СОЦІАЛЬНІ МЕРЕЖІ ЯК ЧИННИК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Огляд інтернет-ресурсів
(31.01–13.02)

2018 № 3

Соціальні мережі
як чинник інформаційної безпеки

Інформаційно-аналітичний бюлетень
Додаток до журналу «Україна: події, факти, коментарі»
Огляд інтернет-ресурсів
(31.01–13.02)
№ 3

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 2018

ЗМІСТ

Орфографія та стилістика матеріалів – авторські

РОЗВИТОК І ПЕРСПЕКТИВИ СОЦІАЛЬНИХ МЕРЕЖ

31.01.2018
В Instagram появится новая функция

Разработчики Instagram тестируют функцию видеозвонков для одноименной социальной сети. Соответствующее нововведение было обнаружено в предварительной версии приложения для платформы iOS авторами блога @WABetaInfo, о чем они рассказали своим читателям в твиттере (InternetUA).

Пиктограмма видеовызова появилась в разделе сообщений, позволяя предположить, что разработчики планируют повысить статус Instagram от социальной сети для демонстрации фотографий и видеозаписей до полноценного мессенджера, способного конкурировать с WhatsApp и Telegram.

Сообщается, что, несмотря на наличие в интерфейсе клавиши для видеозвонка, данная функция остается неактивной даже для участников программы предварительного тестирования. Вполне возможно, что она будет запущена позднее, после налаживания соответствующей инфраструктуры.

***

31.01.2018
Лише 58% українців користуються інтернетом. Дослідження

В Україні налічують майже 26 млн активних користувачів інтернету, що становить 58 % від загальної кількості населення. Про це йдеться у дослідженні міжнародної організації We are social (Espreso.tv).

Також зазначається, що в інтернеті через смартфони «сидять» 18,7 млн громадян України (42 % від загального населення).

Якщо говорити про соціальні мережі, то в Україні налічують рівно 13 млн користувачів, із них 22 % «сидять» у Twitter та інших мережах через смартфони.

13 млн українців хоч раз на місяць з'являються у Facebook. З усіх користувачів більшість становлять жінки (57 %).

Також популярністю в українців користується Instagram. Соціальна мережа для публікації фото та відео налічує 7,2 млн українців. Це 16 % від загальної кількості населення України.

Також у звіті йдеться про збільшення кількості користувачів інтернету у січні 2018 року (до всесвітнього павутиння приєдналось 4 млн користувачів). На стільки ж впала популярність соцмереж. Повідомляється, що 72 % українців користуються інтернетом щодня.

Також Україна з'явилась у списку країн з найповільнішим мобільним зв'язком (114 місце), найсбалансованішим гендерним співвідношенням серед користувачів Facebook, найвищим рівнем зацікавленості (на 3 місці).

***

1.02.2018

Пользователи Facebook стали проводить в соцсети на 50 млн часов в день меньше

Недавнее изменение алгоритмов формирования новостной ленты Facebook привело к тому, что пользователи стали проводить в соцсети на 50 млн часов в день меньше. Об этом сообщил основатель соцсети Марк Цукерберг, комментируя квартальный и годовой отчеты компании (InternetUA).

Напомним, речь идет о том, что теперь Facebook при формировании ленты отдает приоритет записям пользователей, а не публикациям СМИ и брендов и вирусным видеороликам. Таким способом соцсеть стремится сподвигнуть пользователей к взаимодействию вместо пассивного потребления различного контента. По словам Цукерберга, новая стратегия принесет пользу компании в долгосрочной перспективе.

Что же касается опубликованных отчетов Facebook, то в четвертом квартале прошлого года выручка Facebook выросла на 47 % и составила 12,9 млрд долларов. Чистая прибыль увеличилась на 20 % и составила 4,27 млрд долларов (1,44 доллара на акцию). При этом в Facebook отмечают, что квартальная прибыль могла бы составить 2,21 доллара на акцию, но компания вынуждена была заплатить больше налогов в связи с недавней реформой законодательства США в этой сфере.

Годовая выручка компании достигла 40,6 млрд долларов (+47 %), а прибыль составила 15,9 млрд, увеличившись на 56 %.

***

1.02.2018

Михаил Сапитон

Telegram выпустил открытую библиотеку для создания альтернативных клиентов

Вместе с официальным релизом альтернативного клиента Telegram X для Android, мессенджер Павла Дурова также открыл разработчикам доступ к библиотеке TDLib (Telegram Database Library). Инструмент призван сменить Telegram API в качестве основы для создания альтернативных версий приложения (AIN.UA).

С TDLib девелоперам не понадобится беспокоиться про шифрование данных или управление локальным хранилищем, сконцентрировавшись на разработке дополнительных функций. Использовать TDLib можно для разработки на любую платформу (Android, iOS, Windows, macOS, Linux). Библиотека способна исполняться на любом языке, поддерживающем функции C, а также также совместима с Java и C.

TDLib будет оставаться стабильной на медленном и ненадежном интернет-соединении, а также гарантирует, что все обновления будут представлены в правильном порядке. Все локальные данные защищены пользовательским ключом шифрования.

Как и исходный код Telegram, найти TDLib можно в открытом репозитории на GitHub. Команда проекта называет первой демонстрацией возможностей библиотеки клиент Telegram X – используя новый инструментарий, разработчики потратили около года на воспроизведение всех основных функций и добавление множества новых.

***

1.02.2018

В Telegram появилась долгожданная полезная функция

Разработчики Telegram добавили в мессенджер новую функцию, которая позволит пользователям составлять «новостную ленту» из отдельных каналов. Возможность уже появилась в бета-версии приложения для macOS.

Теперь пользователи Telegram смогут выделить все каналы, на которые они подписаны, в отдельную папку «Лента». Благодаря этому подписки не будут смешиваться с основным списком контактов и отвлекать уведомлениями (InternetUA).

Помимо всего прочего, в мессенджере тестируют возможность редактировать тексты прямо в десктопной приложении для macOS. Можно будет выделять текст, добавлять ссылки и так далее, не выходя из программы. Пока неизвестно, когда нововведения станут официально доступны для всех пользователей.

***

5.02.2018

Невероятно полезная и нужная возможность Telegram, о которой обязан знать каждый

С каждым днем мессенджер Telegram становится все более популярным средством для общения. Разработчики всячески способствуют этому, регулярно добавляя в свой сервис полезные функции и возможностей, о которых просят пользователи. Теперь любой чат можно сделать приоритетным, закрепив его в самом верху раздела с сообщениями.

Докладніше

***

6.02.2018

YouTube введёт строгие санкции против вредящих сообществу авторов

YouTube начнёт гораздо строже наказывать владельцев каналов, которые вредят репутации сервиса. Генеральный директор Сьюзен Войжитски (Susan Wojcicki) рассказала о главных целях компании на 2018 год. Одним из самых примечательных обещаний стало введение штрафных санкций против авторов, которые «делают что-то вопиющее, что наносит значительный вред» всему сообществу.

Докладніше

***

7.02.2018

В Telegram появилась одна из функций соцсетей

Шестого февраля у популярного мессенджера появился виджет Telegram Login, который позволяет авторизоваться пользователям Telegram на других сайтах (Телекритика).

Об этом разработчики Telegram написали в своем официальном блоге.

Разработчики сайтов смогут внедрять виджет на свои страницы. При первом взаимодействии с ним пользователь должен будет ввести номер телефона и получить подтверждение в виде кода. Но последующие входы на сторонние сайты при помощи мессенджера будут происходить буквально в два клика.

Владельцы сайтов смогут получить доступ к логину пользователя в Telegram, фотографии профиля и к указанному имени. Однако номер телефона, привязанный к Telegram, будет скрыт.

Владельцы сайтов также смогут запрашивать у пользователя разрешение на отправку сообщений в Telegram при помощи ботов, что сделает мессенджер более полезным для бизнеса.

***

8.02.2018

Instagram позволит делиться постами в историях

Instagram популярен, и это сложно не признавать. Соцсеть постоянно получает интересные нововведения, это позволяет ей держаться на плаву. В этот раз речь пойдет об очередном интересном обновлении, с помощью которого можно будет делиться публикациями друзей у себя в историях (InternetUA).

Со слов TechCrunch, пока лишь небольшой процент пользователей получили возможность делиться постами в историях. При этом к публикации можно добавить стикеры или использовать свои навыки в рисовании, можно также изменять размер изображения и вращать его. В настройках также можно отключить эту возможность (пользователи не смогут делиться вашими публикациями).

Неизвестно, когда именно обновление станет доступно всем пользователям, но, как правило, рассылку начинают в течение нескольких недель с момента начала тестирования.

***

12.02.2018
Google создает новый мессенджер

Инженеры компании Google приступили к разработке нового мессенджера, который призван стать конкурентом WhatsApp и других аналогичных сервисов, сообщаетAndroid Police (IGate).

Ранее поисковой гигант уже пытался создать популярную «общалку», однако ни Hangouts, ни Google Allo не смогли привлечь большую аудиторию пользователей. Поэтому компания сосредоточилась на разработке нового продукта.

Согласно инсайдерским данным, будущий сервис будет совместим с компьютерами. Скорее всего, приложение будет выполнено в виде расширения браузера. Для того, чтобы синхронизировать компьютер и смартфон, пользователю придется отсканировать QR-код. Инженеры работают над тем, чтобы приложение было совместимо со всеми существующими браузерами. В случае успеха, Android-сообщения можно будет прочитать на любом устройстве. Сервис будет работать по принципу Telegram, WhatsApp и других популярных мессенджеров.

Сообщения Android, как и любой другой Rich Communication Service, позволят передавать фото и другие документы, будут отражать статус набора текста и поддерживать возможность совершения платежей. Это будет более безопасно, чем транзакции при помощи Google-кошелька, и позволит оплачивать продукты и услуги сторонних компаний.

***

13.02.2018
Facebook запустил фоторедактор в Историях

Команда социальной сети Facebook запустила специальный редактор для фотографий в Историях (Stories) для десктопных пользователей. Об этом сообщил ресурс TheNextWeb (InternetUA).

Функциональность напоминает стандартный редактор для публикации фото и предлагает различные опции – добавление текста, цветовые фильтры и стикеры. Для доступа к редактору в Историях потребуется просто нажать кнопку «редактировать фото» в правом нижнем углу.

Facebook начала попытки с адаптацией Историей к своему приложению более года назад. Однако, в отличие от Instagram и Snapchat, где Истории пришлись к месту, в Facebook пользователи не пришли от них в восторг.

***

13.02.2018

Ольга Карпенко

Ко Дню влюбленных украинские юристы запустили бота, помогающего развестись

Команда «Юскутум» объявила о новой разработке – это чат-бот для Facebook под названием SudoBot, который поможет парам оформить развод. Бот поможет составить и подать заявление на развод, оплатить услугу и пригласить стороны в суд (AIN.UA).

Как отмечают в компании, обращение к боту избавит пользователя от необходимости идти в суд для того, чтобы подавать исковое заявление. Кроме того, сама процедура обойдется дешевле. «К примеру, бот зарегистрирует ваш иск за 950 грн, а оформление развода в суде стоит около 1500 грн», – отмечают юристы.

Чтобы воспользоваться услугами бота, нужно зайти на его страницу, написать сообщение и начать разговор. В диалоге нужно предоставить ведомости о муже или жене, в результате бот составит готовое заявление. Его подписывают адвокаты «Юскутум» и оно отправляется в суд. Бот также может давать советы о том, как вести себя в суде, и что делать, когда придет повестка.

В Украине услуги бота уже опробовали: 24 января суд принял первое решение о расторжении брака, оформленное с помощью SudoBot.

***

13.02.2018

Вслед за Google. Facebook начал строить сеть «зеркал» в Украине

Сбои при загрузке ленты Facebook, не открывается видео или проблемы с Messenger – в последнее время на это часто жалуются украинские пользователи. После запрета российских соцсетей в Украине Facebook становится коммуникационной платформой №1. И количество местного трафика, проходящего через его сервисы, быстро увеличивается.

Докладніше

***

13.02.2018

Facebook теряет популярность у молодежи в США

В 2018 году количество молодых пользователей Facebook снизится на 5,8 процента. Число активных юзеров Instagram и Snapchat наоборот растет. Социальная сеть Facebook продолжает терять популярность среди американских подростков и молодежи.

Докладніше

СОЦІАЛЬНІ МЕРЕЖІ ЯК ВИЯВ ФОРМУВАННЯ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА

31.01.2018
В сетях вспыхнул PR-скандал вокруг отпуска Луценко

В Twitter пользователи обсуждают недавний отдых генерального прокурора Украины на Сейшельских островах, который, по его словам, был «без излишеств». Именно эта фраза и зацепила украинцев. За аренду двух вилл Луценко заплатил 42 368 евро и отметил, что его зарплата это позволяет. У себя в Фейсбук Юрий Луценко рассказал, откуда взял деньги на отдых и выложил фотокопии соответствующих документов. Пользователей это, однако, не успокоило. Ранее в стране обсуждали отдых президента Украины Петра Порошенко на Мальдивах (Marketing Media Review).

***

3.02.2018
Депутати Київради проїдуться громадським транспортом для селфі

Депутат Київради Сергій Харчук запропонував колегам частіше користуватись громадським транспортом та виставляти свої фото в соціальні мережі з хештегом «#Яобираюгромадськийтранспорт» (Хмарочос).

Як повідомляє Харчук на своїй сторінці у Facebook, на засіданні Комісії з питань транспорту, реклами та зв'язку, він запропонував членам комісії та керівництву Департаменту транспортної інфраструктури зрозуміти проблеми перевізників обираючи для подорожей містом громадський транспорт. Учасники флешмобу викладатимуть селфі з маршруток, трамваїв та тролейбусів та підкріплюватимуть хештег «#Яобираюгромадськийтранспорт».

«Сьогодні пересувався зранку в маршрутці №181. Стара, іржава, перекошена "залізна фіра". Проте, в салоні досить чисто та тепло (бувають гірше). Кожного разу, коли водій відволікаючись, повертає решту, розумієш критичну необхідність впровадження електронного квитка», – пише автор флешмобу Сергій Харчук.

Своє фото в соціальну мережу на підтримку флешмобу вже виклав директор Департаменту транспортної інфраструктури Сергій Симонов.

***

8.02.2018
Підприємці запустили флешмоб «Купуй українське, плати українцям!»

Інтернетом поширюються відео-звернення підприємців з різних регіонів країни, які виступають за прийняття законопроекту «Купуй українське, плати українцям!», ініційованого фракцією РПЛ та промисловим лоббі у Верховній Раді (Економіст).

Вони виробляють якісну продукцію, створюють робочі місця, наповнюють держбюджет та переконані, що підтримка вітчизняного виробника через механізм державних закупівель, як і в розвинених країнах світу, позитивно відобразиться на житті кожного громадянина.

***

12.02.2018

У Facebook – флешмоб на підтримку луцького патрульного

У Facebook запустили флешмоб на підтримку луцького патрульного Дмитра Мандзюка, який захищаючись від нападників, поранив одного з чоловіків (ВолиньPost).

Люди стали на захист поліцейського, який постраждав через зауваження чоловікам, що вживали алкоголь у Центральному парку культури і відпочинку імені Лесі Українки. На своїх сторінках вони пишуть дописи із хештегом #право_на_самозахист, а дехто ще й додає хештег #право_на_зауваження.

Нагадаємо, інцидент стався у суботу, 10 лютого. Патрульний захищаючись, використав складаний ніж, яким поранив одного з порушників громадського порядку. Життю пораненого наразі нічого не загрожує.

***

12.02.2018

«Хто до нас з Польщі прийде, той до Польщі повернеться»: В соцмережі відреагували на затримання Саакашвілі

12 лютого, близько 15:00 українські силовики затримали екс-главу Одеської ОДА Міхеіла Саакашвілі у столичному ресторані «Сулугуні». Згодом у Державній прикордонній службі підтвердили інформацію про затримання і видворення політика з України (Інформатор).

Подію активно коментують користувачі соціальних мереж.

Політтехнолог Віктор Уколов пожартував: «Хто до нас із Польщі прийде, той до Польщі і повернеться».

Політолог Павло Нусс не виключає, що із Польщі Саакашвілі буде перенаправлений в Грузію.

БІЗНЕС І СОЦІАЛЬНІ МЕРЕЖІ

31.01.2018

Facebook забороняє рекламу криптовалют, щоб людей не обдурювали

Facebook вводить заборону на рекламу різних криптовалютних проектів, щоб захистити користувачів від фінансових авантюр. У правилах реклами на Facebook з'явився новий пункт, який стосується заборони реклами сумнівних фінансових продуктів.

Докладніше

***

1.02.2018
Ольга Карпенко
Instagram разрешил бизнесу публиковать отложенные посты

Instagram обновил API – теперь для владельцев бизнес-аккаунтов доступны функции отложенной публикации и планирования постов. Об этом сообщается в официальном блоге компании. Эта новая функция добавлена в рамках апдейта Instagram API до Instagram Graph API, основанного на Facebook Graph API – в связи с этим же, многие старые функции Instagram API будут понемногуотключаться (AIN.UA).

В отличие от Facebook, ранее в Instagram для бизнеса нельзя было планировать и публиковать отложенные посты. Правда, такая возможность доступна не в самом аккаунте, а открывается через API для сторонних сервисов вроде Hootsuite или SocialFlow. По словам Райяна Холмса, CEO Hootsuite, на нее давно существовал запрос: «Планирование и публикация контента в Instagram давно была запросом номер 1 для наших 16 млн клиентов. Сейчас они с легкостью смогут управлять большими объемами контента сразу во многих аккаунтах».

«Создание постов в Instagram всегда занимало много времени. Для обычных пользователей это вряд ли проблема, но если вы – медиакомпания, которая создает более 100 000 постов в месяц, просто невозможно делать все вручную», – говорит CEO SocialFlow Джим Андерсон в комментарии TechCrunch.

***

5.02.2018
Facebook в полтора раза нарастила доход и прибыль в прошлом году

Facebook отчиталась о финансовых итогах четвертого квартала и всего 2017 года (Компьютерное Обозрение).

За квартал социальная сеть получила доход на уровне 12,97 млрд долл., нарастив его за год на 47 %. Прибыль при этом выросла на 20 % до 4,27 млрд долл.

Доходы от мобильной рекламы составили примерно 89 % от рекламных поступлений компании за четвертый квартал 2017 г., по сравнению с примерно 84% в четвертом квартале 2016 г.

Доход по итогам 2017 г. составил 40,65 млрд долл., что на те же 47 % превышает результат предыдущего года. Прибыль за год выросла еще более значительно – на 56 % – и достигла 15,93 млрд долл.

За прошедший год размер месячной активной аудитории Facebook вырос на на 14 % и сейчас составляет 2,13 млрд человек, дневной активной аудитории – также на 14 %, до 1,4 млрд человек.

***

3.02.2018

YouTube будет помечать СМИ, которые получают государственное финансирование

Нововведение пока работает только на территории США (Зеркало недели. Украина).

Видео хостинг YouTube начнет помечать видео от СМИ, которые получают государственное или публичное финансирование, сообщается в блоге хостинга.

Отмечается, что целью нововведения является обеспечение пользователей дополнительной информацией, которая поможет им лучше понять источник новостей, которые они собираются посмотреть.

На данный момент эта функция работает только на территории США, разработчики предлагают пользователям оставить свой отзыв о функции.

Отмечается, что пометка появится под видео, но над его названием и будет содержать ссылку на Википедию для того, чтобы пользователи могли получить подробную информацию о СМИ.

***

4.02.2018

Китайские поисковики и соцсети начали блокировать рекламу криптовалют

Крупные социальные сети и поисковые движки в Китае перестали отображать рекламный или спонсорский контент, связанный с биткоином и другими криптовалютами. Об этом сообщает South China Morning Post (InternetUA).

Так, на поисковые запросы, содержащие слова «биткоин», «криптовалюта» и «ICO», пользователям выдаются исключительно новостные и другие журналистские заметки. Известно, что рекламу, связанную с цифровыми активами, перестали отображать крупнейшая в стране поисковая система Baidu и китайский аналог Twitter – микроблог Weibo.

Представители Weibo подтвердили, что площадка в данный момент действительно блокирует всю рекламу, связанную с биткоином и другими криптовалютами. В Baidu ситуацию комментировать не стали.

По данным издания, блокировка могла оказаться прямым следствием запрета первичных предложений монет (ICO) в сентябре прошлого года. Тогда Народный банк Китая назвал подобные кампании мошенническими. После этого свыше 90 % местных ICO-стартапов вернули средства инвесторам.

***

7.02.2018

Facebook: у криптовалют пока слишком много проблем, чтобы внедрять их в мессенджер

Вице-президент по разработке мессенджера Facebook Дэвид Маркус заявил, что в обозримом будущем компания не планирует запускать на платформе систему криптовалютных платежей, сообщает Coindesk (InternetUA).

По словам Маркуса, пока с существующими криптовалютами связано слишком много проблем и негативных факторов, в том числе высокие комиссии за переводы и низкая скорость подтверждения транзакций.

«Когда индустрия начнет лучше саморегулироваться, когда появится значительное количество достойных продуктов, которым нужна реклама на платформе, – на этом этапе мы что-нибудь придумаем, чтобы интегрировать подобные вещи», – отметил Маркус.

Стоит отметить, что в конце 2017 года он вошел в состав совета директоров крупнейшей американской криптовалютной платформы Coinbase. По словам Маркуса, если сообщество разработчиков «исправит все проблемы», то Facebook может пересмотреть свою позицию.

Такое заявление прозвучало спустя несколько дней после того, как Facebook запретил рекламу криптовалют и ICO.

***

7.02.2018

Facebook объявил войну YouTube

Сообщается, что социальный гигант Facebook рассматривает возможность расширения своего телевизионного сервиса Watch, чтобы превратиться в настоящего конкурента YouTube.

Докладніше

***

7.02.2018

Facebook начнет угадывать социально-экономический статус пользователей

В новом патенте компании Facebook описывается система, которая будет использовать данные пользователя, например, образование, историю

путешествий, количество принадлежащих устройств и домовладений, для предугадывания его социально-экономического статуса. Патент был обнаружен сайтом CBInsights.

Докладніше

***

8.02.2018

Владелец мессенджера Snapchat отчитался о росте выручки и аудитории

В октябре-декабре 2017 года выручка Snap достигла 285,7 млн долларов, что на 72 % больше, чем годом ранее. Чистый убыток возрос примерно вдвое – со 170 млн долларов (20 центов на акцию) до 350 млн долларов (28 центов в расчете на одну ценную бумагу).

Докладніше

***

9.02.2018

Twitter впервые за время существования закончил квартал с прибылью

По итогам отчета за последний квартал 2017 года Twitter показал прибыль в $91 миллион. Это можно считать историческим событием для компании: все предыдущие двенадцать лет сервис микроблогов заканчивал отчетные периоды с убытками. Для сравнения, четвертый квартал 2016 года компания закрыла с минусом в $167 миллионов (InternetUA).

Всего же выручка составила $731 миллион, в то время как аналитики предсказывали цифру на уровне $686 миллионов. При этом пользовательская база не росла в четвертом квартале, а по сравнению с прошлым годом она увеличилась на 4 %.

Отмечается, что на прибыли компании хорошо сказалась работа в области рекламы и видеоконтента.

Twitter появился в 2006 году. Долгое время длина сообщения была ограничена 140 символами, но недавно компания удвоила максимальное количество знаков для одного твита.

***

12.02.2018

Facebook запустила программу по поддержке онлайн-лидеров сообществ

Социальная сеть предусмотрела фонд в $10 млн для награждения пользователей, «которые объединяют людей» на платформе. Компания предоставит пяти «лидерам сообществ» со всего мира по миллиону долларов на

финансирование их идей для проектов. А также пригласит 100 людей для участия в программе по сотрудничеству, которая включает тренинг, менторство и $50,000 на специальную инициативу. «Наша цель найти людей, которые пользуются Facebook, Instagram, WhatsApp и Messenger для того, чтобы сблизить людей, – отметил Цукерберг в посте. – Цель программы в том, чтобы найти и поддержать лидеров сообществ. Они не просто помогают людям сближаться в онлайне. Многие онлайн-сообщества укрепляют физические сообщества, организовывая ивенты, посиделки и поддерживая друг друга в ежедневной жизни, даже на расстоянии». В качестве примера Цукерберг назвал «пастора церкви, тренера небольшой команды или соседа, который всегда рядом и готов помочь» (Marketing Media Review).

***

12.02.2018
Whatsapp тестирует собственную платежную систему

Мессенджер WhatsApp начал тестирование сервиса WhatsApp Pay для оплаты услуг и покупок через смартфон (IGate).

Новый сервис запущен в бета-версии мессенджера на iOS и Android и пока работает только в Индии. Денежные переводы возможны только между кошельками WhatsApp Pay.

Разработчики планируют создать условия, при которых бы платежная система смогла работать и с другими сервисами. Компания уже заключила договоры с ведущими банками Индии, включая Государственный банк, ICICI Bank, HDFC Bank, and Axis Bank. Таким образом, пользователи смогут синхронизировать новый платежный сервис со своей банковской картой.

Когда WhatsApp Pay будет доступен пользователям в других странах, пока не сообщается. Это, в том числе, будет зависеть от успеха тестирования сервиса в Индии.

***

13.02.2018
УНІАН запустив новинного бота

Інформаційне агентство УНІАН запустило новинного чат-бота, за допомогою якого можна отримувати розсилки в Facebook Messenger з головними подіями, корисними статтями і анонсами цікавих заходів.

Докладніше

***

13.02.2018
Крупнейший мировой производитель грозится изъять рекламу из Google и Facebook

Компания Unilever пригрозила снять свою рекламу с онлайн-платформ, таких как Facebook и Google, если они не смогут искоренить контент, который «создает разделение в обществе и способствует разжиганию гнева и ненависти».

Докладніше

СОЦІАЛЬНІ МЕРЕЖІ І ПРОБЛЕМИ СУСПІЛЬНОЇ БЕЗПЕКИ

Інформаційно-психологічний вплив мережевого спілкування на особистість

31.01.2018
Facebook обвинили в завлечении детей в соцсети

Более сотни специалистов в области детского здоровья подписали открытое письмо Марку Цукербергу. В послании эксперты требуют закрыть приложение Messenger Kids, которое, по их мнению, способствует вовлечению детей в суровый мир социальных сетей (InternetUA).

Недавно вышедший Messenger Kids предназначен специально для детей: приложение позволяет родителям контролировать контент, который просматривают их чада. Таким образом Facebook стремится ограничить детей от нежелательной рекламы и прочей информации, которую ребятам лучше не видеть.

Специалисты же полагают, что подобные приложения только вызывают интерес у детей к социальным сетям, в то время как они еще не готовы к контенту и особенностям виртуального общения. Вместе с этим дети станут проводить больше времени за смартфонами и компьютерами, что может негативно сказаться на их развитии.

Facebook в свою очередь отметил, что благодаря Messenger Kids родители всегда могут пообщаться с ребенком.

***

6.02.2018
Facebook встала в защиту платформы Messenger Kids от критиков

Дэвид Маркус, вице-президент Facebook Messaging Products, ответил на критику в адрес Messenger Kids во время выступления на саммите Upfront в Лос-Анджелесе (InternetUA).

По его словам, основная идея состоит в том, чтобы помочь младшим братьям и сёстрам присоединиться к групповым чатам. «Семьям станет легче общаться благодаря этой программе. Я уверен, что это хороший продукт», – отметил Маркус.

Выпущенный в декабре сервис Messenger Kids предназначался для детей в возрасте от 6 до 12 лет. Приложение столкнулось с критикой из-за того, что поощряет молодежь присоединяться к социальным сетям в раннем возрасте. Некоторые противники программы утверждают, что это является нарушением правил COPPA. Маркус настаивал на том, что продукт Facebook для детей не относится к социальным сетям как Snapchat.

«Моя дочь использует его ежедневно. Это позволило мне больше общаться с ней», – заяаил Маркус.

***

1.02.2018

Два школьника довели одноклассницу до суицида издевательствами в сети

Два подростка из Флориды обвиняются в слежке и нападках в интернете на свою знакомую, сообщает издание Forbes. По версии следствия, кибersталкинг и травля довели девочку до самоубийства (InternetUA).

12-летняя Габриэлла Пейтон Грин (Gabriella Peyton Green) стала жертвой издевательств одноклассников. Тщательное исследование содержимого мобильных телефонов школьников показало, что они постоянно травили девочку в социальных сетях.

Эксперты в области информационных технологий неоднократно утверждали, что предоставление детям неограниченного бесплатного доступа к онлайн-сервисам может привести к глобальным проблемам. Множество несовершеннолетних по всему миру воспринимают виртуальную жизнь близко к сердцу и считают проблемы в сети поводом к насилию или самоубийству.

***

4.02.2018

Facebook вредит обществу больше, чем McDonald’s

Возможно, Walmart и McDonald’s и вредят обществу, но по степени негативного воздействия Facebook удалось перегнать их обоих. По крайней мере, так ответили 2000 американцев в опросе исследовательской компании Honest Data, пишет Business Insider.

Докладніше

***

6.02.2018

Пчелы против меда. Бывшие сотрудники Facebook и Google решили побороться с соцсетями

Бывшие сотрудники Google и Facebook основали организацию «Центр гуманных технологий», которая, в частности, будет изучать влияние соцсетей на мир. Возглавляет группу бывший внутренний специалист по этике в Google Тристан Харрис, сообщает Mashable.

Докладніше

Маніпулятивні технології

2.02.2018

Twitter предупредил 1,4 млн пользователей о пропаганде РФ

Социальная сеть Twitter отправила сообщение около 1,4 млн пользователей, которые во время президентской кампании в США в 2016 году следили за аккаунтами, связанными с пропагандой России. Об этом говорится в сообщении в официальном блоге соцсети.

Докладніше

***

5.02.2018

У Франції підготували закон щодо протидії фейковим новинам

У Франції внесли на розгляд законопроект, який стосується протидії несправжнім новинам (fake news). Даний законопроект, за словами міністра культури Франсуа Ніссена, має дати можливість швидко видаляти такі вигадані новини під час виборів. Про це повідомляє видання EU Observer (Главком).

Таким чином цей законопроект допоможе протидіяти швидкому поширенню неправдивої інформації, як заявив Ніссен в інтерв'ю для видання Journal de Dimanche.

Поява цього законопроекту стала наслідком спроби РФ втрутитися у вибори президента Франції навесні 2017 року. Тоді російські хакери і інтернет-тролі намагалися не допустити обрання президентом нинішнього очільника країни Емануеля Макрона.

***

9.02.2018

Facebook придумал специальную кнопку для «чистки» плохих комментариев

Facebook тестирует новую возможность – кнопку, позволяющую пользователям выразить негативное отношение к комментариям других

пользователей. Кнопка называется «downvote», дословно «проголосовать против» (InternetUA).

Восьмого февраля некоторые пользователи социальной сети заметили появление новой кнопки в комментариях к записям в группах Facebook, пишет The Daily Beast, журналистам которого прислали соответствующие скриншоты.

В Facebook на запрос издания первым делом ответили, что не тестируют кнопку «дислайк» («не нравится»). «Мы изучаем функцию, которая позволит людям дать нам оценку комментариев к записям на публичных страницах. Тест проводится только в США на небольшой доле аудитории», – сообщил представитель компании.

Кнопка «проголосовать против» позволяет пользователям «понизить» тот или иной комментарий, в результате читающие увидят их с меньшей вероятностью. Инструмент задуман для борьбы с оскорблениями, троллингом и непристойностями, как средство сделать общение в Facebook более конструктивным и менее токсичным. Однако никто не помешает с таким же успехом использовать «проголосовать против» как орудие онлайн-агрессии.

***

9.02.2018

Twitter заблокировал аккаунты российских троллей, которые писали о Brexit

Социальная сеть Twitter заблокировала 49 аккаунтов российской фабрики троллей. Об этом сообщает Metro (InternetUA).

С помощью записей с этих аккаунтов пытались повлиять на общественное мнение во время референдума по выходу Великобритании из ЕС (Brexit). Они связаны с российской организацией, известной как Агентство интернет-исследований.

Об этом в Вашингтоне сообщили во время расследования доказательств распространения фейковых новостей в YouTube, Facebook, Google и Twitter.

В YouTube заявили, что не нашли никаких доказательств вмешательства России в референдум 2016 года. Ранее YouTube сообщал комитету Сената США о 18 каналах, которые были связаны с Россией.

***

13.02.2018

Розвідка США назвала Росію загрозою цьогорічним виборам до Конгресу

Росія використає проміжні вибори до Конгресу як засіб подальшого розколу Сполучених Штатів (Espreso.tv).

Про це заявив Директор національної розвідки США Ден Коутс, передає CNN.

Коутс заявив, що «не слід сумніватися», що Росія розцінює американські вибори 2018 року як можливість для втручання. У США очікують посилення російської пропаганди та кампаній у соціальних мережах, збільшення фейкових новин та інші способи російського втручання для подальшого політичного та соціального розколу у країні.

«Не слід сумніватися у тому, що Росія вважає свої минулі зусилля успішними і бачить проміжні вибори у Конгрес у 2018 році як потенційну мету для операцій», – заявив Коутс.

***

12.02.2018

Интернет-троллинг может стать уголовным преступлением

Правительство Великобритании планирует ужесточить наказание для интернет-обидчиков. Троллинг может стать уголовным преступлением благодаря инициативе Кэти Прайс, желающей справедливости для своего сына, ставшего жертвой преследований в интернете (GoGetNews.Info).

Министр юстиции Соединенного Королевства Дэвид Гоук сообщил, что правительство намерено пересмотреть законодательство с целью более эффективной борьбы с троллингом – оскорблениями в сети Интернет, исходящими, как правило, от анонимных пользователей. Планы правительства были вынесены на обсуждение в эфире телепередачи ITV, телеведущей которой выступила Кэти Прайс.

Интернет-обидчики должны нести такую же ответственность за словесные оскорбления, что и преступники в «реальном мире», считает Кэти Прайс. Телеведущая выступает за ужесточение наказаний интернет-троллям, злоупотребляющим своей безнаказанностью.

Прайс считает, что необходимо провести черту между безобидным подшучиванием и издевательством над пользователем, которое часто превращается в преследование и наносит психологические травмы объекту насмешек.

Спецслужби і технології «соціального контролю»

31.01.2018

За распространение в соцсетях «антиукраинской пропаганды» жителю Одесской области дали условный срок

В Одессе жителю села Маяки вынесли судебное решение за распространение в соцсетях «антиукраинской пропаганды» (InternetUA).

Согласно информации «Думской», следствие обвиняло жителя Одесской области в призывах к свержению конституционного строя и посягательстве на территориальную целостность и неприкосновенность Украины.

30 января в Киевском районном суде состоялось слушание по его делу. По решению суда молодого человека приговорили к 3–м годам тюрьмы. Учитывая, что обвиняемый пошёл на сделку со следствием, его освободили от отбытия наказания с годичным испытательным сроком.

Также сообщается, что парню вернули изъятый во время обыска ноутбук.

***

4.02.2018

МВД Германии одобрило запуск государственной шпионской программы

Министерство внутренних дел Германии одобрило запуск государственной троянской программы FinSpy, которая позволяет обходить шифрование и перехватывать сообщения в популярных мессенджерах. Теперь немецкие правоохранители смогут отслеживать зашифрованную коммуникацию на мобильных устройствах, осуществляемую через мессенджеры, такие как WhatsApp, Telegram или Signal, сообщает издание Die Welt (InternetUA).

Таким образом полиция надеется повысить эффективность в работе, например, по выявлению лиц, подозреваемых в террористической деятельности, торговле наркотиками и уклонении от уплаты налогов. Для использования возможностей программы сотрудникам полиции придется сначала установить троян на устройство.

Власти ФРГ приобрели коммерческую версию FinSpy (ПО разработано мюнхенской компанией FinFisher) еще в 2013 году, однако не использовали программу по юридическим причинам. По данным Die Welt, 10 января 2018 года МВД дало добро на использование программы федеральным ведомством по уголовным делам.

***

5.02.2018

Как мессенджер WeChat захватил Китай

Ещё в декабре 2017 года в Сети появилась новость о том, что китайский мессенджер WeChat приравнят к паспорту. Он считается одним из самых популярных во всем мире и единственным действующим в Китае. Правительство уже давно взяло мессенджер под тотальный контроль, поэтому о тайне переписки многие могут уже забыть.

Докладніше

***

6.02.2018
Главным регулятором рунета становится ФСБ

Главным контролером рунета становится Федеральная служба безопасности (ФСБ) – к такому выводу пришли эксперты международной правозащитной группы «Агора» в ежегодном докладе, посвященном ограничениям свободы интернета в России.

Докладніше

***

6.02.2018
Европол арестовал распространявших троян Luminosity хакеров

Европейский Центр по борьбе с киберпреступностью при Европоле (Europol's European Cybercrime Centre, EC3) и Национальное агентство по борьбе с преступностью в Великобритании (National Crime Agency, NCA) опубликовали информацию о международной операции правоохранительных органов, нацеленной на продавцов и пользователей трояна для удаленного доступа Luminosity.

Докладніше

***

6.02.2018
Спамера из России разоблачили с помощью iCloud

Полиции США удалось вычислить одного из самых опасных спамеров в мире Петра Левашова. Россиянина обвиняют в соучастии по разработке ботнета Kelihos, а также распространении вредоносного ПО (InternetUA).

Левашов вел и посредническую деятельность, открывая доступ к ресурсам ботнета другим хакерами и спамерам. За плечами россиянина несколько лет активной хакерской деятельности, но все же злоумышленник допустил одну существенную оплошность, засветив личный iCloud по IP.

Учетная запись была зарегистрирована на имя Петра Левашова, а IP-адрес совпал с одной из атак. В результате, полиции удалось вычислить местоположение хакера. В ходе обыска в Люксембурге были найдены два сервера, причастных к ботнету Kelihos, а также конфискована база учетных записей Mail.Ru.

В апреле 2017 года спамер выехал из России на отдых в Барселону, где и был задержан властями Испании по запросу США.

На днях Петр Левашов предстал перед федеральным судом штата Коннектикут. Apple от каких-либо комментариев решила воздержаться, отметив, что «не имеет права вмешиваться в расследование и дела правоохранительных органов».

***

6.02.2018

Утекший документ показал интерес АНБ США к контролю за криптовалютами

Вооруженные силы и Агентство национальной безопасности (АНБ) США способны раскрыть пользователей Tor, I2P и VPN, а также работают над отслеживанием криптовалюты Monero, следует из утекшего в Сеть документа, предположительно принадлежащего ВС США.

Докладніше

***

7.02.2018

Британские спецслужбы отказались от мысли победить хакеров

Британские спецслужбы предотвратили в 2017 году 54 миллиона кибератак. При этом правоохранители признают, что полностью справиться с атаками хакеров не только невозможно, но и незачем. Об этом со ссылкой на доклад Национального центра кибербезопасности (NCSC) пишет Financial Times (InternetUA).

Борьба с кибератаками и ложными сайтами проводилась в рамках программы Great British Firewall. Программа привела к уменьшению объема атак и вредоносного софта в Великобритании на 2 процента с июля 2016 года. За 2017 год были закрыты более 120 тысяч ложных вебсайтов.

По данным NCSC, большая часть атак осуществлялась преступными группировками, целью которых было получение выгоды от продажи личных данных или взлом банковских счетов людей.

«Нет необходимости побеждать киберпреступность, и будет нереалистично думать, что мы могли бы это сделать. Но мы действительно хотим сделать это настолько сложным, насколько возможно, это означает сделать деятельность киберпреступников в Великобритании невыгодной и рискованной», – заявил при этом технический директор NCSC Ян Леви.

***

7.02.2018

Власти Канады просят Google запретить рекламу криптовалют и ICO

Регулятор Канады намекнул Google, что корпорации стоит последовать примеру Facebook и заблокировать всю рекламу, которая касается ICO, криптовалют и вообще всей этой сферы (InternetUA).

Представитель контролирующего органа Канады Джейсон Рой сказал: «Мы очень рады решению Facebook. Надеюсь, Google введет похожую политику в отношении бинарных опционов, ICO и криптовалют».

Также Рой раскритиковал ICO: мол, компании собирают огромные деньги, в то время как за ними в большинстве случаев ничего нет, а люди надеются на большие прибыли.

В последних числах января Facebook объявила о блокировке рекламы ICO, бинарных опционов и криптовалют. Это произошло через месяц после того, как Марк Цукерберг заявил о желании глубоко изучить криптовалюты.

***

12.02.2018

У Росії можуть заблокувати Instagram і YouTube через фото заступника Медвєдєва і Дерипаски з ескортом, – ЗМІ

Через позов російського мільярдера Олега Дерипаски до Насті Рибки у Росії можуть заблокувати Instagram і YouTube (Espreso.tv). Про це пишуть «Ведомости».

Суд виніс ухвалу про внесення у список сайтів із забороненою інформацією 14 постів в Instagram і 7 відеороликів на YouTube, випливає з реєстру Роскомнадзора.

Зазначається, що у Instagram і YouTube за російським законом є три робочих дні, щоб видалити інформацію.

Оскільки не у всіх провайдерів є технічна можливість блокувати окремі інтернет-сторінки, то частина користувачів може залишитися без доступу до Instagram і YouTube.

Представник Роскомнадзора уточнив виданню, що у сервісів є час до вечора 14 лютого.

***

12.02.2018

В Германии суд обвинил Facebook в незаконном использовании персональных данных

В Германии суд признал использование компанией Facebook персональных данных своих пользователей незаконным, поскольку социальная сеть не спрашивала согласия на их обработку надлежащим образом. Об этом сообщает пресс-служба Федерации по защите прав потребителей Германии.

Докладніше

Проблема захисту даних. DDOS та вірусні атаки

31.01.2018

Кількість жертв від кібершахраїв у 2017 році подвоїлася, в українців вкрали 670 млн грн

У 2017 році злочинці викрали у кіберпросторі понад 670 млн гривень, що майже вдвічі більше, ніж у 2016 році (339 млн гривень) (Espreso.tv).

Повідомляється, що найчастіше шахраї користуються методом соціальної інженерії – злочинець підштовхує жертву до грошових переказів під час телефонної розмови.Таким чином виманили чверть мільярда гривень.

За статистикою 77 % опитаних українців знають, що свої банківські реквізити не можна передавати третім особам, однак 76 % все одно роблять це, якщо натрапляють на шахраїв.

Серед найпопулярніших кіберзлочинів: крадіжка через банкомати, виманювання грошей через обіцянки автомобіля чи квартири та продаж у інтернеті неіснуючих товарів.

Українська міжбанківська Асоціація членів платіжний систем «Єма» зафіксувала скорочення «фішингових» сайтів (як виманюють дані платіжної картки) з 174 сайтів у 2016 році до 108 у 2017.

***

31.01.2018

Карточные мошенники перешли из магазинов и банкоматов в интернет

Количество случаев мошенничества с платежной картой при расчетах в торговых сетях, а также при снятии денег в банкоматах уменьшается. При этом доля таких операций в интернете растет. Об этом заявил директор Украинской межбанковской ассоциации членов платежных систем ЕМА Александр Карпов.

Докладніше

***

5.02.2018

Вредонос WannaMine обходит защиту традиционных антивирусов

Как сообщают эксперты Panda Security, новый вариант вредоносной программы под названием «WannaMine» стал заражать многие компьютеры во всем мире, чтобы использовать их ресурсы для майнинга криптовалюты под названием Monero.

Докладніше

***

5.02.2018

Как полностью стереть себя из интернета

Если Вы когда-то задумывались о том, чтобы полностью стереть о себе информацию из интернета, описаны способы, как достаточно быстро и бесплатно удалить себя отовсюду.

Докладніше

***

5.02.2018

Создан бесплатный инструмент для полностью автоматических кибератак

Опубликована программа AutoSploit, способная автоматически искать уязвимые устройства и атаковать их, используя пакет Metasploit.

Докладніше

***

5.02.2018

Компьютеры на Windows оказались под угрозой

Специалисты обнаружили новые угрозы, жертвами которых могут стать пользователи популярных версий операционной системы Windows. Принцип работы трех видов вредоносных программ опубликован на GitHub.

Докладніше

***

5.02.2018

Стали известны новые подробности об уязвимости нулевого дня в Flash Player

Исследователи кибербезопасности из компаний FireEye и Cisco Talos проанализировали атаки, в которых эксплуатировалась недавно выявленная уязвимость нулевого дня в Adobe Flash Player и связали их с группой, известной своими атаками на цели в Южной Корее.

Докладніше

***

5.02.2018

Уязвимость в WordPress позволяет любому отключить атакуемые сайты

В WordPress обнаружена простая, но серьезная уязвимость на уровне приложения, позволяющая вызвать отказ в обслуживании и отключить множество сайтов. Как правило, для осуществления подобной DDoS-атаки на уровне сети нужны большие объемы трафика, однако недавно обнаруженная уязвимость позволяет добиться желаемого эффекта с помощью всего лишь одного компьютера.

Докладніше

***

5.02.2018

Как хакеры взламывают аккаунты в соцсетях под видом техподдержки

В соцсети «ВКонтакте» начала практиковаться новая схема взлома аккаунтов. Хакер пишет жертве под видом техподдержки и выманивает логин и пароль, после чего учётная запись уводится (InternetUA).

Злоумышленник регистрирует во «ВКонтакте» страницу с названием вроде «Техническая поддержка VK» или «Агент поддержки № 1» и ставит аватарку с логотипом VK, собакой Дурова на зелёном фоне и чем-то подобным. Затем он присылает потенциальной жертве сообщение о том, что на её аккаунт поступили жалобы и необходимо подтвердить, не был ли он угнан, а для этого требуется перейти по ссылке и ввести логин и пароль. Чтобы жертва испугалась и как можно скорее перешла на сайт, в сообщении может быть указано, что аккаунт будет заблокирован в течение нескольких минут, если не подтвердить его. Сайт, на который даётся ссылка, как нетрудно догадаться, выглядит как VK.com, но расположен на другом домене и предназначен для кражи логинов и паролей.

Как обезопасить себя от такого взлома? Сообщения от администрации и техподдержки «ВКонтакте» легко отличить от остальных: имя отображается зелёным цветом, а на странице должна стоять галочка верификации, означающая, что аккаунт подтверждён администрацией VK и действительно принадлежит тому, кто указан в имени. «ВКонтакте» иногда действительно просит повторно ввести пароль от учётной записи, но не на постороннем сайте, а либо в приложении, либо на vk.com.

***

6.02.2018

Найдена новая угроза для всех Android-устройств

Специалисты обнаружили новый ботнет, атакующий владельцев устройств на базе операционной системы Android. Об этом сообщает Bleeping Computer (InternetUA).

Ботнет нацелен на поиск открытых портов отладки, в том числе на порт 5555, который используется важным компонентом системы Android и предоставляет доступ к ключевым функциям. Проникая в устройство, вредоносная программа заставляет его добывать криптовалюту Monero.

По словам исследователей из организации QiHo 360, обнаруживших ботнет, опасность угрожает всем устройствам на Android – от смартфонов до умной техники.

По данным специалистов, заражены уже около 7,4 тысячи устройств, а сам ботнет растет впечатляющими темпами. Большинство пострадавших пока

находятся в Китае (около 40 процентов) и в Южной Корее (около 30 процентов).

Опасная программа, прозванная ADB.miner, использует компоненты кода у Mirai – ботнета, появившегося в 2016 году и считающегося самым большим в мире. Тогда Mirai заразил тысячи устройств по всему миру и стал причиной остановки работы множества крупных сайтов.

***

6.02.2018

Хакеры могут заставить бытовую технику майнить криптовалюту

Специалисты из аналитической компании Stratfor предупредили о возможности использования высокотехнологичных холодильников, печей и стиральных машин, оснащенных компьютерными процессорами, для майнинга криптовалюты (InternetUA).

По словам аналитиков, «умные» дома с рядом взаимосвязанных устройств могут быть особенно уязвимыми к кибератакам данного типа.

«Если у вас есть централизованный домашний помощник, такой как Google Home или [Amazon] Alexa, который подключается ко многим другим устройствам, будь то источники света, термостаты, холодильники, посудомоечные машины и другие приборы, то у злоумышленников появляется возможность использовать данный узел для атаки», – заявил вице-президент по тактическому анализу Stratfor Скотт Стюарт (Scott Stewart).

По словам Стюарта, хакеры уже используют вычислительные мощности бытовой техники для осуществления DDoS-атак.

Как заявили представители Google изданию Express.co.uk, безопасность устройств имеет для компании первостепенное значение и все коммуникации с системой Google Home зашифрованы по умолчанию.

По словам представителей Amazon, компания серьезно относится к безопасности клиентов, и принимает меры для обеспечения безопасности устройств Echo.

***

6.02.2018

Укренерго витратить на нову систему кібербезпеки $20 млн

Державне підприємство Укренерго планує витратити $20 млн на нову систему кіберзахисту для компанії, яка за останні два роки кілька разів страждала від кібератак (InternetUA). Про це повідомляє Reuters.

Система повноцінно запрацює в 2020 році. Вона буде містити нове програмне забезпечення і «адміністративні заходи». Міжнародні консультанти визначили близько 20 загроз у сфері інформаційної безпеки і нова система забезпечить від них повний захист.

«Ми розробили нову концепцію кібербезпеки, ключова мета якої – зробити фізично неможливим вплив зовнішніх загроз на українську енергосистему», – сказав глава підприємства Всеволод Ковальчук на прес-конференції за підсумками 2017 року.

За минулий рік Укренерго також прийняла концепцію захисту автоматизованих систем підприємства, стратегію розвитку інформаційної безпеки на 3 роки, концепцію розвитку IT-інфраструктури.

Крім цього, в компанії створили Центр реагування на кіберінциденти й реорганізували відділ IT-безпеки.

***

6.02.2018

Google удалила 89 вредоносных расширений нового типа из магазина Chrome

Недобросовестные разработчики расширений используют новый способ кражи конфиденциальной информации жертв (InternetUA).

Исследователи из Trend Micro назвали новое семейство вредоносных расширений Droidclub. Расширение Droidclub включают в себя так называемые «скрипты повторения сеанса», которые используют аналитические фирмы.

Обычно «Скрипты повторения сеанса» позволяют владельцу сайта «стоять за спиной» у посетителей, записывая и воспроизводя нажатия клавиш, движения мыши и моменты прокрутки колесом. Это помогает оптимизировать работу сайта и улучшить продажи интернет-магазинов.

В руках злоумышленников этот скрипт записывает и воспроизводит все действия пользователя на каждом посещаемом веб-сайте. Также эти программы помогали авторам добывать криптовалюту Monero. Компания Google недавно удалила 89 вредоносных расширений из интернет-магазина Chrome, которые были установлены на более чем 420 000 браузерах.

Когда пользователи сообщают о вредоносных расширениях Droidclub, они перенаправляются на выбранную злоумышленником страницу. Попытки удалить вредоносную программу также приводят пользователя к поддельной странице, которая сообщает ему, что расширение было удалено, хотя на самом деле – нет.

***

6.02.2018

Обнаружен троянец-шифровальщик GandCrab для Windows

Компания «Доктор Веб» предупреждает о распространении очередного шифровальщика. Троянец, названный создателями «GandCrab!», был добавлен в вирусные базы Dr.Web под именем Trojan.Encoder.24384. Он присваивает зашифрованным файлам расширение *.GDCB. В настоящее время известно две версии этого энкодера (Компьютерное Обозрение).

Запустившись на атакуемом устройстве, работающем под управлением Microsoft Windows, Trojan.Encoder.24384 может собирать информацию о наличии запущенных процессов антивирусов. Затем, выполнив проверку с целью предотвращения повторного запуска, он принудительно завершает процессы программ по заданному вирусописателями списку. Установив свою копию на диск, для обеспечения своего автоматического запуска энкодер модифицирует ветвь системного реестра Windows.

Троянец шифрует содержимое фиксированных, съемных и сетевых дисков, за исключением ряда папок, среди которых имеются служебные и системные. Каждый диск шифруется в отдельном потоке. После окончания шифрования троянец отправляет на сервер данные о количестве зашифрованных файлов и времени, потраченном на шифрование.

Троянец использует управляющий сервер, доменное имя которого не разрешается стандартными способами. Для получения IP-адреса этого сервера шифровальщик выполняет команду nslookup и ищет нужную информацию в ее выводе.

В настоящее время расшифровка файлов, зашифрованных троянцем Trojan.Encoder.24384, невозможна. Поэтому наиболее надежным способом уберечь свои файлы является своевременное резервное копирование всех важных данных, при этом для хранения резервных копий желательно использовать внешние носители информации.

***

6.02.2018

Уязвимость в расширении Grammarly раскрывала данные пользователей

Разработчики Grammarly, популярного расширения для проверки грамматики в браузере Google Chrome, исправили в своем продукте серьезную уязвимость, позволяющую получить доступ к учетной записи пользователя, а также его личным документам и данным (InternetUA).

По словам обнаружившего уязвимость исследователя безопасности из Google Project Zero Тэвиса Орманди (Tavis Ormandy), расширение раскрывало аутентификационные токены всем web-сайтам. Таким образом любой сайт мог получить доступ к документам пользователя, истории, журналам и другим данным.

Исследователь также продемонстрировал, как можно проэксплуатировать уязвимость с помощью всего четырех строк кода.

Разработчики расширения оперативно отреагировали на сообщение исследователя и выпустили обновление, исправляющее уязвимость.

***

7.02.2018

«Нову Пошту» обвинили в утечке конфиденциальной информации пользователей

Базы данных клиентов компании «Нова Пошта» выставлены на продажу неустановленными лицами. Об этом сообщил консультант по кибербезопасности Егор Папишев на своей странице в Facebook (IGate).

По его словам, таких баз пока две: на 500 тыс и на 18 млн пользователей. Одна содержит информацию с персональными данными, в том числе ФИО, телефон, город, серию и номер паспорта и e-mail. Вторая менее информативна – только ФИО и телефон.

Папишев связался с продавцом, который сразу озвучил цены в гривнах, а также предоставил произвольную часть базы.

«Во-первых, предоставлен произвольный кусок базы. Во-вторых, я попросил прислать мне значение записей из базы, дав ему несколько номеров телефонов для идентификации. Номера принадлежали совершенно разным людям из разных городов и никак не были связаны друг с другом. Ответ пришел менее чем через пять минут, и содержал абсолютно точные и свежие данные о клиентах (включая измененную фамилию в связи с недавним замужеством одного из них). Для дополнительной проверки я задал еще несколько телефонных номеров, которые априори не могли быть использованы в сервисе «Нова Пошта» (это корпоративные номера) и верно – их в этой базе не оказалось» – написал специалист по кибербезопасности.

***

8.02.2018

«Нова Пошта» прокомментировала утечку данных пользователей

На днях в сети распространилась информация о том, что якобы база данных клиентов компании «Нова Пошта» выставлена на продажу в интернете неизвестным лицом. Седьмого февраля компания сделала официальное заявление по этому поводу на своей странице в Facebook (IGate):

«Наша позиция такова: любая попытка незаконно завладеть данными наших клиентов получит жесткую реакцию с нашей стороны. Мы начали собственное расследование с того, что сами проанализировали информацию. Наш вывод: файл с данными физлиц в посте ФБ-пользователя не содержит никаких признаков того, что это база именно клиентов “Нова Пошта”. Это дает основания говорить о том, что файл может принадлежать любой другой украинской компании».

Кроме того, представители компании связались с автором публикации. Он готов сотрудничать и помочь выяснить обстоятельства, о которых он написал. Также почтовый оператор обратился в Департамент киберполиции, чтоб продолжить расследование с содействием со стороны правоохранителей:

***

7.02.2018

Украинцев предупредили о новой афёре при оплате картой

Мошенники придумали новый технологичный способ отъёма денег у посетителей кафе, баров и ресторанов с использованием фальшивых терминалов оплаты (InternetUA).

Как информирует издание «Обозреватель» со ссылкой на Telegram-канал Criminal Bio, злоумышленники ищут в социальных сетях официантов, администраторов и других людей, которые могут проводить расчёт клиентов. Под видом «подработки» им предлагают подменить терминал оплаты на спецустройство, делающее копии банковских карт.

Внешне устройство полностью повторяет стандартный POS-терминал, однако вместо оплаты оно считывает сведения о картах, в том числе пин-код. Для маскировки при проведении операции с картой фальшивый терминал выдаёт чек, сообщающий о том, что связь с банком отсутствует.

После того, как устройство считает карту, мошенники подключают его к компьютеру и с помощью спецпрограммы копируют всю информацию.

***

7.02.2018

Хакеры атакуют Центр информации о правах человека, чтобы помешать работе в оккупированном Крыму

Центр информации о правах человека подвержен хакерским атакам: правозащитники получают зараженные вирусами письма, фишинговые сообщения, аккаунты сотрудников подвержены атакам (InternetUA).

Как передает Цензор.НЕТ со ссылкой на Крым.Реалии, об этом рассказала председатель правления украинского Центра информации о правах человека Татьяна Печончик, это может быть связано с работой правозащитников в Крыму.

«Это делается для того, чтобы получить внутренние данные организации. К примеру, наша организация от начала оккупации Крыма работает там и, конечно, какое-либо раскрытие информации про наших активистов очень небезопасно. Это может использоваться для получения информации про особенность работы организации в конфликтных зонах, какие-либо данные организации, могут быть опубликованы в интернете с целью дискредитации», – указала председатель правления Центра.

Печончик настаивает на том, что цифровая гигиена «должна быть доведена до автоматизма», это поможет уберечься от утечки информации и нежелательных атак.

***

7.02.2018

Російські хакери намагалися зламати пошту розробників американської зброї

Російські кібершпигуни, які намагаються вивідати секрети військових безпілотників США, намагалися хитрістю отримати адреси електронної пошти ключових працівників (Espreso.tv). Про це передає Голос Америки.

Що остаточно було викрадене – невідомо, але хакери, очевидно, скористалися загальнонаціональною вразливістю в сфері безпеки – погано захищеною електронною поштою і практично повною відсутністю прямих повідомлень про це постраждалим.

Група кібершпіонажу Fancy Bear, яка також втручалася у вибори в США, намагалося отримати координати щонайменше 87 осіб, які працюють над військовими безпілотниками, ракетами, винищувачами-Stealth, або виконували іншу секретну роботу.

В поле зору хакерів потрапили як співробітники малих компаній, так і таких гігантів оборонної промисловості, як Lockheed Martin, Raytheon, Boeing, Airbus Group і General Atomics.

Кілька людей працювали в галузевих організаціях, були членами рад директорів або працювали за контрактом в союзних США країнах.

***

8.02.2018

Конгрес США підтримав законопроект про захист України від російської кіберзагрози

Палата представників Конгресу США підтримала законопроект про посилення співробітництва між Україною та США у сфері кібербезпеки (Espreso.tv). Про це повідомляє у Facebook посольство України в США.

На підтримку законопроекту проголосували 404 конгресмени.

Законопроект спрямований на просування активнішої взаємодії між Україною і США у сфері кібербезпеки в умовах протидії російській гібридній агресії.

Документ передбачає допомогу Україні в удосконаленні стратегії кібербезпеки, зокрема, щодо посилення захисту комп'ютерних мереж органів державної влади, зменшення залежності України від російських інформаційних та комунікаційних технологій, сприяння участі України у програмах обміну інформацією.

У законопроекті підтверджується відданість США Хартії про стратегічне партнерство з Україною, Будапештському меморандуму про гарантії безпеки та підтримці співробітництва України з НАТО.

Для набуття чинності законопроект має бути проголосований також Сенатом та підписаний президентом США.

***

8.02.2018

Check Point Software представляет CloudGuard для всесторонней киберзащиты облака

Компания Check Point представила линейку решений CloudGuardtm для защиты организаций от кибератак «Пятого поколения» на облачные приложения и инфраструктуру.

Докладніше

***

8.02.2018

У США викрили засновану українцем міжнародну мережу кіберзлочинців. Ті хотіли вкрасти дані 4,3 млн кредитних карток

Співробітники правоохоронних органів США викрили мережу кіберзлочинців Infraud, яку в 2010 році заснував українець Святослав Бондаренко (Espreso.tv). Про це повідомляє DW.

У Міністерстві юстиції США зазначають, що група кіберзлочинців діяла під гаслом «In Fraud We Trust», тобто «Ми віримо в шахрайство».

Зловмисники створили розгалужену й добре організовану мережу, що протизаконним шляхом отримувала особисті дані інтернет-користувачів, у тому числі ті, що надавали доступ до банківських та електронних рахунків.

На думку слідчих, члени угруповання намагалися отримати дані про 4,3 мільйона кредитних карток та банківських рахунків.

В американському відомстві наголошують, що за час існування угруповання злочинці завдали своїми діями збитків на понад $530 млн.

Наразі слідчі вважають причетними до злочинного угруповання загалом 36 осіб. 13 членів кібербанди вже заарештували. Арешти проводилися в США, Австралії, Великобританії, Франції, Італії, Косові, Сербії та Албанії, зазначається в повідомленні.

***

9.02.108

Активисты обнародовали личные данные более 2 тыс. итальянских политиков

Активисты AnonPlus опубликовали в соцсети Twitter базу данных «Демократической партии Италии», которая является одной из крупнейших политических партий в стране (InternetUA).

В общей сложности документ содержит персональные данные 2653 политиков. База включает имена, фамилии, номера телефонов, адреса электронной почты и другую личную информацию. В числе пострадавших от утечки оказались видные политические деятели Италии, включая мэра Флоренции Дарио Нарделлу (Dario Nardella) и бывшего председателя Совета

министров Италии, а ныне лидера Демократической партии Маттео Ренци (Matteo Renzi).

По словам активистов AnonPlus, база данных была загружена из неназванного источника. Для того чтобы избежать обнаружения, участники движения использовали IP-адрес в Германии. Активисты отдельно отметили, что не имеют никакого отношения к активистам движения Anonymous, а также не связаны с какой-либо политической партией.

***

12.02.2018

Для Windows 10 создана новая система защиты

Многие пользователи уже давно поняли, что использование обычных паролей для защиты своих данных является устаревшим способом (iLenta.com).

Именно поэтому рядом компаний разрабатываются новые надежные решения. Одним из них является Windows Hello, которая впервые появилась в Windows 10 в 2015 году. Она использует отпечаток пальца или сканирует лицо для разблокировки.

Эта функция хороша, но тоже не идеальна, поэтому Fujitsu и Microsoft создали новую уникальную систему, которая вместе с Windows Hello сможет распознавать владельца ПК с помощью сканирования венозной схемы его ладони.

Для этого будет использоваться специальный сканер, который по размерам чуть больше сканера отпечатков пальцев. Его можно подключать через USB, либо встраивать в устройство. Пользователю необходимо лишь поместить ладонь над сканером, который молниеносно распознает ее.

Fujitsu эту технологию называет PalmSecure. Подобные сканеры сейчас используются в ПК Fujitsu с Windows 10 Pro.

***

12.02.2018

Google будет маркировать http-сайты, как небезопасные

В Google собираются маркировать все сайты, работающие по протоколу HTTP, как потенциально опасные. Нововведения вступят в силу летом нынешнего года (Украинский телекоммуникационный портал).

Компания собирается оказать давление на web-разработчиков, стимулируя их перейти на использование HTTPS-шифрования. В Google объясняют такую инициативу стремлением обезопасить своих пользователей от потенциальных уязвимостей. Новый принцип маркировки сайтов будет введен в июле текущего года, когда выйдет версия Chrome 68.

Эта практика уже дала свои плоды, поскольку 81 из 100 топ-сайтов интернета уже перешли на более защищенный протокол.

В Google сообщают, что свыше 68 % трафика через браузер Chrome, установленный на устройствах с ОС Android и ОС Windows теперь защищено. Для операционных систем Chrome OS и Mac этот показатель еще выше – более 78 % трафика считается безопасным.

Таких результатов компания добилась все теми же изменениями в маркировке. В частности, в версии Chrome 56, вышедшей в январе прошлого года, иконка «Not sequre» появилась на HTTP-сайтах, передающих пароли, данные кредиток и пр.

***

12.02.2018

Во время церемонии открытия Олимпийских игр произошла масштабная кибератака

Олимпийские чиновники сообщили, что во время церемонии открытия Зимних Олимпийских игр в Пхенчхане произошла массированная кибер-атака. Организаторы говорят, что хотя она и затронула телетрансляции и доступ в интернет, атака «не поставила под угрозу какую-либо критическую часть мероприятия» (IGate).

Согласно сообщениям, доступ в интернет и Wi-Fi оказался под угрозой в пятницу во время церемонии открытия Игр. Официальный олимпийский веб-сайт также «лег», что помешало участникам распечатать билеты.

Представитель Олимпийского оргкомитета подтвердил, что произошла атака, но ее последствия были предотвращены. Он также сказал, что следователи на данном этапе не будут раскрывать источник атаки.

Игры уже подверглись атаке со стороны хакеров: в прошлом месяце эксперты McAfee заявили, что выявили атаку на олимпийских чиновников, которые получили письма с вредоносными кодом. Компания предупредила, что возможны дальнейшие атаки.

Среди предполагаемых источников атак были названы Северная Корея, а также Россия, чьи спортсмены были отстранены от участия в Играх.

***

12.02.2018

На сайтах правительств США и Великобритании майнили криптовалюту

Более 4200 интернет-сайтов оказались заражены взломанной версией популярного расширения Browsealoud от британской компании Texthelp, которая позволяет проговаривать вслух текст на странице для слабовидящих людей, пишет Reuters со ссылкой на The Register (InternetUA).

В числе зараженных сайтов оказались также ресурсы правительств США и Великобритании, сообщает издание. Взломанная версия расширения запускала встроенное в нее программное обеспечение для майнинга

криптовалюты Monero, используя для этого компьютеры заходивших на подвергшиеся нападению ресурсы.

И пока представители британских и американских органов не прокомментировали ситуацию, компания Texthelp отключила расширение на всех компьютерах и занимается расследованием произошедшего инцидента.

***

11.02.2018

Новый вирус похищает данные карт с помощью DNS-запросов

Исследователи кибербезопасности из фирмы Forcepoint обнаружили новое вредоносное ПО для PoS-терминалов, позволяющее похищать данные кредитных карт с помощью DNS-запросов.

Докладніше

***

12.02.2018

Мобильный вымогатель Android/Locker.B требует выкуп подарочными картами iTunes

Eset предупреждает о новом мобильном вымогателе Android/Locker.B. Он распространяется под видом легитимных приложений и меняет PIN-код экрана блокировки Android-устройств (Компьютерное Обозрение).

Android/Locker.B распространяется через форумы, специально созданные злоумышленниками, и файлообменные сервисы. Он маскируется под программу для работы с камерой в WhatsApp, антивирус для Android, мобильное приложение Dropbox или Flash Player.

После установки вредоносное приложение запрашивает права администратора устройства. Получив необходимые разрешения, он блокирует доступ к операционной системе, меняя PIN-код экрана блокировки. Далее Locker.B выводит на экран требование выкупа.

Сумма выкупа варьируется – 25 или 50 долл. или евро. Интересно, что злоумышленники принимают выкуп подарочными картами iTunes и предоставляют жертвам подробную инструкцию по их покупке и использованию.

Данная версия вымогателя наиболее активна в странах Латинской Америки. 71 % срабатываний антивирусных решений Eset приходится на Мексику. Тем не менее, в компании отмечают, что злоумышленникам не составит труда переориентировать угрозу на другие регионы.

***

12.02.2018

Любое приложение на Mac может следить за пользователем

Разработчик платформы для продвижения приложений FastLane Феликс Крузе опубликовал любопытную заметку, связанную с работой приложений в операционной системе macOS (InternetUA).

По заверению Крузе, любое, установленное на Mac приложение, может без ведома пользователя записывать все, что происходит на экране.

Крузе отмечает, что абсолютно неважно, активно ли приложение в настоящий момент или работает в фоне. У любой программы есть возможность снимать скриншоты и получать доступ к каждому пикселю на экране. Самое печальное, что полученная информация может отправляться на удаленные сервера, где посредством OCR-алгоритмов изображения преобразуются в текст.

Используя лишь пару программных строк вроде *CGWindowListCreateImage*, любой разработчик может получить прямой доступ к экрану пользователя. И самое грустное, что захват скриншотов открывает доступ к ряду дополнительной информации, вроде:

- паролей и ключей от менеджеров паролей;
- определения веб-служб;
- чтения электронных писем и сообщений;
- любой конфиденциальной информации, которую вы просматриваете на Mac.

***

13.02.2018

У Чернігові хакер продавав базу даних міжнародної компанії за 3 біткоїни

У Чернігові 20-річний хакер продавав базу даних клієнтів міжнародної компанії за 3 біткоїни. Про це повідомляє прес-служба кіберполіції (Espreso.tv).

Зазначається, що доступ до бази зловмисник отримав під час виявлення уразливості веб-ресурсу цієї компанії.

Як встановили оперативники, ця міжнародна компанія-перевізник, орієнтована на поставку товарів зі США у більш як 10 країн світу, в тому числі і в Україну.

Під час обшуку правоохоронці виявили на комп’ютері хакера повну базу даних клієнтів міжнародної компанії. У цій базі налічується персональна інформація щодо 120 тисяч осіб, серед яких були і українці.

Крім цього, хлопець також скупляв на скомпрометовані платіжні картки різноманітні товари з інтернет-майданчиків, які потім планував перепродати.

Правоохоронці отримали також інформацію щодо банків-емітентів кардерських карток.

***

13.02.2018

Михаил Сапитон

Facebook предлагает воспользоваться своим VPN-сервисом. Почему это плохая идея

Редакция AIN.UA рассказывает, почему лучше не пользоваться VPN-сервисом, который рекламирует (и принадлежит) Facebook.

Докладніше

***

13.02.2018

В Telegram обнаружена опасная уязвимость

Специалисты «Лаборатории Касперского» заявили об обнаружении уязвимости в Telegram для Windows, которая использовалась хакерами для майнинга криптовалют и установки шпионского ПО, сообщает «Коммерсантъ» (Зеркало недели. Украина).

Отмечается, что на серверах злоумышленников были обнаружены данные о переписке пользователей. Предположительно, жертвами хакеров могли стать до тысячи пользователей. О проблеме уведомили разработчиков мессенджера, уязвимость уже закрыта.

Злоумышленники устанавливали шпионское ПО, для этого киберпреступники использовали уязвимость для доставки бэкдора. После установки он работал, ничем не обнаруживая себя. В результате хакеры получали удаленный доступ к компьютеру жертвы: бэкдор выполнял различные команды злоумышленников, в том числе установку шпионского ПО.

Обнаруженные артефакты позволяют предположить русскоязычное происхождение преступников. Так, некоторые строчки во вредоносном коде были на русском языке, а в «засветившихся» email-адресах злоумышленников фигурировали русские слова и имена.

Отмечается, что пользователи скачивали вирус под видом, например, картинки и сами запускали его не подозревая, что это исполняемый файл.

ДОДАТКИ

Додаток 1

5.02.2018

Невероятно полезная и нужная возможность Telegram, о которой обязан знать каждый

С каждым днем мессенджер Telegram становится все более популярным средством для общения. Разработчики всячески способствуют этому, регулярно добавляя в свой сервис полезные функции и возможностей, о которых просят пользователи. Несколько месяцев назад создатели Telegram добавили в него крайне полезную и нужную опцию, о существовании которой просто обязан

знать каждый человек, поскольку она может значительно упростить жизнь (InternetUA).

Как правило, с какими-то абонентами через Telegram нужно общаться чаще всего, однако из-за обилия других чатов приоритетные отходят на второй план. Ситуация усугубляется еще и тем, что многие пользователи подписаны на несколько каналов, регулярно публикующих различную информацию, а она выглядит так, словно ее отправил собеседник. К счастью, теперь любой чат можно сделать приоритетным, закрепив его в самом верху раздела с сообщениями.

Чтобы сделать это необходимо открыть раздел со всеми чатами, после чего нажать и удерживать палец на том собеседнике или канале, который нужно закрепить в самом верху. Если все было сделано правило, то уже спустя 1-2 секунды на экране смартфона отобразится меню, в котором будет опция «Закрепить». На нее и нужно нажать, после чего выбранный чат закрепится в верхней части мессенджера Telegram и будет там абсолютно всегда, даже если поступили более свежие сообщения.

Таких закрепленных чатов может быть не более пяти, однако никак перемещать их друг между другом нельзя, поэтому стоит заранее задуматься над тем, в каком порядке они будут располагаться. Сначала нужно закреплять те чаты, которые должны быть ниже, а уже затем те, что выше. Это невероятно полезная и нужная возможность Telegram, о которой знают лишь единицы. С ее помощью можно выделить из общей массы сообщения от конкретных каналов или людей, чтобы всегда видеть их в первую очередь.

(вгору)

Додаток 2

6.02.2018

YouTube введёт строгие санкции против вредящих сообществу авторов

YouTube начнёт гораздо строже наказывать владельцев каналов, которые вредят репутации сервиса. Генеральный директор Сьюзен Войжитски (Susan Wojcicki) рассказала о главных целях компании на 2018 год. Одним из самых примечательных обещаний стало введение штрафных санкций против авторов, которые «делают что-то вопиющее, что наносит значительный вред» всему сообществу (InternetUA).

«Такие случаи редки, но они могут навредить репутации и доходу других авторов, поэтому мы хотим ввести правила, которые позволят нам реагировать соответствующим образом», – написала Войжитски.

Долгое время у YouTube не было чёткой системы наказаний для авторов, которые нарушают правила сервиса. Теперь компания решила взять за политику всерьёз – всего спустя несколько недель после скандала с видеоблогером Логаном Полом (Logan Paul), опубликовавшим видео с телом самоубийцы. Его поступок вызвал бурную реакцию общественности, а

YouTube исключила блогера из рекламной программы Google Preferred. Компания также заявила, что ужесточит ограничения монетизации каналов, из-за чего владельцы небольших каналов начали паниковать.

Действия Логана Пола отрицательно сказались на репутации YouTube, но это уже далеко не первый такой случай. Войжитски отметила, что есть вещи, по отношению к которым компания вынуждена принять «чёткую, осведомлённую, принципиальную позицию». В частности, сервис наймёт для борьбы с нарушениями больше людей и начнёт ещё активнее использовать машинное обучение.

«Мы осознаём, что несём серьёзную социальную ответственность за решение проблем с политикой сервиса, поэтому обращаемся за советом к десяткам консультантов и сторонних экспертов», – сказала Войжитски.

(вгору)

Додаток 3

13.02.2018

Вслед за Google. Facebook начал строить сеть «зеркал» в Украине

Сбои при загрузке ленты Facebook, не открывается видео или проблемы с Messenger – в последнее время на это часто жалуются украинские пользователи. После запрета российских соцсетей в Украине Facebook становится коммуникационной платформой №1. И количество местного трафика, проходящего через его сервисы, быстро увеличивается. Но готов ли Марк Цукерберг к волне запросов на контент из нашей страны (InternetUA)?

YouTube уже закеширован

Во время недавнего интервью с директором Google в Украине Дмитрием Шоломко выяснилось, что американская корпорация очень тщательно продумывает развитие местной инфраструктуры, чтобы сервисы Google (преимущественно YouTube) работали без сбоев. Google предоставляет нашим провайдерам свои кеширующие серверы в бесплатную аренду в рамках программы Google Global Cache. Они избавляют провайдера от необходимости снова и снова загружать тяжелый контент, например видео, из дата-центров за океаном. Вместо этого наиболее популярные в регионе ролики хранятся прямо на площадках у украинских интернет-провайдеров и подгружаются быстрее. К тому же это в разы дешевле – не нужно платить за международные каналы связи.

Количество таких серверов в Украине, по словам Дмитрия Шоломко, уже исчисляется сотнями. Он подписывает по 3-4 договора об аренде каждый месяц. По словам менеджера, в Украине нет ни одного крупного провайдера, который бы не сотрудничал с Google по этой программе. У крупнейшего интернет-оператора Укртелеком, по словам представителей его пресс-службы, «зеркала» (локальные серверы) Google есть в шести городах, и это заметно упрощает компании жизнь.

К слову, 4 года назад свои кеш-серверы в Киеве хранила и «ВКонтакте». Однако они были изъяты в ходе обыска налоговиков, которые искали информацию по одной недобропорядочной компании. Но в результате конфисковали «железяки» со всем кешем соцсети на $0,5 млн «для их детального изучения».

Facebook догоняет

О программе Facebook по поддержке своей инфраструктуры в Украине мало что известно. Шоломко упомянул, что не так давно соцсеть Марка Цукерберга искала в нашей стране человека, который будет отвечать за это направление. Но он не знает, увенчались ли поиски успехом. Как выяснила LIGA.net, этот человек уже появился. Его зовут Эд Кейв. А должность называется Interconnection Support Manager. По информации представителя одного из операторов, именно этот человек коммуницирует с украинскими компаниями и предлагает «зеркала». Редакция с ним связалась. Но Кейв сказал, что не уполномочен общаться с прессой.

Блиц-опрос редакции показал, что Facebook, в отличие от Google, не так давно начал устанавливать свои серверы на площадках украинских провайдеров. Очевидно, катализатором послужило перераспределение трафика после блокировки ВКонтакте и Одноклассников. В пресс-службах Укртелекома (№1 по абонентской базе) и Воли (игрок №3) заявили, что сейчас с представителями Facebook идут переговоры. Как уточняет глава Интернет ассоциации Украины Александр Федиенко, трафик с сервисов Facebook у интернет-провайдера должен быть более 3 Гбит. «Тогда можно смело писать к ним заявку на серверы», – подчеркивает он.

К операторам поменьше Facebook уже пришел. Руководитель группы компаний Триолан Вадим Сидоренко отмечает, что в прошлом году «приехали два комплекта» – один для Харькова, а другой – для Киева. У Ланет, как писал его гендиректор Мариан Ивасюк в октябре прошлого года, на техплощадке были размещены серверы Facebook на 40 Гбит/с.

После установки «зеркал» Facebook явно начинает работать лучше. «Более 80 % трафика Facebook, как и Google (более трети всего трафика), доступно всем абонентам Ланет на уровне локальной сети. То есть с на два порядка меньшей задержкой, чем в ближайших дата-центрах (2-3 мс вместо 150-350 мс) и на скорости порта доступа (100 или 1000 Мбит/с)», – писал Мариан Ивасюк.

Примечательно, что для Facebook, так же, как и для Goolge, размещение бесплатных серверов в Украине – удовольствие недешевое. Опрошенные редакцией представители операторов говорят, что по цене они сопоставимы друг с другом. «Один нормальный сервер подобного уровня стоит около $10 000», – говорит один из собеседников редакции. Для крупных операторов речь явно не идет об одном сервере. Таким образом, можно предположить, что Марк Цукерберг должен вложить в украинскую инфраструктуру десятки миллионов гривень, чтобы видео с котиками в ленте загружались быстро, да еще и в хорошем качестве.

(вгору)

Додаток 4

13.02.2018
Facebook теряет популярность у молодежи в США

В 2018 году количество молодых пользователей Facebook снизится на 5,8 процента. Число активных юзеров Instagram и Snapchat наоборот растет. Социальная сеть Facebook продолжает терять популярность среди американских подростков и молодежи. Как утверждает компания eMarketer, специализирующаяся на исследованиях рынка, в 2018 году в США количество пользователей Facebook в возрасте от 18 до 24 лет снизится на 5,8 процента. Для подростков 12-17 лет ожидается, что пользоваться Facebook впервые будут меньше 50 процентов представителей этой возрастной категории (InternetUA).

Эта тенденция продолжится и в 2019-2020 годах, предполагают эксперты. Они также убеждены, что больше всего новых пользователей в возрасте от 12 до 24 лет получит мессенджер Snapchat, а также блогплатформа для фото и видео Instagram.

Facebook пока впереди

Однако Facebook с большим преимуществом остается самой популярной соцсетью в США – ее пользователями считаются 170 миллионов человек. Instagram, являющейся дочерним предприятием Facebook, пользуются более 104 миллиона человек. У Snapchat – 86,5 миллиона пользователей.

Snapchat, особенно популярный среди подростков и молодежи, пытается завоевать и более старшую аудиторию. Однако, по оценке специалистов, пока остается открытым вопрос, будет ли молодое поколение по-прежнему считать Snapchat привлекательным для себя, если более старшие поколения также будут активно пользоваться тем же мессенджером. «Это дилемма, с которой уже сейчас сталкивается Facebook», – говорят эксперты.

(вгору)

Додаток 5

31.01.2018
Facebook забороняє рекламу криптовалют, щоб людей не обдурювали

Facebook вводить заборону на рекламу різних криптовалютних проектів, щоб захистити користувачів від фінансових авантюр (Espreso.tv). Про це повідомляє Engadget.

У правилах реклами на Facebook з’явився новий пункт, який стосується заборони реклами сумнівних фінансових продуктів.

У новому пункті під номером 29 в один ряд ставляться бінарні опціони, ICO, реклама криптовалюти, фондів на їх основі і сервісів по їх обміну. У розділі вказується: «Оголошення не повинні рекламувати фінансові продукти і

послуги, які часто пов’язані з шахрайськими проектами, такими як бінарні опціони, ICO або криптовалюта».

Facebook наводить приклади забороненої реклами. Так, тепер в соцмережі заборонені наступні типи рекламних оголошень:

- «Клікни сюди, щоб дізнатися про безпечну криптовалюту, яка дозволить здійснювати платежі по всьому світу»
- «Нове ICO! Купи токени з 15% знижкою»
- «Скористайся пенсійними накопиченнями, щоб інвестувати в біткоїн»
- «Почни торгівлю опціонами зараз і отримаєш бонуси»

Соціальна мережа вважає такі рекламні оголошення потенційно шахрайськими і хоче позбавити від них аудиторію.

«Наш основний принцип реклами в тому, що вона повинна бути безпечною. Оголошенням, що вводять користувачів в оману, немає місця на Facebook. Ми проводимо нову політику, яка забороняє рекламу, що просуває фінансові продукти і послуги, які часто пов’язані з обманом», – пише менеджер по продукту Роб Лізерн.

Роб додає, що соціальна мережа хоче, щоб люди мали можливість скористатися будь-яким продуктом, рекламованим на FB, без ризику бути обдуреними. Але серед компаній, які рекламують схеми швидкого заробітку, рідко можна зустріти ті, що грають за правилами.

Представник Facebook каже, що в подальшому компанія буде уважніше вивчати найрізноманітніші сигнали про незаконну рекламу.

(вгору)

Додаток 6

7.02.2018
Facebook объявил войну YouTube

Facebook, быть может, не первая платформа, которая приходит на ум, когда люди задумываются о потенциальных угрозах для бизнес-модели YouTube. Однако, по мнению CNBC, всё может измениться в ближайшее время. Сообщается, что социальный гигант рассматривает возможность расширения своего телевизионного сервиса Watch, чтобы превратиться в настоящего конкурента YouTube (InternetUA).

По словам источников, для решения этой далеко не тривиальной задачи Facebook откроет Watch для пользователей, которые хотят создавать свои собственные передачи и шоу. Поступив так, компания может избежать высоких издержек, связанных с покупкой у создателей прав на показ, вместо этого выбрав модель распределения доходов от рекламных объявлений между площадкой и создателями контента. То есть пойти по пути YouTube.

Учитывая более чем 2-млрд базу пользователей ведущей социальной сети в мире (ежедневно к ней обращается более 1,4 млрд человек), такое предложение может оказаться весьма заманчивым для авторов

видеоматериалов. Особенно если учесть, что доходы от рекламы на YouTube у последних значительно сократились в течение 2017 года.

Один из источников CNBC отметил, что долгосрочная стратегия Facebook заключается в создании самодостаточной видеоплатформы, полностью поддерживаемой рекламой и пополняемой преимущественно пользовательским контентом, за который сама социальная сеть в значительной степени не будет платить – по крайней мере, не напрямую.

Стоит отметить, что эти дискуссии всё ещё находятся на ранней стадии и окончательное решение ещё не принято. Тем не менее, тот факт, что столь влиятельная интернет-компания, как Facebook, проявляет интерес к созданию подобной YouTube платформы, говорит о том, что Google, возможно, потребуется предпринять дополнительные ответные усилия, если она хочет сохранить своё доминирование на рынке.

(вгору)

Додаток 7

7.02.2018

Facebook начнет угадывать социально-экономический статус пользователей

В новом патенте компании Facebook описывается система, которая будет использовать данные пользователя, например, образование, историю путешествий, количество принадлежащих устройств и домовладений, для предугадывания его социально-экономического статуса. Патент был обнаружен сайтом CBInsights (InternetUA).

Почему это важно: социальная сеть Facebook уже попадала под огонь за то, что слишком много знает о своих пользователях. Она могла бы использовать такую систему, чтобы лучше ориентировать рекламу и контент на конкретную аудиторию.

Это исследование позволит получать более подробную информацию о пользователях. Оно станет ключом к тому, чтобы рекламодатели могли достучаться до конкретных людей в подходящее время.

Как это работает: патент в Facebook описывает систему, которая использует «древо принятия решений» для классификации учётных записей. Некоторым данным будут присвоены баллы вероятности для прогнозирования их социального класса. Большое количество баллов будет говорить о высоком финансовом статусе. Исходя из этого, человеку будет попадаться реклама более дорогих товаров.

Например, пользователю в возрасте от 30 до 40 лет, которому принадлежит дом, будет присвоено 10 баллов, если он живет в глубинке, 20 очков для жителей городов и 30 очков за проживание в мегаполисе.

Как дела обстоят на самом деле: компании постоянно регистрируют патенты, даже не разрабатывая их в будущем. Facebook может никогда не

воспользоваться такой системой, однако она явно заинтересована в такой возможности.

(вгору)

Додаток 8

8.02.2018

Владелец мессенджера Snapchat отчитался о росте выручки и аудитории

Компания Snap, владеющая мессенджером Snapchat, сообщила о росте выручки и аудитории, после чего акции существенно подорожали (InternetUA).

В октябре-декабре 2017 года выручка Snap достигла 285,7 млн долларов, что на 72 % больше, чем годом ранее. Чистый убыток возрос примерно вдвое – со 170 млн долларов (20 центов на акцию) до 350 млн долларов (28 центов в расчете на одну ценную бумагу).

На скорректированной основе убыток оказался равным 13 центам на акцию, тогда как опрошенные Thomson Reuters I/B/E/S аналитики ожидали такой убыток на уровне 16 центов в расчете на одну ценную бумагу при выручке в 253,2 млн долларов.

Выручка Snap в пересчете на одного пользователя составила 1,53 доллара, что на 46 % больше показателя годичной давности. Расходы компании на одного участника сервиса Snapchat увеличились на 5 %, до 1,02 доллара.

Количество участников Snapchat, которые пользуются сервисом не реже одного раза в день, к концу декабря 2017 года составило 187 млн человек против 178 млн тремя месяцами ранее. На Уолл-стрит ожидали такую аудиторию в размере 184,2 млн.

В годовом исчислении суточная база пользователей повысилась на 18 %, однако динамика замедляется. За ней пристально следят инвесторы, которые надеялись, что растущая аудитория будет способствовать подъему рекламных доходов, отмечает информационное агентство «Рейтер».

По словам аналитиков исследовательской фирмы eMarketer, Snapchat постепенно переманивает к себе рекламодателей на рынке интернет-рекламы, на котором доминируют Facebook и Google, контролируя примерно половину выручки.

Сервис Snapchat, начавший работу в 2011 году, позволяет обмениваться сообщениями, фотографиями и видеороликами. Особенностью проекта стала заявленная разработчиками конфиденциальность: фото- и видеосообщения после просмотра удаляются не только с устройств пользователей, но и с серверов компании.

По данным Mediascope, количество пользователей из России, которые зашли в приложение Snapchat хотя бы один раз в июне 2017 года, составляло 412,7 тысячи человек.

Компания вышла на биржу в начале марта 2017 года. Это IPO стало самым крупным в технологической отрасли за весь прошлый год.

(вгору)

Додаток 9

13.02.2018
УНІАН запустив новинного бота

Інформаційне агентство УНІАН запустило новинного чат-бота, за допомогою якого можна отримувати розсилки в Facebook Messenger з головними подіями, корисними статтями і анонсами цікавих заходів (МедиаБизнес).

Задача бота – поліпшити доставку актуальних новин читачам УНІАН. Цифровий помічник працює за принципом push-повідомлень, які починають надходити у месенджер після підписки на новини. Також користувач може самостійно вибрати зручний час для отримання інформаційної розсилки: вранці, протягом дня або ввечері. Всі повідомлення доступні на українській і російській мовах.

У меню чат-бота користувач має доступ до 5 основних розділів сайту УНІАН: «Економіка», «Спорт», «Війна», «Думки», «Публікації». Особливу увагу при розробці цифрового помічника було приділено розділу «Спорт»: чат-бот буде вести текстову онлайн-трансляцію зимової Олімпіади 2018. Крім того, в рамках сервісу «Погода УНІАН» бот сповіщає читача про метеорологічні зміни.

«Час – найцінніший ресурс. Для того, щоб нашим читачам не доводилось витрачати його на постійний моніторинг новинних стрічок − усе найважливіше з допомогою бота зможе відфільтрувати та надати команда редакторів УНІАН у максимально комфортний спосіб. Віримо, що користувачам буде зручніше отримувати важливі новини через месенджер», − коментує Михайло Ганницький, шеф-редактор інформаційного агентства УНІАН.

Чат-бот УНІАН для Facebook Messenger є проектом департаменту 1+1 Digital.

(вгору)

Додаток 10

13.02.2018
Крупнейший мировой производитель грозится изъять рекламу из Google и Facebook

Компания Unilever пригрозила снять свою рекламу с онлайн-платформ, таких как Facebook и Google, если они не смогут искоренить контент, который «создает разделение в обществе и способствует разжиганию гнева и ненависти» (Телекритика).

Кит Вид, главный специалист по маркетингу многонациональной компании, чьи бренды включают Dove, Magnum, Persil, Rexona и Marmite, сказал, что онлайн-платформы «чуть лучше болота». Он сказал крупным

рекламным, медиа и технологическим компаниям, собравшимся на конференции в Калифорнии: «Как один из крупнейших рекламодателей в мире, мы не можем рекламироваться в среде, в которой наши потребители не доверяют тому, что видят».

По словам аналитиков, реклама на Google и Facebook составляет почти три четверти всей цифровой рекламы в США. В Великобритании им принадлежит более 60 % цифровой рекламы.

Ультиматум Unilever был поставлен в то время, когда социальные медиа столкнулись с растущей критикой за неспособность защитить детей от нежелательного контента, бороться с фейковыми новостями и искоренить ненависть и экстремизм. В прошлом году Procter & Gamble, владелец брендов, в числе которых Pantene и Pampers, выпустил аналогичное предупреждение перед тем, как сократить расходы на рекламу в $100 млн. На продажах это никак не сказалось.

Вид заявил: «Фейковые новости, расизм, сексизм, терроризм, сообщения о ненависти, токсичные материалы, направленные на детей, – это среда интернета, в которой мы оказались, и она находится в миллионах миль от того, где мы планировали оказаться».

Unilever – второй по величине в мире маркетинговый гигант, который потратил 7,7 млрд евро в прошлом году на рекламу своих брендов, в том числе PG Tips, Vaseline и Bertolli.

На первом месте Procter & Gamble (P&G), который потратил $10,5 млрд на рекламу.

(вгору)

Додаток 11

4.02.2018

Facebook вредит обществу больше, чем McDonald’s

Возможно, Walmart и McDonald’s и вредят обществу, но по степени негативного воздействия Facebook удалось перегнать их обоих. По крайней мере, так ответили 2000 американцев в опросе исследовательской компании Honest Data, пишет Business Insider (InternetUA).

Респонденты должны были выбрать, какая из предложенных в списке компаний наносит максимальный урон обществу. Среди прочих, в нем были Marlboro, Walmart, Facebook, McDonald’s и Coca-Cola. Самой вредоносной компанией 43% американцев признали Marlboro. Facebook оказался на втором месте, набрав 27 %. Далее идут McDonald’s (21 %) и Walmart (18 %). Правда, 36 % респондентов поставили «галочку» напротив пункта «Ни одна из вышеперечисленных».

По словам основателя Honest Data Тэйвиса МакГинна, он совсем не удивлен такому отношению к Facebook, учитывая, сколько обвинений компания была вынуждена выслушать за минувший год. «Люди все чаще

задаются вопросом, какое влияние социальные сети оказывают на их психологическое состояние», – написал он.

Бывший вице-президент Facebook Чамат Палихапития высказался гораздо более категорично, заявив, что чувствует «невероятную вину» за то, какого «монстра» помог вырастить. Палихапития уверен, что Facebook – это инструмент, разрывающий социальную структуру общества и призывает отказаться от использования соцсетей. Подобные заявления сделали первый инвестор компании Шон Паркер и бывший менеджер по продукту Facebook Антонио Гарсиа-Мартинез.

Их слова подтверждают и последние исследования в области психологии. Люди, проводящие огромное количество времени в соцсетях, гораздо больше подвержены депрессии, беспокойству и суицидальным настроениям. И, похоже, здесь прослеживается не корреляция, а причинно-следственная связь.

В другом опросе американцы должны были выбрать технологическую компанию, оказавшую наихудшее влияние на общество. Лидером снова стала Facebook, сразу на ней идет Twitter. А вот Google, Netflix, и LinkedIn остались далеко позади. Однако, пункт «Ни одна из вышеперечисленных» отметили 53 % опрошенных.

Разумеется, Марк Цукерберг не мог оставить такую ситуацию без внимания. На днях он заявил, что пользователи Facebook стали на 50 млн часов меньше проводить в социальной сети. Это произошло благодаря новым алгоритмам, которые показывают меньше вирусных роликов, делая акцент на постах друзей и интересных людей.

(вгору)

Додаток 12

6.02.2018

Пчелы против меда. Бывшие сотрудники Facebook и Google решили побороться с соцсетями

Бывшие сотрудники Google и Facebook основали организацию «Центр гуманных технологий», которая, в частности, будет изучать влияние соцсетей на мир (InternetUA).

Возглавляет группу бывший внутренний специалист по этике в Google Тристан Харрис, сообщает Mashable.

Новая коалиция посвящена изучению влияния технологии. «Центр гуманных технологий» ставит перед собой задачу предупредить о вреде, который технологии могут причинить здоровью. В частности, группа готовится начать рекламную кампанию, которая рассказывает о технической наркомании.

«Facebook создал бизнес-модель, которая по существу сделал мнение людей, которые верят в теории заговора, более ценным. Это было в интересах Facebook, чтобы обратиться к страху и гневу», – сказал бизнесмен Роджер Макнейм, который инвестровал в Facebook на ранней стадии развития компании. Макнейм признался, что он был очарован Facebook в своих ранних

разговорах с Цукербергом, но манипуляции, которые он видел, заставили инвестора изменить мнение.

Среди людей, которые вошли в коалицию, бывший производственный директор Facebook Сэнди Паракилас, бывший директор по коммуникациям Apple и Google Линн Фокс, бывший топ-менеджер Facebook Дейв Морин, создатель кнопки «лайк» и соучредитель Asana Джастин Розенштейн и другие знаковые для Кремниевой долины личности. Джим Штейер, исполнительный директор и основатель Common Sense выразил надежду, что «Центр гуманных технологий» сможет повлиять на IT-гигантов и привлечь их внимание к проблеме.

«Мы были внутри этой системы. Мы знаем, какую информацию о людях получают компании», – рассказал глава коалиции Тристан Харрис.

Коалиция планирует продвигать законодательство, которое бы заставило технологические компании вносить изменения в свою продукцию. В частности, законопроект сенатора Эда Марки направлен на то, чтобы государственные институты изучили роль и влияние электронных СМИ на развитие детей. Также коалиция поддерживает законопроект сенатора Боба Герцберга, который будет требовать от онлайн-платформ, таких как Instagram и Twitter, определять, не является ли учетная запись ботом. Этот законопроект, как ожидается, будет подан на этой неделе.

Также группа намерена запустить сайт Ledger of Harms, на котором будут представлены данные исследований о влиянии технологий на здоровье и способах создания более безопасных продуктов.

(вгору)

Додаток 13

2.02.2018

Twitter предупредил 1,4 млн пользователей о пропаганде РФ

Социальная сеть Twitter отправила сообщение около 1,4 млн пользователей, которые во время президентской кампании в США в 2016 году следили за аккаунтами, связанными с пропагандой России. Об этом говорится в сообщении в официальном блоге соцсети (InternetUA).

«Мы увеличили количество людей, которым сообщили о взаимодействии с учетными записями Twitter, потенциально связанными с пропагандистской деятельностью российской правительственной организации, известной как Агентство интернет-исследований», – отметила администрация.

Рассылку получили граждане, которые находятся на территории США и во время избирательной кампании подписывались, цитировали или упоминали твиты почти 4 тыс. аккаунтов, связанных с российским агентством.

В октябре 2016 года власти США официально обвинили Россию во взломе серверов американских партий, а также во вмешательстве в процесс президентских выборов в стране. В опубликованном докладе американской

разведки говорится, что начать кампанию приказал президент РФ Владимир Путин.

Руководители из Facebook, Twitter и Alphabet дали показания в трех комитетах Конгресса по предполагаемым попыткам России распространить дезинформацию до и после президентских выборов в США в 2016 году.

80 тысяч постов были опубликованы в период с июня 2015 года по август 2017 года, и большинство из них были направлены на раскол американского общества относительно социальных и политических проблем. Среди них – расовые отношения и право на оружие, сообщает Facebook.

Twitter передает, что идентифицировал несколько тысяч фейковых учетных записей, что гораздо больше, чем заявленное ранее количество – 201. По словам компании, учетные записи, связанные с российскими троллями, опубликовали порядка 1,4 миллионов сообщений о выборах 2016 года, что составляет 0,74 % от общего количество сообщений, связанных с выборами. Twitter предоставил американским законодателям имена всех фейковых учетных записей.

(вгору)

Додаток 14

5.02.2018

Как мессенджер WeChat захватил Китай

Ещё в декабре 2017 года в Сети появилась новость о том, что китайский мессенджер WeChat приравнят к паспорту. Он считается одним из самых популярных во всем мире и единственным действующим в Китае (InternetUA).

Правительство уже давно взяло мессенджер под тотальный контроль, поэтому о тайне переписки многие могут уже забыть.

По этому поводу журналисты The Verge написали целую статью, содержанием которой мы хотели бы с вами поделиться.

Самый популярный мессенджер в Китае, WeChat, всегда поддерживал тесные отношения с китайским правительством. Причём он был взят под контроль аж в 2011 году.

Теперь WeChat будет играть еще большую роль. Сейчас ведется работа по интеграции WeChat с электронной системой идентификации в Китае.

Пользователям WeChat становится все труднее и труднее отказаться от мессенджера. – Юхуа Ван, бывший житель Шанхая, написавший статью «Как WeChat превращается в огромную часть нашей жизни» для Школы коммуникаций и журналистики в Анненберг

Иностранцы, как правило, загружают приложение для обмена сообщениями, чтобы оставаться на связи. В стране запрещены другие американские приложения.

WeChat уже готов идентифицировать граждан

Теперь WeChat готова стать системой электронной идентификации китайских граждан, как сообщает Xinhua. Компания выдаст виртуальные ID,

которые люди будут использовать вместо физических удостоверений личности, выданных государством.

В мессенджере можно зарегистрироваться только с реальным именем, идентификаторы впоследствии не меняются.

Профессор Гарвардской школы бизнеса Вилли Ши (соавтор тематического исследования по WeChat) называет переход к электронной системе идентификации «предсказуемой эволюцией».

Как происходило тестирование выдачи виртуальных ID

Проект уже прошёл тестовый режим, начавшийся в декабре прошлого года. Для участия в пилотной программе пользователи открывали мини-приложение в WeChat для подачи заявки на получение сертификата.

После этого WeChat выдавал цифровую черно-белую идентификационную карту, которая работает при более неформальном использовании. Например, для регистрации в интернет-кафе (в Китае необходимо предоставить идентификатор для входа в систему).

Пользователи также могут подать заявку на обновление до цветного удостоверения личности. Оно может использоваться для банковских операций и регистрации бизнеса. Для защиты учетных записей также есть возможность установить восьмизначный пароль. А технология распознавания лиц будет использоваться для проверки заявителей, дабы избежать мошенничества.

Кроме того, приложение будет записывать отпечаток пальца человека и чип карты из их соответствующего физического идентификатора.

В 2016 году Бюро общественной безопасности Ухана в провинции Хубэй, Китай, сотрудничало с платежной системой Alipay для запуска аналогичной электронной системы идентификации.

Правда, после тестирования 400000 пользователей, проект перестал работать. Поэтому остался только WeChat.

Многие все ещё переживают за конфиденциальность данных

Многие пользователи стали переживать за конфиденциальность предоставленной WeChat информации. И все после того, как мессенджер стал подконтролен государству.

Сама компания заявляет, что хранит данные только «до тех пор, пока это необходимо», чтобы «соответствовать применимым законам и правилам».

В начале этого месяца бизнесмен Ли Шуфу заявил, что генеральный директор Tencent (владелец WeChat) Ма Хуатэн «должен следить за всеми нашими чатами каждый день».

В компании опровергли этот факт.

Тем не менее, WeChat считается самым подконтрольным мессенджером вне зависимости от того, что говорят представители компании.

«Но даже если компания говорит иначе, на техническом уровне она не предоставляет пользователям большую защиту от государственного надзора. Tencent заработал 0 баллов из 100 за отсутствие в WeChat защиты свободы слова и отсутствие сквозного шифрования», – выдержка из отчета Amnesty.

Tencent не говорит, когда правительство запрашивает данные пользователя и не дает никаких подробностей о типе шифрования, если оно вообще есть.

Мэтт Райт из AngelHack уверен в том, что простые пользователи совершенно не интересны государству.

Пока вы не делаете ничего странного и не замышляете ничего против правительства, они не собираются копаться в ваших данных.

Многие эксперты говорят, по сути, одно и то же: «Это не проблема, потому что у вас нет конфиденциальных данных».

Рост WeChat в Китае сопровождался цензурой иностранных приложений, правительственными субсидиями и интеграцией с государственными учреждениями. И теперь шаг в сторону ещё большей интеграции мессенджера в сторону идентификации пользователей по ID, сделает его по-настоящему официальным приложением Китая.

(вгору)

Додаток 15

6.02.2018

Главным регулятором рунета становится ФСБ

Главным контролером рунета становится Федеральная служба безопасности (ФСБ) – к такому выводу пришли эксперты международной правозащитной группы «Агора» в ежегодном докладе, посвященном ограничениям свободы интернета в России (InternetUA).

Мониторинг ситуации правозащитники ведут уже 10 лет и все это время росла не только аудитория рунета, но и давление на него, констатируют эксперты. В 2017 г. каждый день в среднем блокировалось 244 интернет-страницы, каждые шесть дней пользователи подвергались нападению или угрозам, а каждые восемь дней выносился приговор к реальному лишению свободы за размещенную в сети информацию. В общей сложности в течение 2017 г. зафиксировано 115 706 фактов ограничения свободы интернета, абсолютное большинство из них (более 110 000) связаны с блокированием и фильтрацией контента, а также с запретом информации по различным основаниям.

Увеличилось как общее число случаев привлечения к уголовной ответственности пользователей (с 298 в 2016 г. до 411 в 2017 г.), так и количество приговоров к реальному лишению свободы (с 32 до 43), отмечается в докладе. При этом количество уголовных дел о призывах к экстремистской деятельности (ст. 280 Уголовного кодекса, УК) в 2016–2017 гг. стабилизировалось, зато виден значительный рост доли и числа подследственных ФСБ дел об оправдании терроризма и призывах к террористической деятельности (ст. 205.2 УК), а также части дел о призывах к экстремизму, следствие по которым также ведет ФСБ. С 2013 г. количество уголовных дел по ст. 205.2 увеличилось более чем в 20 раз, в то время как дел

по ст. 280 и ст. 282 стало лишь вдвое больше. И если в 2014 г. доля приговоров за публичные высказывания по делам, которые вела ФСБ, составляла 18 %, а в 2015 г. даже снизилась до 16 %, то в 2016 г. таких дел стало уже 21 %, а в первом полугодии 2017 г. и все 30 %.

Перераспределение веса «экстремистских» статей в общей статистике уголовного преследования пользователей интернета демонстрирует активизацию ФСБ и снижение роли Следственного комитета и МВД (в том числе Центра по противодействию экстремизму), отмечает руководитель международной «Агоры» Павел Чиков. Причем ФСБ оказывает все большее влияние на отрасль и в других секторах, например в сфере технологий, добавляет эксперт.

2017 г. стал рекордным и по числу законодательных инициатив, направленных на «суверенизацию» рунета, а фактически – на усиление контроля над коммуникациями пользователей и распространением информации в сети. С января 2018 г. вступил в силу закон, обязывающий интернет-мессенджеры идентифицировать пользователей: дешифрование переписки и идентификация пользователей становятся ключевыми аспектами обеспечения нацбезопасности. При этом функция контроля над интернетом продолжает постепенно перетекать из рук Роскомнадзора, созданного в качестве регулятора отрасли, в руки прокуратуры и органов госбезопасности, считают авторы доклада. В самом Роскомнадзоре постоянно подчеркивают, что выполняют лишь технические функции, руководствуясь решениями иных ведомств.

От концепции черных списков, использованной в 2012 г. для технического оформления блокировок интернет-сайтов, власти постепенно переходят на новый уровень – криминализации сетевой активности. Первой массовой кампанией уголовно-правового характера, прямо направленной против пользователей интернета, стало преследование «групп смерти». Кроме того, в 2017 г. УК пополнился новыми составами преступлений (например, была криминализована пропаганда терроризма), что фактически стало реакцией на неэффективность блокировок как средства ограничения распространения информации, уверен Чиков. От политики запретов власти переходят к уголовному преследованию пользователей, делают вывод авторы доклада.

Пресс-служба ФСБ не ответила на запрос «Ведомостей». Интернет-омбудсмен Дмитрий Мариничев говорит, что практику ограничения распространения информации в сети трудно признать эффективной – напротив, именно свободное обсуждение дает обществу возможность выработать своего рода иммунитет к наиболее радикальным проявлениям.

(вгору)

Додаток 16

6.02.2018

Европол арестовал распространявших троян Luminosity хакеров

Європейський Центр по борьбе с киберпреступностью при Европоле (Europol's European Cybercrime Centre, EC3) и Национальное агентство по борьбе с преступностью в Великобритании (National Crime Agency, NCA) опубликовали информацию о международной операции правоохранительных органов, нацеленной на продавцов и пользователей трояна для удаленного доступа Luminosity (InternetUA).

В операции принимали участие сотрудники более десятка различных правоохранительных органов из Европы, США и Австралии. Операция была проведена в сентябре 2017 года, однако ведомство обнародовало подробности только сейчас.

Правоохранительные органы заинтересовались Luminosity, также известном как LuminosityLink, в сентябре 2016 года, когда в Великобритании был арестован человек, подозреваемый в преступлениях, связанных с хакерством. После ареста хакера было принято решение провести международную операцию, по итогам которой правоохранительным органам удалось остановить продажу трояна и привести в нерабочее состояние его существующие копии.

С сентября 2017 года правоохранительные органы провели серию арестов и обысков на территории Европы, Северной Америки и Австралии, ориентируясь как на продавцов, так и на пользователей Luminosity. По словам представителей NCA, ответственными за распространение трояна была небольшая группа лиц из Великобритании.

Luminosity впервые появился в мае 2015 года и был доступен для покупки всего за $40. Троян для удаленного доступа позволял хакерам получить полный контроль над зараженными компьютерами, в том числе отключать антивирусы, считывать нажатия клавиш, похищать пароли и другие данные и шпионить за жертвами через web-камеру устройства.

(вгору)

Додаток 17

6.02.2018

Утекший документ показал интерес АНБ США к контролю за криптовалютами

Вооруженные силы и Агентство национальной безопасности (АНБ) США способны раскрыть пользователей Tor, I2P и VPN, а также работают над отслеживанием криптовалюты Monero, следует из утекшего в Сеть документа, предположительно принадлежащего ВС США (InternetUA).

В документе говорится об успехах спецслужб касательно компрометации сервисов по анонимизации, таких как Tor, I2P и VPN, а также о совместном проекте команды киберзащиты армии США (US Army Cyber Protection Team, CPT) и сотрудников АНБ по отслеживанию криптовалют. Фотография документа датирована 21 августа 2017 года и была опубликована на сайте 4chan.

Как следует из документа, у спецслужб возникли некоторые трудности в отслеживании криптовалют, основанных на CryptoNote, который является протоколом уровня приложений, реализованным в нескольких децентрализованных криптовалютах, ориентированных на конфиденциальность пользователей. Спецслужбы запрашивают у правительства дополнительные ресурсы для отслеживания виртуальных валют, таких как Monero (XMR), Anonymous Electronic Online CoiN (AEON), DarkNet Coin (DNC), Fantomcoin (FCN) и Bytecoin (BCN). Как полагают власти США, Monero может стать основной криптовалютой в киберпреступном подполье.

По данным издания DeepDotWeb, указанный в документе контактный номер телефона подлинный и по факту принадлежит команде киберзащиты армии США в Форт-Гордон, штат Джорджия. Издание попросило разработчиков Monero и другие источники, имеющие отношение к армии США прокоментировать ситуацию. Все они подтвердили подлинность документа. В настоящее время неясно, кто именно стал источником утечки.

(вгору)

Додаток 18

12.02.2018

В Германии суд обвинил Facebook в незаконном использовании персональных данных

В Германии суд признал использование компанией Facebook персональных данных своих пользователей незаконным, поскольку социальная сеть не спрашивала согласия на их обработку надлежащим образом. Об этом сообщает пресс-служба Федерации по защите прав потребителей Германии (Der Verbraucherzentrale Bundesverband, vzbv) (InternetUA).

По словам представителей федерации, настройки по умолчанию в приложении Facebook и некоторые из ее условий обслуживания нарушают потребительское законодательство, вследствие чего суд признал части пользовательского соглашения об использовании персональных данных недействительными.

«Facebook скрывает настройки по умолчанию и не предоставляет пользователям достаточной информации об использовании их данных при регистрации… Это не соответствует определению информированного согласия», – заявили правозащитники.

Одна из проблем заключалась в том, что в приложении Facebook для смартфонов была по умолчанию активирована услуга отображения местоположения пользователя его собеседнику.

Помимо этого, в настройках конфиденциальности были по умолчанию активированы функции, позволяющие поисковым системам ссылаться на временную шкалу пользователя, позволяя быстро и легко найти профиль конкретного пользователя.

«Согласно постановлению суда, все пять настроек по умолчанию в приложении Facebook, о которых жаловалась правозащитная организация, признаны незаконными», – говорится в заявлении федерации.

Как заявили представители Facebook, компания в любом случае обжалует решение суда. Они также добавили, что в условия пользования и рекомендации по защите данных уже внесены существенные изменения для соответствия новым правилам Европейского союза, которые должны вступить в силу в июне 2018 года.

(вгору)

Додаток 18

31.01.2018

Карточные мошенники перешли из магазинов и банкоматов в интернет

Количество случаев мошенничества с платежной картой при расчетах в торговых сетях, а также при снятии денег в банкоматах уменьшается. При этом доля таких операций в интернете растет (InternetUA).

Об этом заявил директор Украинской межбанковской ассоциации членов платежных систем ЕМА Александр Карпов.

«Если клиент банка использует карту в торговой сети, то только в 2 % случаев могут возникнуть проблемы. Три года назад этот показатель составлял 12 %», – сообщил Карпов.

В ЕМА отмечают, что расчеты в торговых сетях являются наиболее безопасным способом оплаты картой.

«Доля проблемных операций в интернете и при переводах с карты на карту выросла с 50 % практически до 70 %», – сообщил Карпов.

Самый популярный вид мошенничества, когда у владельцев платежных карт обманным путем выясняют данные. Согласно оценкам ЕМА, в 2017 году общая сумма похищенных таким образом средств и средств похищенных при расчетах в интернете выросла почти вдвое до 669,63 млн грн.

В Национальном банке в свою очередь подсчитали, что доля мошеннических операций с картами уменьшается.

«В 2017 году доля мошеннических операций по отношению ко всем операциям по картам составила 0,0077 %, то есть это 77 грн на 1 млн грн, потраченных с помощью карточки», – сообщил директор Департамента платежных систем и инновационного развития НБУ Александр Яблуновский. Годом ранее эта цифра была близка к 0,01 %, что составляет 100 грн на 1 млн грн.

В то же время средний чек в мошенничестве за год вырос с 1900 грн до 2100 грн. Но при этом на 1 млн всех платежных операций приходится лишь 25 мошеннических операций (0,0025 %).

(вгору)

Додаток 20

5.02.2018

Вредонос WannaMine обходит защиту традиционных антивирусов

Как сообщают эксперты Panda Security, новый вариант вредоносной программы под названием «WannaMine» стал заражать многие компьютеры во всем мире, чтобы использовать их ресурсы для майнинга криптовалюты под названием Monero (Компьютерное Обозрение).

WannaMine был впервые обнаружен Panda Security в октябре прошлого года, но только сейчас эта вредоносная программа привлекла внимание общественности благодаря ряду громких заражений. Но в отличие от других вариантов вредоносных программ, оказывается, что WannaMine очень сложно обнаружить и заблокировать.

Если говорить упрощенно, то WannaMine был разработан для майнинга криптовалюты под названием Monero. Эта вредоносная программа скрытно заражает компьютер жертвы, а затем использует его для запуска сложных процедур расшифровки, которые позволяют создавать новые Monero. Затем валюта добавляется в цифровой кошелек, принадлежащий хакерам, которые готовы тратить ее по своему выбору.

Существует несколько серьезных проблем, связанных с WannaMine. Во-первых, то, как зловред пытается максимально использовать ресурсы процессора и оперативной памяти, в результате чего компьютер начинает работать под максимальными нагрузками. В конце концов, ПК начинает сбоить, может привести к дорогостоящему ремонту или даже его полной замене.

Вторая серьезная проблема связана с тем, как WannaMine распространяет себя. Изначально нет ничего не обычного: путем обмана пользователей заставляют скачать вредоносную программу из вложенного в электронное письма файла или на зараженных веб-сайтах. После того, как вредоносная программа была установлена, WannaMine начинает использовать несколько очень изощренных «трюков», чтобы распространиться по сети.

С помощью двух встроенных утилит Windows (PowerShell и инструментарий управления Windows Management Instrumentation), WannaMine пытается перехватывать регистрационные данные, которые позволяют удаленно подключаться к другим компьютерам. Если это не получается, то WannaMine возвращается к использованию того же эксплойта безопасности (EternalBlue), что использовался шифровальщиком WannaCry для собственного распространения.

В силу того, что данная угроза использует встроенные в Windows утилиты, WannaMine относится к «безфайловым» угрозам, что делает ее чрезвычайно сложной в обнаружении и блокировке. На самом деле, некоторые исследования показывают, что многие традиционные антивирусные приложения не могут обнаруживать WannaMine и защищать пользователей от этой угрозы.

Единственный способ обнаружить инфекцию WannaMine – это тщательный мониторинг приложений и служб, запущенных на компьютере, используя технику, аналогичную Adaptive Defense.

Поддержание компьютера в обновленном состоянии и установка решения безопасности поможет блокировать эту вредоносную программу по майнингу криптовалюты до того, как она сможет захватить контроль над ПК.

(вгору)

Додаток 21

5.02.2018

Как полностью стереть себя из интернета

Если Вы когда-то задумывались о том, чтобы полностью стереть о себе информацию из интернета, но либо у Вас не доходили руки исполнить этот трудоемкий процесс, либо знакомые утверждали, что это невозможно – выход есть. Ниже описаны способы, как достаточно быстро и бесплатно удалить себя отовсюду(InternetUA).

Ищем аккаунты

Если вы использовали почту Gmail или Microsoft для регистрации аккаунтов, поможет сервис Deseat.me. Он находит аккаунты в разных сервисах (от Airbnb до Uber), которые вы привязывали к учетной записи, и предоставляет ссылки на страницы для удаления этих аккаунтов.

Работает это так: логинитесь на Deseat.me через Google-аккаунт или учетную запись Microsoft, ждёте несколько секунд и получаете список привязанных к аккаунту учётных записей.

Чтобы добавить аккаунт в список на удаление, нажимаете Add, и он попадает из нижнего списка в верхний. Затем в нижнем списке нажимаете Delete и переходите на страницу удаления аккаунта.

Конечно, порой придётся напрячься и вспомнить пароль или восстановить его через почту. Но всё быстрее, чем искать вручную, где вы регистрировались и что писали. Жаль, что историю сообщений с аккаунтов пока ни один сервис автоматически не стирает.

Некоторые сайты не позволяют удалить аккаунт. Тогда стоит попробовать его деактивировать.

Другой вариант: если на сайте нет деактивации и удаления аккаунта, а также нельзя оставлять пустые поля, сотрите все правдивые данные о себе, заменив их ложными, и привяжите учётную запись к новому адресу электронной почты, не связанному со старым.

Мы не рекомендуем удалять почту, к которой привязаны аккаунты. В некоторых сервисах ваш почтовый адрес через некоторое время может занять злоумышленник, и тогда он получит доступ к вашим данным.

Убиваем себя в соцсетях

Для удаления всей информации из аккаунтов в Facebook, MySpace, LinkedIn и Twitter есть забавный сервис Web 2.0 suicide machine. Он призван вырвать пользователя из лап социальных сетей и стереть всю информацию в аккаунте.

Пользоваться крайне просто: авторизуетесь в сервисе с помощью своей учётной записи, а дальше он методично удаляет все ваши фото, посты, сообщения, друзей и т. п. Восстановить данные будет невозможно.

Сервис утверждает, что автоматически удалит Facebook-аккаунт с тысячей друзей за 52 минуты. Если делать это вручную, потребовалось бы 9 часов 35 минут.

Настраиваем оповещения

На Google Alerts можно заполнить форму и получать оповещения о новых станицах о вас на e-mail. В качестве критериев поиска удобно указывать имя и фамилию, ник, номер телефона, домашний адрес и e-mail.

Итоги

Существуют специальные сервисы вроде DeleteMe, Reputation, RemoveYourName, которые за деньги обещают удалить информацию о вас из интернета. Но они знают о вас меньше, чем вы сами. Поэтому к услугам таких сервисов прибегают либо люди, репутация которых действительно стоит миллионы, либо не слишком опытные пользователи.

Однако нужно учитывать, что страницы из кэша поисковых систем, ссылки в закладках и личных сообщениях всё равно остаются. Но если действовать последовательно, подавляющее большинство упоминаний о себе можно убрать довольно быстро и бесплатно.

(вгору)

Додаток 22

5.02.2018

Создан бесплатный инструмент для полностью автоматических кибератак

Опубликована программа AutoSploit, способная автоматически искать уязвимые устройства и атаковать их, используя пакет Metasploit (InternetUA).

«Хакер-автомат»

На GitHub опубликована программа AutoSploit, представляющий собой «автоматизированный» инструмент для кибератак. Он сам выискивает в Сети уязвимые устройства и пытается атаковать их, используя пакет Metasploit. Таким образом, пользователям AutoSploit вообще не нужно обладать какими-либо хакерскими навыками, чтобы с успехом взламывать уязвимые ресурсы.

Написанный на Python, AutoSploit использует, в первую очередь, поисковик Shodan.io, который способен выявлять доступные из Сети компьютеры, серверы, устройства интернета вещей и промышленные контроллеры. После обнаружения таких устройств, AutoSploit «подтягивает» базу данных библиотеки эксплойтов Metasploit, широко используемую как

легитимными экспертами по безопасности для проведения пен-тестов, так и хакерами – для кибератак.

В описании AutoSploit говорится: «Были отобраны существующие модули Metasploit для осуществления удаленного запуска кода, для попытки получение реверс-шелла (способ удаленного перехвата доступа, при котором атакуемая машина обращается к порту атакующей – прим. CNews) или сессии Meterpreter».

Ниже указывается, что запуск подобного кода с компьютера, который легко отследить, «может быть не лучшей идеей, с точки зрения операционной безопасности». Это замечание справедливо уже хотя бы потому, что любые вредоносные кибератаки чреваты юридическими и уголовными последствиями.

Эксперты по безопасности встретили появление этого кода неодобрительно.

«Программа подразумевает отсутствие каких-либо специальных навыков со стороны потенциального взломщика; иными словами, любой школьник может с помощью AutoSploit попытаться «хакнуть», например, электростанцию, и далеко не факт, что его попытка не увенчается успехом, – считает Роман Гинятуллин, эксперт по информационной безопасности компании SEC Consult Services. – Само по себе появление общедоступных - во всех смыслах – инструментов для кибератак, это всегда дополнительный фактор риска».

С другой стороны Гинятуллин признает, что появление чего-то подобного AutoSploit было вопросом времени: «Рано или поздно это произошло бы в любом случае, это было очевидно. Вопрос в возможных последствиях, – полагает эксперт. – И вот тут стоит отметить, что появление такого «автохакера» окончательно закрывает вопрос о том, работает ли популярный и поныне подход «нас не взломают, потому что мы никому не нужны». Нет, не работает. Для «хакера-автомата» неважно, кто вы и для чего предназначен ваш сервер. Имеет значение только его доступность и наличие уязвимостей».

Полный автомат

Идея AutoSploit не нова. Автоматизированные средства для кибератак существуют уже давно – например, Armitage в Metasploit позволяет автоматически перебирать уязвимости и эксплойты к ним, но не поиск самой мишени. AutoSploit представляет опасность именно тем, что способен автоматизировать весь процесс. Хотя и это не значит, что кибератака увенчается успехом.

«В фреймворк Metasploit входит огромное количество эксплойтов, однако большинство потребует дополнительной настройки для срабатывания по конкретным мишеням, – уточняет Гинятуллин. – Вариант «из коробки» на практике срабатывает очень редко».

(вгору)

Додаток 23

5.02.2018

Компьютеры на Windows оказались под угрозой

Специалисты обнаружили новые угрозы, жертвами которых могут стать пользователи популярных версий операционной системы Windows. Принцип работы трех видов вредоносных программ опубликован на GitHub (InternetUA).

Эксплоиты, называемые EternalSynergy, EternalRomance и EternalChampion, занимаются поиском уязвимостей в системе и эксплуатируют их. Они работают по принципу EternalBlue – разработки Агентства национальной безопасности США, которую злоумышленники взяли за основу при создании опасного вируса-вымогателя WannaCry.

Каждый из описанных пользователем эксплоитов имеет удаленные модули управления командами и кодом, которые основаны на адаптации, называемой zzz_exploit. Они используют специфические структуры связи (протокол SMB) для получения администраторского доступа к системе.

Специалист по кибербезопасности Кевин Бомонт (Kevin Beaumont) подтвердил эффективность эксплоитов: по его словам, любые вариации Windows от Windows 2000 до серверной модификации 2016 года можно взломать совершенно беспрепятственно и с большим уровнем защиты соединения. Он также самостоятельно провел успешные эксперименты на Windows 2000 и Windows XP.

Также известно, что эксплоиты обладают способностями к самовоспроизводству, которые позволяют быстро распространять их действие на множество машин. Специалисты предупреждают, что если не исправить уязвимости в программном обеспечении, они захватят большинство компьютеров в мире.

(вгору)

Додаток 24

5.02.2018

Стали известны новые подробности об уязвимости нулевого дня в Flash Player

Исследователи кибербезопасности из компаний FireEye и Cisco Talos проанализировали атаки, в которых эксплуатировалась недавно выявленная уязвимость нулевого дня в Adobe Flash Player и связали их с группой, известной своими атаками на цели в Южной Корее (InternetUA).

Ранее компьютерная группа реагирования на чрезвычайные инциденты (CERT) Южной Кореи сообщила о новой уязвимости нулевого дня в Adobe Flash Player, эксплуатируемой хакерами в реальных атаках. Проблема (CVE-2018-4878) позволяет удаленному злоумышленнику выполнить произвольный код и затрагивает текущую версию продукта 28.0.0.137 и более ранние. По словам исследователей безопасности, уязвимость эксплуатируется по меньшей

мере с середины ноября 2017 года. Adobe подтвердила наличие проблемы и заявила о выходе патча в ближайшее время.

Исследователи из FireEye провели расследование, в ходе которого им удалось связать атаки с хакерской группировкой, которую они назвали TEMP.Reaper. Считается, что данная группировка действует из Северной Кореи, поскольку IP-адреса, с которых они связывались с C&C-серверами, принадлежат интернет-провайдеру Star JV – совместному предприятию Северной Кореи и Таиланда.

«Большая часть атак была сосредоточена на южнокорейской правительственной, военной и оборонной промышленной базе, однако в прошлом году они расширили географию своих атак и начали атаковать цели в других странах. Они проявили интерес к вопросам, имеющим большое значение для Корейской Народно-Демократической Республики (КНДР), таким как попытки объединения Кореи и прием северокорейских перебежчиков», – отметили исследователи.

Как выяснили эксперты, хакеры эксплуатировали уязвимость в Flash Player с помощью вредоносных документов Microsoft Office, содержащих специально сформированный SWF-файл. В случае успешной эксплуатации уязвимое устройство заражается вредоносным ПО DOGCALL (по класификации FireEye).

Специалисты Cisco Talos также сообщили об атаках с использованием данного вредоносного ПО, которое они назвали Rokrat . Исследователи связали атаки с той же хакерской группировкой, которая фигурирует в отчетах Cisco Talos под названием Group 123. В прошлом месяце специалисты из Talos подробно описали несколько кампаний, проведенных данной группировкой против южнокорейских чиновников и правозащитных организаций.

(вгору)

Додаток 25

5.02.2018

Уязвимость в WordPress позволяет любому отключить атакуемые сайты

В WordPress обнаружена простая, но серьезная уязвимость на уровне приложения, позволяющая вызвать отказ в обслуживании и отключить множество сайтов. Как правило, для осуществления подобной DDoS-атаки на уровне сети нужны большие объемы трафика, однако недавно обнаруженная уязвимость позволяет добиться желаемого эффекта с помощью всего лишь одного компьютера (InternetUA).

Производитель отказывается выпускать исправление, поэтому уязвимость (CVE-2018-6389) присутствует практически во всех версиях WordPress, выпущенных за последние девять лет, в том числе в последнем стабильном релизе 4.9.2. Проблема была обнаружена израильским исследователем безопасности Бараком Тауили (Barak Tawily) и связана с тем, как встроенный в

систему скрипт load-scripts.php обрабатывает определяемые пользователем запросы.

С помощью файла load-scripts.php администраторы могут улучшать производительность сайтов и повышать скорость загрузки страниц путем объединения (на стороне сервера) нескольких JavaScript-файлов в один запрос. Однако для включения load-scripts.php на странице администратора (wp-login.php) авторизация не требуется, то есть, функция доступна каждому.

В зависимости от установленных плагинов и модулей файл load-scripts.php выборочно вызывает необходимые файлы JavaScript, передавая их имена в параметр «load» через запятую, например: https://your-wordpress-site.com/wp-admin/load-scripts.php?c=1&load=editor,common,user-profile,media-widgets,media-gallery.

При загрузке сайта load-scripts.php (упомянутый в начале страницы) пытается найти имя каждого файла JavaScript, указанного в URL-адресе, добавить их содержимое в один файл и отправить обратно браузеру пользователя.

По словам Тауили, злоумышленник может заставить load-scripts.php вызвать все возможные файлы JavaScript (то есть, 181 скрипт), передав их имена в URL-адресе. Таким образом атакующий сможет существенно замедлить работу сайта. Тем не менее, одного запроса недостаточно для того, чтобы полностью «положить» сайт. Поэтому Тауили использовал PoC-скрипт doser.py, отправляющий большое количество одновременных запросов на один и тот же URL-адрес, пытаясь использовать как можно больше ресурсов процессоров серверов и тем самым снизить их производительность.

(вгору)

Додаток 26

8.02.2018

Check Point Software представляет CloudGuard для всесторонней киберзащиты облака

Компания Check Point представила линейку решений CloudGuardtm для защиты организаций от кибератак «Пятого поколения» на облачные приложения и инфраструктуру (ITnews).

Check Point также представляет CloudGuard SaaS, который обеспечивает защиту предприятий от атак на SaaS-приложения (Software-as-a-service). CloudGuard – это часть инфраструктуры Check Point Infintiy, в основе которой лежат зарекомендовавшие себя на рынке и отмеченные наградами технологии, обеспечивающие продвинутую защиту «Пятого поколения» (Gen V) для облака.

Современные компании все активнее используют облачные решения. Они стремятся повысить адаптивность бизнеса и производительность за счет внедрения гибридных облачных инфраструктур типа Amazon Web Services, Microsft Azure, VMware NSX и перехода на облачные приложения – например, Microsoft Office365, Google G-Suite, Salesforce, Servicenow, Slack, Box, Dropbox,

Egnyte и т.д. В то же время по всему миру наблюдается увеличение числа многовекторных атак как на облачную инфраструктуру, так и на облачные приложения. В качестве примеров можно привести вредоносное ПО и кражу учетных записей – количество таких происшествий растет. По данным исследования Check Point, половина всех случаев незаконного использования корпоративных приложений SaaS – результат похищения учетных данных пользователей.

«Проблемы безопасности по-прежнему остаются основным барьером к повсеместному внедрению облака, — отмечает Гил Швед (Gil Shwed), главный исполнительный директор (CEO), Check Point Software Technologies. – Новая линейка решений CloudGuard обеспечивает надежную комплексную защиту облачных SaaS-приложений и облачной инфраструктуры».

CloudGuard SaaS – это первый в отрасли пакет технологий для безопасности, разработанный для усовершенствованной защиты и предотвращения угроз в отношении SaaS-приложений. CloudGuard SaaS также предотвращает кражу пользовательских учетных записей и взлом приложений SaaS с помощью технологии ID-Guard, которая скоро будет запатентована.

Ключевые преимущества решения:

Защита от угроз нулевого дня: Решение помогает обезопасить контент приложений SaaS от APT-атак и неизвестного вредоносного ПО «нулевого дня» с помощью технологий «песочницы», применяемых в режиме реального времени, а также технологий защиты от программ-вымогателей, ботов и постоянно обновляемой базы данных об угрозах в облаке.

Технология защиты идентификации пользователей ID-Guard (в процессе получения патента): Решение обнаруживает и блокирует злоумышленников, которые пытаются получить доступ к учетным записям SaaS, а также отключает незарегистрированных пользователей и небезопасные устройства.

Защита данных: Решение автоматически шифрует конфиденциальные данные, блокирует попытки несанкционированного обмена конфиденциальными файлами и помещает их в карантин.

«После миграции нашей организации в Office365 и OneDrive мы искали глобальное решение для их кибербезопасности и выбрали Check Point CloudGuard, – прокомментировал Амир Шай, сотрудник службы безопасности Neopharm Group. – Как только мы внедрили CloudGuard SaaS, решение заблокировало многочисленные атаки на наши приложения, включая захват учетных записей, фишинг и атаки вымогателей».

CloudGuard IaaS (прежнее название vSEC) теперь является частью линейки CloudGuard. CloudGuard IaaS предлагает продвинутую защиту и предотвращение угроз «Пятого поколения» от атак на инфраструктуру и рабочие нагрузки всех ведущих публичных и частных облачных платформ, в том числе: Amazon Web Services, Google Cloud Platform, Microsoft Azure, Cisco ACI, OpenStack, VMware NSX, VMware Cloud on AWS, VMware ESX, Alibaba Cloud, KVM, Hyper-V и пр.

«Вопросом безопасности внедрения облачных технологий обеспокоены многие компании, – отметил Дуг Кахил, руководитель группы и старший аналитик по кибербезопасности, Enterprise Strategy Group. – Компании, которые ищут решения по облачной безопасности, должны обратить внимание на линейку Check Point CloudGuard, которая не только обеспечивает продвинутый уровень защиты от киберугроз, но и поддерживает безопасность приложений, инфраструктуры и данных внутри облака».

Кибератаки «Пятого поколения» (Gen V) определяются как крупномасштабные и динамичные атаки на мобильные, облачные и локальные сети. Такие продвинутые атаки без труда преодолевают традиционные статичные решения защиты, которые сегодня применяются в большинстве организаций. Из-за того, что владельцами активов в облаке одновременно являются как поставщики облачных услуг, так и конечные пользователи, определить, кто несет ответственность за их безопасность, не так-то просто. Эта ситуация создает дополнительные трудности. CloudGuard – единственная в отрасли полная линейка решений для облачной безопасности. Их общей задачей является продвинутое предотвращение угроз и защита корпоративных облачных приложений, инфраструктуры и данных от кибератак «Пятого поколения».

(вгору)

Додаток 27

11.02.2018

Новый вирус похищает данные карт с помощью DNS-запросов

Исследователи кибербезопасности из фирмы Forcepoint обнаружили новое вредоносное ПО для PoS-терминалов, позволяющее похищать данные кредитных карт с помощью DNS-запросов (InternetUA).

Ранее специалисты FireEye сообщали о вредоносе Multigrain, использующем аналогичный метод хищения пользовательских данных. Как отметили исследователи из Forcepoint, если Multigrain использовался в реальных атаках, то данный вредонос, получивший название UDPoS, пока еще никак себя не проявил.

По словам экспертов Роберта Ньюмана (Robert Neumann) и Люка Сомервилла (Luke Somerville), UDPoS выглядит менее сложным по сравнению с другими образцами вредоносных программ для PoS-терминалов. Это может говорить о том, что разработчик данного ПО еще не до конца освоил технологию PoS-систем.

Как отметили специалисты, стиль написанного кода и функционал вредоносной программы вряд ли можно назвать выдающимися. В коде UDPoS обнаружены ошибки, кроме того, программа использует файлы данных, записанные на диск, вместо того, чтобы работать преимущественно в памяти. Тем не менее, используемый метод полностью выполняет свою задачу.

Эксперты называют недостаток опыта злоумышленников основной причиной отсутствия атак с применением UDPoS. В общей сложности было обнаружено две «приманки», содержавшие вредонос. В первом случае вредоносное ПО было скрыто в установщике LogMeIn, а во втором – внутри пакета, рекламирующего службы обновления Intel. Оба случая имели место в октябре 2017 года, и с тех пор UDPoS больше нигде появлялся.

Вредоносное ПО, скрывающее данные внутри DNS-запросов, встречается довольно редко. В основном это обусловлено сложностью его разработки. Однако, автор UDPoS обладает достаточными навыками и вполне способен в скором времени представить доработанную версию программы, заключили эксперты.

(вгору)

Додаток 28

13.02.2018

Михаил Сапитон

Facebook предлагает воспользоваться своим VPN-сервисом. Почему это плохая идея

Редакция AIN.UA рассказывает, почему лучше не пользоваться VPN-сервисом, который рекламирует (и принадлежит) Facebook (AIN.UA).

Что случилось?

iOS-пользователи Facebook (сначала в Америке, а потом и по всему миру) заметили новую вкладку в навигационном меню приложения – «Protect», пишет TechCrunch. Под значком щита скрывается ссылка на VPN-приложение в App Store. Соцсеть создала его на основе израильского сервиса Onavo Protect, поглощенного в 2013 году.

Программа «Onavo Protect – VPN Security», у которой около 33 млн пользователей на iOS и Android, предлагает безопасный браузинг и защиту подключения от стороннего вмешательства. Пользователю обещают надежную защиту персональных данных при логинах и оплатах на сторонних сайтах. Также Onavo предупреждает о посещении вредоносных или спамерских ресурсов.

Как это работает?

VPN – сокращение от Virtual Private Network, что переводится как частная виртуальная сеть. Это дополнительная «надстройка» над стандартным подключением к интернету, которая формирует защищенный «туннель» передачи данных. Пользователь, установивший на свое устройство VPN-клиент, обращается к удаленному серверу, а уже через него получает данные из всемирной сети. В ходе этого трансфера они надежно шифруются для всех третьих лиц: к примеру, ваш провайдер будет видеть лишь список запросов к VPN-серверу вместо полной истории браузинга.

VPN-клиенты очень популярны в странах с интернет-цензурой: они помогают обойти региональные блокировки, скрыть IP-адрес, а также

предохраняют от государственной слежки за трафиком. Иногда это просто удобно – долгое время пользователи Netflix использовали VPN-подключения для доступа к фильмам и сериалам, недоступным в отдельных странах.

Что не так?

VPN-сервис может защитить вас от слежки со стороны провайдера (или любого пользователя публичного Wi-Fi), но сам оказывается в таком же положении. Если компания начнет хранить логи пользовательской активности, то получает в свои руки лишь больше контроля. Проблема в том, что Onavo практикует именно такие методы. Пользователи не платят за VPN-подключение деньгами, а взамен сервис анализирует статистику их активности и сохраняет сведения. Такая слежка абсолютна легальна – Onavo упоминают про сбор информации в положениях пользовательского договора. Не стесняется упоминаний об этом и Facebook.

Как сообщают СМИ, до поглощения компании, Facebook ежегодно выплачивала Onavo около $100 000 за доступ к мобильной аналитике. Покупка, которую оценивают в $150 млн, вряд ли изменила ситуацию в лучшую сторону – теперь соцсеть может еще детальнее изучать поведение пользователей. Подключение к VPN-сети, предоставленной Onavo, регистрируется на серверах Facebook.

Зачем это Facebook?

Все просто – узнать о вас еще больше, а также сформировать дорожную карту развития проектов. Опубликованная летом прошлого года статья The Wall Street Journal упоминает несколько подобных случаев. Соцсеть заранее узнала о замедлении роста пользовательской базы Snapchat на фоне запуска Stories в Instagram, а также решилась на крупнейшую сделку в истории, покупку мессенджера WhatsApp за $22 млрд после информации от Onavo, согласно которой программа была установлена на 99 % Android-телефонов в Испании. Источники WSJ рассказали, что обнаружение популярности приложений с лайв-стримами подтолкнуло Facebook на запуск трансляций в собственных мобильных клиентах.

Что делать?

Парадоксально, но лучше проигнорировать предложение Facebook, ведь настоящей конфиденциальности Onavo Protect не предлагает. Можно воспользоваться другими VPN-сервисами. Хотя и тут стоит быть настороже – если сервис предлагается бесплатно, то почти наверняка хранит логи пользователей для последующей продажи.

Есть и другие проблемы. В 2017 году Государственное объединение научных и прикладных исследований Австралии провело детальный анализ 283 VPN-программ из Google Play и опубликовало неутешительные выводы. 18 % приложений вообще не шифровали трафик в «туннелях», еще 20 % пользовались устаревшими протоколами безопасности, что обесценивало использование VPN-подключения. Почти все рекламировались под эгидой улучшение приватности, но в то же время 75 % использовали программные

библиотеки для трекинга данных, а 82 % запрашивали у пользователей доступ к дополнительным сведениям на смартфоне вроде текстовой переписки.

Так что лучший вариант обеспечить себя надежной защитой – платить за VPN-сервис. В упомянутом выше исследовании, например, отметку за соблюдение всех стандартов приватности заслужил F-Secure Freedome VPN. Пользование им обойдется в $6/мес, зато ваши данные не станут продавать сторонним лицам, а встроенные инструменты также обеспечат защиту от рекламы. Кредит доверия получил и Private Internet Access – даже ФБР, которые хотели через суд получить персональные данные одного из пользователей, подтвердили отсутствие логов у VPN-сервиса.

(вгору)

Соціальні мережі

як чинник інформаційної безпеки

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

Упорядник **Терещенко** Ірина Юріївна

Редактор О. Федоренко

Свідоцтво про державну реєстрацію КВ № 5358 від 03.08.2001 р.

Видавець і виготовлювач
Національна бібліотека України
імені В. І. Вернадського
03039, м. Київ, Голосіївський просп., 3
Тел. (044) 524-25-48, (044) 525-61-03
E-mail: siaz2014@ukr.net
Сайт: http://nbuviap.gov.ua/
http://сіаз.укр/
Свідоцтво про внесення суб'єкта видавничої справи
до Державного реєстру видавців виготівників
і розповсюджувачів видавничої продукції
ДК № 1390 від 11.06.2003 р.