном мире. Тем не менее, согласно отчету экспертов лондонского аналитического центра «Королевский институт международных отношений» (Chatham House), звездные войны куда более реальны, чем может показаться (InternetUA).

По мнению экспертов, киберпреступники, вражеские государства и даже террористы могут избрать в качестве вектора атак спутники. В настоящее время вопрос уязвимостей в спутниках и других искусственных космических объектах до конца не изучен, чем могут воспользоваться злоумышленники.

«В обсуждениях киберугроз, представляющих опасность для критической инфраструктуры государства, уязвимость спутников и других космических объектов к кибератакам всегда упускается из виду. Это большая ошибка, учитывая значительную и постоянно растущую зависимость общества от спутниковых технологий, используемых для навигации, связи, дистанционного зондирования Земли, мониторинга и в бесчисленном множестве соответствующих приложений», – говорится в отчете Chatham House.

Станции на Земле, спутники и отправляемые в космос аппараты уязвимы ко всем видам кибератак, таким как повреждение, перехват и похищение данных, создание помех и спуфинг. Поэтому аналитики призывают исследователей безопасности как можно скорее обнаружить и устранить уязвимости в космических аппаратах.

По словам вице-президента по вопросам сбора информации американской компании CrowdStrike А. Мейерса (Adam Meyers), в последнее время участились попытки злоумышленников атаковать спутниковые системы, в особенности израильской телекомпании. «Они (хакеры. – Ред.) вмешиваются в работу систем, но не с целью сбора информации. Мы наблюдаем подобную активность все чаще, и она, безусловно, требует дополнительного изучения специалистами в области безопасности», – цитирует А. Мейерса издание HackRead.

***

28.09.2016

Хакеры по-прежнему заинтересованы в эксплуатации уязвимости Shellshock

В минувшие выходные исполнилось ровно два года с момента обнаружения серьезной уязвимости Shellshock. Тем не менее,

киберпреступники отнюдь не забыли о ней, о чем свидетельствуют собранные IBM X-Force данные телеметрии. Согласно этим данным, сканирование на наличие в UNIX-системах уязвимости Shellshock проводятся на регулярной основе (InternetUA).

Shellshock (CVE-2014-6271) является проблемой безопасности в GNU bash. Уязвимость затрагивает все выпущенные за последние 20 лет версии командной оболочки и все UNIX-системы, в которых они используются. Подробности о Shellshock были опубликованы 24 сентября 2014 г., и практически сразу же вышло исправление, однако владельцы серверов не спешили его устанавливать.

После того, как стало известно о проблеме, эксперты IBM зафиксировали порядка 2 тыс. инцидентов с использованием CVE-2014-6271. По их словам, с тех пор количество сканирований UNIX-систем на наличие этой уязвимости возросло в несколько сотен тысяч раз. Поскольку эксплоит для нее находится в открытом доступе, а использовать его проще простого, любой скучающий хакер-подросток мог атаковать уязвимые серверы лишь ради забавы.

По прошествии двух лет количество сканирований уменьшилось, но не намного – показатель нынешнего года такой же, как и в прошлом году, что удивительно для уязвимости двухлетней давности. По данным экспертов, количество сканирований на наличие уязвимости четырехлетней давности Heartbleed в среднем достигает нескольких сотен в месяц, тогда как для Shellshock этот показатель равен 10 тыс. Только в текущем месяце было осуществлено 20 тыс. сканирований.

46 % всех сканируемых систем находятся в США. Свыше 46 % систем принадлежат компаниям телекоммуникационной сферы и только 26 % – финансовой.

***

29.09.2016

Спамеры активно воруют IP-адреса в сетях IPv4

Специалисты некоммерческой организации SpamHaus, специализирующейся на противодействии распространению спама и вредоносного ПО, предупредили о росте активности спамеров, заинтересованных в присвоении неиспользуемых IP-адресов в сетях на основе протокола IPv4 (InternetUA).

В большинстве случаев злоумышленники изобретают различные методы «присвоения» неиспользуемых блоков адресов IPv4. По данным некоммерческой организации ARIN (American Registry for Internet Numbers - Американский реестр интернет-адресов), чаще всего для этой цели мошенники регистрируют фиктивные компании или повторно регистрируют старые доменные имена.

В блоге SpamHaus приведен случай такого мошенничества. По информации организации, одному из спамеров удалось присвоить IPv4-адреса,

принадлежащие легитимной компании, используя контактную информацию лица (умершего за несколько лет до инцидента), на которое было зарегистрировано доменное имя предприятия. Похищенные адреса злоумышленник в дальнейшем использовал в спам-кампаниях.

Довольно часто спамеры «присваивают» адресные пространства, не используемые в течение длительного периода времени. Преступники практически во всеуслышание «объявляют» всему Интернету, что данные адреса находятся во владении принадлежащего им хостинг-сервиса, и в случае отсутствия каких-либо возражений получают полный контроль над диапазоном IP-адресов.

***

29.09.2016

Check Point Software Technologies отметил всплеск активности кибервымогателей

Согласно отчету Check Point Software в августе 2016 г. заметно росло количество вариаций вредоносного ПО для вымогательства и объем атак в целом (ITnews).

Компания выделила наиболее активные виды вредоносного ПО за этот период.

В августе число видов активного вымогательского ПО возросло на 12 %, в то время как число обнаруженных попыток атак с использованием ransomware возросло на 30 %. Две трети всех обнаруженных кибервымогателей поднялись в рейтинге, большинство из них более чем на 100 позиций. Специалисты Check Point считают, что рост числа вымогательского ПО – следствие относительной легкости внедрения, а также того, что некоторые компании просто платят мошенникам, чтобы получить критические данные. В результате, такие атаки становятся прибыльным и привлекательным направлением для киберпреступников.

Количество атак на компании в России в августе 2016 г. не изменилось с прошлого месяца – в рейтинге наиболее атакуемых стран Threat Index наша страна занимает 50-е место. В топ-10 вредоносных семейств, атаковавших российские сети, вошли Kometaur, Conficker, InstalleRex, Ramnit, Zeus, Locky,Cryptowall, Sality, Dorkbot, Angler ek.

Check Point обнаружил, что число уникальных и активных семейств вредоносного ПО осталось таким же, как и в прошлом месяце, однако их использование в атаках остается неизменно высоким. В целом, Conficker был самым активным – на него пришлось 14 % всех распознанных атак; второе место занимает JBossjmx – 9 %; Sality также отвечает за 9 %. На топ-10 самых популярных семейств пришлось 57 % всех зарегистрированных атак.

1. – Conficker – Червь, обеспечивающий удаленное исполнение операций и загрузку вредоносного ПО. Инфицированный компьютер управляется ботом, который обращается за получением инструкций к своему командному серверу.

2. – JBossjmx – Червь, нацеленный на системы, на которых установлены уязвимые версии JBoss Application Server. Зловред создает вредоносную страницу JSP на уязвимых системах, которая выполняет произвольные команды. Кроме того, создается еще один бэкдор, который принимает команды от удаленного сервера IRC.

3. – Sality – Вирус, который заражает ОС Microsoft Windows и позволяет удаленные действия и загрузки других вредоносных программ. Из-за своей сложности и способностей к адаптации Sality считается на сегодняшний день одной из самых опасных вредоносных программ.

Семейства мобильных вредоносных программ по-прежнему представляют серьезную угрозу для корпоративных мобильных устройств. В течение пяти месяцев HummingBad оставался самым распространенным мобильным зловредом, однако число обнаруженных инцидентов сократилось более чем на 50 %.

***

2.10.2016

Взломы Yahoo!, Dropbox, LinkedIn и Tumblr дело рук одной хакерской группировки

Атаки на популярные сервисы Yahoo!, Dropbox, LinkedIn, Tumblr, «ВКонтакте» и прочие, в результате которых было похищено в общей сложности три миллиарда учетных записей, предположительно являются делом рук небольшой восточноевропейской группы Group E, включающей всего пять хакеров (InternetUA).

Как рассказал изданию The Register эксперт по информационной безопасности А. Комаров, группировка зарабатывает деньги на взломах компьютерных сетей компаний и продаже похищенных данных различным покупателям, включая правительства разных стран.

По словам эксперта, помимо популярных ресурсов, хакеры также проникли в сети ряда технических компаний, однако А. Комаров не раскрыл информацию, о каких именно предприятиях идет речь и о масштабах утечек, сославшись на конфиденциальность расследования.

Как отметил эксперт, официальные данные о количестве похищенной информации в результате взлома Yahoo! существенно занижены. По его словам, злоумышленники похитили не 500 млн учетных записей, а в два раза больше – 1 млрд.

По словам эксперта, в ходе атак хакеры эксплуатируют уязвимости в web-приложениях, а также инфицируют целевые системы вредоносным ПО. Похищенные базы данных злоумышленники продают через посредника, известного как Tessa88. Услугами этого брокера также пользуется другая группировка For Hell, предположительно взломавшая ресурсы Ashley Madison, Adult Friend Finder и сайт Турецкой национальной полиции.

***

1.10.2016

В атаке на сайт Информцентра СНБО силовики нашли «российский след» – СМИ

Как сообщил источник в силовых структурах, отвечающих за кибербезопасность, пока удалось выяснить, что хакерская атака на сайт была осуществлена по направлению, ведущему в сторону территории РФ (InternetUA).

«Удалось проследить путь хакерской атаки в направлении РФ. По крайней мере, известно, что атака на сайт Информцентра СНБО, после которого произошла поломка, была осуществлена с оккупированной территории Донбасса. Далее путь ведет в РФ, однако он не один и эту информацию следует проверить», – рассказали специалисты по кибербезопасности в силовых структурах.

Там также отметили, что хакерская атака является мощной и когда удастся возобновить работу ресурса – пока не известно.

***

1.10.2016

Хакерские атаки лишают Китай 15 млрд долл. ежегодно

Число хакерских атак в Китае достигает 400 тыс., а нанесенный ими ущерб оценивается в 15 млрд долл., сообщает Bloomberg (InternetUA).

По словам главного инженера компании по кибербезопасности FireEye Б. Боланда, в стране существует большая преступная экосистема.

Согласно опросу PwC, проведенному среди 330 генеральных директоров IT-компаний, работающих на территории Китая и Гонконга, только за 2016 г. число обнаруженных кибератак увеличилось на 417 %.

PwC отмечает, что эти взломы нацелены на базу данных клиентов и собственные записи компаний и обычно обходятся каждой корпорации в 2,6 млн долл. ежегодно.

Одна из причин, по которой Китай является привлекательной мишенью для хакеров, – активное использование населением технологий мобильного платежа: кошельков WeChat, Alipay и др. Также в Китае распространены автоматические соединения с Wi-Fi, многие из которых являются ложными и могут получить доступ к вашим данным посредством вируса.

В связи с постоянными нападениями хакеров власти Китая создали законопроект о кибербезопасности, который прошел две стадии рассмотрения и может быть введен к концу этого года. Этот законопроект поможет переосмыслить значение новых технологий в безопасности сети и даст больше свободы действий в киберзащите.

***

2.10.2016

Защитить клавиатуры от хакеров может шум

Для блокирования атак на компьютерную клавиатуру, производимых по акустическим побочным каналам, исследователи из Алабамского университета предложили использовать активный шум (InternetUA).

При атаках этого типа злоумышленники записывают звуки, издаваемые клавиатурой, на скрытно размещённые микрофоны. Каждая клавиша при нажатии генерирует свойственный только ей звук, благодаря чему хакер, применив статистический анализ, способен идентифицировать всю вводимую последовательность символов.

В работе, представленной на конференции по финансовой криптографии и безопасности данных, адъюнкт-профессор Н. Саксена (Nitesh Saxena) и его ассистент А. Ананд (S Abhishek Anand) показали, что различные фоновые шумы могут служить средством маскировки утечки звука от клавиш, обеспечивая практическую защиту от атак по побочным акустическим каналам.

Точность результатов, получаемых в результате таких атак, обычно довольно высока. Имитируя их, А. Ананд и Н. Саксена угадывали правильный символ в случайным образом сгенерированном шестизначном пароле со средней точностью 66 %.

Ранее, для защиты от нападений по акустическим побочным каналам предлагали беззвучные клавиатуры и гомофонные конструкции, в которых все клавиши звучат одинаково, а также звукоизолированные помещения для набора критической информации. Решение инженеров из Алабамы значительно проще, дешевле и надёжнее всех этих вариантов. Оно использует программное обеспечение, которое устанавливается на ПК и заставляет его издавать маскирующий звуковой сигнал каждый раз при нажатии кнопки на клавиатуре. Механизм защиты предусматривает возможность его включения или отключения – автоматически или самим пользователем.

Тестирование на трёх системах паролевой аутентификации показало, что наименее эффективно маскирует нажатия белый шум, лучше действует имитация звука срабатывания других кнопок, а максимальный эффект обеспечивает сочетание обоих этих сигналов.

Авторы указывают, что реализовать такое решение можно даже на смартфоне, установив на него соответствующее приложение и поместив его поблизости от клавиатуры, на которой предстоит набирать пароль.

***

2.10.2016

Эксперты пресекли работу ботнета GozNym

Специалисты Cisco Talos остановили работу одного из ботнетов, организованных гибридным банковским трояном GozNym, сочетающим функционал двух известных вредоносов Gozi и Nymaim (InternetUA). В

настоящее время команда принимает меры по пресечению деятельности остальных ботнетов GozNym.

Экспертам удалось остановить работу ботнета, взломав алгоритм генерации доменных имен (DGA), используемый трояном для связи с постоянно меняющимися C&C-серверами злоумышленников. По данным Cisco Talos, ботнет включает по меньшей мере 23 062 инфицированных хостов, большинство из которых расположены в Германии, США, Польше, Канаде и Великобритании.

Исследователи зафиксировали несколько целевых фишинговых кампаний по распространению вредоносного ПО GozNym. В ходе атак злоумышленники рассылали вредоносные документы Microsoft Word, содержащие загрузчик, который загружал и выполнял вредоносный код.

В апреле нынешнего года троян GozNym был замечен в ряде кампаний, направленных на пользователей в США и Канаде, а затем распространившихся на Европу. Спустя несколько месяцев специалисты buguroo Threat Intelligence Labs зафиксировали новый виток атак с использованием GozNym, нацеленных на банки и финансовые сервисы в Испании, Польше, Японии и в ряде случаев – на пользователей из Канады, Италии и Австралии.

***

1.10.2016

Банковский троян Dridex скрывается в защищенных паролями документах

Независимый исследователь, автор блога MalwareTech, заметил, что операторы известного банкера Dridex изменили почерк. Так, в последнее время спам, распространяющий троянца, все чаще исходит с легитимных сайтов, которые были скомпрометированы злоумышленниками. Раньше операторы банкера использовали для распространения трояна ботнет Necurs, однако, судя по всему, сейчас операторы малвари испытывают новую тактику. Исследователь пишет, что из-за изменения паттерна вредоносный спам снова обходит фильтры (InternetUA).

Еще одно изменение, тоже призванное обмануть фильтры, это использование защищенных паролем документов.

«Вредоносные RTF-файлы (документы Word) защищены паролем, который приводится прямо в письме. Это не дает автоматическим системам извлечь и просканировать содержимое вложения на предмет вредоносного кода, так как большинство из них неспособны обнаружить пароль и расшифровать документ», – пишет исследователь.

Но если автоматика не может заглянуть внутрь такого файла, это без труда может сделать пользователь: достаточно открыть файл с помощью приведенного в письме пароля. Как только жертва запустит такой RTF-файл, ее попросят разрешить работу макросов (для этого, как обычно, используется социальная инженерия). Если пользователь попался на удочку атакующих и

включил макросы, вредоносный скрипт скачивает с управляющего сервера лоадер Dridex, который тоже отличается от предыдущих версий. Исследователь пишет, что перед началом работы лоадер запускает интерфейс командной строки и 250 раз пингует один из DNS-серверов Google. Судя по всему, таким образом авторы трояна реализовали отложенный старт работы малвари, потому что после Dridex запускается, независимо от результатов пингов.

В заключении автор MalwareTech пишет, что в целом эта кампания не сильно отличается от обычных компаний Dridex, но, тем не менее, похоже, что в этом случае операторы трояна нацелились на более защищенные цели. Похоже, что эта версия Dridex ориентирована на заражение корпоративных систем, которые защищены не в пример лучше обычных пользователей

***

1.10.2016

Россия усиливает киберкампанию против США

Американские власти уверены, что хакер Guccifer 2.0 является частью синдиката, используемого РФ для маскировки своей причастности к ряду кибератак, в частности, взлому серверов Национального комитета Демократической партии и ее организаций. Об этом пишет издание The Wall Street Journal со ссылкой на осведомленные источники (InternetUA).

Хотя Guccifer 2.0 отрицает связь с российским правительством, американские чиновники и независимые эксперты в области информационной безопасности говорят об усилении кампании со стороны России, направленной на известных американских спортсменов, членов партий и военных чиновников.

По мнению властей США, по крайней мере две связанные с правительством РФ группировки (Fancy Bear и Cozy Bear) причастны к хищению больших объемов данных, которые затем были опубликованы на трех ресурсах – WikiLeaks, DCLeaks.com и в блоге Guccifer 2.0. Как считают эксперты, DCLeaks.com и Guccifer 2.0 часто сотрудничают между собой и имеют непосредственную связь с российскими хакерами.

Согласно мнению ряда аналитиков, целью России может являться дискредитация политических партий и ведомств правительства США.

Соціальні мережі

як чинник інформаційної безпеки

Інформаційно-аналітичний бюлетень
Додаток до журналу «Україна: події, факти, коментарі»

Упорядник **Терещенко** Ірина

Редактори: Т. Дубас, О. Федоренко, Ю. Шлапак

Свідоцтво про державну реєстрацію КВ № 5358 від 03.08.2001 р.

Видавець і виготовлювач
Національна бібліотека України
імені В. І. Вернадського
03039, м. Київ, просп. 40-річчя Жовтня, 3
Тел. (044) 524-25-48, (044) 525-61-03
E-mail: siaz2014@ukr.net
www.nbuv.gov.ua/siaz.html

Свідоцтво про внесення суб'єкта видавничої справи
до Державного реєстру видавців виготівників
і розповсюджувачів видавничої продукції
ДК № 1390 від 11.06.2003 р.