СОЦІАЛЬНІ МЕРЕЖІ ЯК ЧИННИК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Огляд інтернет-ресурсів
(1.10–16.10)

2018 № 17

Соціальні мережі
як чинник інформаційної безпеки

Інформаційно-аналітичний бюлетень
Додаток до журналу «Україна: події, факти, коментарі»
Огляд інтернет-ресурсів
(1.10–16.10)
№ 17

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

1.10.2018
Microsoft рассказала о дальнейших улучшениях Skype

Многие жалуются на качество работы Skype, а с приходом новых версий на настольные компьютеры и мобильные устройства шквал критики и негодования начал попросту зашкаливать. Microsoft попросту не смогла проигнорировать все это. Команда разработчиков Skype поделилась подробностями о дальнейших улучшениях сервиса.

Докладніше

***

1.10.2018
Facebook планирует знакомить и женить людей. Цукерберг задумал создать свой Tinder

Facebook тестирует свой новый продукт – сервис знакомств Facebook Dating. Пилотный запуск уже осуществляется в Колумбии. Когда сервис запустится в других странах, пока неизвестно.

Докладніше

***

2.10.2018
WhatsApp отключил шифрование переписки

Плюсов у сервиса WhatsApp крайне много, начиная от возможности бесплатно передавать какую-либо информацию и заканчивая надежной системой сквозного шифрования, обойти которую не могут даже сотрудники силовых ведомств. Тем не менее, компания Facebook купила WhatsApp в 2014 году за более чем $2 млрд долларов, сделав его своей собственностью.

Докладніше

***

3.10.2018
Instagram «впав»: що відбувається

По всьому світу користувачі Instagram скаржаться на масові збої в роботі соціальної мережі (Espreso.tv).

Згідно з даними порталу DownDetector, постраждали зокрема східне узбережжя США, країни Центральної і Східної Європи, а також Індонезія і Австралія.

Проблеми почались близько 10.00. Стрічка користувачів не оновлюється, а при спробі зайти на сайт з комп'ютера, він видає помилку «5xx Server Error».

В Україні головним епіцентром збоїв став Київ. При спробі відкрити соцмережу через додаток мобільного гаджета вантажаться лише іконки, а потім з'являється повідомлення про неможливість оновити стрічку.

Офіційних коментарів керівництво Instagram поки не надало: ані інформаційний центр, ані соцмережі компанії не містять інформації щодо проблем. Окрім цього, з 2 жовтня користувачі скаржаться і на роботу соцмережі Фейсбук.

Тим часом деякі користувачі фотосервісу тимчасово «переїхали» у Twitter, щоб ділитися мемами і жартами про долю Instagram.

***

8.10.2018

Дмитрий Демченко

Instagram запустил аналог QR-кодов для удобного поиска профилей

Instagram запустил аналог QR-кодов – они предназначены для удобного поиска профилей. О новой функции сервис рассказал в своем блоге (AIN.UA).

Чтобы создать собственный QR-код нужно перейти в профиль, нажать на кнопку с тремя горизонтальными полосками в правом верхнем углу и выбрать функцию «Instagram-визитка». Ее можно украшать с помощью селфи, стикеров и эмодзи.

Чтобы отсканировать чужой QR-код, нужно открыть камеру приложения и навести на визитку объектив. Это позволит быстро перейти к профилю человека. Функция доступна в актуальных версиях Instagram на iOS и Android.

***

9.10.2018

Украинские разработчики создали Telegram-бота, отслеживающего скидки на Booking

Двое украинцев – Николай Кравчук и Денис Лищенко – придумали простой способ отслеживания изменения цен на гостиничные номера. В этом должен помочь специальный Telegram-бот, которого и создали разработчики.

Бот следит за ценой на выбранные номера и присылает оповещения, как только она меняется. По статистике, предоставленной авторами проекта, использование Hotelhunt помогает сэкономить порядка 15 % от первоначальной стоимости. В некоторых случаях экономия достигает 60 % (IGate).

Для того, чтобы воспользоваться ботом, нужно запостить в чат прямую ссылку на понравившееся предложение с сайта Booking.com, после чего бот начнет уведомлять о всех ценовых изменениях в рамках выбранной с страницы. Hotelhunt можно давать неограниченное число ссылок для отслеживания.

По словам разработчиков, в будущем, помимо контроля цен, бот научится самостоятельно проверять наличие свободных мест, прогнозировать ценовые изменения, а также подбирать отели в соответствии с предпочтениями пользователей.

***

9.10.2018

Ирина Фоменко

Facebook будет транслировать ваше домашнее видео, даже если вы не станете сидеть на месте

Facebook Inc. объявил о выпуске новых устройств Portal для видеочата, вместе с камерами, отслеживающими движение. На демонстрации девайса в Сан-Франциско руководители объяснили, что благодаря камере слежения пользователи смогут перемещаться во время видеовстречи. Голосовые команды обрабатываются непосредственно на устройстве, а не в центре данных Facebook.

Докладніше

***

8.10.2018

Instagram планирует сливать Facebook данные о ваших перемещениях

Разработчики компании Facebook, которая владеет Instagram, планируют встроить в мобильный клиент сервиса для обмена фотографиями программный передатчик, который будет делиться с социальной сетью данными о перемещениях пользователей.

Докладніше

***

11.10.2018

В Viber появилась новая полезная функция

Мессенджер Viber обновился до версии 9.7. Одной из новых функций в приложении стала возможность редактировать отправленные сообщения (InternetUA).

Чтобы изменить отправленное сообщение, достаточно тапнуть на него и выбрать в появившемся меню опцию «Редактировать». После сохранения сообщения на нем появится отметка, что оно было исправлено.

Напомним, что пользователи Viber могут также пересылать и удалять сообщения (в любое время после отправки), закреплять важные уведомления в диалоге, отмечать сообщение как непрочитанное для получателя и многое другое.

Функция редактирования доступна владельцам Andorid-устройств. Для пользователей iOS-гаджетов возможности редактирования станут доступны в ближайшее время.

***

12.10.2018
Facebook позволил постить 3D фото в ленте

Несмотря на название, фото не будут по-настоящему 3D. К примеру, фото нельзя будет покрутить, чтобы увидеть объект с разных сторон. Но на изображениях можно будет увидеть вещи с разных углов. Facebook отмечает, что эффект будет такой, будто вы смотрите на объект для фото, стоя за стеклом. Не все пользователи смогут сделать такие фото. Для этого нужен телефон с двойной камерой. Можно воспользоваться портретным режимом iPhone. Когда снимок сделан, Facebook использует AI для создания остальной части снимка, исходя из того, что захватили камеры. Социальная сеть выпустила руководство, как правильно делать 3D снимки, среди основных правил – не следует стоять слишком близко и фотографировать предмет с интересным цветом и текстурой. Просматривать 3D фото уже можно с 12 октября, а загружать через несколько недель (Marketing Media Review).

***

15.10.2018
Facebook позволит отменить сообщение у отправителя и получателя

Некоторое время назад разгорелся скандал из-за того, что Facebook удалила сообщения, которые раннее отправлялись Марком Цукербергом (iLenta).

Естественно, такое положение вещей разозлило обычных пользователей, так как каждый хотел бы иметь возможность удалять отправленные раннее сообщения. После волны жалоб и возмущений, Facebook пошла на уступки и пообещала внедрить функцию «unsend» (отмена отправленных сообщений) для всех, но не указала никаких сроков и подробностей относительно нововведения.

Представитель соцсети опубликовала в Twitter скриншоты «unsend» в приложении Messenger для Android. Как видно, пользователям станет доступна опция «Отменить отправленное сообщение», которая находится в перечне с «Удалить сообщение». Если воспользоваться новой опцией, то перед удалением пользователь увидит уведомление: «Сообщение будет удалено из чата и у вас», а это означает, что оно исчезнет, как у отправителя, так и у получателя. Кроме того, пользователи смогут установить точное время отмены сообщения.

Facebook пока проводит внутреннее тестирование «unsend», поэтому неизвестно, когда функция станет общедоступной.

СОЦІАЛЬНІ МЕРЕЖІ ЯК ВИЯВ ФОРМУВАННЯ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА

2.10.2018

#KyivNotKiev: МЗС запустило флешмоб, закликаючи іноземні ЗМІ правильно писати назву Києва

Відомство закликає небайдужих приєднатися.

Міністерство закордонних справ закликає іноземні ЗМІ відкоригувати правопис назви Києва.

Про це йдеться у повідомленні прес-служби відомства (ТСН).

Відомо, що іноземні медіа, зокрема одні з найпопулярніших, назву столиці України пишуть некоректно, а саме – Kiev. Це подібно до звучання слова в російській мові, проте для передачі назви так, як вона звучить українською, варто писати Kyiv.

Тож МЗС закликає користувачів Мережі публікувати звернення до іноземних ЗМІ, вказуючи з хештегом їхню назву, і додавати до них хештеги #KyivNotKiev і #CorrectUA. Також небайдужі можуть розмістити на сторінках у соціальних мережах відповідну обкладинку (кавер).

***

8.102.018

Активісти запустили флешмоб проти зняття санкції з РФ у Раді Європи. Часу лишилося до 9 жовтня

Українці запустили акцію з метою протистояти зняттю санкціям з Росії в Раді Європи 9 жовтня (Рубрика). Про це повідомляє спільнота Save Oleg Sentsov.

«Цього вівторка 9 жовтня Парламентська Асамблея Ради Європи буде голосувати за резолюцію, щоб зняти санкції з Росії. У документі немає про це ні слова, але всі розуміють, що запропоновані зміни до регламенту ПАРЄ зроблять просто неможливими їх продовження», – зазначає спільнота.

За їхніми словами, це особливо цинічно враховуючи, що жодна вимога Ради Європи до Путіна про припинення порушень в Криму і на Донбасі так і не була виконана.

Тому, активісти починають акцію #SaveCouncilEurope!, під час якої особисто кожен має звернутися до європейських політиків.

***

13.10.2018

Львів'ян запрошують долучитись до флешмобу #КапелюхаНаВуха

До Всесвітнього дня паліативної допомоги, який припадає на другу суботу жовтня, міжнародний фонд «Відродження» запускає флешмоб #КапелюхаНаВуха, йдеться на Facebook сторінці фонду (Твоє місто).

Жителів Львова та України закликають долучатись до флешмобу, щоб привернути увагу до невиліковно хворих дітей, які потребують паліативної допомоги.

«За останні роки ситуація з наданням паліативної допомоги українцям поліпшилася. Наприклад, було зареєстровано дитячу форму морфіну. Водночас низка проблем чекають рішень, як-от відсутність мережі закладів, де надають медичну й психосоціальну допомогу людям із невиліковним захворюванням», – заявляють у фонді.

Щоб взяти участь у флешмобі, опублікуйте своє фото у капелюсі (шапці, кепці, панамці тощо) з хештегами #КапелюхаНаВуха і #HatsOn4CPC.

***

15.10.2018

Рівняни продовжують флешмоб-подяку Вселенському Патріарху за підтримку Єдиної Церкви в Україні

Флешмоб-подяка Вселенському Патріарху Варфоломію за підтримку Єдиної Церкви в Україні, набирає популярності в Рівному (Крапка).

Так, діти недільної школи, викладачі, священики, семінаристи записують відео, яким висловлюють свою вдячність Константинополю за те, що підтримали ідею надання Томосу Українській Церкві.

Цього разу рівняни передали естафету флешмобу Львівській єпархії.

Друзі! Продовжуємо наш Флешмоб. Сьогодні до нього долучилися майбутні священнослужителі Єдиної Помісної Української Православної Церкви: викладачі та вихованці Рівненської Духовної Семінарії передали естафету студентам Львівської Православної Богословської Академії. Єдиним серцем і устами проспівали многоліття Патріархам Варфоломію та Філарету, всім архієреям та священнослужителям які відстояли істину, Президенту України Петру Порошенку та представникам влади, які приклали для цього багато зусиль, а також воїнам, які зупинили агресора і зараз бережуть наші кордони. #Флешмоб #За_Єдину_Помісну_Церкву #Майбутні_Священнослужителі_підтримують_Утворення_Єдиної_Церкви

Першими свою відео-подяку Вселенському Патріарху записали вихованці недільної школи Свято-Воскресенського собору.

***

15.10.2018

«Виталик, дай горяченькой воды»: в сети начался флешмоб «с тазиками и кастрюльками»

В Киеве вот уже полгода нет горячей воды. Это приносит массу дискомфорта, так как многим жителям столицы приходится греть воду в кастрюлях или устанавливать оборудование для нагрева воды. В сети из-за постоянных переносов даты включения горячей воды начался флешмоб с обращениями к городской власти. Начала флешмоб #нетгрячейводы #обращениекключко телеведущая Светлана Вольнова в Facebook (РБК-Україна).

***

15.10.2018

Хакеры забавно потроллили россиян в День защитника Украины: сеть насмешило фото

Хакеры из организации Ukrainian Cyber Alliance решили весело и с юмором отметить День защитника Украины, потроллив россиян в нескольких российских регионах. Об этом говорится в сообщении на странице в Facebook киберальянса (InternetUA).

Для этого на взломанных российских ресурсах – https://bit.ly/2QPU3oa, http://archive.is/JjLKz и других (всего сайтов оказалось около полутора сотен), пользователи которых выражали свою нелюбовь к Украине, было размещено «поздравление».

«Ukrainian Cyber Alliance поздравляет всех с праздником! С Днем защитника Украины! И тех, кто с оружием в руках защищает нашу землю, всех, кто приближает нашу будущую победу над кремлевским оккупационным режимом. Мы всегда будем помнить, как началась война, кто ее начал и почему. Крым, Донецкая и Луганская области всегда были украинскими. И мы уверены, что оккупированные Россией части Украины будут освобождены и там снова будет поднят наш флаг. Слава Україні!», – написали хакеры.

Идея пришлась по душе пользователям, которые оценили тонкий троллинг кибер-хакеров.

БІЗНЕС І СОЦІАЛЬНІ МЕРЕЖІ

1.10.2018

Под видео на YouTube можно будет покупать билеты в кино и бронировать поездки

Команда видеосервиса YouTube продолжает расширять рекламный функционал, предлагая все новые форматы взаимодействия пользователей с маркетинговыми продуктами. Очередные новшества были анонсированы компанией 1 октября. Отныне рекламодатели могут добавить к своим видеообъявлениям дополнительные формы: к примеру, под трейлером нового фильма можно будет сразу просмотреть расписание сеансов в кинотеатре и

приобрести на него билет, а под видео о достопримечательностях города зрители смогут забронировать место в близлижайшем к ним отеле (IGate).

Если смотреть видео с настольного компьютера, такой формат рекламы будет демонстрироваться прямо на самом ролике, а в мобильном приложении – под ним.

Стоит отметить, что помимо нового формата объявлений, YouTube внедрил и новые метрики. В частности были добавлены lifted users – статистика привлечённых пользователей, и cost-per-lifted-user – цена за каждого привлеченного пользователя.

***

2.10.2018

Google вдосконалює рекламу в YouTube, прив'язуючи її до пошукових запитів

Компанія Google розширює можливості реклами у YouTube, що базується на поведінці користувачів у мережі (Prportal).

Як пише The Verge, тепер реклама на відеоплатформі підбиратиметься більш точно, оскільки результати вибірки базуватимуться на пошукових запитах користувачів. Очевидно, що Google планує зробити більш тісними зв'язки самого пошуковика та YouTube. На форумі Advertising Week компанія також заявила, що YouTube є другим за популярністю пошуковиком у США (першим є сам Google).

У компанії кажуть, що після того, як користувачі отримали результати пошуку, вони часто переходять на відеоплатформу для того, щоб подивитися огляди продукту, трейлери до фільму, тощо.

Лише минулого року Google почала дозволяти рекламодавцям налаштовувати рекламу у YouTube, виходячи з пошукових звичок користувачів на самому сайті, а не просто показувати оголошення за типом вмісту, який переглядається. Схоже, що зараз компанія інтегрує свої пошукові напрацювання більш глибше у екосистему YouTube. Подібні новації від IT-гіганта можуть бути відповіддю на ріст впливу компаній Facebook та Amazon.

Раніше Google представила нову версію веб-браузера Chrome, який автоматично реєструє юзерів у самому браузері після входу в акаунти на Gmail чи YouTube. Такі зміни дозволять Google легше слідкувати за поведінкою користувачів та більш ефективно налаштовувати рекламу.

***

6.10.2018

Независимость Instagram закончилась: чем недоволен Цукерберг

Компания Facebook, владеющая Instagram, назначила нового руководителя фотоплатформы. Им стал 35-летний Адам Моссери, работающий на Марка Цукерберга в течение десяти последних лет.

Докладніше

***

8.10.2018
ПУМБ запустил первый в Украине банкинг в мессенджерах

Первый Украинский Международный Банк (ПУМБ) впервые в Украине представил полноценный банкинг в мессенджерах. В октябре 2018 года ПУМБ запустил банковский сервис в мессенджере Telegram.

Докладніше

СОЦІАЛЬНІ МЕРЕЖІ І ПРОБЛЕМИ СУСПІЛЬНОЇ БЕЗПЕКИ

Інформаційно-психологічний вплив мережевого спілкування на особистість

3.10.2018
Facebook анонсировал новые инструменты борьбы с буллингом

Теперь за жертву смогут вступиться друзья, а общественным деятелям обеспечат более комфортное пребывание в соцсети (Телекритика).

Согласно нововведениям, пользователи смогут удалять сразу несколько комментариев к своим публикациям. В Facebook также появятся новые способы поиска и блокировки оскорбительных комментариев по отдельным словам.

Также сообщается, что друзья пользователя смогут сообщать администраторам Facebook о запугивании или издевательствах над потерпевшим. Компания заявляет, что такой вариант подачи жалоб необходим, ведь некоторым жертвам буллинга некомфортно самим сообщать о жестоком обращении с ними.

«Каждый заслуживает ощущения безопасности в Facebook, и важно, чтобы мы помогали людям, которые сталкиваются с хулиганами и притязаниями в интернете. Мы знаем, что наша работа никогда не прекращается, когда речь идет о безопасности людей, и мы будем продолжать слушать отзывы о том, как нам создавать лучшие инструменты и совершенствовать нашу политику», – комментирует руководитель отдела глобальной безопасности компании Facebook.

Также компания пообещала эффективнее защищать общественных деятелей от буллинга и преследований.

***

4.10.2018

Ирина Фоменко

Игровые приложения для смартфонов превращают пользователей в наркоманов

В Google обнаружили, что смартфоны, работающие, как «карманные игровые автоматы», превращают своих владельцев в наркоманов. Об этом сообщает The Telegraph.

Докладніше

***

4.10.2018

Ученые изучили статистику трагических смертей из-за селфи

Индийские ученые посчитали, что с 2011 по 2017 год 259 человек лишились жизни из-за селфи. Об этом 3 октября пишет Washington Post (InternetUA).

Согласно сообщению, ученые из Всеиндийского института медицинских наук в Нью-Дели изучили статистику количества смертельных случаев во время селфи с телефона и обнаружили, что 259 случаев закончились трагически. По данным исследования, больше всего трагических случаев зафиксировано в Индии, Пакистане, США и России.

В погоне за эффектным кадром люди погибали под колесами поезда, разбивались, упав с высоты, а также тонули. Отмечается, что большинство погибших – молодые люди в возрасте от 10 до 30 лет.

Ученые также считают, что реальное количество погибших на самом деле больше, поскольку о многих трагичных случаях просто нигде не сообщается.

***

10.10.2018

Instagram представил новые функции для борьбы с буллингом

Администрация соцсети Instagram ужесточила меры к оскорбительным и нежелательным фотографиям, а также к неприятным комментариям, которые оставляют пользователи. Об этом говорится в заявлении компании (ProPro).

«Сегодня мы представляем новейшие инструменты для помощи в борьбе с буллингом, в том числе новый способ распознавания буллинга на фотографиях и отправки жалоб», – подчеркнули представители соцсети.

Специалисты обучили искусственный интеллект распознавать фото, которые размещают с целью травли, и автоматически отправлять такие материалы для рассмотрения модераторами.

Кроме того, во время видеотрансляций пользователи смогут включить фильтр, который будет отсеивать оскорбительные комментарии.

Маніпулятивні технології

4.10.2018

Twitter ужесточает борьбу с нарушителями правил сервиса в преддверии промежуточных выборов в США

Сервис микроблогов Twitter анонсировал ряд изменений в правилах, которые должны сделать более эффективной борьбу с троллями и другими пользователями, которые пытаются распространять через Twitter политические фейки или иным образом вмешиваются в демократические процессы.

Докладніше

***

8.10.2018

В США полицейские борются с преступностью с помощью фейковых Facebook-аккаунтов

В США сотрудники полиции специально создают фейковые аккаунты в социальной сети Facebook, чтобы отслеживать протестные настроения в обществе, вычислять потенциальных преступников или определить их местоположение.

Докладніше

***

11.10.2018

Ирина Фоменко

Facebook и WhatsApp обливают избирателей волнами фейковых новостей

В преддверии выборов в Бразилии политические кампании могут быть скомпрометированы огромным количеством лжи, распространяемой через Facebook и WhatsApp. Об этом сообщает The Guardian.

Докладніше

***

12.10.2018

У Google утекла внутренняя презентация о цензуре и свободе слова

В открытый доступ утекла противоречивая внутренняя презентация Google, посвященная вопросам цензуры и свободы слова. Она показывает, насколько непростыми являются эти вопросы для компании, имеющей немалую власть над информацией в интернете.

Докладніше

Спецслужби і технології «соціального контролю»

2.10.2018
Ирина Фоменко
Европейское законодательство может уничтожить свободу Интернета

В начале следующего года высший суд Европейского союза, как ожидается, примет решение по одной из самых спорных тем относительно интернета: права на забвение. Право, закрепленное в законе о неприкосновенности частной жизни, позволяет европейцам требовать, чтобы информация о них была удалена из результатов онлайн-поиска, если она устарела, не имеет значения или «чрезмерна».

Докладніше

***

4.10.2018
Російські кібершпигуни намагалися викрасти матеріали слідства по MH17, – Нідерланди

Хакери військової розвідки РФ спробували втрутитися у розслідування справи збитого над Донбасом у 2014 році пасажирського рейсу MH17 (Espreso.tv).

Про це заявила міністр оборони Нідерландів Анк Бійлевельд, передає Associated Press.

«Ми усвідомлювали зацікавленість російських спецслужб щодо цього розслідування та вжили відповідних заходів. Ми дуже пильнуємо щодо цього», – зазначила Бійлевельд.

За даними Міноборони Нідерландів, російські кібершпигуни намагалися отримати доступ до документів слідства.

***

4.10.2018
Пенс призвал Google прекратить разработку поисковика для КНР

Вице-президент США Майк Пенс заявил, что компания Google должна прекратить разработку поискового приложения Dragonfly, которое ориентировано на китайский рынок. Об этом сообщает Reuters (InternetUA).

По его словам, данное приложение укрепит цензуру правительства Китая на территории страны.

Он также подчеркнул, что это поставит под угрозу «конфиденциальность китайских клиентов».

Google ведет разработку Dragonfly с 2017 года. В настоящее время китайские пользователи не могут получить доступ к обычному поисковику Google из-за правительственного проекта «Золотой щит».

***

12.10.2018

Facebook уперше заблокував російські акаунти за збір особистих даних

Соцмережа Facebook уперше заблокувала в Росії більше десятки акаунтів, які запідозрили у нелегальному зборі та аналізі даних користувачів. Про це написав The Bell з посиланням на офіційне повідомлення Facebook.

Докладніше

***

12.10.2018

Facebook удалила сотни подозрительных страниц перед выборами в США

Представители Facebook заявили, что из социальной сети удалены сотни аккаунтов, которые игнорировали правила против спама и осуществляли «скоординированные неаутентичные действия». Заявление опубликовано в официальном блоге компании (InternetUA).

В блоге говорится, что были удалены 559 страниц и 251 учетная запись, которые, считают в соцсети, распространяли спам и заведомо ложную информацию. В компании рассказали, что с их помощью в социальную сеть попадал «огромный объем информации», который связан с предстоящими промежуточными выборами в США.

Проблема захисту даних. DDOS та вірусні атаки

1.10.2018

Facebook можуть оштрафувати на $1,6 млрд через злам 50 млн акаунтів // Штраф, за новим законом ЄС про захист персональних даних, складаєме 4 % від річного прибутку компанії

Компанію Facebook можуть зобов'язати сплатити $1,6 млрд після виявлення серйозної вразливості в безпеці платформи, яка дала змогу хакерам отримати доступ до 50 млн акаунтів соціальної мережі. Про це повідомляє The Sun (mind).

Зазначається, що вищезазначена вразливість дозволила хакерам не лише увійти до 50 млн облікових записів користувачів, а й отримати доступ до будь-яких сервісів, пов'язаних Facebook, як наприклад Spotify, Tinder та Instagram.

Цей штраф загрожує компанії у відповідності до нового закону ЄС щодо захисту персональних даних GDPR. Максимальну сума штрафу, згідно із ним,

може складати 20 млн євро або 4 % від річного обороту компанію, в залежності від того, яка сума є більшою.

Видання повідомляє, що в 2017 році соціальна мережа отримала прибуток у розмірі $40,653 млрд, тому максимальний штраф складає $1,63 млрд.

Днями Facebook розкрив «проблему з безпекою», яка зачепила майже 50 млн акаунтів. Хакери, як виявилось, скористались вразливістю у коді, який дозволяв людям побачити свою сторінку так, як бачать її інші користувачі.

***

2.10.2018

Банки США пожаловались на участившиеся кибератаки

В США некоторые крупные банки проинформировали об увеличении количества кибератак, которые были совершены в отношении их компьютерных систем в последнее время. Об этом пишет The Wall Street Journal (InternetUA).

По словам источников издания, действия хакеров коснулись деятельности таких финансовых учреждений, как Bank of America, Wells Fargo, JPMorgan Chase и Citigroup. Согласно предварительной информации, кибератаки должны были выявить «слабые места в компьютерных сетях фирм».

Как уточняется доступ к таким данным может привести к дестабилизации рыночной ситуации. В связи с произошедшим власти посоветовали банкам позаботиться о мерах безопасности, которые помешают хакерам проникнуть в их компьютерные системы.

***

2.10.2018

Президент підписав Закон, спрямований на створення додаткового механізму для боротьби з піратством і порушенням прав суб'єктів авторського права

Президент Петро Порошенко підписав Закон України «Про внесення змін до статті 5 Закону України «Про розповсюдження примірників аудіовізуальних творів, фонограм, відеограм, комп'ютерних програм, баз даних» (Офіційне інтернет-представництво Президента України).

Метою Закону є удосконалення процесу маркування контрольними марками примірників аудіовізуальних творів, фонограм, відеограм, комп'ютерних програм, баз даних. Завдяки підвищенню прозорості процесу маркування правовласники зможуть ефективно контролювати процес видачі марок і вчасно протидіяти шахрайству і незаконному використанню цих захисних елементів.

Реалізація Закону сприятиме створенню додаткового механізму для боротьби з піратством і порушенням прав суб'єктів авторського права.

***

2.10.2018
Facebook взломан, Instagram уязвим: о чем умолчал Цукерберг

Из-за уязвимости в системе социальной сети Facebook пострадало по меньшей мере 50 млн пользователей – об этом заявила служба безопасности компании, обнаружившая хакерскую атаку. Тем временем, эксперты рекомендуют сменить пароль и в Instagram, так как фотоплатформа тоже могла стать целью киберпреступников.

Докладніше

***

2.10.2018
В Telegram найдена уязвимость
Юри Костубати

В Telegram была найдена уязвимость. Как выяснилось, во время звонков через десктопную версию мессенджера, были видны IP-адреса пользователей, который обычно зашифрованы.

Программное обеспечение Telegram для ПК пропускало и частные, и публичные IP-адреса. В мобильных версиях данная уязвимость не найдена. Также сообщается, что в Telegram уже исправили данную проблему. Обнаружил проблему с IP-адресами эксперт по кибербезопасности Дхирадж Мишра. Компания-разработчик выплатила ему премию в 2000 евро (IT новости).

***

2.10.2018
Владимир Кондрашов
У преступников три года был доступ к реестру пропусков в зону АТО

Группа злоумышленников с августа 2015-го года по средину марта 2018 года незаконно пользовалась идентификаторами, ключами, логинами и паролями Электронного реестра разрешений для перемещенных лиц в районе проведения АТО и беспрепятственно оформляла для граждан Украины, иностранцев и лиц без гражданства разрешения на пересечение линии разграничения с оккупированной территорией Донецкой и Луганской областей. Об этом стало известно из приговора Краматорского городского суда Донецкой области.

Докладніше

***

3.10.2018

Хакеры могут взломать любой голосовой помощник с помощью звуков, которые не слышны человеку

Хакеры могут взломать голосовые помощники с помощью неразличимых для слуха человека звуков. Такие звуки могут транслироваться по телевидению или радио и маскироваться под привычные – например, под пение птиц. Об этом говорится в исследовании Рурского университета, которое приводит Fast Company (InternetUA).

Уязвимость, обнаруженная учеными, относится к классу критических. Она лежит в основе технологий распознавания речи, которые встроены во все без исключения голосовые помощники.

Злоумышленники могут прятать такие звуки в музыку, скачиваемую или прослушиваемую на пиратских сайтах, в видеозаписи или в любой другой контент, в котором содержится аудиодорожка. С их помощью хакеры могут совершить покупки, заблокировать устройства или полностью отключить все компоненты умного дома, включая сигнализацию и камеры видеонаблюдения.

Исследователи отмечают, что на данный момент им не удалось обнаружить ни одного случая взлома с использованием этой уязвимости. Но для того, чтобы устранить ее, ученым придется заново написать все алгоритмы для распознавания речи, говорится в докладе.

***

3.10.2018

Владимир Кондрашов

Предприимчивый хакер организовал сервис по взлому страниц «ВКонтакте»

Предприимчивый хакер зарабатывал на том, что через собственный сайт предоставлял услуги взлома страниц в запрещенной ныне в Украине соцсети «ВКонтакте». Горе-бизнесмен поставил взлом «на конвейер» и в результате получил 3 года лишения свободы с испытательным сроком на один год.

Докладніше

***

3.10.2018

Владимир Кондрашов

Законопроект о псевдо борьбе со спамом отправят на доработку

Комитет Верховной Рады Украины по вопросам информатизации и связи рекомендовал отправить на доработку скандально известный законопроект №8186, известный как законопроект «О борьбе со спамом», авторства нардепов Березы, Усова и Емца.

Докладніше

***

3.10.2018

Мошенники нашли хитрый способ завалить жертв спамом

Хакеры массово принялись использовать функцию подписки на уведомления в браузере, чтобы заваливать жертв спамом. Об этом сообщает The Bleeping Computer (InternetUA).

Вредоносные сайты распространяются через всплывающие окна или поисковые системы. Когда пользователи попадают на такие страницы, их обязывают подписаться на уведомления, чтобы получить доступ к сервису или посмотреть заблокированное видео.

Если юзер выполнит требование, его либо автоматически перенаправляют на другую страницу, либо дают возможность посмотреть ролик. Однако вместе с этим жертва постоянно будет видеть назойливый спам прямо на рабочем столе компьютера. В частности, пользователям регулярно будут предлагать установить вредоносные расширения для браузера, посетить порносайты и мошеннические распродажи.

Проблема заключается в том, что многие пользователи не понимают, откуда им приходит спам. Чтобы избавиться от сообщений, достаточно удалить подписку на вредоносный сайт в настройках браузера.

***

3.10.2018

Ирина Фоменко

Нью-Йорк хочет создать киберармию

На сегодняшний день Нью-Йорк является глобальным центром финансов, недвижимости, юридических услуг, технологий и многих других отраслей. Значение технологий и данных возросло, поэтому особое внимание уделяется атакам, направленных на них. Согласно докладу McAfee и Центра стратегических и международных исследований, последствия от киберпреступности и кибервойн обходятся компаниям в сотни миллиардов долларов.

Докладніше

***

3.10.2018

Из каждых 6 домашних маршрутизаторов только один защищён от киберугроз

Из каждых 6 домашних маршрутизаторов только один защищён от киберугроз (Компьютерное Обозрение).

Исследование, проведённое некоммерческой потребительской организацией American Consumer Institute (ACI), показало, что на подавляющее

большинство домашних маршрутизаторов не устанавливаются нужные обновления защиты, из-за чего устройства, а также их пользователи и присоединённые к ним устройства IoT остаются уязвимыми для взлома.

Докладніше

***

3.10.2018

Мощный ботнет перехватывает трафик, предназначенный для бразильских банков

Киберпреступники модифицировали настройки DNS более 100 тыс. маршрутизаторов таким образом, чтобы они перенаправляли пользователей на фишинговые страницы. Порядка 88 % этих маршрутизаторов находятся в Бразилии, а перенаправление осуществляется только при попытке пользователя зайти на страницы электронного банкинга бразильских финансовых организаций (InternetUA).

Вредоносная кампания продолжается как минимум с середины августа, когда была замечена ИБ-экспертами из Radware. На прошлой неделе специалисты из Qihoo 360 представили свой подробный отчет о деятельности стоящей за кампанией группировки.

Согласно отчету, злоумышленники сканируют пространство бразильских IP-адресов в поисках маршрутизаторов со слабыми паролями или вообще без паролей и в настройках меняют легитимный DNS интернет-провайдера на свой собственный. Все проходящие через скомпрометированные маршрутизаторы DNS-запросы перенаправляются на DNS-серверы злоумышленников, которые отправляют некорректные данные для 52 сайтов.

В основном эти сайты представляют собой страницы бразильских банков и хостинговых сервисов. При попытке зайти на них, пользователи попадают на фишинговые страницы, предназначенные для похищения их учетных данных.

Атаки осуществляются с помощью трех модулей: Shell DNSChanger, Js DNSChanger и PyPhp DNSChanger. Третий модуль является самым мощным. Он развернут на более ста облачных серверах Google, а в его распоряжении имеется 69 скриптов для брутфорса паролей 47 моделей маршрутизаторов с различными прошивками.

***

3.10.2018

Соцсеть Facebook рассказала о последствиях атаки хакеров

Вице-президент по управлению продуктом в Facebook Гай Розен заявил, что взломавшие 50 млн аккаунтов хакеры не получили доступ к другим ресурсам, где применялись те же самые учетные данные. Об этом говорится в официальном заявлении компании (InternetUA).

По словам Розена, в Facebook провели анализ всех случаев входа, которые во время кибератаки осуществили сторонние организации.

«Расследование к настоящему моменту не обнаружило свидетельств того, что злоумышленники получили доступ к каким-либо приложениям, использующим логин Facebook», – подчеркивается в заявлении.

Розен добавил, что в настоящее время идет работа над созданием инструмента, который позволит предотвратить подобные ситуации в будущем.

***

3.10.2018
Ольга Карпенко
Взлом Facebook обнажил проблему всего интернета

Недавно стало известно, что из-за уязвимости могло пострадать около 50 млн аккаунтов в Facebook, а безопасность еще 40 млн – под вопросом. Журналисты Wired сообщили, что последствия у взлома могут быть куда хуже, чем доступ к данным аккаунтов. Чем грозит одна из крупнейших утечек данных в этом году?

Докладніше

***

4.10.2018
НАТО допомагає Україні створити центр реагування на кіберзагрози

Північноатлантичний альянс допомагає Україні у створенні центру реагування на кіберзагрози, аби убезпечити українську кібермережу (Espreso.tv)

Про це під час брифінгу заявив генеральний секретар НАТО Єнс Столтенберг, повідомляє прес-центр організації.

Він зазначив, що Альянс вже допомагає Україні в зміцненні її кіберзахисту, зокрема через свої трастові фонди з кібербезпеки.

«НАТО зараз допомагає Україні створити центр реагування на кіберзагрози, який стане одним із способів допомогти їм впоратися зі спробами втручання або зламу їхніх кібер-мережі», – наголосив Столтенберг.

Він також додав, що під час саміту Альянсу пообіцяв президенту Петру Порошенку, що союзні держави будуть продовжувати надавати підтримку Україні, в тому числі і через трастові фонди.

***

4.10.2018
У Нацполіції буде створено управління для допомоги правоохоронним органам у розкриті злочинів із кіберелементом

У Нацполіції буде створено управління для допомоги правоохоронним органам у розкриті злочинів із кіберелементом. Новий підрозділ увійде до складу Департаменту кіберполіції.

Докладніше

***

4.10.2018

Хакерська атака на Facebook: зламані акаунти почали продавати у «даркнеті»

Зламані облікові записи Facebook продаються на теренах «даркнету» після масштабної хакерської атаки, яка зачепила більше 50 мільйонів користувачів (Espreso.tv). Про це повідомляє The Independent.

Редакція видання побачила «десятки списків» на чорних ринках «даркнету»: розділ Інтернету, доступний тільки зі спеціалізованим програмним забезпеченням пропонує покупцям особисті дані користувачів Facebook всього за 3 долари.

Якщо вони експлуатуються злочинцями, експерти з безпеки попереджають, що дані можуть використовуватися для крадіжки особистих даних або шантажу користувачів Facebook з компрометуючою інформацією.

Зламані облікові записи продаються за ціною від 3 до 12 доларів США, хоча їх можна купити тільки з використанням напіванонімних цифрових валют, наприклад біткоїна.

Якщо продавати кожен аакаунт окремо за цими цінами, вартість вкрадених даних на чорному ринку загально складе від 150 до 600 млн доларів.

Експерти з безпеки повідомили The Independent, що цінність таких даних для кіберзлочинців означає продовження такої тенденції як прибуткового бізнесу.

«Особисті дані просто занадто цінні у “темній павутині”. Поки викрадені дані продовжують отримувати високі ціни і постачати злочинців засобами, необхідними для здійснення атак, організації повинні застосовувати всі заходи щоб виявляти це і захищати свої мережі, пристрої та користувачів», – сказав генеральний директор кібербезпеки SonicWall Білл Коннер, який консультував як уряд США, так і Великобританії з питань безпеки.

«Те, що злочинці можуть або мають намір робити з величезною кількістю інформації про громадян країни, слід сприймати дуже серйозно».

***

4.10.2018

На Facebook поскаржились за незаконний збір даних про дітей

Коаліція груп захисту дітей і споживачів звинуватила Facebook в незаконному зборі даних про дітей через новий додаток Messenger Kids (Espreso.tv). Про це повідомила американська The Hill.

За даними агенції, у скарзі йдеться про те, що механізм згоди додатка легко маніпулюється, що дозволяє дитині обійти його і створити обліковий запис без допомоги батьків. Так саме легко будь-кому з дорослих створювати дочірні акаунти-підробки.

«Наше власне тестування показує, що неважко створити підроблену обліковий запис, який може схвалити користувача Messenger Kids. Ми створили абсолютно новий обліковий запис Facebook для вигаданого 18-річного. Потім ми використовували цей обліковий запис для затвердження вигаданого користувача Messenger Kids. Весь процес зайняв п’ять хвилин», – йдеться в скарзі.

Крім того зазначається, що Messenger Kids порушує Закон про захист конфіденційності дітей в Інтернеті, оскільки він не гарантує, що дорослий, який дає дитині дозвіл на використання додатка, є фактичним опікуном користувача.

***

4.10.2018

Министр обороны Нидерландов сообщила об атаке российских хакеров

Министр обороны Нидерландов Анк Бейлевелд заявила, что власти страны предотвратили атаку российских хакеров. По ее словам, страна выслала четырех российских разведчиков. Об этом сообщает агентство Associated Press (InternetUA).

Выступая на пресс-конференции в Гааге, Бейлевелд призвала Россию прекратить «кибератаки с целью подрыва западных демократий». Согласно ее заявлению, четверо россиян прибыли в Нидерланды 10 апреля 2018 года и были пойманы со шпионским оборудованием в отеле неподалеку от штаб-квартиры Организации по запрещению химического оружия (ОХЗО).

По словам министра, в этот момент в лаборатории ОХЗО исследовали образцы яда, которым в марте этого года были отравлены в Солсбери Сергей Скрипаль и его дочь Юлия. Одновременно там находились образцы химического оружия, использованного в сирийской Думе.

Предполагаемых шпионов арестовали и депортировали из страны 13 апреля.

***

4.10.2018

Китайские шпионские чипы обнаружили в технике Apple и Amazon

ЦРУ США обнаружило в компьютерах и гаджетах Apple и Amazon шпионские чипы, которые могли быть внедрены в технику на производстве в Китае. Об этом сообщает Bloomberg (InternetUA).

Отмечается, что по различным оценкам, Китай поставляет около 90 % компьютеров и 75 % мобильных телефонов. По данным агентства, к внедрению чипов в технику может быть причастна компания Supermicro.

В Apple и Amazon опровергли эту информацию, заявив, что никогда не находили подозрительных чипов.

***

4.10.2018

В США за 8 лет хакеры украли данные о 176 миллионах пациентов. Они продаются дороже, чем информация о банковских картах

За восемь лет различные организации в США, которые отвечают за здравоохранение, сообщили о 2149 кражах данных, которые затронули более 176 миллионов пациентов. Судя по статистике, эти цифры растут каждый год, и инциденты, которые затрагивают конфиденциальность клиентов больниц, происходят все чаще (InternetUA).

Результаты, опубликованные в медицинском журнале JAMA, еще раз подтверждают аргумент о том, что здравоохранение особенно уязвимо для хакеров. Рост электронных медицинских карточек, по-видимому, ухудшил ситуацию, поставив под угрозу пациентов, поставщиков медицинских услуг, страховщиков и другие заинтересованные стороны.

По статистике, один взлом затронул от 500 до 79 миллионов пациентов. Отчеты показывают, что в дальнейшем они продаются в даркнете за 300-400 долларов. Это куда более дороже, чем украденная информация о кредитных картах, которая стоит около 2 долларов.

***

4.10.2018

Кибергруппа из КНДР пыталась украсть более $1 млрд из банков по всему миру

Киберпреступная группировка APT38, предположительно связанная с правительством Северной Кореи, причастна к серии масштабных «агрессивных» кибератак на банки и другие организации по всему миру, в ходе которых злоумышленники пытались вывести более чем $1,1 млрд, утверждается в докладе компании FireEye.

Докладніше

***

4.10.2018

Мошенники отмывают деньги с карт украинцев: как работает схема незаконного заработка

В интернете существует много способов заработка, и далеко не все из них законные. Так, украинцы в сети могут зарабатывать до $1,5 тыс. на переводах (нужно принять на свою карту крупную сумму, а потом обналичить их, перевести в биткоин либо пополнить другую карту с помощью терминала).

Докладніше

***

4.10.2018

Вредоносы продолжают использовать USB-устройства для заражения ПК

Эксперты «Лаборатории Касперского» обнаружили, что USB-устройства по-прежнему используются злоумышленниками для распространения вредоносного ПО. Список из десяти киберугроз для съёмных носителей, основанный на данных глобальной облачной сети Kaspersky Security Network (KSN), включает семейство троянцев Windows LNK, уязвимость CVE-2010-2568, которую применили при внедрении Stuxnet, и известного криптомайнера Trojan.Win64.Miner.all (Компьютерное Обозрение).

Согласно отчёту «Лаборатории Касперского», число жертв растёт с каждым годом, хотя диапазон и количество подобных атак относительно невелики. Несмотря на то, что USB-устройства заработали репутацию небезопасных носителей информации, они остаются популярным инструментом в бизнесе и, как следствие, становятся всё более привлекательными для киберпреступников.

Криптомайнер, детектируемый KSN как Trojan.Win32.Miner.ays и Trojan.Win64.Miner.all, известен с 2014 г. Он загружает приложение для майнинга на заражённое устройство, затем устанавливает и незаметно запускает его. Доля обнаружений 64-битной версии этого вредоноса увеличивается: в 2017 г. она выросла на 18 % по сравнению с 2016 г., а в 2018 г. – еще на 16 %.

Наиболее широко в коммерческих целях USB-устройства используются в странах развивающихся рынков. Поэтому самыми уязвимыми к заражению вредоносным ПО, распространяемым с помощью съёмных носителей, являются такие регионы, как Азия, Африка и Южная Америка. При этом отдельные случаи таких заражений фиксировались в Европе и Северной Америке.

***

4.10.2018

Google выпустила программу для обхода блокировок в интернете

С каждым днем контроль правительств различных стран мира за интернетом усиливается, в результате чего ежедневно сотни ресурсов блокируют за то, что они размещают противозаконную информацию, которой

могут быть какие-то «опасные материалы» или же пиратский контент (Украинский телекоммуникационный портал).

Компания Google недовольна таким положением дел, поэтому она выпустила программу для обхода блокировок в интернете, которая обеспечивает 100 % гарантию защиты от действий государственных регуляторов. Корпорация Google является частью холдинга Alphabet, который 4 октября 2018 года выпустил программу для обхода блокировок в интернете.

Речь идет о программном обеспечении под названием Intra. Оно может быть установлено на смартфоны, планшеты и прочие электронные устройства, функционирующие на базе операционной системы Android. В ближайшем будущем разработчики планируют разработать ПО для iOS, Linux, Mac, Windows и прочих платформ.

Особенность приложения Intra в том, что оно создает защищенное соединение между различными устройствами на базе Android и DNS-серверами, которые привязаны к доменным именам, по которым и осуществляется блокировка сайтов, например, Роскомнадзором или иными государственными регуляторами в других регионах мира. Все это приводит к тому, что интернет-провайдер не получает информации о том, какой сайт открывает пользователь, тем самым позволяя получить к нему доступ. Главный плюс такого ПО, в отличие от прокси и VPN, заключается в том, что скорость интернета никак не снижается, то есть все работает максимально быстро, словно никакой обход блокировки и не осуществляется. В настоящее время от приложения Intra от Jigsaw Operations LLC нет никакой защиты. Государственные регуляторы, интернет-провайдеры и сотовые операторы никак не могут помешать его работе, но в будущем, конечно, все может измениться. Сообщается, что данная программа является лишь экспериментальным проектом. Если она будет пользоваться среди пользователей популярностью и собирать хорошие отзывы, то разработчики создадут более продвинутые решения, предназначенные для обхода блокировок сайтов.

***

6.10.2018

Хакеры взломали латвийскую соцсеть и разместили там фотографию Путина

В Латвии в день парламентских выборов хакеры взломали социальную сеть Draugiem.lv, передает Delfi (InternetUA).

При заходе на сайте звучит гимн России, а также появлялись фотографии президента России Владимира Путина и российского флага.

Представитель Draugiem Group Янис Палкавниекс подтвердил, что на сайт Draugiem.lv совершена кибератака.

***

7.10.2018

Киберпреступники научились обходить ловушки в облачных сервисах

В облачных сервисах хранится много ценной информации, что делает их привлекательной мишенью для киберпреступников. Злоумышленники постоянно изобретают новые способы получения доступа к чужим учетным записям и похищения их содержимого (InternetUA).

В свою очередь, у специалистов в области безопасности облачных сервисов есть собственные методы усиления защиты учетных записей и противодействия кибератакам. На случай, если кому-то все-таки удастся прорвать защиту, безопасники оставляют специальные цифровые ловушки. Эти ловушки, так называемые ханитокены (honeytoken), срабатывают при проникновении постороннего и подают соответствующий сигнал.

В роли ханитокена зачастую выступают данные, оставленные ИБ-специалистами для привлечения киберпреступников. К примеру, это может быть отправленное самому себе электронное письмо с темой «Важные банковские данные» и ссылкой-ханитокеном. Если кто-то прошел по ней, значит, учетная запись была взломана. Ханитокены для облачных сервисов представляют собой учетные данные – лакомый кусочек для любого хакера.

Как сообщают эксперты Rhino Security Labs, киберпреступники научились обходить расставленные для них ловушки. Словно мышь, укравшая кусок сыра прямиком из мышеловки, они похищают данные в обход ханитокенов, используемых крупнейшим облачным провайдером Amazon Web Services (AWS).

Данная проблема имеет две составляющие. Первая – сервис CloudTrail, используемый AWS для управления токенами. CloudTrail не поддерживает целый пласт нишевых сервисов – на них не распространяются функции видимости и не создаются записи активности, а для киберпреступников отсутствие записей означает отсутствие следов.

Вторая составляющая проблемы – слишком информативные сообщения об ошибках. В частности, в них отображается Amazon Resource Name – название учетных данных, использовавшихся для отправки запроса. Amazon Resource Name также указывает, используется ли ханитокен. Атакующий может просто вызвать ошибку и увидеть, с каким пользователем имеет дело и есть ли ханитокены, а в CloudTrail не появится об этом ни единой записи.

***

7.10.2018

Мошенники от имени журналиста «Схем» массово рассылают подозрительные электронные письма

Неизвестные массово рассылают фишинговые электронные письма от имени Михаила Ткача, журналиста-расследователя программы «Схемы:

коррупция в деталях». Об этом сообщает РБК-Украина со ссылкой на «Радио Свобода» (InternetUA).

Отмечается, что за прошедшую неделю десятки людей сообщили о получении писем с поддельного электронного адреса tkach.mixailo@gmail.com. Среди людей, что получили письмо – рядовые граждане, народные депутаты, судьи, политики и чиновники, друзья и коллеги журналиста.

«Мошенники создали “цифрового двойника” Михаила Ткача: электронный адрес с его именем, фамилией и фото, а также использовали в подписи журналиста логотип редакции Радио Свобода. Сам текст письма имитирует запрос на комментарий, которые в такой форме никогда не рассылались ни от имени “Схем”, ни от имени авторов-расследователей программы», – сообщили в редакции «Схем».

Сообщается, что в письмах, которые мошенники рассылают по электронной почте-клона, предлагается перейти по ссылке на сторонний сайт, который требует от пользователя ввести его пароль от электронной почты.

Как рассказали в редакции «Схем», о фейковой рассылке они узнали от самих пользователей, которые начали массово сообщать Михаилу Ткачу о подозрительных письмах от его имени.

Подчеркивается, что редакция не видит очевидной связи между теми, кто пострадал от фишинговой атаки.

Кроме того, все пересылаемые пользователями фишинговые письма редакция «Схем» направила для анализа глобальной службы внутренней информационной безопасности Радио Свобода. Также независимое расследование в отношении организаторов и целей фишинговой атаки проводит украинская «Лаборатория цифровой безопасности».

***

8.10.2018
В популярной операционной системе найдена опасная уязвимость

Эксперт в области разработки приложений Томас Рид (Thomas Reed) обнаружил опасную уязвимость в системе macOS. Угрозу для компьютеров от Apple он описал в блоге Virus Bulletin.

Докладніше

***

8.10.2018
Владимир Кондрашов
В Минюсте используют софт для взлома Windows

На одном из сайтов Главного территориального управления Юстиции Министерства юстиции Украины в открытом доступе находились десятки файлов и программ, среди которых – весьма специфическое программное

обеспечение, предназначенное для взлома Windows и использования нелицензионных копий операционной системы и других продуктов Microsoft.

Докладніше

***

8.10.2018

В августе инфраструктура Trend Micro заблокировала более 4,3 млрд угроз

Trend Micro каждый месяц публикует новый отчет по ландшафту киберугроз, которые удалось обнаружить исследователям по всему миру. В августе инфраструктура Trend Micro Smart Protection Network заблокировала более 4,3 млрд угроз (на 12 % больше по сравнению с июлем) по всему миру (Компьютерное Обозрение).

Самым распространенным спам-вложением в Украине, согласно отчету, полученным за этот период, стали распространяющиеся по почте файлы типа .XLS, их число составило более 30 млн. На первом месте по этому показателю оказались США (более 800 млн), далее за ними идут Китай, Бразилия, Франция и Россия.

Общее количество почтовых угроз в Украине при этом достигло 29,75 млн. Касательно остальных вредоносов, то на территории Украины было за месяц зафиксировано 69 тыс. случаев обнаружения зловредного ПО (malware). Вредоносные URL-ссылки фиксировались компанией 136 тыс. раз за месяц.

***

9.10.2018

Максим Саваневський

Закриття соцмережі Google+ може бути відволікаючим маневром перед загрозою Cambridge Analytica – 2

Google закриває соціальну мережу Google+, яка лежала мертвим грузом вже багато років. Компанія у своєму офіційному релізі пояснила закриття низькою популярності Google+ серед користувачів – 90 % сеансів становлять менше п’яти секунд.

Докладніше

***

10.10.2018

Пентагон не смог отразить атаку условных хакеров

Во время проверки кибербезопасности Пентагона условным хакерам удалось взять под контроль системы вооружений. Об этом говорится в докладе

Главного контрольно-бюджетного управления при правительстве Соединенных Штатов (InternetUA).

Как отмечается, условным противникам удалось легко и незаметно получить контроль над системами ведомства. При этом не уточняется, какие именно уязвимости были обнаружены.

«…используя относительно простые инструменты и методы, испытатели смогли получить контроль над системами и действовать практически незаметно», – подчеркивается в докладе.

Согласно предоставленной информации, среди обнаруженных проблем указаны незашифрованные коммуникации и неправильное обращение с паролями.

***

11.10.2018

СБУ: Об’єкти українських держструктур знову атакували хакери

Служба безпеки України отримала чергові докази ведення агресивних дій російських спецслужб проти України в кіберпросторі з використанням підконтрольного хакерського угруповання відповідального за проведення протягом 2015-2017 років кібератак на об’єкти критичної інфраструктури України відомих як BlackEnergy та NotPetya (InternetUA).

Фахівці спецслужби зафіксували нову цілеспрямовану атаку на інформаційно-телекомунікаційні системи державних органів України. Хакери використали нові зразки шкідливого програмного забезпечення, функціональні можливості якого передбачають віддалене адміністрування процесів операційної системи та копіювання файлів, стеження за діями користувачів, перехоплення паролів.

За результатами розслідування проведеного фахівцями СБУ у взаємодії з відомою антивірусною компанією встановлено, що ці комп’ютерні віруси є оновленими версіями бекдору Industoyer. Вони мають низку схожих характерних ознак, зокрема використовують подібні фрагменти програмного коду, процедури розгортання, використання обчислювальних можливостей заражених систем тощо.

Крім того, зафіксовано використання окремих інструментів, що належать цьому хакерському угрупованню, які були виявлені під час розслідування попередніх кібератак.

Ситуаційним центром забезпечення кібербезпеки СБ України встановлені об’єкти вказаної кібератаки, надано допомогу в локалізації її наслідків та мінімізації кіберзагроз ІТ-інфраструктурам органів державної влади.

***

11.10.2018

Пользователей популярного мессенджера предупредили об опасности взлома

В популярном мессенджере WhatsApp обнаружилась критическая уязвимость, которой не преминули воспользоваться хакеры. В момент, когда пользователь отвечает на видеозвонок, приложение блокируется, а злоумышленники получают доступ к персональным данным (InternetUA).

Уязвимым для хакеров оказался как WhatsApp для Android-устройств, так и версия для iPhone. Проблемы в Android-версии были замечены 28 сентября, а уже через пять дней обнаружилось, что и владельцы iPhone попадают в зону риска. После вмешательства злоумышленников чат-мессенджер перестает работать и выдает ошибку о переполнении памяти.

Сообщившие о проблемах пользователи говорят, что руководители WhatsApp ничего не комментировали публично, но ошибку, похоже, вычислили и устранили. Активным пользователям WhatsApp рекомендуется обновить приложение, чтобы избежать рисков.

***

12.10.2018

Кибершпионы атакуют военные и правительственные организации по всему миру

Эксперты компании Symantec раскрыли подробности о деятельности киберпреступной группировки Gallmaker, атакующей правительственные и военные организации по всему миру с целью кибершпионажа. Примечательно, злоумышленники не используют вредоносное ПО для перехвата контроля над системами жертв – в атаках применяются легитимные инструменты, например, фреймворк Metasploit и оболочка PowerShell.

Докладніше

***

12.10.2018

Ольга Карпенко

Что такое баг-баунти платформы и как они помогают компаниям защищаться от хакеров

Что такое баунти-платформы, как они работают, и в чем смысл таких программ для бизнеса, в своей колонке для AIN.UA рассказывает Марк Савчук, директор по коммуникациям в Hacken.

Докладніше

***

12.10.2018

Британія розкрила участь ГРУ РФ в кібератаці на київське метро і одеський аеропорт

Лондон надав Києву інформацію про участь ГРУ РФ в кібератаці на Київський метрополітен і одеський аеропорт у жовтні 2017 року (InternetUA).

Про це заявив міністр інфраструктури України Володимир Омелян, пише прес-служба відомства.

«Надана Національним центром кібербезпеки Великої Британії інформація свідчить про участь фахівців ГРУ Російської Федерації в атаці на підприємства в жовтні 2017 року. Немає гарантії, що спроби виведення з ладу критичних підприємств галузі не повторяться», – йдеться у повідомленні.

Міжнародний аеропорт «Одеса» та Київський метрополітен вже впроваджують низку проектів «цифрової трансформації», запевняють у Мінінфраструктури.

***

15.10.2018

Google Play нужно срочно удалить с Android

Приложение Google Play следует срочно удалить со смартфона, об этом пишут эксперты в области кибербезопасности из компании Cisco. Они обнаружили совершенно новый троян для Android, который уже начал распространяться по всему миру.

Докладніше

***

15.10.2018

Взлом Facebook: В Южной Корее начнут расследование кражи данных граждан страны

Комиссия по коммуникациям Южной Кореи сообщила об утечке данных 34 891 южнокорейских пользователей Facebook (InternetUA).

По информации агентства «Рёнхап», в результате взлома были украдены персональные данные, включая имена, номера телефонов, почтовые адреса 15 623 владельцев аккаунтов Facebook, в остальных более 18 тыс. случаях – похищены были сведения о регионах проживания владельцев аккаунтов, их семейном положении и религии.

Южнокорейская комиссия по коммуникациям в скором времени намерена начать расследование кражи данных граждан страны. Ее интересуют, в частности, возможные нарушения со стороны Facebook процедур безопасности. В комиссии не исключили, что количество выявленных утечек может возрасти в ходе расследования.

Ранее Facebook рассказала, что хакеры получили доступ к личным данным 29 млн пользователей во время взлома, о котором стало известно в конце прошлого месяца.

***

15.10.2018

ИИ-антивирус защищает личные данные подобно иммунной системе организма

Darktrace – ведущий британский стартап в области кибербезопасности. Там обещают наглядную визуализацию скрытых угроз и постоянное самообучение системы на основе ИИ.

Докладніше

***

16.10.2018

Взлом аккаунта в Facebook: появился способ узнать о хакерской атаке

Издание TechCrunch составило инструкцию, по которой можно проверить, не подвергся ли твой аккаунт в Facebook недавним хакерским атакам (Politeka).

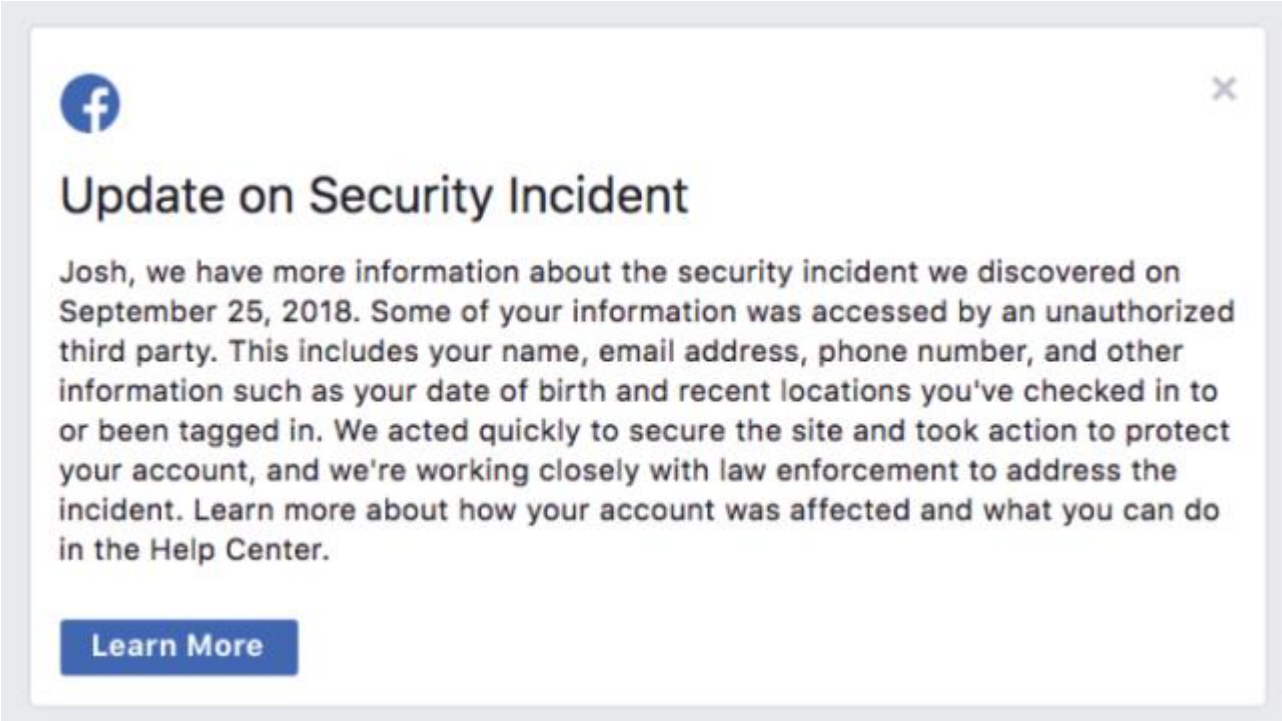
Представители соцсети сообщают, что пострадавших от хакерских атак можно разделить на группы по информации, которую они потеряли. Половина взломанных аккаунтов лишилась номера телефона и электронной почты, у другой половины украли данные об устройствах, с которых используется соцсеть, личные данные с указанием пола, языка, статуса отношений, а также сведения об образовании, работе и дату рождения.

Вот как можно проверить, не взломали ли тебя на Facebook:

1. Зайди на свою страницу и перейди в службу поддержки соцсети по ссылке https://www.facebook.com/help/securitynotice?ref=sec

2. Найди в раздел «Is my Facebook account impacted by this security issue?»

3. Служба поддержки выдаст ответ «да» или «нет». Если аккаунт был взломан, над лентой новостей на главной странице появится вот такое сообщение:



Если твоя страница была взломана, не обязательно сразу менять пароль или данные кредитки, поскольку, по словам Facebook, хакеры не получили доступа к этой информации. Но в следующий раз издание советует подумать, стоит ли доверять соцсети личную информацию.

ДОДАТКИ

Додаток 1

1.10.2018
Microsoft рассказала о дальнейших улучшениях Skype

Многие жалуются на качество работы Skype, а с приходом новых версий на настольные компьютеры и мобильные устройства шквал критики и негодования начал попросту зашкаливать. Microsoft попросту не смогла проигнорировать все это. Наконец разработчики начали прислушиваться к мнению своей аудитории и постепенно улучшать сервис, исходя из отзывов и пожеланий пользователей. Команда разработчиков Skype поделилась подробностями о дальнейших улучшениях сервиса. На форумах Microsoft опубликовали список, который демонстрирует функции, над которым работают сейчас, и над которым будут работать дальше (InternetUA).

Основы

– В работе: улучшения производительности, руководство по клавиатурным шорткатам и демонстрация версии Skype на экране логина.

– Далее: еще больше улучшений производительности, изменяемый размер левой панели на десктопном клиенте, а также свайп на мобильных устройствах.

Звонки

– В работе: настройка воспроизведения звонка при входящем вызове на втором устройстве, дополнительные настройки веб-камеры, отдельный регулятор громкости Skype на Mac, настройки для уведомлений входящих звонков в режиме «Не беспокоить».

– Далее: индикация пользователя, разговаривающего в данный момент в больших групповых звонках, улучшенное переключение между камерами, а также выбор приложения или окна для скриншэринга.

Сообщения

– В работе: поиск внутри диалога, настройки размера шрифта на десктопном клиенте, возможность поделиться контактом Skype, глобальный поиск с отображением более 20 результатов, кастомизация работы кнопки Enter, опция «сохранить как» для MP3-файлов, скрытие чатов в списке и настройка для отключения предварительного просмотра ссылок.

– Далее: поиск в текущем диалоге с отображением более 30 результатов, Skype SMS Connect.

Контакты / люди

– В работе: настройка, позволяющая Skype-Skype звонки только от контактов, улучшенная система статусов, возможность добавить телефонный номер как контакт, глобальный поиск людей с отображением больше 20 результатов.

– Далее: возможность добавить номер телефона к существующим контактам, больше элементов управления статусом, настройка, позволяющая разрешить звонки на номер Skype только от контактов и синхронизация с адресной книгой на Mac.

Windows 10-версия приложения

– В работе: улучшенные механизмы копирования-вставки на номеронабирателе, иконка приложения в области уведомлений.

– Далее: поддержка Split View.

Кстати, о Windows 10-версии Skype: Microsoft начнет рассылать версию 14 (основанная на Skype 8) где-то в ноябре. Она получит часть функций Skype 8, а также улучшенную интеграцию с некоторыми системными функциями. Поддержка старых настольных версий закончится 1 ноября, а мобильных версий 15 ноября.

Приятно видеть, что разработчики открыто рассказывают пользователям о процессе разработки мессенджера и наконец хотя бы пытаются прислушиваться к мнению аудитории. Хотя репутация Skype очень сильно испорчена, все еще есть надежда, что Microsoft сможет хотя бы немного исправить работу своего мессенджера.

(вгору)

Додаток 2

1.10.2018

Facebook планирует знакомить и женить людей. Цукерберг задумал создать свой Tinder

Facebook тестирует свой новый продукт – сервис знакомств Facebook Dating. Пилотный запуск уже осуществляется в Колумбии. Когда сервис запустится в других странах, пока неизвестно (InternetUA).

В чем идея

Марк Цукерберг анонсировал запуск сервиса еще в мае на конференции F8 в американском городе Сан-Хосе. Он отметил, что отличительной чертой их сервиса будет ориентация на создание серьезных отношений: «Никаких мимолетных связей!» Сервис будет недоступен для людей, которые указали в анкете личный статус «в браке» или «в отношениях».

Почему Колумбия

Продуктовый менеджер сервиса Dating Натан Шарп отвечает на этот вопрос журналисту TechCrunch: «В Колумбии 30 миллионов месячных активных пользователей Facebook. Это также связано с тем, что для большей части Южной Америки онлайн-знакомства уже органично вписываются в культуру».

Как это работает

Сервис будет встроен в мобильное приложение Facebook, но профиль для знакомств не будет подвязан к стандартному персональному аккаунту.

От пользователей будут требовать создание новой учетной записи, для активации которой нужно будет ответить на 20 вопросов в духе «Как выглядит ваш идеальный день?», написать короткий рассказ о себе и приложить фотографии. Обязательным условием является указание реального возраста и геопозиции.

Для общения пользователей с потенциальными партнерами Facebook разрабатывает новый мессенджер. Руководство решило, что использование Messenger или What’s App в таких целях нецелесообразно.

Умные алгоритмы Facebook исключают из ленты рекомендованных для знакомства людей друзей и заблокированных пользователей. Чтобы связаться с понравившемся пользователем, взаимного одобрения, как, например, в Tinder, не требуется.

Написать можно любому человеку из результатов поиска, но не более чем сотне людей в день. При этом сервис будет искать потенциальных партнеров только в радиусе 100 км.

Сегодня компания рассматривает Facebook Dating как полностью бесплатный сервис.

Личные данные

После анонсирования плана запуска сервиса Марком Цукербергом на конференции F8 акции Match Group (Tinder) упали на 22 %, и глава компании Мэнди Гинзберг выступила с официальным заявлением для The Verge: «Мы удивлены временем анонсирования сервиса, учитывая количество конфиденциальных данных в этой сфере».

В своем заявлении она намекнула на то, что Facebook еще не успел отойти от самого стрессового в истории социальной сети скандала, связанного с использованием личных данных пользователей.

Но в компании уверяют, что доверие аудитории для них превыше всего, поэтому данные профилей сервиса Dating не планируют использовать даже в целях таргетированной рекламы.

(вгору)

Додаток 3

2.10.2018
WhatsApp отключил шифрование переписки

Вот уже как несколько лет мессенджер WhatsApp является самым популярным в мире сервисом для общения из всех, которые когда-либо существовали. По свежим официальным данным, его используют в настоящее время более чем 1,6 млрд человек, то есть крайне много людей, проживающих в различных регионах планеты (Украинский телекоммуникационный портал).

Плюсов у данного сервиса крайне много, начиная от возможности бесплатно передавать какую-либо информацию и заканчивая надежной системой сквозного шифрования, обойти которую не могут даже сотрудники силовых ведомств. Тем не менее, компания Facebook купила WhatsApp в 2014 году за более чем $2 млрд долларов, сделав его своей собственностью.

Теперь данный мессенджер развивает так, как она пожелает. В конце лета нынешнего года появилась информация о том, что власти США оказывают давление на самый популярный в мире сервис для общения, а связано оно с тем, что сотрудники силовых ведомств не могут читать переписку, в том числе по решению суда, так как она слишком надежно защищена.

В итоге, Facebook начали заставлять отключить шифрование, чего компания всеми доступными способами не хотела делать, но в конечном итоге все же пришлось. 1 октября 2018 года мессенджер WhatsApp отключил шифрование переписки у всех пользователей, по крайне мере на устройствах под управлением Android.

Теперь, при попытке сделать резервную копию данных, появляется информация о том, что она будет сохранена в Google Drive в незащищенном виде.

Нужно сразу же заметить, что сотрудники полиции ряда стран мира, включая США, имеют доступ ко всем данным в облачном хранилище Google Drive с момента его запуска.

Проще говоря, теперь они смогут без каких-либо сложностей получать файлы резервных копий интересующих их пользователей WhatsApp, а затем использовать в своих целях. Избежать слежки можно – нужно не делать резервные копии, а если таковые уже были переданы в G Drive, то они уже оказались в руках третьих лиц – это гарантированный факт.

К счастью, в настоящее время не защищены шифрованием лишь резервные копии с устройств на базе Android, тогда как таковые на гаджетах под управлением iOS перед отправкой в фирменной облачное хранилище iCloud Drive от Apple подвергаются защите от просмотра третьими лицами. Впрочем, конечно, вскоре защита пропадет и оттуда – к этому нужно быть морально готовым.

(вгору)

Додаток 4

9.10.2018

Ирина Фоменко

Facebook будет транслировать ваше домашнее видео, даже если вы не станете сидеть на месте

Facebook Inc. объявил о выпуске новых устройств Portal для видеочата, вместе с камерами, отслеживающими движение. Об этом сообщает Bloomberg. На демонстрации девайса в Сан-Франциско руководители объяснили, что благодаря камере слежения пользователи смогут перемещаться во время видеовстречи. Голосовые команды обрабатываются непосредственно на устройстве, а не в центре данных Facebook (InternetUA).

«Конфиденциальность очень, очень, очень важна. Мы сознательно отказались от возможности записывать разговор. Если пользователи не доверяют “выключенному” переключателю для камеры, есть небольшая пластиковая крышка, которой они могут прикрыть объектив», – заявил вице-президент Portal Рафа Камарго.

Facebook – компания-разработчик программного обеспечения, выпускающая продукты, корректируя их в зависимости от уровня шума. Portal является своего рода вызовом для Facebook, поскольку такое аппаратное обеспечение сложно настроить. В компании должны были предотвратить возможные проблемы в процессе создания через тестирование продукта пользователями. Facebook также уделил особое внимание конфиденциальности, так как устройства будут находиться в личных помещениях, например, в жилых комнатах и кухнях.

Facebook работал над устройствами, первыми из группы Building 8, менее двух лет. Изначально компания планировала представить их в мае, но отложила презентацию из-за скандала с Cambridge Analytica.

Динамики с видеокамерами и сенсорными экранами называются Portal и Portal+. Устройства могут обрабатывать видеочаты, проигрывать музыку, включать фото и видео. Главные отличия – размер экрана и качество звука.

Portal, похожий на Echo Show от Amazon.com Inc., имеет 10-дюймовый горизонтальный дисплей. Portal+ – 15-дюймовый дисплей на подставке, его можно ставить как в вертикальное положение, так и в горизонтальное. Portal стоит 199 долларов, Portal+ – 349 долларов.

Устройствами в основном управляют голосом. Фраза «Hey Portal» включает видеочат. Тем не менее, Facebook использует цифрового помощника Amazon, поэтому пользователи должны сказать «Alexa» для более сложных задач, например, чтобы узнать прогноз погоды.

Основной функцией устройств Portal является видеоконференция, в которой одновременно могут участвовать до 6 человек, также Portal может поддерживать вызовы с Facebook Messenger.

Facebook пытается выделиться от конкурентов широкоугольным объективом камеры, который автоматически масштабируется и фокусируется на определенных людях или движениях. У модели Portal+ дисплей больше, чем в других устройствах, а видеочаты могут взаимодействовать с приложениями потоковой музыки, такими как Pandora и Spotify, поэтому несколько пользователей могут одновременно слушать одну и ту же песню.

Во время демонстрации сотрудник Facebook зачитал одну из анимированных книг для детей: когда по сюжету появился волк, на лицо работника программа наложила цифровые уши и мех. В компании заявили, люди могут использовать эту функцию для чтения своим детям во время поездок.

Устройства Portal будут поставляться с приложением Facebook Watch для просмотра видео, но на данный момент нет приложения для Instagram TV или других популярных видеоуслуг, таких как Netflix и YouTube. В ближайшее время Facebook планирует выпустить инструменты для сторонних разработчиков для создания приложений для Portal.

(вгору)

Додаток 5

8.10.2018

Instagram планирует сливать Facebook данные о ваших перемещениях

Разработчики компании Facebook, которая владеет Instagram, планируют встроить в мобильный клиент сервиса для обмена фотографиями программный передатчик, который будет делиться с социальной сетью данными о перемещениях пользователей. С таким заявлением выступила разработчик Джейн Манчун Вонг, обнаружившая отсылки к соответствующему нововведению в программном коде приложения Instagram. В случае активации данная функция сможет работать независимо от наличия на устройстве клиента Facebook, транслируя сведения по удаленному соединению (InternetUA).

Описываемое нововведение предусматривает отслеживание координат пользователей при помощи GPS с последующей передачей на сервера Facebook. Очевидно, что полученные данные будут использоваться социальной сетью для демонстрации пользователям более релевантных рекламных объявлений, повышая тем самым конверсию и, как следствие, собственный заработок как одной из наиболее эффективных платформ для продвижения товаров и услуг.

Почему Кригер и Систром ушли из Instagram

Перспектива появления в Instagram встроенного трекера была негативно встречена не только правозащитниками, являющимися противниками всякой слежки, но и создателями сервиса. По слухам, основатели Instagram Систром и Кригер до последнего боролись с Марком Цукербергом, стараясь убедить его сохранить фактическую независимость сервиса от Facebook, однако сдались и были вынуждены покинуть компанию.

На вопрос TechCrunch о сроках введения функции трекинга в эксплуатацию представители Facebook сообщили, что тестируют множество нововведений, однако далеко не все из них появляются в финальных версиях фирменных приложений. «Мы не вносили изменений в настройки геопозиционирования [Instagram], – гласит отчет пресс-службы Facebook. – Как вы, вероятно, знаете, мы регулярно тестируем разного рода нововведения, которые могут появляться или не появляться в наших сервисах. В настоящее время Instagram не сохраняет историю ваших перемещений».

(вгору)

Додаток 6

6.10.2018

Независимость Instagram закончилась: чем недоволен Цукерберг

Свято место недолго оставалось пустым – после ухода отцов-основателей Instagram Кевина Систрома и Майка Кригера руководителем фотоплатформы стал Адам Моссери. По слухам, он является приближенным Марка Цукерберга, а значит не будет иметь с ним идеологических разногласий, как его предшественник (InternetUA).

Бывший дизайнер и друг Цукерберга

Компания Facebook, владеющая Instagram, назначила нового руководителя фотоплатформы. Им стал 35-летний Адам Моссери, работающий на Марка Цукерберга в течение десяти последних лет.

«Мы счастливы объявить Адама Моссери, вице-президента по продуктам компании, новым главой Instagram. Мы передаем бразды правления лидеру с дизайнерским прошлым, который специализируется на прикладной работе и простоте, а также обладает глубоким пониманием важности всего сообщества. Это те ценности и принципы, которых мы придерживались с самого старта Instagram, и мы рады, что Адам станет их продолжателем», – заявили сооснователи Instagram Кевин Систром и Майк Кригер, покинувшие компанию на прошлой неделе.

Кто же такой Адам Моссери?

Он начал свою карьеру в Facebook в качестве дизайнера в 2008 году, впоследствии переключившись на продакт-менеджмент.

Моссери занимался мобильной версией Facebook, а также лентой новостей, которая является одним из важнейших элементов Facebook, а в 2016 году был завербован Систромом и Кригером, и перешел в Instagram. В том же

году он был назначен вице-президентом Facebook, став ценным кадром в управленческой команде Цукерберга и заодно приближенным лицом миллиардера.

В мае 2018 году Моссери получил должность руководителя отдела разработки Instagram, после чего появились слухи о скором увольнении Систрома и Кригера. Несмотря на то, что назначение Моссери повлекло за собой уход обоих основателей, он считается популярной фигурой среди сотрудников Instagram – хотя бы потому, что проводит много времени в офисе, в отличие от других вице-президентов и руководящего состава.

«Я польщен и счастлив, что у меня появилась возможность вести за собой команду Instagram. Я хочу поблагодарить их [Систрома и Кригера] за те ценности, которые они привнесли. Я сделаю все возможное, чтобы они, команда и Instagram-сообщество могли мной гордиться», – написал Адам Моссери в своем Instagram.

Сообщается, что акции Facebook упали менее чем на 1 % после назначения Моссери на должность.

Минимум автономии

Кевин Систром и Майк Кригер покинули свои посты в Instagram после десяти лет успешной работы в компании. Несмотря на то, что их прощальное сообщение было максимально нейтральным и дружелюбным, источники внутри Facebook намекают на большое количество противоречий между основателями и Марком Цукербергом, который всегда рассматривал платформу не как отдельную компанию, а как часть активов Facebook.

По слухам, именно отсутствие необходимой автономии и стало причиной ухода Систрома и Кригера. После того, как Цукерберг купил Instagam за $1 млрд, Систром и Кригер имели возможность не соглашаться с некоторыми инициативами руководства Facebook, если чувствовали, что они противоречат их видению развития Instagram.

Тем не менее, это не устраивало Марка Цукерберга, который делает большую ставку на фотосервис в планировании будущего всей компании из-за его популярности и успешности.

Теперь, после ухода отцов-основателей, Instagram рискует превратиться в одно из подразделений материнской компании и потерять остатки самостоятельности. Этому будет способствовать и тот факт, что Моссери является ставленником Цукерберга, а значит поддержит любые его решения.

Эксперты интернет-сообщества обратили внимание на другую деталь – Адам Моссери был назначен главой Instagram (Head of Instagram), в то время как Кевин Систром был генеральным директором компании (CEO), что тоже предрекает будущую потерю автономности для фотоплатформы.

Ранее Facebook покинули основатели мессенджера WhatsApp, который также был куплен Цукербергом. При этом причиной ухода Брайана Эктона и Яна Кума также стали противоречия между ними и создателем социальной сети. Похоже, что Марк Цукерберг ужесточает контроль над всеми

приложениями, принадлежащими Facebook, и хочет быть уверен, что его окружают надежные люди, которым он сможет доверять.

По всей видимости, Систром, Кригер, Эктон и Кум в их число так и не вошли.

(вгору)

Додаток 7

8.10.2018

ПУМБ запустил первый в Украине банкинг в мессенджерах

Первый Украинский Международный Банк (ПУМБ) впервые в Украине представил полноценный банкинг в мессенджерах (ITnews).

В октябре 2018 года ПУМБ запустил банковский сервис в мессенджере Telegram. Ранее в апреле 2018 года был запущен банковский сервис в мессенджере Viber. В ближайших планах ПУМБ также запуск банкинга в Facebook messenger.

Банкинг в мессенджерах позволяет клиенту самостоятельно с помощью одного лишь мессенджера оформить заявку на кредит или кредитную карту ПУМБ, и в дальнейшем осуществлять полный цикл обслуживания этого продукта. В формате 24/7 в течении нескольких секунд клиент может получить информацию о:

– сумме следующего платежа по кредиту;

– сумме последнего зачисленного платежа по кредиту;

– сумме просроченной задолженности по кредиту;

– сумме полного погашения задолженности по кредиту;

– минимальном платеже и сумме полного погашения по кредитной карте.

Также через банкинг в мессенджерах можно узнать актуальный курс валют и пополнить мобильный телефон, а также выбрать язык интерфейса. Кроме этого, с помощью банкинга в Viber клиенты ПУМБ могут оформить электронный полис страхования для автомобилей.

«Глобальная диджитализация – серьезный вызов для банковского сектора. Все большее количество сервисов, в том числе финансовых, становится доступно через мобильные приложения. Именно поэтому ПУМБ решил идти на территории, которые привычны и удобны для наших клиентов. Мы искали возможность, которая бы позволила в очень короткие сроки разворачивать банковский сервис на различных платформах в мессенджерах. Мы нашли такое технологическое решение совместно с нашими партнерами – компанией Middleware Inc. Благодаря этому мы запустили десятки банковских сервисов в Viber мессенджере, а добавление функционала в мессенджер Telegram заняло всего два дня», – комментирует Сергей Черненко, председатель правления ПУМБ.

Запуск в краткие сроки банковского сервиса ПУМБ в мессенджерах стал возможен благодаря созданию специальной бот-платформы, что является частью общей стратегии «цифровой трансформации», которую банк реализует

с 2016 года. В рамках этой стратегии ПУМБ совместно с партнером – компанией Middleware Inc – разработал собственное «цифровое ядро» на базе облачной технологии Corezoid Process Engine, что позволяет автоматизировать любой процесс без затрат на написание программного кода, ускорить цикл внедрения изменений в банке.

«Теперь не только IT-специалисты, но и представители бизнес-направлений банка могут быстро и самостоятельно настраивать, и изменять бизнес-процессы, экспериментировать с новыми идеями, постоянно улучшая качество обслуживания и повышая эффективность процессов. При этом IT-департамент банка, вместо хардкодинга и программирования бизнес-логики, может сосредоточиться на разработке необходимого количества API. Такое распределение ролей позволяет избежать очереди на ИТ-разработку и значительно ускоряет вывод на рынок новых продуктов и сервисов», – комментирует Александр Витязь, Founder&CEO Middleware Inc.

(вгору)

Додаток 8

4.10.2018

Ирина Фоменко

Игровые приложения для смартфонов превращают пользователей в наркоманов

В Google обнаружили, что смартфоны, работающие, как «карманные игровые автоматы», превращают своих владельцев в наркоманов. Об этом сообщает The Telegraph (InternetUA).

Исследования двух сотрудников Google выявили, что дизайн «триггера, действия, вознаграждения» популярных приложений вызывают у владельцев мобильных телефонов «фантомные» сигналы – им казалось, что они получали сообщение, хотя на самом деле этого не было.

Некоторые участники неоднократно обновляли приложение, надеясь, что новый контент появится или будет опубликован в социальных сетях исключительно для «создания новых триггеров» в форме ответов, лайков или репостов от их сверстников.

Технологический гигант провел исследование с 19 участниками в возрасте 18-65 лет в Цюрихе, Швейцарии и Калифорнии, США, чтобы выяснить, почему люди становятся настолько зависимыми от своих телефонов и как противодействовать этому.

Все говорили, что смартфон «критически затрудняет разъединение», причем один участник описывал свой телефон как «карманный игровой автомат». Исследование показало, что функции, обнаруженные в Instagram, Facebook и Twitter, скорее всего, вызывают зависимость у людей.

Хоть в исследовании и не названы отдельные приложения, авторы отметили «автоматические триггеры», которые обычно встречаются в

социальных сетях, например, «бесконечная прокрутка» – пользователи никогда не доходят до конца ленты новостей.

«В некоторых приложениях или веб-сайтах созданы автоматические триггеры (например, бесконечная прокрутка, рекомендуемый контент), которые поддерживают взаимодействие с пользователем», – говорится в исследовании. – «В обоих случаях участники использовали телефоны больше, чем хотели».

В прошлом году Facebook признал, что пассивная прокрутка делает пользователей более несчастными, в то время как комментарии под фотографиями или личные сообщения – счастливее.

Исследования, проведенные в Мичиганском университете, показали, что у учеников, случайно назначенных читать Facebook в течение 10 минут, настроение в конце дня было хуже, чем у тех, кто разговаривал с друзьями или публиковал информацию на веб-сайте.

Второе исследование, проведенное UC San Diego и Yale, показало, что люди, которые нажимали на примерно в четыре раза больше ссылок, или которым нравилось в два раза больше публикаций, сообщили о худшем психическом здоровье.

Ранее Марк Цукерберг объявил, что он меняет ленту новостей в Facebook для стимулирования людей к общению. Он удалил видеоролики из новостных организаций, у знаменитостей и друзей в хронике. Теперь социальная сеть показывает рекомендуемые сообщения в зависимости от местоположения пользователей и друзей, сообщений и просматриваемых страниц.

Instagram также имеет функцию рекомендации «Для вас», где пользователи могут бесконечно прокручивать учетные записи Instagram. У Snapchat есть аналогичная опция – Discover.

(вгору)

Додаток 9

4.10.2018

Twitter ужесточает борьбу с нарушителями правил сервиса в преддверии промежуточных выборов в США

Сервис микроблогов Twitter анонсировал ряд изменений в правилах, которые должны сделать более эффективной борьбу с троллями и другими пользователями, которые пытаются распространять через Twitter политические фейки или иным образом вмешиваются в демократические процессы. Эти обновления приурочены к намеченным на ноябрь промежуточным выборам в Конгресс США (InternetUA).

Согласно обновленным правилам, теперь фейковыми аккаунтами в Twitter могут быть признаны учетные записи со стоковыми или ворованными аватарками, ворованным или скопированным описанием профиля, а также вводящей в заблуждение информации о пользователе, включая ложно указанное местонахождение владельца аккаунта.

Кроме того, теперь в случае выявления подозрительного аккаунта, связанного с организацией, ранее уличенной в нарушении правил Twitter, администрация сервиса сможет принимать меры и в отношении других связанных с этой организацией учетных записей. Меры будут приниматься и в отношении профилей, копирующих ранее заблокированные аккаунты.

Наконец, правила сервиса теперь прямо запрещают распространять добытые хакерами сведения, содержащие приватную информацию, коммерческую тайну или способные иным образом навредить людям. Блокировка также будет грозить учетным записям, авторы которых берут на себя ответственность за хакерские атаки или публично заявляют о намерении их совершить. Комментарии или новостные материалы, посвященные хакерам, не будут подпадать под перечисленные запреты.

В компании также похвастались некоторыми успехами в деле борьбы с политической пропагандой. Так, в августе из Twitter было удалено около 50 аккаунтов, владельцы которых выдавали себя за членов Республиканской партии США. Помимо этого, в сообщении напомнили о нашумевшем удалении аккаунтов, связанных с Ираном.

Как отмечается в сообщении, усилия компании в деле борьбы со спамов в Twitter приносят плоды. Если в мае администрация получала в среднем около 17 тысяч жалоб на спам в день, то в сентябре этот показатель сократился до примерно 16 тысяч жалоб.

6 ноября 2018 года в США пройдут промежуточные выборы, на которых будет полностью переизбран состав Палаты представителей Конгресса США, а также будут избраны 25 из 100 американских сенаторов. Тогда же пройдут выборы губернаторов в 39 штатах.

США обвиняют Россию в умышленном вмешательстве в американские выборы 2016 года за счет распространения дезинформации и фейковых новостей в социальных сетях. Спецпрокурор Минюста США Роберт Мюллер ведет расследование о возможной причастности России к итогам выборов и возможном сговоре победившего на выборах президента Дональда Трампа с Москвой.

(вгору)

Додаток 10

8.10.2018

В США полицейские борются с преступностью с помощью фейковых Facebook-аккаунтов

В США сотрудники полиции специально создают фейковые аккаунты в социальной сети Facebook, чтобы отслеживать протестные настроения в обществе, вычислять потенциальных преступников или определить их местоположение (InternetUA).

Об этом сообщает NBC News – новостное подразделение американской телевизионной сети NBC.

Тем самым полицейские нарушают правила соцсети, но это правоохранителей не останавливает. Как отмечает NBC, в Facebook начало появляться множество поддельных аккаунтов, тайно создаваемых сотрудниками американских правоохранительных органов.

Например, летом 2015 года, когда Мемфис взорвался протестами в связи с убийством полицейским 19-летнего парня, в Facebook появился пользователь по имени Боб Смит. В качестве фото профиля в его аккаунте была маска Гая Фокса (символ антиправительственного инакомыслия). Боб Смит делал вид, что поддерживает протестующих, и они дали ему доступ к своему онлайн-сообществу. В течение последующих трех лет Смит наблюдал за частными дискуссиями недовольных: об организации маршей, митингов и демонстраций. В публичных и частных дискуссиях Facebook он называл себя левым демократом и «сторонником протеста».

На самом же деле под именем Боб Смит скрывался сотрудник управлении национальной безопасности полиции Мемфиса, чья работа заключалась в том, чтобы следить за местными активистами и инакомыслящими.

Как отмечает NBC, данный случай является очень показательным и демонстрирует то, как американские правоохранительные органы работают в Интернете, пользуясь слабым контролем в социальных сетях, и вмешиваются в частную жизнь граждан.

Некоторые из сотрудников полиции в США имеют несколько фейковых аккаунтов одновременно. Администрация Facebook пытается бороться с этим явлением, но пока не слишком успешно. Так, согласно статистике Фонда электронных рубежей (EFF) – организации по защите прав человека в Сети, таких фейковых аккаунтов становится пока только больше.

Правоохранители не под своими именами ведут переписку с пользователями, несмотря на правила Facebook, согласно которым использование поддельных профилей является нарушением условий обслуживания.

По факту, фейковые аккаунты не противоречат закону. При этом информация, собранная полицией через соцсеть, может использоваться в качестве доказательств в уголовных и гражданских делах.

Представители Facebook уже отправили первое предупреждение полицейским в департамент Мемфиса. Кроме того, были обновлены правила соцсети специально для подобных случаев (введен запрет использовать поддельные аккаунты любым пользователям).

Стоит отметить, что EFF давно критикует политику Facebook, согласно которой от пользователей требуется использовать их настоящие имена. По мнению представителей Фонда электронных рубежей, возможность анонимно высказывать мнения в Сети является правом каждого человека. В Facebook, в свою очередь, настаивают, что эта политика необходима «для создания безопасной среды, где люди могут доверять друг другу».

(вгору)

Додаток 11

11.10.2018
Ирина Фоменко
Facebook и WhatsApp обливают избирателей волнами фейковых новостей

В преддверии выборов в Бразилии политические кампании могут быть скомпрометированы огромным количеством лжи, распространяемой через Facebook и WhatsApp. Об этом сообщает The Guardian (InternetUA).

Восьмого октября избирательный суд Бразилии приказал Facebook удалить ссылки на 33 новостных материала, направленных против политика коммунистической партии Мануэлы Д'Авила.

Хоть в партии и были рады этому решению, другие эксперты считают, что оно ничего не означает. «Это капля в океане, и не имеет никакого отношения ко лжи и атакам на выборах. На данный момент очень мало правдивой информации», – заявил профессор государственной политики в Университете Сан-Паулу Пабло Ортелладо.

В постановлении избирательного суда судья Сержио Банхос дал Facebook 24 часа для предоставления IP-адресов компьютеров, используемых для регистрации учетных записей, которые размещали фейковые новости, и личных данных администраторов страниц. В Facebook заявили, что предоставят требуемую информацию, а ссылки удалили.

Согласно судебным документам, на страницах были отредактированы видеоролики с демонстрацией в Рио-де-Жанейро; изображения двух обнаженных людей с распятиями; Д'Авила, говорящего о кампании против гомофобии; и «образы, которые вызывают гиперсексуальность у детей».

Кампания Болоснару атаковала Хадад и Партию рабочих за программу учебных материалов, направленных на борьбу с гомофобией в школах 2011 года. Фейковые новости пестрили заголовками о том, что д'Авила хочет «сексуализировать» детей. «Это главная тема кампании Болоснару», – прокомментировал Ортелладо.

В некоторых поддельных материалах говорилось о повышении Болоснару налогов для бедных слоев населения (хотя на самом деле речь шла о понижении), в других – о нападении на Болоснару с ножом – якобы он сфабриковал эту историю, чтобы повысить рейтинг.

За последние десять недель Comprova – проект мониторинга, созданный 24 медиа-организациями, – расследовал 110 предполагаемых фейковых новостей на WhatsApp и Facebook. «Мы не можем остановить цунами лжи. Все больше поддельных материалов распространяется через WhatsApp, сеть, которую невозможно контролировать, поскольку большинство групп – частные», – заявил исполнительный директор Comprova Серхио Людтке.

(вгору)

Додаток 12

12.10.2018

У Google утекла внутренняя презентация о цензуре и свободе слова

В открытый доступ утекла противоречивая внутренняя презентация Google, посвященная вопросам цензуры и свободы слова. Она показывает, насколько непростыми являются эти вопросы для компании, имеющей немалую власть над информацией в интернете (InternetUA).

Презентация попала в руки Breibart News и была опубликована целиком. Она называется «Хороший цензор» и представляет собой находки и открытия, полученные из разнообразных материалов, в частности интервью с журналистами, академиками, критиками искусства и культуры. В первом слайде указана цель презентации – «убедить мир в том, что Google ограждает пользователей от вредного поведения, в то же время поддерживая свободу слова».

Просматривая презентацию, можно заглянуть в самое сердце морально-этической внутренней борьбы Google. Авторы презентации задаются вопросом, можно ли не допускать негативных аспектов свободы слова, таких как угрозы насилия, поддельные новости, боты, троллинг, пропаганда или влияние на политические выборы, при этом создавая платформу, где каждый может высказаться.

Авторы презентации не отрицают, что «цензура дает компаниям и правительствам инструменты для ограничения свободы людей», но также они признают, что такие крупные платформы как Youtube и Google отвечают за контент, который они распространяют, поскольку неоднократно случалось так, что ни правительства стран, ни технологические компании не могли справиться со злоумышленниками в интернете.

В качестве одного из примеров негативного контента упоминается даже Логан Пол и его печально известный ролик про лес самоубийств в Японии. Также в документе есть информация о том, что за последние два года утроилось количество правительственных запросов на блокирование определенного контента, в основном роликов на YouTube.

В заключении есть рассуждения о противоречивой позиции, в которой находятся такие компании как Google, Twitter и Facebook, им приходится проявлять твердость и держать тонкий баланс между цензурой и свободой речи – хотя вряд ли существует «правильная степень цензуры», которая устроит всех. «Интернет – говорится в презентации, – создавался на основании утопических принципов свободы слова».

И, хотя в документе речь идет о цензуре, в нем не упоминается Китай, его социальный авторитаризм и цензура, а также секретный проект Dragonfly, поисковик и новостной портал для Китая, над которым по слухам работают в Google.

В ответ на информацию об утечке представитель Google пояснил изданию The Verge, что в презентации не стоит усматривать официальную позицию компании, это скорее исследование мнения пользователей о таких

важных вопросах. Также он отметил, что Google выступает за свободное выражение идей, и даже вводя правила управления контентом, придерживается политического нейтралитета, ни в коем случае не давая предпочтение какой-то одной идеологии.

(вгору)

Додаток 13

2.10.2018
Ирина Фоменко
Европейское законодательство может уничтожить свободу Интернета

В начале следующего года высший суд Европейского союза, как ожидается, примет решение по одной из самых спорных тем относительно интернета: права на забвение, пишет Bloomberg (InternetUA).

Право, закрепленное в законе о неприкосновенности частной жизни, позволяет европейцам требовать, чтобы информация о них была удалена из результатов онлайн-поиска, если она устарела, не имеет значения или «чрезмерна». В данном случае речь идет о споре между Google и регуляторами Франции, которые в 2015 году приказали компании соблюдать эту норму на всех своих сайтах по всему миру – не только google.fr, но также google.com и так далее.

В свою очередь, в Google, естественно, не согласились. Как, впрочем, технологическая индустрия и общество в целом: право на забвение угрожает свободе слова, обременяет частные компании, вторгается в суверенитет и чревато рисками. Кроме того, оно не имеет ничего общего с достижением заявленных целей.

Цензурирование законной и фактической информации является сомнительным принципом и ошибочным методом защиты конфиденциальности. Это также и существенная дополнительная работа: с 2014 года Google пришлось обработать более 727000 запросов на делистинг, охватывающих около 2,8 миллиона веб-адресов. Каждый запрос должны анализировать люди, чтобы определить, разумно ли это или доступ к информации важен для общества – процесс, занимающий несколько дней.

В Google не склонны принимать такие решения. И, естественно, страны имеют разные предпочтения относительно «баланса» свободы слова и конфиденциальности. Всего три государства – Франция, Германия и США – генерируют 51 % от всех запросов на делистинг. В США соблюдение права может быть неконституционным: такая сложная задача является вопросом для законодательных органов, а не для частных компаний.

Множество авторитарных правительств хотели бы контролировать информацию за пределами границ своих государств. Будет ли Google уважать подобные требования Турции? Или соблюдать закон в Таиланде? Эксперты называют сложившуюся ситуацию «гонкой уступок» – страны с самыми

жесткими ограничениями будут эффективно определять политику во всем мире.

Аналитики убеждены, что такое законодательство не пойдет на пользу защите частной жизни. Регуляторы Франции заявили, что право на забвение бессмысленно, если информация по-прежнему появляется при поиске через VPN или зарубежные версии Google.

Новая норма полезна только в одном отношении: в усилении ухудшающейся глобальной напряженности. Все большее число юрисдикций пытается использовать технические компании для экспорта своих законов и ценностей. Например, новый режим конфиденциальности в Европе применяется ко всем компаниям, которые касаются данных европейских граждан. Аналогичным образом, суды в Австрии и Канаде пытаются заставить социальные медиапредприятия уничтожать неприемлемую информацию, несмотря на иностранную юридическую позицию.

Управление техническими платформами для обеспечения национальных приоритетов поставит под угрозу открытость Интернета. Компании должны уважать местные законы, где бы они ни действовали. Но требование их придерживаться одной юрисдикции во всем мире было бы сомнительно, ошибочно и имело бы серьезные негативные последствия.

(вгору)

Додаток 14

12.10.2018

Facebook уперше заблокував російські акаунти за збір особистих даних

Соцмережа Facebook уперше заблокувала в Росії більше десятки акаунтів, які запідозрили у нелегальному зборі та аналізі даних користувачів (Espreso.tv).

Про це написав The Bell з посиланням на офіційне повідомлення Facebook.

Зазначається, що акаунти були пов’язані із компанією Social Data Hub.Так, Facebook надіслав листа за адресою реєстрації компанії в Ірландію з вимогою негайно припинити збір і аналіз даних. Також Facebook вимагає надати соцмережі до 12 жовтня список всіх використаних відомостей і всіх клієнтів, які мали до них доступ, включно з державними структурами.

У листі зазначили, що усі дані, зібрані у Facebook, повинні бути знищені.

Facebook також заблокувала більше 66 аккаунтів, профілів, сторінок і додатків Social Data Hub, яка раніше порівнювала себе з Cambridge Analytica.

«Видалення сторінок викликано тим, що компанія займалася скрейпінгом (технологія аналізу і отримання даних користувачів – ред.), що є порушенням нашої користувальницької угоди», – йдеться у повідомленні.

Зазначається, що засновник компанії Social Data Hub Артур Хачуян також керує підприємством Fubutech. Він очолював відділ кібернетики рекламного

агентства «Апостол» Тіни Канделакі до 2014 року. У обох компаніях працює одна і та ж команда з 62 чоловік.

Обидві компанії займаються збором, обробкою і аналізом даних. Social Data Hub виконує комерційні замовлення, а Fubutech – державні.

У коментарі The Bell Хачуян зняв із себе відповідальність за те, як державні органи розпоряджаються отриманими даними.

А у коментарі РБК він заявив, що подасть позов до суду проти Facebook у разі, якщо соцмережа не відновить аккаунти.

(вгору)

Додаток 15

2.10.2018

Facebook взломан, Instagram уязвим: о чем умолчал Цукерберг

Из-за уязвимости в системе социальной сети Facebook пострадало по меньшей мере 50 млн пользователей – об этом заявила служба безопасности компании, обнаружившая хакерскую атаку. Тем временем, эксперты рекомендуют сменить пароль и в Instagram, так как фотоплатформа тоже могла стать целью киберпреступников (InternetUA).

Никто не в безопасности

В конце прошлой недели социальная сеть Facebook стала жертвой хакерской атаки – с помощью уязвимости в функции «Посмотреть как», позволяющей увидеть свою страницу так, как ее видят другие пользователи, злоумышленники смогли получить доступ к 50 млн аккаунтов.

Как сообщил вице-президент по продакт-менеджменту Facebook Гай Розен, компания оперативно устранила использованную уязвимость, а также проинформировала о случившемся правоохранительные органы.

Так как в результате атаки хакеры получили маркеры доступа к 50 млн профилей Facebook, служба безопасности социальной сети приняла решение сбросить их значения. Кроме того, такие же меры были приняты в отношении 40 млн других аккаунтов, которые могли быть затронуты в ходе кибервзлома.

Помимо прочего, функция «Посмотреть как» была временно отключена.

«Так как мы только начали расследование, нам еще предстоит определить, были ли эти аккаунты злонамеренно использованы и была ли утечка информации. Кроме того, мы не знаем, кто стоит за этими атаками, и где они базируются... В дополнение к этому, если мы найдем другие пострадавшие аккаунты, то мы немедленно сбросим их маркеры доступа», – заявил Гай Розен.

Как заметили некоторые ИБ-эксперты, в официальном заявлении компании речь идет только о пользователях Facebook. Тем не менее, 90 млн человек, чьи маркеры доступа предположительно попали в руки хакеров, рекомендуется проверить и аккаунты в Instagram. Дело в том, что в Instagram можно авторизоваться через Facebook, так как эта фотоплатформа тоже принадлежит Марку Цукербергу.

Если пользователь, чей аккаунт был скомпрометирован, залогинился в свой Instagram через Facebook, то в зоне риска оказываются оба его профиля.

По данным блога о кибербезопасности Krebs On Security, эту информацию подтвердил представитель Facebook, но в обновленный пресс-релиз ее так и не включили. «Цепная реакция» характерна не только для Instagram, но и для любых других приложений, использующий логин через социальную сеть Цукерберга, например, Uber или Tinder.

Розен подчеркнул, что на текущий момент нет достоверных данных о вероятных последствиях взлома, которые могут проявиться не сразу, а лишь через некоторое время. Кроме того, нет информации и о пострадавших пользователях других приложений, и такая неизвестность, по меньшей мере, пугает.

Чтобы узнать, пострадал ли ваш аккаунт от действий злоумышленников, специалисты рекомендуют зайти в Facebook и проверить, остались ли вы залогинены в системе. Если соцсеть просит заново ввести свои личные данные, то велика вероятность, что хакеры пытались получить доступ к профилю. В таком случае требуется незамедлительно сменить пароль.

Совпадение или хитрость

Так как Facebook сообщила о хакерской атаке только три дня спустя, ей может грозить крупный штраф в размере £1,25 млрд (около $1,62 млрд), вследствие нарушения Общего регламента по защите данных, вступившего в силу в Европе 25 мая 2018 года.

Кроме того, пользователи сообщают о том, что социальная сеть блокировала распространение сообщений о хакерской атаке в своей новостной ленте.

Как только публикация Гая Розена появилась в блоге Facebook, и СМИ подхватили эту историю, пользователи со всего мира стали делиться ссылками со своими друзьями.

Через какое-то время публикации со ссылками на порталы The Guardian и Associated Press, освещавших хакерскую атаку, прекратились. Как оказалось, Facebook запретила вставлять эти материалы из-за опасности «спама».

С одной стороны, этот инцидент наглядно демонстрирует хорошую работу спам-фильтра в социальной сети, но с другой – в данной ситуации он блокировал распространение подробностей о хакерской атаке от проверенных источников, среагировав лишь на массовость подобных публикаций. Учитывая, что в Facebook часто появляются одни и те же новости от одних и тех же информационных агентств, эта неожиданная блокировка вызывает некоторые вопросы. Есть вероятность, что Марк Цукерберг пытался таким образом приуменьшить масштаб утечки, но не стоит исключать и банальное совпадение, случившееся в неудачное для компании время.

(вгору)

Додаток 16

2.10.2018

Владимир Кондрашов
У преступников три года был доступ к реестру пропусков в зону АТО

Группа злоумышленников с августа 2015-го года по средину марта 2018 года незаконно пользовалась идентификаторами, ключами, логинами и паролями Электронного реестра разрешений для перемещенных лиц в районе проведения АТО и беспрепятственно оформляла для граждан Украины, иностранцев и лиц без гражданства разрешения на пересечение линии разграничения с оккупированной территорией Донецкой и Луганской областей. Об этом стало известно из приговора Краматорского городского суда Донецкой области, передает (InternetUA).

Согласно тексту приговора, уроженец Тореза Донецкой области вместе со своим знакомым в августе 2015 незаконно получили программное обеспечение, которое предоставляет доступ к Электронному реестру разрешений для перемещенных лиц в районе проведения АТО (https://urp.ssu.gov.ua). Завладев идентификаторами, ключами, логинами и паролями, которые предоставляют возможность работать с реестром, вносить соответствующие изменения, дополнения и тому подобное, злоумышленники организовали схему беспрепятственного оформления для всех желающих разрешений на пересечение линии разграничения с оккупированной территории Донецкой и Луганской областей.

Мошенники разместили в сети объявление о беспрепятственном срочном оформлении разрешений, указав свои номера телефонов.

– Лица (клиенты), которые в течение периода с августа 2015 по 16.03.2018 года обращаются по указанным объявлениям, получают инструкции о необходимости перечисления определенной суммы денежных средств (от 200 до 500 грн.) на открытые банковских счетов обвиняемого и соучастника преступления. После этого клиенты, перечислив условленную сумму на счета злоумышленников, пересылают им с помощью мессенджеров на вышеуказанные номера телефонов копии собственных паспортов и других идентификационных документов (или сообщают данные о них в телефонном режиме), – говорится о схеме в приговоре. – Далее подозреваемые через незаконно полученное программное обеспечение вносят сведения в Электронный реестр разрешений для перемещенных лиц в районе проведения АТО. В результате клиенты незаконно получают соответствующее электронное разрешение на пересечение линии разграничения в районе проведения АТО.

Сколько всего человек таким образом оформили себе разрешения, в приговоре не упоминается.

Уроженец Тореза пошел на сделку со следствием и полностью признал свою вину. Суд утвердил ранее оговоренное в результате сделки с прокурором наказание: три года лишения свободы с лишением права занимать должности, предусматривающие работу с электронным реестром разрешений для перемещенных лиц в районе проведения ООС сроком на 1 год. Этим же

приговором суд освободил обвиняемого от назначенного основного наказания с испытательным сроком на 1 (один) год.

(вгору)

Додаток 17

3.10.2018

Владимир Кондрашов

Предприимчивый хакер организовал сервис по взлому страниц «ВКонтакте»

Предприимчивый хакер зарабатывал на том, что через собственный сайт предоставлял услуги взлома страниц в запрещенной ныне в Украине соцсети «ВКонтакте». Горе-бизнесмен поставил взлом «на конвейер» и в результате получил 3 года лишения свободы с испытательным сроком на один год (InternetUA).

Об этом пишет InternetUA со ссылкой на приговор Яворивского районного суда Львовской области.

Как стало известно, безработный мужчина в марте 2017 года создал сайт xakercki-poslygu.hol.es, через который принимал заказы на взлом страниц. Суд признал «предпринимателя» виновным во взломе более чем шести десятков страниц «ВКонтакте». Кроме того, хакеру удалось взломать страницы пользователей Facebook и Instagram. Один из взломанных аккаунтов мужчина использовал для того, чтобы написать о своей же работе позитивный отзыв в своем же сообществе в одной из социальных сетей.

Кроме взлома страниц в соцсетях мужчина также распространил вредоносную программу «mt_stabile.apk» Android. С помощью этого же ПО ему удалось получить доступ к смартфону ещё одной жертвы.

Получал ли мужчина денежное вознаграждение за свою «работу» или занимался взломом страниц «для себя» – в решении суда не уточняется.

13 июня этого года в ходе досудебного расследования между прокурором и обвиняемым было заключено соглашение о признании виновности. Обвиняемый признал вину в совершенных преступлениях и раскаялся в содеянном. Суд же утвердил соглашение, признав мужчину виновным в совершении уголовных преступлений, предусмотренных ч.1 ст.361, ч.2 ст.361, ч.1 ст.361-1 УК Украины. Путем поглощения менее строгого наказания более строгим обвиняемый получил окончательное наказание по совокупности преступлений в виде лишения свободы на срок три года с испытательным сроком в один год.

Кроме того, хакер-предприниматель заплатит пять тысяч семьсот двадцать гривен за экспертизы, проведенные следствием.

(вгору)

Додаток 18

3.10.2018

Владимир Кондрашов
Законопроект о псевдо борьбе со спамом отправят на доработку

Комитет Верховной Рады Украины по вопросам информатизации и связи рекомендовал отправить на доработку скандально известный законопроект №8186, известный как законопроект «О борьбе со спамом», авторства нардепов Березы, Усова и Емца (InternetUA).

Проект закона о внесении изменений в некоторые законодательные акты Украины относительно противодействия спаму, согласно пояснительной записке, декларирует своей целью «внедрение механизма защиты абонента телекоммуникационных услуг от несанкционированных электронных, текстовых и/или мультимедийных сообщений, с последующим использованием их контактных данных и возможностью использования этой информации в мошеннических целях».

Однако, не смотря на декларируемую цель, документ оказался «сыроват», поэтому был отправлен на доработку – множественные замечания общественности, отрасли и регулятора документом не были учтены. Несмотря на то, что законопроект, как утверждали его авторы, был полностью переписан.

В частности, законопроект пытается регулировать то, что уже регулируется Правилами предоставления и получения телекоммуникационных услуг, утвержденными постановлением Кабинета Министров Украины в апреле 2012 года. При этом даже само определение «спама» не соответствует действующим Правилам. Фактически авторы законопроекта, вместо того, чтобы сосредоточиться на борьбе с новыми видами спама, предлагают регулировать уже регулируемое.

Претензии у специалистов и к целому ряду других новшеств законопроекта. В частности, законопроект, как неоднократно заявлялось, обяжет операторов нарушить тайну переписки и телефонных разговоров, и даже обязывает идти на преступление.

– Данный законопроект ни по логике своей, ни по содержанию не соответствует тем нормам, которые он декларирует, – отметил во время заседания Комитета ВР Вице-президент УСПП Иван Петухов. – В законопроекте есть норма о том, что оператор, провайдер телекоммуникаций должен убеспечить от спама прохождение информации по ряду протоколов. То есть, если любой человек с помощью любого устройства зашел на свой почтовый ящик, а оператор, провайдер телекоммуникаций начинает перлюстрировать этот ящик, – это уже преступление, предусмотренное статьей 360 Уголовного кодекса Украины.

Иван Петухов отметил: законопроект устарел на несколько десятков лет и, к тому же, содержит коррупционные нормы, позволяющие, при желании, «закрыть» любого оператора.

Не смотря на критику, и отрасль, и общественность, и народные избранники понимают: закон о противодействии спаму нужен. Но качественный закон.

– Практически все специалисты высказались о том, что вопрос спама урегулирован уже сейчас. Но, я считаю, что нужно работать над Правилами. Да, вопрос спама урегулирован, но технологически устарел – прогресс в коммуникациях не стоит на месте: спам уже давно перешел в платформу не sms-сообщений, а сообщений на платформе WhatsApp, Viber и других мессенджеров! А за этот тип канала оператор мобильной связи не несет ответственность. Но со спамом надо бороться! Это еще вопрос нашей безопасности, – считает Глава Правления Интернет Ассоциации Украины Александр Федиенко.

Возможно, именно качественный законопроект получится наработать совместными усилиями: на протяжении 10 дней Комитет по вопросам информатизации и связи будет собирать предложения к законопроекту, чтобы создать документ, соответствующий своему времени, который не будет ущемлять права и свободы абонентов и деятельность телеком-операторов.

(вгору)

Додаток 19

3.10.2018
Ирина Фоменко
Нью-Йорк хочет создать киберармию

На сегодняшний день Нью-Йорк является глобальным центром финансов, недвижимости, юридических услуг, технологий и многих других отраслей, пишет TechCrunch. Значение технологий и данных возросло, поэтому особое внимание уделяется атакам, направленных на них. Согласно докладу McAfee и Центра стратегических и международных исследований, последствия от киберпреступности и кибервойн обходятся компаниям в сотни миллиардов долларов (InternetUA).

Тем не менее, Нью-Йорк едва ли стал бастионом для индустрии кибербезопасности. В настоящее время Бостон и Вашингтон оказывают огромное влияние на эту сферу, так же, как и Сан-Франциско и Израиль. Теперь руководители Нью-Йорка стремятся построить новую локальную империю, которая станет оплотом для других ведущих экосистем.

Сегодня New York City Economic Development Corporation (NYCEDC) объявила о запуске Cyber NYC, 30-миллионном стартапе, «стимулирующем» приток инвестиций, направленных на быстрое развитие экосистемы города и инфраструктуры для кибербезопасности.

«Кибербезопасность – невероятная возможность, но в то же время и огромная угроза. Финансовая индустрия была жизненной основой этого города на протяжении всей нашей истории, расходы на киберпреступность быстро растут. Мы проиграем, если не сможем инвестировать в инновации, делающие город сильным. И победим, если мы сможем создать новшество здесь, как и соответствующие рабочие места», – заявил генеральный директор NYCEDC Джеймс Патчетт.

Программа Cyber NYC состоит из:

– Партнерство с Jerusalem Venture Partners. Hub.NYC будет развивать предприятия кибербезопасности, связывая их с консультантами и клиентами.

– Сотрудничество с SOSA, город создаст новый совместный рабочий центр Global Cyber Center площадью 15 000 квадратных футов в Челси, где профессионалы смогут учиться друг у друга.

– С Fullstack Academy и Laguardia Community College будет создан Cyber Boot Camp.

– Благодаря «Applied Learning Initiative» студенты смогут получить степень «CUNY-Facebook Master's Degree» в области кибербезопасности. В программе участвуют Городской университет Нью-Йорка, Нью-Йоркский университет, Колумбийский университет, Cornell Tech и iQ4.

– С Technology Ventures NYCEDC представит программу «Inventors to Founders», которая будет работать над коммерциализацией университетских исследований.

По оценкам NYCEDC, в Нью-Йорке работают около 6000 специалистов по кибербезопасности. Посредством этих программ число может увеличиться еще на 10 000 человек.

Из Иерусалима в Нью-Йорк

Для достижения заявленных целей в области кибербезопасности NYCEDC сотрудничает с двумя венчурными фирмами, Jerusalem Venture Partners (JVP) и SOSA. JVP является постоянным инвестором, который должен помочь учредителям в Hub.NYC получить доступ к капиталу, а также отраслевой и предпринимательский опыт.

«Сегодня, если вы хотите создать ведущие компании следующего поколения, вы должны быть не только там, где разрабатывают идеи, но также и там, где приобретают решения. Вам нужно работать с крупнейшими клиентами в мире», – убежден основатель JVP Эрел Маргалит. Таким местом, по мнению Эрела, является Нью-Йорк.

С момента своего создания JVP (1993) успешно привлекла 1,1 млрд долларов, включая вложения фонда по кибербезопасности в размере 60 млн долларов. За этот период JVP «выпустила» 32 компании, в том числе CyberArk (IPO в 2014 году) и CyActive (PayPal приобрел в 2013 году).

Открытие инноваций с помощью SOSA

SOSA – это глобальная сеть корпораций, инвесторов и предпринимателей, которая объединяет крупные институты с инновационными стартапами, занимающимися основными потребностями. В сферу компетенции группы входят кибербезопасность, финтех, автоматизация, энергетика, мобильность и логистика. Хоть штаб-квартира SOSA в Тель-Авиве, компания недавно открыла инновационную лабораторию в Нью-Йорке, поддерживаемую крупными партнерами, включая HP, RBC и Jefferies.

«Global Cyber Center станет основным центром для всей индустрии кибербезопасности, где эксперты из Нью-Йорка, Штатов, Израиля и других

стран смогут встречаться, взаимодействовать и общаться», – прокомментировал генеральный директор SOSA Узи Схеффер.

Благодаря своему присутствию в Нью-Йорке местная сеть SOSA может помочь в участии в плане EDC, в то время как глобальная сеть компании – превратить Нью-Йорк в мирового лидера кибербезопасности.

Не случайно оба венчурных партнера EDC знакомы с израильской экосистемой кибербезопасности. Израиль долгое время считался лидером в инновациях и политике в области кибербезопасности, и выиграл от такой же успешной координации между государственным и частным секторами, которую Нью-Йорк надеется повторить.

Большие планы, большие результаты?

Стоит обратить внимание и на образовательные программы NYCEDC: студенты смогут проходить занятия в любом университете в консорциуме из пяти человек и свободно переносить кредиты. Facebook присоединился к Городскому университету Нью-Йорка для обучения нового класса лидеров кибербезопасности.

«У вас, вероятно, не хватает времени – два года – чтобы получить степень магистра, поэтому гибкость программы должна обеспечить лучший доступ к большему числу профессионалов», – считает Патчетт.

По мере того, как мир сталкивается с постоянно растущим количеством киберугроз, индустрия кибербезопасности может стать одной из главных отраслей, которая сможет обеспечить необходимую защиту для развития других сфер Нью-Йорка.

(вгору)

Додаток 20

3.10.2018

Из каждых 6 домашних маршрутизаторов только один защищён от киберугроз

Из каждых 6 домашних маршрутизаторов только один защищён от киберугроз (Компьютерное Обозрение).

Исследование, проведённое некоммерческой потребительской организацией American Consumer Institute (ACI), показало, что на подавляющее большинство домашних маршрутизаторов не устанавливаются нужные обновления защиты, из-за чего устройства, а также их пользователи и присоединённые к ним устройства IoT остаются уязвимыми для взлома.

Свои выводы эксперты ACI основывают на анализе выборки из 186 маршрутизаторов Wi-Fi категории SOHO (small office/home office) от 14 различных вендоров, представленных на рынке США. Авторы отчёта проверяли версии прошивки, с которыми работали эти устройства, определяя по открытым базам данных наличие известных дефектов безопасности для них.

«В общей сложности в выборке было обнаружено ошеломляющее количество, 32003 известных уязвимостей, – отмечают эксперты ACI в

исследовании, опубликованном на прошлой неделе. – Наш анализ показал, что из 186 выбранных маршрутизаторов 155 (87 %) имели уязвимости к потенциальным кибератакам в своей прошивке. В среднем на каждый маршрутизатор приходилось 172 уязвимости или 186 – на каждое из 155 проблемных устройств».

Более четверти из всех 32 тыс. изъянов в защите имели два высочайших рейтинга опасности – «critical» и «high-risk». Таким образом, в среднем, каждый роутер из выборки имел 12 критических уязвимостей и 36 – представляющих высокий риск.

Согласно выводам авторов, использование библиотек с открытым кодом является одной из главных причин наличия дефектов безопасности в прошивке маршрутизаторов, поскольку та наследует уязвимости от составляющих её меньших компонентов.

Кроме того, многие их этих устройств, особенно старых моделей, остаются уязвимыми из-за отсутствия механизмов автоматического обновления: сам пользователь вспоминает о необходимости установить патчи, обычно, уже после хакерской атаки, с использованием таких штаммов вредоносных программ, как Mirai и VPNFilter.

«Регулярное закрытие прошивки от известных онлайновых угроз может быть сопряжено с расходами для производителей, но без этого потребителям приходится коллективно нести бремя потенциально гораздо более высоких издержек от киберпреступности», – считают эксперты ACI.

(вгору)

Додаток 21

3.10.2018
Ольга Карпенко
Взлом Facebook обнажил проблему всего интернета

Недавно стало известно, что из-за уязвимости могло пострадать около 50 млн аккаунтов в Facebook, а безопасность еще 40 млн – под вопросом. Журналисты Wired сообщили, что последствия у взлома могут быть куда хуже, чем доступ к данным аккаунтов. Чем грозит одна из крупнейших утечек данных в этом году (AIN.UA)?

Facebook много ругали за масштабную уязвимость, позволившую хакерам не только подобраться как минимум к 50 млн аккаунтов, но также получить доступ к данным сайтов сторонних компаний, чьи пользователи были авторизованы с помощью Facebook. Ситуацию только ухудшает то, что исправить ее – не по силам одному лишь Facebook.

Некоторые из популярнейших сайтов в сети все еще не внедрили базовые правила безопасности, которые бы ограничили эффект от взлома Facebook, согласно последнему исследованию Университета Иллинойса в Чикаго. Если бы они с большей осторожностью отнеслись к функции Facebook Single Sign-On, которая позволяет логиниться с одного аккаунта на разные сайты, вместо

того, чтобы для каждого придумывать пароль – влияние взлома скорей всего ограничилось бы самим Facebook.

Вместо этого, хакеры, возможно, получили доступ ко всему – от частной переписки на Tinder до паспортных данных на Expedia, и все это – не оставив ни следа. Даже хуже: пользователь мог попасть в группу риска, ни разу в жизни не используя Facebook для логина на сторонних сайтах.

Ключ от всех дверей

В статье, опубликованной в августе ученый в области вычислительной техники Джейсон Полакис с коллегами анализировали многочисленные способы, с помощью которых хакеры могли бы пользоватьс функцией Single Sign-On. Facebook в этом не одинок. У Google есть подобная опция, как и у многих других сервисов. Но функция авторизации через Facebook – самая распространенная.

Этому есть серьезные причины. Во-первых, это просто и экономит пользователю время на создание еще одного пароля. И, по крайней мере, в теории, это безопаснее.

«Создание безопасной инфраструктуры, управление пользовательскими данными, зашифрованные соединения – это все довольно тяжело. Так что вместо того, чтобы полагаться на сотни сайтов помельче, вы доверяете одному, у которого лучше механизмы безопасности», – объясняет ученый.

Конечно, эти удобства несли свои риски. Если кто-то взломает Single Sign-On – неважно, у Facebook, Google или иного сервиса – потенциальное влияние будет очень велико. Исследователи постарались выяснить полный масштаб потенциальной опастности выкраденного аккаунта. Какие данные получит хакер? Узнают ли пользователи о том, что были взломаны? И что смогут предпринять в связи с этим? Тогда эти наблюдения заставляли понервничать, сейчас – кажутся провидческими.

28 сентября Facebook объявил, что хакеры смогли пробраться к токенам доступа 50 млн пользователей (а это эквивалент цифровых ключей к Facebook-аккаунту). С этими токенами хакеры могут получить полный контроль над аккаунтами, а благодаря функции Single Sign-On – еще и к другим сайтам, куда эти 50 млн пользователей логинились через Facebook.

Случилось все по сценарию чуть ли не идентичному описанному Полакисом и его коллегами. В том случае исследователям удалось воспользоваться кукиз на пользовательском устройстве, а также уязвимостью (сейчас уже исправленной) в iOS-приложении сети. Но, пишет Полакис, как только хакер получил контроль над чьим-то аккаунтом, доступ к сайтам сторонних разработчиков – дело времени.

После того, как Facebook раскрыл уязвимость, он переустановил токены для всех 50 млн пользователей, и еще для 40 млн, которые были в группе риска. «Мы все еще проводим расследование, чтобы узнать, получили ли атакующие доступ к приложениям третьих сторон», – заявила представитель сети Кэти Дормер в комментарии Wired.

Ограниченная защита

Есть способы, которыми «третьи стороны» должны защищать своих пользователей в случае, если функцию Single Sign-On используют для взлома. Но проблема в том, что мало кто из них реально этим занимается.

Например, сайты, которые используют Single Sign-On, могут либо автоматически залогинивать пользователя, если он уже залогинен в Facebook в другой вкладке браузера, либо требовать Facebook-пароль каждый раз, когда пользователь хочет авторизоваться. Второй сценарий – более безопасный, поскольку хакерам понадобится больше данных, чем токены доступа. Им понадобятся пароли.

Но во время ручной проверки 95 самых популярных веб- и мобильных сайтов, которые пользуются Facebook-авторизацией, от Uber и Airbnb до The New York Times and The Washington Post, исследователи обнаружили, что только два сайта требуют каждый раз вводить пароль.

Полакис описывает это как классический сценарий, когда компании выбирают юзабилити в ущерб безопасности.

«Если бы все сайты выбрали безопасность, хакеры не смогли бы добраться до сервисов сторонних разработчиков», – пишет он.

Сторонние разработчики также могли бы дать пользователям возможность просматривать активность в своих аккаунтах. Facebook, к примеру, советовал пользователям проверить активные сессии, чтобы заметить несанкционированный доступ, если он был. Но не все сайты дают такую возможность, как и возможность почистить сессии. Фактически, из 95 исследованных сайтов, только 10 предлагают такое. Из-за этого хакеров не только сложно поймать, но и отрезать им доступ к данным.

Исследователи также проанализировали подмножество сайтов, чтобы выяснить, что случается на этих сайтах, когда пользователь меняет почту или пароль. Оказалось, что из 29 сайтов 15 позволяют менять почту в аккаунте, не запрашивая пароль, из них 6 позволяют переустановить пароль без ввода старого пароля. Остальные требуют формальную процедуру смены пароля. Но если хакер уже поменял почту, он сможет пройти всю процедуру с использованием нового адреса.

Представители сети говорят, что компания дает советы сторонним разработчикам о том, как решить этот вопрос и готовит дополнительные рекомендации для них.

Наверное, самое удивительное открытие в этом исследовании – то, что человеку даже необязательно быть залогиненным в приложение стороннего разработчика через Facebook, чтобы пострадать от взлома. К примеру, вы авторизовались на сайте с помощью такой же почты, которая привязана к вашему Facebook-аккаунту. Если хакер постарается залогиниться на этот же веб-сайт с помощью Single Sign-On, некоторые сайты (в том числе, фитнес-приложение Strava) свяжут эти два аккаунта.

«Если у вас Facebook-аккаунт и вы никогда не использовали его, чтобы логиниться на другом сайте… хакер может все равно использовать

токен Facebook и получить доступ к вашему аккаунту на сайтах сторонних разработчиков», – пишет Полакис.

Избыток данных

Какие данные оказались под угрозой? В контролируемых экспериментах исследователи смогли проследить поездки «жертвы» в реальном времени в Uber. В одном из случаев они даже оставили водителю чаевые с атакующего устройства уже после того, как поездка была завершена. На Tinder им удалось прочесть личную переписку, при том, что в самом взломанном аккаунте сообщения все еще отмечались как непрочитанные. На Expedia им удалось добыть паспортную информацию. А это все же небольшой контролируемый эксперимент на малом числе аккаунтов. Атака, о которой сообщил Facebook, затронула миллионы пользователей.

Wired связался с с некоторыми сервисами, включая Strava, Tinder, Expedia и Airbnb. В Uber заявили, что отозвали токены для Facebook-аккаунтов, которые могли подвергнуться риску. По словам представительницы компании Мелани Инсайн, это означает всех, кто логинился в Uber с нового девайса.

Сейчас в Facebook проверяют, достаточно ли переустановки токенов для того, чтобы закрыть доступ к приложениям сторонних разработчиков (судя по исследованию Полакиса – нет). Масштаб угрозы и вреда все еще не оценен. Facebook еще не публиковал рекомендации для разработчиков сторонних сервисов, использующих его авторизацию, но Полакис предлагает: Single Sign-Off (т. е. вылогиниться из всех активных сессий).

Facebook определенно заслуживает порицания. Он проник в каждый уголок интернета еще десятилетие назад, иногда – не понимая вполне последствий своей вездесущности. Также ясно, что в интересах более комфортного использования приложениями веб-гиганты часто жертвуют безопасностью пользователей. А сейчас наступило время расплаты за это.

(вгору)

Додаток 22

4.10.2018

У Нацполіції буде створено управління для допомоги правоохоронним органам у розкриті злочинів із кіберелементом

У Нацполіції буде створено управління для допомоги правоохоронним органам у розкриті злочинів із кіберелементом. Новий підрозділ увійде до складу Департаменту кіберполіції. Планується, що управління надаватиме підтримку не тільки поліцейським, а й іншим правоохоронним структурам. Про це йшлося 3 жовтня під час зустрічі Голови Національної поліції Сергія Князєва та керівника кіберполіції Сергія Демедюка з Міністром Великої Британії з питань безпеки паном Беном Воллесом (Урядовий портал).

Під час зустрічі сторони обговорили співробітництво поліцейських двох країн у боротьбі із кіберзлочинністю.

Міністр Великої Британії з питань безпеки Бен Воллес наголосив, що для кіберзлочинців немає кордонів, тому у боротьбі із ними важлива взаємодія поліцейських різних країн.

«Дуже радий, що вже зараз ми говоримо про налагоджену взаємодію між підрозділами кіберполіції Великої Британії та України. Різновиди кіберзлочинів змінюються та постійно еволюціонують. І так само люди, які з ними борються, мають змінюватися», – зазначив Міністр.

Керівник Департаменту кіберполіції Сергій Демедюк наголосив, що співробітництво із кіберполіцейськими Великої Британії є цінним для українських поліцейських та корисним у протидії кіберзлочинам. За його словами, наразі вперше за останні кілька років поліцейські цих двох країн можуть безпосередньо обмінюватися оперативною інформацією.

Під час зустрічі українські поліцейські презентували британській стороні проект створення на базі Департаменту кіберполіції нового підрозділу.

«Планується, що завданням управління стане допомога по всіх загальнокримінальних злочинах у державі, які мають кіберскладову. Управління зможе надавати допомогу будь-якому підрозділу в режимі реального часу не лише поліції, а й іншим правоохоронним органам України», – розповів Сергій Демедюк.

Глава Нацполіції Сергій Князєв зазначив, що одним із напрямків роботи підрозділу стане допомога не тільки правоохоронним, а й приватним структурам.

«Ми змінюємо підхід до роботи, у тому числі, це стосується й захисту бізнесу від кіберзлочинів. Наша основна ідея – допомагати та захищати», – підкреслив очільник Нацполіції.

(вгору)

Додаток 23

4.10.2018

Кибергруппа из КНДР пыталась украсть более $1 млрд из банков по всему миру

Киберпреступная группировка APT38, предположительно связанная с правительством Северной Кореи, причастна к серии масштабных «агрессивных» кибератак на банки и другие организации по всему миру, в ходе которых злоумышленники пытались вывести более чем $1,1 млрд, утверждается в докладе компании FireEye (InternetUA).

В последние четыре года с момента взлома компании Sony Pictures Entertainment в 2014 году в СМИ неоднократно появлялись сообщения об активности киберпреступной группировки, известной как Lazarus Group. Согласно отчету, под названием Lazarus Group действуют три подразделения – два специализируются на политическим кибершпионаже (TEMP.Hermit и Lazarus Group), а третий сконцентрирован исключительно на хищениях средств у банков и других финансовых организаций (APT38).

APT38 провела операции против 16 организаций в по меньшей мере 11 странах, иногда атаки происходили одновременно. По мнению экспертов, число пострадавших может быть намного больше. Согласно оценкам компании, с 2014 года группировке удалось похитить более сотни миллионов долларов.

Злоумышленники действуют по одному сценарию: на первом этапе осуществляется сбор необходимой информации (данные о сотрудниках организации, сторонних поставщиках, специфике работы системы SWIFT). Далее злоумышленники проводят атаки типа watering hole (заражение вредоносным ПО сайтов, часто посещаемых жертвой) или эксплуатируют уязвимости в устаревших версиях фреймворка Apache Struts 2. На последующих этапах киберпреступники проводят внутреннюю разведку, собирают учетные данные и сканируют системы, изучают работу системы SWIFT, выводят деньги и удаляют логи, а также внедренное вредоносное ПО для сокрытия своей деятельности.

Ранее американские власти опубликовали отчет о новой схеме хищения денег из банкоматов, применяемой киберпреступной группировкой Hidden Cobra (также известной как Lazarus и Guardians of Peace) еще с 2016 года.

(вгору)

Додаток 24

4.10.2018

Мошенники отмывают деньги с карт украинцев: как работает схема незаконного заработка

В интернете существует много способов заработка, и далеко не все из них законные. Так, украинцы в сети могут зарабатывать до $1,5 тыс. на переводах (нужно принять на свою карту крупную сумму, а потом обналичить их, перевести в биткоин либо пополнить другую карту с помощью терминала). О том, как «обнальщики» отмывают «грязные» деньги с помощью украинцев, пишет «Обозреватель» (InternetUA).

«Отмою ваши деньги»

В «темной части» интернета работает целая сеть «обнальщиков». Большинство из них – всего лишь маленькое звено в преступной цепочке. Первый шаг – завладеть деньгами жертвы. Для этого используют любые методы: начиная от шантажа, вымогательства и заканчивая звонками от имени банка, полиции и воровством данных карты. Второй шаг – обналичить деньги. И если крупные компании используют для этого подставные фирмы и фейковые сделки, то преступники средней руки втягивают в свою деятельность простых украинцев.

В украинском сегменте анонимной части интернета, который также называют «Даркнет», можно найти десятки объявлений с вакансиями для «обнальщиков». Условия простые: на свою банковскую карту нужно принять крупную сумму денег – от 5 до 100 тыс. грн. Комиссию (в среднем 20 % суммы) можно оставить себе, а остальное – потратить на покупку криптовалюты и

перевести на кошелек работодателя. Чаще всего для этого используют биткоин. Специальные форумы, на которых желающие незаконно заработать находят «обнальщиков», требуют внести залоговую сумму и проверяют участников сделки.

Так, журналистам «Обозревателя» удалось устроиться «на работу» на одном из форумов «Даркнет». Общение с потенциальным работодателям проходило в анонимном чате на псевдо-домене onion. С обычного браузера зайти в «Даркнет» не получится, для этого необходимо установить несколько специальных приложений. Чтобы вступить в диалог с продавцом, он должен прислать приглашение в чат. Спустя несколько часов после переписки ее содержимое удаляется автоматически.

«На новеньких больше 5 тыс. грн не даем. Перевод проходит раз в неделю. Твоя комиссия – 20 %. Деньги должен обязательно снять в банкомате, потом пополнить свой кошелек и купить на них биткоины. Их переведешь на кошелек, который сброшу тебе…» – рассказывает об условиях работы анонимный собеседник.

Он – агент, который также получает комиссию с каждой операции. Его задача – находить доверчивых украинцев, которые согласны получить на собственный счет «грязные деньги».

«А если будут вопросы от банка или полиция обнаружит?» – поинтересовались журналисты у «обнальщика».

Собеседник посоветовал сказать, что «деньги по ошибке перевели, ты обрадовался, подумал, может ошибка банка, и пошел снял их, чтобы не списали обратно, все законно». На вопрос о том, если вдруг заставят вернуть средства, также есть определенный совет: сказать, что потратил, а чеки не сохранились.

После еще нескольких вопросов потенциальный работодатель перестал отвечать и в скрытом диалоге, и в личном кабинете форума.

Откуда берут деньги

В Украине значительно выросло количество мошенничества с картами. Хакеры создают целые площадки, маскируют их под платежные системы и воруют данные карт. Узнав пароль, номер карты и CVV, деньги переводят на разные аккаунты онлайн-кошельков. Уже оттуда – снова переводят средства на банковские карты «обнальщиков». Они в свою очередь уже маленькими порциями возвращают средства в биткоинах или же пополняют другую карту с помощью терминалов.

Раскрыть такую цепочку, рассказывает финансовый консультант Владимир Мазуренко, практически невозможно. Онлайн-кошельки очень быстро блокируют, а «обнальщики» между собой не знакомы. Каждый год через такие схемы проходят сотни миллионов гривен. Согласно данным Киберполиции, только в прошлом году со счетов украинцев украли 670 млн грн. Помимо этого, такими схемами пользуются продавцы запрещенных веществ, вымогатели и т. д.

«Больше всего граждане страдают от злоумышленников, которые через телефон или интернет обманным путем получают доступ к данным банковских

карт (социальная инженерия)», – отмечают в Межбанковской ассоциации членов платежных систем.

Если же полиции удастся доказать, что украинцы сознательно согласились отмыть деньги, им грозит до трех лет тюрьмы с конфискацией «заработанного». Согласно ст 209 Уголовного кодекса, минимальное наказание за «легализацию денежных средств» – штраф в 8500 грн.

Несколько месяцев назад Министерство нацбезопасности США изъяло у продавцов «Даркнет» около 2 тыс. биткоинов. По действующему курсу это больше $13 млн. Злоумышленникам предлагали «отмыть» незаконно заработанные средства на популярных в «темной сети» площадках. На этих же сайтах находят и украинцев, которые хотят заработать на незаконных схемах. Новичкам обещают платить за «обнал» до $1,5 тыс. в месяц. Но стоит учитывать, как только банк обнаружит подозрительную операцию и передаст информацию правоохранителям, все полученные средства могут изъять, а владельца счета – посадить.

(вгору)

Додаток 25

8.10.2018

В популярной операционной системе найдена опасная уязвимость

Эксперт в области разработки приложений Томас Рид (Thomas Reed) обнаружил опасную уязвимость в системе macOS. Угрозу для компьютеров от Apple он описал в блоге Virus Bulletin (InternetUA).

Уязвимость связана с особенностями проверки файлов в macOS. Исследователь обнаружил, что установленные приложения, в отличие от только что загруженных пользователем, не проверяются системой безопасности. После установки программа помещается в список достоверных, а повторные проверки инициируются крайне редко. Злоумышленнику достаточно внедрить вредоносный код в уже функционирующие приложения.

Со слов Рида, эту уязвимость очень легко использовать. «Можно легко захватить официальное приложение, которое уже установлено в системе, не вызывая никакой проверки подписи кода. Хуже всего, что большинство разработчиков не знают об этом и не добавляют собственные проверки», – заключает он.

По мнению специалиста, таким образом может быть скомпрометировано большое число приложений. При этом сама система macOS функционирует должным образом, поэтому исправить эту уязвимость могут разве что сами разработчики ПО, добавив возможность частых повторных проверок.

Ранее специалисты обнаружили новый вирус, поражающий компьютеры на macOS. Исследователь Патрик Вардл (Patrick Wardle) в своем блоге дал ему прозвище «дурак» (OSX.Dummy). Вредоносная программа требовала от пользователей самостоятельно ввести команды, а затем загружала внешний файл и закрепляла его в системе.

(вгору)

Додаток 26

8.10.2018
Владимир Кондрашов
В Минюсте используют софт для взлома Windows

На одном из сайтов Главного территориального управления Юстиции Министерства юстиции Украины в открытом доступе находились десятки файлов и программ, среди которых – весьма специфическое программное обеспечение, предназначенное для взлома Windows и использования нелицензионных копий операционной системы и других продуктов Microsoft.

«Уязвимость» сайта ГТУ Юстиции в Полтавской области обнаружил эксперт по кибербезопасности, ведущий разработчик компании ИТ Лаборатория Александр Галущенко, передает InternetUA.

Эксперт обнаружил незащищенное соединение на сайте www.just.gov.ua. На портале управления юстиции доступны директории и программы с десятками файлов и программ. Есть и запрещенное ПО – архивы программ AAct Network 1.1.4 Portable by Ratiborus и Windows Loader DAZ 2.2.2. Оба появились в директории /Program/ 4 сентября этого года.

Согласно инструкции, вложенной в архив AAct Network 1.1.4 Portable by Ratiborus, эта программа является KMS-активатором для операционных систем Windows VL редакций (Vista, 7, 8, 8.1, 10, Server 2008, 2008 R2, 2012, 2012 R2, 2016), а также Office 2010, 2013, 2016. Также благодаря AAct возможна активация Office 2010 VL на Windows XP.

Windows Loader DAZ 2.2.2. антивирусные программы распознают как вредоносное программное обеспечение. В сети можно найти описание ПО – его рекламируют как «активатор Microsoft Windows 7/Vista/2008 R2/Server 2012, который устанавливает сертификат одной из фирм (по выбору), после чего активирует копию Windows и дает возможность проходить проверку подлинности».

Еще один архив, обнаруженный на сайте, – mail.zip – является архивом программы для просмотра паролей от электронной почты.

Кроме того, весьма «сомнительно» и происхождение некоторых программ, используемых Минюстом. Например, в архив с программой Movavi Screen Capture Studio v 5.0.0 вложен архив Crack.rar и документ с инструкцией по установке ПО с помощью взломщика.

Также в директории можно найти программы Adobe Reader, CCleaner, TeamViewer, Total Commander (с папкой «keys»), которыми полтавская юстиция «светила» в сеть.

Кроме «общераспространенного» ПО и драйверов к различным принтерам, на сайте можно найти и ряд более специфического программного обеспечения, используемого органами юстиции для своей работы. В том числе – и для работы с Государственным казначейством.

К счастью, на эти программы умудрились поставить пароли, но само наличие их в открытом доступе показывает отношение служащих к «чувствительной информации».

Полтавское управление юстиции также делиться с пользователями сети рядом документов, среди которых – Коллективный договор между ГТУ Юстиции в Полтавской области и местным профсоюзом, График работы мобильных точек доступа к системе бесплатной правовой помощи, копии свидетельств о регистрации государственных нотариальных контор и многое другое.

В ГТУ Юстиции в Полтавской области нашему журналисту не смогли объяснить, что делает нелицензионное и явно незаконное программное обеспечение на их сайте: в приемной порекомендовали обратиться в отдел материально-технического обеспечения ГТУ, предупредив, что сегодня праздник (День юриста) и можно уже никого не застать. В самом отделе выслушали вопросы журналиста и порекомендовали направить письменный запрос, а информацию об «уязвимости» тут же пообещали передать администратору сайта.

Спустя 5 минут после телефонного разговора с журналистом InternetUA папка Program и несколько других исчезли с сайта управления Юстиции.

(вгору)

Додаток 27

9.10.2018

Максим Саваневський

Закриття соцмережі Google+ може бути відволікаючим маневром перед загрозою Cambridge Analytica – 2

Google закриває соціальну мережу Google+, яка лежала мертвим грузом вже багато років. Компанія у своєму офіційному релізі пояснила закриття низькою популярності Google+ серед користувачів – 90 % сеансів становлять менше п’яти секунд (Watcher).

В компанії також поскаржились на значні складнощі для розробки і підтримки Google+ на тому рівні, який очікують користувачі. «Беручи до уваги ці складнощі, а також з урахуванням низької активності користувачів, ми прийняли рішення закрити призначену для користувача версію Google+», – йдеться в повідомленні компанії.

Але чи дійсно через це Google закриває свою соціальну мережу?

Повідомлення про закриття Google+ з’явилось в блозі компанії Google всього через годину після появи розслідування Wall Street Journal, в якому йшлося про те, що з 2015 по березень 2018 року сторонні додатки могли отримувати доступ до персональних даних користувачів без їх згоди. Мова йде про сотні тисяч користувачів.

Схема витоку була дуже схожою до ситуації збору даних користувачів Facebook, які згодом потрапили до Cambridge Analytica. Сторонні додатки

отримували доступ до прихованих особистих даних користувачів, які є друзями людини, яка авторизувалась у додатку.

Зважаючи на те, що баг у Google виявили саме в березні 2018 року під час спеціального внутрішнього дослідження, можна припустити, що це могло бути пов'язано зі скандалом навколо Cambridge Analytica, який якраз ввійшов в активну фазу саме в березні. Очевидно, що великі IT-компанії почали перевіряти чи немає в них схожих проблем. І Google знайшов проблему в себе, але що найгірше – не повідомив про це користувачів.

Наприклад, європейські регуляції щодо захисту персональних даних (GDPR) зобов'язують компанії повідомляти користувачів про витоки персональних даних протягом 72 годин після виявлення інциденту. Google повідомив лише на 7й місяць у своєму блозі, де розповів про закриття Google+ і про факт проблеми з доступом до приватних даних. Правда, GDPR почав діяти в Європі лише у травні (4 місяці тому). Та це не виключає проблем компанії з регулюючими органами ЄС. Штраф може скласти 2 % від річного доходу. Тобто близько $2-3 млрд.

Наразі не зрозумілі розміри витоку даних. За інформацією WSJ, Google зберігала обмежену кількість логів (записів про активність), і через це зараз важко оцінити кількість користувачів, які могли постраждати за 3 роки існування діри в безпеці. Хоча сама компанія заявила про півмільйона потенційних жертв. Окрім того Google має обмежені права щодо проведення аудиту сторонніх розробників.

Наразі компанія, за інформацією WSJ, не проводила зустрічі з жодним з розробників, які могли отримати доступ до приватних даних через діру.

То що ж з приводу закриття Google+? Як такі дві різні новини – глобальна проблема з витоком даних і закриття соцмережі потрапили в один реліз в блозі компанії? І чому це сталось всього через годину після оприлюднення журналістського розслідування про те, що Google 7 місяців тому прийняв рішення приховати цю інформацію?

Ймовірно, що закриттям своєї соцмережі компанія намагається перебити або хоча б зменшити інформаційну хвилю, яка виникне внаслідок публічного оприлюднення даних про діру.

З комунікаційної точки зору Google прийняв правильне рішення.

Правда розслідування з боку регулюючих органів (в першу чергу в США і ЄС) та різноманітних судових позовів компанії вже точно не уникнути.

Причому ситуація у Google може бути навіть гіршою, ніж те, що було у Facebook протягом березня-червня 2018 року. Адже Google протягом 7 місяців мовчав. І причину цього мовчання важко виправдати.

Наслідки цього скандалу точно вдарять по всій галузі і посилять тиск з боку урядів багатьох країн щодо контролю персональних даних та використання їх IT-гігантами.

(вгору)

Додаток 28

12.10.2018

Кибершпионы атакуют военные и правительственные организации по всему миру

Эксперты компании Symantec раскрыли подробности о деятельности киберпреступной группировки Gallmaker, атакующей правительственные и военные организации по всему миру с целью кибершпионажа. Примечательно, злоумышленники не используют вредоносное ПО для перехвата контроля над системами жертв – в атаках применяются легитимные инструменты, например, фреймворк Metasploit и оболочка PowerShell (InternetUA).

Группировка активна по меньшей мере с декабря 2017 года. Список ее жертв включает ряд зарубежных посольств одной из стран Восточной Европы (о каком государстве идет речь, не раскрывается) и несколько военных структур в странах Среднего Востока. Специалисты не могут с уверенностью сказать, спонсируется ли Gallmaker каким-либо правительством, но отмечают, что за операциями стоит «весьма компетентная организация».

В ходе атак злоумышленники рассылают фишинговые письма с документами на правительственную, военную или дипломатическую тематику. Для компрометации систем жертвы злоумышленники эксплуатируют функцию Dynamic Data Exchange (DDE) в приложении Word. Протокол DDE применяется для обмена информацией между программами пакета Office, которые используют общие данные или общую память. В минувшем году компания Microsoft выпустила обновление, отключающее функционал в Word и Excel.

Вместо вредоносного ПО группировка Gallmaker применяет различные легитимные процессы и инструменты, доступные в интернете или включенные в состав Windows. К примеру функция WindowsRoamingToolsTask используется для планирования задач и скриптов PowerShell, а с помощью инструмента Metasploit злоумышленники обфусцируют шелл-код, исполняемый из PowerShell. Для связи с управляющим сервером и выполнения команд участники группы используют официальную версию архиватора WinZip, а также применяют библиотеку Rex PowerShell для создания и манипуляции скриптами PowerShell. По завершении атакующие удаляют инструменты с компьютера жертвы, чтобы замести следы.

По данным Symantec, в период с декабря 2017 года по июнь 2018 года злоумышленники провели 20 атак, насколько они оказались успешными, специалисты выяснить не смогли.

(вгору)

Додаток 29

12.10.2018

Ольга Карпенко

Что такое баг-баунти платформы и как они помогают компаниям защищаться от хакеров

Что такое баунти-платформы, как они работают, и в чем смысл таких программ для бизнеса, в своей колонке для AIN.UA рассказывает Марк Савчук, директор по коммуникациям в Hacken (AIN.UA).

Сегодня хакерские атаки становятся обыденным делом. Оно и неудивительно – согласно отчету McAfee и Center for Strategic and International Studies, мировая экономика теряет около $600 млрд в год из-за киберпреступности.

Спрос на услуги по кибербезопасности также бьет рекорды. В 2018 году размер отрасли составит более $96 млрд. На фоне возникновения все новых угроз рождаются новые инновационные решения и методы борьбы с киберпреступниками. Одним из таких решений являются баг-баунти программы.

«Программа баг-баунти» предусматривает «получение вознаграждения (баунти) за нахождение уязвимости (баг) в коде, которое предлагается «белым» хакерам. Соответственно, баг-баунти программа – это процесс, в котором компания приглашает любого желающего протестировать их продукт на уязвимости. Если хакер находит баг – получает вознаграждение.

Первая баг-баунти программа стартовала в 1983 году. Компания Hunter & Ready тестировала свою операционную систему Versatile Real-Time Executive. Любой, кто нашел баг и сообщил об ошибке, мог получить Volkswagen Beetle.

Со временем баг-баунти программы получали все большую популярность. Компании Microsoft, Google, Facebook стали запускать свои собственные баг-баунти программы. Однако так поступали лишь большие компании. Для всех остальных баг-баунти программы были недоступны. Причины заключались в следующем:

Проблема номер один – это медийность. Только самые большие компании имели достаточный visibility, чтобы привлечь «критическую массу» хакеров, чтобы получить хороший результат. К тому же, зачем белому хакеру работать с каким-то ноу-неймом, как он будет уверен, что ему действительно заплатят за его работу? Большие компании – более безопасный выбор. Да и могли себе позволить заплатить достойную «баунти» за найденные уязвимости.

Второе – компания должна иметь достаточно квалифицированный персонал в IT-департаменте, чтобы грамотно обрабатывать поток найденных багов, который присылают ресерчеры. Потому баг-баунти программы в основном и проводились high-tech-компаниями.

По мере развития интернета и диджитализации бизнеса потребность в баг-баунти программах дошла и до среднего бизнеса. Однако самостоятельно их провести они не могли в силу причин описанных выше. Поэтому начали появляться баг-баунти платформы (например, Hackerone, HackenProof, Bugcrowd). Они помогают проводить баг-баунти программы компаниям, которые бы никогда не справились с данной задачей самостоятельно.

Что из себя представляет баг-баунти платформа?

Тикетная система, через которую белые хакеры могут подавать отчеты (репорты), в которых есть детальное описание уязвимости, а также необходимые шаги для устранения этих уязвимостей.

Квалифицированный персонал, который проверяет отчеты ресерчеров, верифицирует баги (этот процесс называется «триаж»), фильтрует дубликаты (когда два разных ресерчера нашли один и тот же баг, в этом случае баунти получает тот, кто сообщил о баге первым) и осуществляет ежедневную коммуникацию с клиентом и ресерчерами.

Сообщество белых хакеров. Это, наверное, самый главный элемент платформы. Баг-баунти платформы постоянно работают над увеличением количества белых хакеров на своей площадке. В этом их «суперсила» и основная ценность для бизнеса.

Как проходит процесс баг-баунти на платформе?

Первым делом компания-клиент и баг-баунти платформа совместно составляют «скоуп работ». Этот документ четко описывает, какие именно ресурсы клиента подлежат тестированию, за какие именно уязвимости будут выплачены награды и в каком размере.

Запуск баг-баунти программы. Составленный скоуп работ публикуется на сайте и баг-баунти платформа инициирует маркетинговые активности, чтобы привлечь свое сообщество белых хакеров к данной баг-баунти программе. Начинается сам процесс – белые хакеры ищут уязвимости в продукте.

Ресерчеры (они же белые хакеры) присылают отчеты о найденных уязвимостях через баг-баунти платформу, с описанием самой уязвимости и часто с рекомендациями как ее устранить.

Триаж-команда баг-баунти платформы верифицируют баги, которые присылают хакеры. Как только баг был верифицирован и клиент исправил уязвимость в своем продукте – белый хакер получает баунти, то есть, деньги. Одновременно с этим ему начисляют репутацию. На платформах существуют специальные лидборды для рейтингования хакеров.

Стоит подчеркнуть, что именно баг-баунти платформы, и высокая потребность в таких специалистах дают возможность белым хакерам монетизировать свои способности.

До появления баг-баунти платформ и программ фактически не существовало простого и легального способа хакерам зарабатывать деньги. Теперь же, они могут помогать бизнесу, получать достойную заработную плату (размер баунти может доходить и до $100 000 за одну уязвимость) и получать публичное признание.

В чем конкурентное преимущество баг-баунти платформ?

Почему баг-баунти программы лучше обычных компаний, которые предоставляют услуги по кибербезопасности? Несмотря на то, что баг-баунти программы не являются панацеей и не отменяют потребность проведения тестов на проникновение, баг-баунти программы имеют несколько ключевых достоинств:

– Количество доступных специалистов. В стандартном тесте на проникновение, будет принимать не более 2-5 специалистов. В то время как баг-баунти платформа обладает в своем распоряжении сотнями белых хакеров. Как правило, эти люди с разных уголков света и имеют разную специализацию, что повышает шанс того, что ресерчеры найдут уязвимость в продукте (их больше и у них разный бэкграунд).

– Время тестирования. Опять же – стандартный тест на проникновение длится около от нескольких недель до нескольких месяцев в зависимости от объема работа и является точечной оценкой конкретной версии продукта, в то время как баг-баунти программы могут длится годы и являются непрерывным механизмом по оценке безопасности. И все это время ресерчеры будет пытаться найти уязвимость в вашем продукте.

– Система вознаграждения. При проведении стандартного теста на проникновение компания заплатит в любом случае – получит она результат или нет. В то время как система вознаграждения в баг-баунти программах основана на оплате за результат, т.е. за каждый верифицированный баг.

Почему компании дают себя хакнуть?

Напоследок главный вопрос – почему компании добровольно отдают свои продукты на растерзание белым хакерам?

Потому что парадигма «я построю суперстену и меня не взломают» не работает, банально потому что технологии и софт обновляется чуть ли не каждую неделю. Новые «дыры» появляются постоянно. Режим «я в домике» уже давно не работает. Вопрос кибербезопасности перешел из временной проблемы в постоянную (нужно постоянно мониторить и улучшать свою защиту). Поэтому передовые компании сменили свое мышление с «Я в домике» на «Если мою систему, будут постоянно пытаться взломать лучшие белые хакеры в мире – то они найдут в моем коде все “дыры”, и когда придет черед настоящей атаки, злоумышленники не смогут прорваться сквозь нашу защиту».

Стоит понять, что киберугрозы никуда не уйдут, а будут только усиливаться со временем. Откладывание этого вопроса «на потом» может привести к губительным последствиям для компании. Кибербезопасность станет такой же мейнстримовой задачей, как и ведение бухгалтерского учета.

Однако паниковать не стоит. Передовые технологии и новые подходы к кибербезопасности смогут защитить компании завтра. На каждого хакера есть свой белый хакер.

(вгору)

Додаток 30

15.10.2018
Google Play нужно срочно удалить с Android

На все смартфоны для международного рынка, если их выпускает не Apple, установлена операционная система Android со встроенными в нее сервисами от Google, в число которых в первую очередь входит магазин

программного обеспечения под названием Google Play, откуда пользователи могут устанавливать программы и игры на свое собственное усмотрение (Portaltele).

Как удалось выяснить 15 октября, это приложение следует срочно удалить со смартфона, об этом пишут эксперты в области кибербезопасности из компании Cisco. Они обнаружили совершенно новый троян для Android, который уже начал распространяться по всему миру.

Он попадает на смартфон под видом обновленного приложения Google Play, запрашивая полный набор различных разрешений на полноценное управление телефоном. Как только пользователь их выдает, программное обеспечение создает иконку на рабочем столе и заменяет все ярлыки запуска настоящего магазина программного обеспечения на фейковое. Специалисты назвали опасную программу именем GPlayed, но на самом деле она называется Google Play. После того, как пользователь запускает такое приложение, оно запрашивает дополнительные разрешения и запускает внутри себя настоящий магазин ПО. При этом, модифицированная версия популярной плеймаркета умеет воровать любые данные, которые хранятся во встроенной памяти телефона, отправлять сообщения SMS и совершать звонки, а также выполнять многие другие действия, которые наносят вред пользователю.

На основании этого эксперты советуют не устанавливать никакие сторонние магазины Google Play, какие бы новые возможности и функции не обещали их распространители. В конечном итоге все закончится тем, что данные банковской карты окажутся украдены, а подобный исход гарантированно придется не по вкусу каждому человеку. В связи с этим, нужно срочно проверить свой смартфон на базе Android на наличие вирусов, удалив фейковый магазин ПО.

(вгору)

Додаток 31

15.10.2018

ИИ-антивирус защищает личные данные подобно иммунной системе организма

Darktrace – ведущий британский стартап в области кибербезопасности. Там обещают наглядную визуализацию скрытых угроз и постоянное самообучение системы на основе ИИ. Оценки эффективности решения расходятся, но инвесторов это не смущает: последний раунд оценил компанию в $1,65 млрд (InternetUA).

Darktrace называет себя «ведущей мировой ИИ-компанией в области кибербезопасности». Ее решение для бизнеса – подключаемый к сети сервер, распознающий и реагирующий на скрытые угрозы. Darktrace утверждает, что система благодаря машинному обучению замечает вещи, которые игнорируют традиционные антивирусы и файрволлы. Среди ее клиентов – лондонский

аэропорт «Гэтвик», американская страховая компания AIG и лондонский Музей естественной истории.

В конце сентября в очередном раунде инвестиций компания привлекла $50 млн при оценке в $1,65 млрд. Однако, как пишет Financial Times, мнения экспертов о значимости технологии и роли пиар-департамента в бурном развитии стартапа расходятся.

В Darktrace сравнивают работу своего сервера с иммунной системой человека: предполагается, что ИИ изучает новые угрозы и самостоятельно на них реагирует.

Все данные визуализируются на красивой трехмерной модели, напоминающей то, как изображают деятельность хакеров в Голливуде.

Части клиентов такой подход нравится – это гораздо лучше, чем просматривать миллионы строчек лог-файлов, утверждает глава техслужбы Музея естественной истории Иэн Голдинг.

Однако довольны не все. FT приводит пример компании из Лондона, которая каждый месяц перечисляет Darktrace за услуги $10 000.

Один из инженеров заявил, что сервер генерирует слишком много ложноположительных предупреждений. В итоге на них не обращают внимания, а информацию просматривают не чаще раза в день.

Опрошенные FT эксперты считают, что компаниям с небольшими ИТ-отделами сложно оценить объемные отчеты об угрозах, которые предоставляет система «сетевого иммунитета».

В Darktrace не видят в этом проблемы. Во-первых, объясняет один из пары исполнительных директоров компании Поппи Густафссон, система хорошо справляется с угрозами и самостоятельно. Во-вторых, Darktrace может предоставить специалиста для анализа. Правда, за отдельную плату.

Эксперт по онлайн-безопасности компании Gartner Лоуренс Оранс считает, что Darktrace определенно сильна в маркетинге. Созданная в 2013 году, она одной из первых начала подчеркивать, что опирается на ИИ и машинное обучение.

Трехмерный интерфейс – «это секси» и наглядно, добавляет Оранс. А сервер для трехнедельной демонстрации потенциальные клиенты получают бесплатно.

Представитель Darktrace, впрочем, уверяет, что эта компании – «больше чем хайп». По данным самой компании, ежеквартально число клиентов удваивается. Выручка за год с июня 2017-го по июнь 2018 года выросла на 80 %. Правда, это по-прежнему ниже расходов на маркетинг и бесплатную доставку серверов клиентам.

Вопросы кибербезопасности стремительно выходят на законодательный уровень: теперь это не просто бизнес, а вопрос национальной безопасности и влияния. Так, в Британии хотят создать ведомство по интернет-цензуре, а Калифорния принимает первый в мире закон о кибербезопасности устройств умного дома.

(вгору)

Соціальні мережі

як чинник інформаційної безпеки

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

Упорядник **Терещенко** Ірина Юріївна

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.