СОЦІАЛЬНІ МЕРЕЖІ ЯК ЧИННИК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Огляд інтернет-ресурсів
(15.11–28.11)

2017 № 19

Соціальні мережі
як чинник інформаційної безпеки

Інформаційно-аналітичний бюлетень
Додаток до журналу «Україна: події, факти, коментарі»
Огляд інтернет-ресурсів
(15.11–28.11)
№ 19

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 2017

ЗМІСТ

Орфографія та стилістика матеріалів – авторські

РОЗВИТОК І ПЕРСПЕКТИВИ СОЦІАЛЬНИХ МЕРЕЖ

15.11.2017

Bloomberg и Twitter запустят круглосуточную новостную социальную сеть

Bloomberg нанял порядка 50 человек для нового проекта, который будет существовать только в Twitter. Это будет первая новостная социальная сеть, работающая 24 часа в сутки, сообщает mediamedia.me. Новый проект Bloomberg и Twitter будет запущен 18 декабря. Основными партнёрами проекта стали Goldman Sachs, Infiniti, TD Ameritrade, CA Technologies, AT&T и CME Group. Стоимость за партнёрство в этом проекте составляет сумму от $1,5 млн до $3 млн (Marketing Media Review).

«Когда миром правит дуэт Google/Facebook, единственным способом преуспеть стали инновации. Привилегия взрывного развития не должна быть исключительно у технологических компаний (так же известных и как «медиакомпании»). Существенные возможности роста есть у всех, но они требуют от лидеров больше агрессии, нового мышления и новых моделей», – отметил Джастин Смит, глава Bloomberg Media.

***

15.11.2017

Skype запускает аккаунты нового типа

Microsoft вскоре намерен начать тестирование нового типа аккаунта Skype, ориентированного на индивидуальное удаленное предпринимательство: репетиторство, онлайн-консультации и пр.

Докладніше

***

15.11.2017

Telegram для iOS и Android получил крупное обновление

Разработчики Telegram обновили приложение для iOS и Android до версии 4.5. Мессенджер получил много нововведений, оптимизирован для iPhone X, а также обзавелся специальным чатом для избранных сообщений (InternetUA).

Нововведения в версии 4.5:

– Группировка фотографий. При отправке нескольких фотографий или видео их можно сгруппировать в один альбом. Также можно выбрать порядок, в котором находиться фотографии.

– Избранные сообщения. Чтобы сохранить важные сообщения, их можно переслать в чат «Избранное». Перейти к сохраненным сообщениям можно из списка чатов или из боковой панели. Если раньше для этого вы использовали

чат с собой, а сейчас потеряли его – не паникуйте, все сообщения из него переместились в «Избранное».

– Улучшенный поиск. Новый алгоритм глобального поиска по каналам и ботам позволяет искать их по заголовкам. Вверху поиска выводятся самые популярные группы и боты.

– Закрепленные сообщения. Администраторы каналов получили возможность закреплять сообщения вверху чата, чтобы подписчики не пропустили важные объявления. Раньше такая возможность была только в чатах групп.

– Фотографии профиля. Появилась возможность добавить до 10 фотографий профиля пользователя, которые можно перелистывать и выбирать для превью.

***

15.11.2017

Дмитрий Демченко

Украинцы запустили Telegram-бота для отслеживания цен на авиабилеты

Украинцы Николай Кравчук и Денис Лищенко создали Telegram-бота AirTrack для мониторинга цен на авиабилеты. Об этом сообщают «Факты ICTV» (AIN.UA).

Для того, чтобы начать отслеживать цену на билеты по конкретному направлению, пользователю нужно указать дату и место вылета. Далее AirTrack выдаст варианты, которые доступны на текущий момент, и предложит мониторить стоимость билетов. После этого бот будет отправлять уведомления об изменении в ценах.

Как отмечают «Факты», AirTrack мониторит 98 % авиакомпаний мира, в частности – Wizzair, Ryanair и другие лоукосты, которые покрывают Европу. Сейчас бот понимает украинский, английский и русский. В будущем создатели планируют добавить больше языков, а также улучшить понимание человеческой речи.

AirTrack – не первый подобный бот, созданный украинцами. Ранее один киевлянин создал Telegram-бота для мониторинга цен на ж/д билеты, а другой – для отслеживания стоимости поездки на Uber.

***

15.11.2017

Новое приложение для Twitter позволяет транслировать видео с вашего телефона

Стараясь совершенствоваться и идти в ногу со временем, Twitter решил запустить сервис потокового видео, который, в скором времени, может конкурировать и с YouTube. Как стало известно, новое бесплатное приложение

Periscope призвано транслировать потоковое видео в режиме «онлайн» со смартфона на Twitter пользователя. При этом можно передавать не только видео, но и звук, и географические координаты. Во время прямого эфира, Periscope отслеживает комментарии и лайки от посетителей странички. От этих показателей зависит рейтинг видео, которое может быть доступно пользователям в течении 24 часов (HiTech-News.ru).

В случае необходимости, приложение можно настроить на приватный режим, в результате чего прямой эфир будет доступен к просмотру только избранным пользователям. Эксперты полагают, что разработчики Twitter обратили внимание на то, что потоковое видео стремительно набирает популярность, повышая рейтинги YouTube. А с помощью Periscope они намерены составить конкуренцию известной видео-платформе. Новое приложение пока доступно всего лишь на iPhone, хотя, по словам разработчиков, версию под Android осталось ждать совсем недолго.

***

17.11.2017
Facebook обновила сервис Stories

Компания Facebook выпустила крупное обновление в рамках сервиса Facebook Stories, который позволяет людям обмениваться разными событиями жизни друг с другом.

Докладніше

***

17.11.2017
Twitter работает над новой программой верификации аккаунтов

Компания Twitter сообщила о работе над новой программой верификации и установки подлинности аккаунтов (InternetUA).

В заявлении говорится, что ранее подразумевалось, что верификация устанавливает подлинность личности владельца страницы. Но затем значок верификации в глазах пользователей превратился в свидетельство «одобрения» или «индикатор важности».

«Мы осознаем, что создали эту путаницу, и работаем над ее устранением», – отметили в компании.

Также руководство соцсети добавило, что заявки на верификацию временно не принимаются.

***

21.11.2017
Facebook добавит маркер отличия для проверенных издательств

Компания Facebook ввела новую отметку, которой будут награждаться новостные посты издательств, прошедших дополнительную проверку на подлинность информации.

Докладніше

***

21.11.2017

Facebook выпустила приложение для авторов видео

В попытке переманить авторов видеоконтента с YouTube на Facebook компания выпустила для них специальное приложение. Оно называется Facebook Creator и включает ряд инструментов для проведения трансляций, создания историй и отправки сообщений (InternetUA).

У компании и раньше было приложение для управления страницами, а также специальная программа для знаменитостей под названием Facebook Mentions. Новый продукт компании – это на самом деле обновлённая и переименованная версия последней (хоть Mentions из App Store пока никуда не исчезла).

В Facebook Creator есть два основных раздела. В первом доступны уникальные функции Facebook Live, среди которых – создание пользовательских вступлений и концовок. Через приложение также можно делать и редактировать фотографии, а затем публиковать их в социальной сети в виде историй и на других платформах.

Второй раздел связан с общением. Это единый ящик для комментариев из Facebook и Instagram и сообщений из мессенджера компании. Благодаря этому ящику вам не нужно переключаться между разными приложениями, чтобы ответить тому или иному человеку.

Помимо прочего, в Facebook Creator есть вкладка с анализом просмотров вашего контента. Приложение доступно на iOS, а на Android появится в ближайшие месяцы.

***

20.11.2017

Twitter будет следить за поведением проверенных пользователей за пределами собственного ресурса

Не так давно представителей всех крупных компаний и социальных сетей США вызвали в Конгресс для обсуждения проблем проверки пользователей и того, какой материал допускается к распространению в рамках предоставляемых сервисов. Ответная реакция с посылом ужесточить процедуру верификации не заставила себя ждать.

Докладніше

***

20.11.2017
В мобильном клиенте YouTube появится давно ожидаемая функция

При изучении новой версии мобильного клиента YouTube выяснилась интересная деталь: инженеры Google активно готовятся к внедрению в приложение темной темы. Соответствующие строки были обнаружены в исходном коде APK-приложения YouTube версии 12.45. Оформление в черных оттенках сделает просмотр видео на YouTube более комфортным для глаз в темное время суток. Особенно это нововведение оценят обладатели мобильных устройств с OLED-экранами (IGate).

Темная тема уже давно доступна пользователям настольной версии YouTube, а теперь она готовится к релизу и на мобильных устройствах. Сильнее других это нововведение оценят владельцы OLED-смартфонов, на которых отображение черного цвета не требует потребления электроэнергии, а значит экономит заряд аккумулятора.

***

26.11.2017
В Twitter появятся закладки

Социальная сеть добавит функцию сохранения твитов в закладки, чтобы к ним можно было вернуться позже (InternetUA).

Функция появится в списке в основном меню на боковой панели. К сохраненному твиту можно будет вернуться, чтобы прочесть его.

Сейчас сохранить понравившийся твит можно отметив его, как понравившийся, сделав репост или же отправив его себе в личное сообщение. Однако, ни один из этих методов не является идеальным и по-настоящему удобным для пользователей.

Функция пока находится в стадии разработки. Планируется, что она появится одновременно у всех пользователей сервиса. О сроках пока ничего не известно.

***

27.11.2017
Telegram-каналов об образовании, науке и криптовалюте

10 Telegram – отличная альтернатива социальным сетям. Здесь нет умной ленты, которая показывает новости только по известному ей алгоритму. Новости от друзей не смешиваются с постами от групп. Многие паблики из социальных сетей уже давно перекочевали в Telegram. Плюс множество авторских каналов, которые есть только внутри мессенджера.

Докладніше

***

27.11.2017
Олег Дмитренко
За останні 12 місяців українці завантажили додаток Telegram майже 2 млн разів

За останні 12 місяців Telegram завантажили понад 74 мільйонів разів (дані за листопад 2016 – жовтень 2017). Про це свідчать дані App Annie.
Докладніше

СОЦІАЛЬНІ МЕРЕЖІ ЯК ВИЯВ ФОРМУВАННЯ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА

15.11.2017
«Мені не заплатили»: Швачки Zara додавали до одягу прохання допомогти

Майстрині з Туреччини вкладали у кишені пошитого одягу бірки, у яких ішлося, що їм не дають зарплату. Їм вдалося привернути увагу, оскільки користувачі соцмереж, які знайшли записки в одязі, започаткували флешмоб #BravoIscileriIcinAdalet (#СправедливістьДляПрацівниківBravo).
Докладніше

***

15.11.2017
Владимир Кондрашов
Полиция Киевской области отчиталась, что у неё лапки

В официальном твиттер-аккаунте Главного Управления Национальной полиции в Киевской области отчитались о том, что у них лапки (InternetUA).
Твит «Мы хорошие полицейские, но у нас лапки», появился в твиттере ГУНП в Киевской области около 14-30 15 ноября.
На данный момент запись уже удалена, но её можно просмотреть в архиве по ссылке, сообщает InternetUA.
В ГУ НП в Киевской области нашему изданию не смогли прокомментировать данный инцидент. В их официальном твиттер-аккаунте всего 319 подписчиков.
Согласно порталу Memepedia, мем «не могу, у меня лапки» – шутливая фраза, которая означает нежелание или неспособность выполнять какое-то действие. В начале 2017 года в пабликах «ВКонтакте» и твиттере начала распространяться картинка с котом-доктором, который не может открыть аптечку, потому что «у него лапки». В августе популярность мема достигла своего пика. Украинское представительство магазина техники «Эльдорадо» использовало фразу «У меня лапки» для своей рекламы.

***

20.11.2017

У Facebook набирає обертів новий флешмоб #читайукраїнське

Український інститут книги розпочав флешмоб Читай українське (Новое время).

Для поширення ідеї книголюбів у Facebook необхідно зробити допис про останню прочитану книгу українського видавництва, сфотографувати та поділитися враженням про неї.

Про це повідомила на своїй сторінці у Facebook заступниця директора Інституту книги з розвитку Анастасія Левкова.

Хештегами флешмобу стали: #читайукраїнське і #ireadua.

Інститут книги радить затегати друзів до посту, аби передати естафету.

Швидкий аналіз нового флешмобу у Facebook видає дописи як звичайних поціновувачів літератури, так і представників влади. Зокрема, серед першопрохідців #читайукраїнське – прем'єр Володимир Гройсман, міністр соціальної політики Павло Розенко, мінстр культури Євген Нищук, Посольство України в Китаї та інші.

***

27.11.2017

У соцмережах запустили флешмоб, присвячений праці волонтерів

У соціальних мережах 27 листопада дали старт флешмобу, присвяченому Всесвітньому дню волонтера, який відзначатимуть 5 грудня.

Докладніше

***

28.11.2017

Заради Палацу моряків одесити влаштували флешмоб у мережі // Сфотографуватися, щоб врятувати пам'ятку архітектури

Одесити влаштували незвичайний протест проти будівництва на території Палацу моряків на Приморському бульварі. Десятки людей зібралися біля старовинної будівлі, щоб підписати звернення до чиновників з проханням не допустити будівництва багатоповерхового готелю (Сьогодні).

Учасники сфотографувалися перед палацом з креативними плакатами, які свідчили «Сумую за концертам і кіно на моїй сцені» і «Мрію про реставрацію», і запустили в соцмережі флешмоб #SaveMe. Під цим хештегом городян просять публікувати свої знімки на тлі палацу і розповідати пов'язані з ним життєві історії, адже раніше там проходили концерти та кінопокази під відкритим небом.

Глава міськуправління з питань охорони об’єктів культурної спадщини Андрій Шелюгін заявив, що зараз проекту реконструкції будівлі немає. «Всі попередні проекти відхилили, оскільки вони спотворювали історичне середовище Приморського бульвару», – запевнив чиновник.

***

28.11.2017

Depo.ua запустив флешмоб, щоб змусити мера Кличка ремонтувати дороги

Усе, що потрібно для участі у флешмобі – сфотографувати яму на дорозі і запостити її на своїй сторінці у Facebook (Depo.ua).

Зокрема, Depo.ua розпочинає флешмоб #знайди_яму_для_Кличка.

Не забувайте вказувати адресу, де виявлена яма на дорозі.

Фотографії з виявленими вами ямами, будуть опубліковані на сайті Depo.ua.

БІЗНЕС І СОЦІАЛЬНІ МЕРЕЖІ

16.11.2017

YouTube блокирует блоггеров с обзорами iPhone X

Видеоролики, посвященные iPhone X и выложенные на YouTube, не могут заработать на рекламе, потому что видеохостинг ограничивает их сотрудничество с рекламодателями. При этом ролики не содержат никакого контента, нарушающего правила YouTube. Возможные причины – сбой в алгоритме оценки контента или его неадекватная реакция на букву «X».

Докладніше

***

20.11.2017

Как брендам вовлечь миллениалов?

Новое исследование SendinBlue отметило, что email и онлайн-опыт – ключ к сердцу большинства покупателей-миллениалов. 60 % представителей поколения Y предпочитают получить маркетинговое сообщение по е-мейлу, чем по другому каналу. Более две трети (68 %) миллениалов проверяют почту от двух до пяти раз в день. Относительно контента для рассылок: не делайте акцента на «предложениях» Черной пятницы и Киберпонедельника. Исследователи обнаружили, что треть миллениалов ждет 1 декабря, чтобы начать праздничный шоппинг. 40 % из них совершают половину покупок в онлайне. 25 % респондентов согласны отказать от покупок в оффлайне, но не в онлайне. Социальные медиа также играют важную роль для этого поколения. 40 % миллениалов пишут о своих достижениях в сетях – о новой работе, доме,

так как ищут одобрения своих достижений. Представители этого поколения также используют сети, чтобы задавать вопросы о продуктах, поделиться своими любимыми продуктами или опытом с брендом/магазинами (Marketing Media Review).

***

20.11.2017
Дмитрий Демченко
В чат-боте CoinyPay стали доступны переводы с карту на карту

В чат-боте CoinyPay для Facebook Messenger появилась возможность переводить деньги с карты на карту. Как отмечает основатель проекта Михаил Скричевский, бот работает с картами всех украинских банков (AIN.UA).

Изначально CoinyPay был создан для оплаты счетов в ресторанах через Facebook Messenger. Теперь бот можно использовать для перевода денег с карты на карту. Для начала пользователю нужно один раз ввести данные своей банковской карты и получить идентификационный код CoinyID. Чтобы отправить деньги, нужно узнать CoinyID получателя, ввести его и нужную сумму. Получателю нужно подтвердить транзакцию, нажав на соответствующую кнопку. Как отмечают представители CoinyPay, с помощью чат-бота пользователю не нужно знать и вводить реквизиты (номер карты) получателя. Также он может выбрать, с какой карты отправлять или на какую зачислять деньги. Перевод средств осуществляется без комиссии.

Также с помощью CoinyPay можно оплачивать счета в киевских ресторанах. Сейчас бот работает в Milk Bar, Dogs and Tails, Pho.Kiev и Tayger Pizza Bar.

СОЦІАЛЬНІ МЕРЕЖІ І ПРОБЛЕМИ СУСПІЛЬНОЇ БЕЗПЕКИ

Інформаційно-психологічний вплив мережевого спілкування на особистість

16.11.2017
Як соціальні мережі виявляють психологічні потреби особистості
Валерія Цихоня, практикуючий психолог

За якихось неповних 20 років людство перейшло на новий формат спілкування та передачі інформації. Це має свої зручності, але часто в новому контексті знаходять своє втілення й індивідуальні психологічні проблеми.

Докладніше

***

18.11.2017

Ученые связали детскую депрессию и тягу к самоубийству с использованием смартфонов

Чрезмерное увлечение подростков смартфонами может привести к повышению у них уровня депрессии и риска совершить суицид. Выводы были сделаны на основании опроса полумиллиона школьников в возрасте от 13 до 18 лет. Ученые указали на значительный рост количества суицидов среди девочек, а также увеличение количества страдающих от депрессии (InternetUA).

Дальнейшие опросы указали на то, что дети, сообщающие о психологических проблемах, чаще пользуются смартфонами – электронные устройства занимают значительную часть их свободного времени.

Оказалось, что подростки, который проводят за смартфоном более пяти часов в день, в 48 % демонстрируют суицидальные наклонности против 28 % у детей, использующих электронные девайсы около часа в день.

Дети, ведущие активную социальную жизнь, намного реже демонстрируют симптомы депрессии.

***

20.11.2017

Исследование: пользователи осознали опасность смартфонозависимости

Тревожность, депрессия, проблемы со сном, неспособность сконцентрироваться на значительное время – вот далеко не полный список проблем, с которыми могут столкнуться люди в результате чрезмерного использования смартфонов.

Докладншіе

***

20.11.2017

Facebook и другие социальные сети могут продлевать жизнь

В течение 6 месяцев сотрудники Калифорнийского университета мониторили активность 12 миллионов пользователей Facebook.

Дружба необходима нам для психологического благополучия, но преимуществами обладает не только офлайн-общение. Новое исследование ученых из Калифорнийского университета в Сан Диего показало, что социальные сети могут продлить жизнь, если мы будем использовать их правильно.

Докладніше

***

25.11.2017

По лайкам в Facebook можно узнать сексуальную ориентацию и IQ

Всего пара лайков в Facebook могут определить сексуальную ориентацию, а также политические или религиозные предпочтения пользователя, считают исследователи нескольких американских вузов, опубликовавшие свое исследование в журнале Big Data. И лучше иметь возможность скрыть эту информацию от рекламодателей.

Докладніше

Маніпулятивні технології

16.11.2017

Як у соціальних мережах маніпулюють українцями: розкрито схеми

У соціальних мережах останнім часом точаться справжні бої: “порохоботи” зчепилися із “зрадофілами”, “білі хакери” воюють з кремлівськими “ботами” і “тролями”. З території спілкування соцмережі перетворилися на місце, де політтехнологи і пропагандисти різного ґатунку маніпулюють суспільною свідомістю. Згідно зі звітом міжнародної правозахисної організації Freedom House, уряди по цілому світу не лише підтримують, а часто й ініціюють подібні маніпуляції, що загрожує укріпленням авторитарних режимів.

Докладніше

***

18.11.2017

Сотрудник рассказал о работе российской «фабрики троллей»

Сотрудник российской «фабрики троллей» рассказал о работе секретного агентства по производству контента, который видели миллионы американцев в преддверии президентских выборов в США 2016 года.

Докладніше

***

20.11.2017

Солдаты информационной войны. Как Ольгинские и другие тролли завоевывают интернет

Мощная и высокобюджетная фабрика интернет-троллей в России становится серьезной силой, существенно влияющей на ситуацию в собственной стране и способной расшатать мир.

Докладніше

***

18.11.2017

Facebook будет помечать публикации СМИ «индикатором доверия»

Соцсеть Facebook объявила об очередном способе борьбы с фейковыми новостями. Так, постепенно все информационные статьи в соцсети получат специальный «индикатор доверия», сообщает Cossa (Телекритика).

Кликнув на соответствующую кнопку, пользователи смогут узнать политику издателя в отношении фактчекинга, этики и правок. Кроме того, раздел будет включать информацию о владельцах и другие выходные данные новостного ресурса.

***

21.11.2017

Ольга Карпенко

От лайков к шантажу: как работает индустрия фейковых профилей на Facebook

Один подозрительный пост на Facebook порой может привести к раскрытию работы целой подпольной сети, чья цель – обманом заставлять пользователей делиться приватными изображениями и затем – шантажировать их.

Докладніше

***

21.11.2017

Google понизит российские RT и Sputnik в результатах выдачи

Интернет-гигант Google работает над алгоритмом, позволяющим снизить в поисковике уровень выдачи российских сайтов, на которых содержится пропаганда. Как пишет Motherboard, об этом сообщил исполнительный директора материнской компании Alphabet Эрик Шмидт на Форуме Галифакса по международной безопасности в Новой Шотландии (Телекритика).

На такой шаг Google идет после критики в свой адрес из-за того, что принадлежащие Кремлю сайты размещены в «Новостях» и рекламных платформах поисковика.

Как уточнил Шмидт, речь идет об изданиях Sputnik и RT.»"Мы работаем над тем, чтобы деранжировать подобные типы сайтов», – сказал он. При этом топ-менеджер уточнил, что полная блокировка не имеется в виду: «Мы не хотим блокировать эти сайты. Я – большой противник цензуры, но очень поддерживаю ранжирование».

***

22.11.2017

У Facebook з'явиться можливість перевірити сторінки на причетність до російської пропаганди

Facebook планує ввести розділ, де користувачі зможуть перевірити, чи є серед сторінок, на які вони підписані, пов'язані з російською пропагандою (InternetUA).

Його запуск планується протягом одного-двох місяців, передає hi-tech.ua.

До слова, те ж саме буде доступно і для аккаунтів у Instagram. Активність сторінок буде аналізуватися за період з січня 2015 року по серпень 2017-го.

***

23.11.2017

Facebook показуватиме юзерам, чи їх атакували російські «тролі»

Але він не зможе показати користувачам проплачений контент.

Facebook працює над розробкою нового інструменту, за допомогою якого користувачі зможуть побачити, чи були вони атаковані проплаченою рекламою та повідомленнями російських тролів (ТСН).

Функція запрацює вже до кінця 2018 року – пише USA Today.

«Новий інструмент, який, за твердженнями компанії Facebook, буде доступний до кінця року в меню "Довідкового центру", вперше надасть можливість користувачам дізнатися, чи були вони обдурені акаунтами, пов'язаними з Російським агентством інтернет-досліджень», – зазначається в повідомленні.

***

25.11.2017

Одессит через Интернет занимался антиукраинской пропагандой

Одессит через Интернет занимался антиукраинской пропагандой, агитировал и популяризировал террористические организации «ДНР/ЛНР». Также через соцсети призывал к изменению госграницы в пользу России (InternetUA).

В отношении указанного гражданина возбуждено уголовное дело и проводятся все необходимые процессуальные действия.

***

27.11.2017

Большинство русскоязычных аккаунтов в Twitter являются ботами

Около 60 % всех русскоязычных учетных записей в Twitter имеют вид автоматизированных, то есть ботов (InternetUA).

Об этом говорится в докладе Центра передового опыта НАТО по стратегическим коммуникациям (NATO Strategic Communications Centre of

Excellence), базирующегося в Риге исследовательского центра, который способствует трансформации альянса, сообщает «Голос Америки».

«Русскоязычные боты создают примерно 70 % всех российских сообщений о НАТО в странах Балтии и Польше. В общем 60 % активных русскоязычных учетных записей имеют вид автоматизированных. Для сравнения 39 % англоязычных учетных записей является ботами», – отмечает доклад.

Авторы доклада проанализировали 6 200 сообщений в социальной сети, каждый третий из которых был написан на русском языке. Всего было отобрано 3 500 активных пользователей, прокомментировавших действия НАТО в регионе. Подобная тематика, как особо отмечают авторы, «в целом не характерна для Twitter».

Аналитики отметили заметный рост активности этих аккаунтов во время проведения военных учений Steadfast Pyramid 2017 и Steadfast Pinnacle 2017 в Латвии, учений сил самообороны в Эстонии.

Исследование под названием Robotrolling отмечает, что его выводы основаны на анализе твитов, которые касались НАТО в странах Балтии и Польше.

***

25.11.2017

СБУ разоблачила механизм накрутки голосов в петициях

Сотрудники СБУ разоблачили механизм искусственной накрутки голосов при подании петиции про импичмент Президента Украины (InternetUA).

Оперативники СБ Украины установили, что петиция на сайте исполнительного комитета Ивано-Франковска была зарегистрирована через IP-адресс из Центральной Азии. Обращение было подписано гражданином Украины, который подозревается в сепаратизме, и в тот момент находился под стражей.

Сотрудники службы установили, что для создания адреса была создана электронная почта, зарегистрированная с использованием серверного оборудования, которое размещено на временно оккупированной территории Луганской области.

Когда петицию подписали более 700 пользователей, правоохранители установили, что только 6 из них были реальными, а остальные имели очевидные признаки «ботов».

***

28.11.2017

Facebook і Twitter передадуть Британії інформацію про російське втручання у Brexit

Facebook і Twitter погодилися передати інформацію стосовно розміщення у соцмережах особами, пов'язаними з Росією, постів у період референдуму щодо Brexit, за даними наглядової ради Палати громад (Mind).

Про це пише The Guardian з посиланням на голову комітету з цифрових технологій, культури, медіа та спорту британської Палати громад Деміана Коллінза.

Ця інформація, за словами Коллінза, допоможе краще скласти уявлення про те, чи намагалася Росія вплинути на голосування під час референдуму.

У Facebook повідомили, що поділяться цією інформацією на початку грудня, у Twitter запевнили, що нададуть відповідь в найближчі тижні.

В США Facebook уже передав в Конгрес інформацію стосовно можливого втручання Росії в американські президентські вибори. Згідно з цією інформацією, пости з фейковими новинами та пропагандою, розміщені «пітерською фабрикою тролів», побачило 126 млн людей.

Коллінз зазначив, що Великобританії та США відомо про діяльність тільки одного агентства в Санкт-Петербурзі, але, імовірно, можуть бути й інші.

Дослідники з Едінбургського університету ідентифікували 419 акаунтів у Twitter, через які поширювалася пропаганда з Росії з метою вплинути на внутрішню політику Великої Британії. З них під час референдуму було надіслано 3468 Twitter-повідомлень.

Спецслужби і технології «соціального контролю»

15.11.2017

Владимир Кондрашов

Провайдеры заявляют о подмене понятий в законодательстве о кибербезопасности

Операторы и провайдеры – члены ИнАУ 14 ноября призвали экспертов Совета Европы помочь в «противодействии мошеннической практике подмены понятий в законодательстве о кибербезопасности».

Докладніше

***

20.11.2017

Парламент ЕС рассматривает возможность блокировки веб-сайтов в рамках защиты прав пользователей

Согласно новому закону, принятому на днях в парламенте Евросоюза, теперь появится возможность заблокировать неугодные веб-сайты, которые по тем или иным причинам нарушают права пользователей.

Докладніше

***

20.11.2017

Власти Германии призвали родителей уничтожать смарт-часы их детей

Федеральное сетевое агентство Германии запретило продажу смарт-часов, ориентированных на детей. В качестве аргумента приводится тот факт, что эти устройства могут быть использованы для шпионажа. Более того, телекоммуникационный регулятор также настоятельно рекомендует родителям детей, у которых уже есть «умные» часы, поскорее избавиться от них (IGate).

Запрет немецкого агентства был изложен в конце доклада Европейской организации потребителей, в котором говорилось, что большинство детских смарт-часов с GPS-модулем имеет множество недостатков в плане безопасности, поэтому они уязвимы для хакеров. Злоумышленник может использовать микрофон и камеру для записи разговоров или подменить местоположение устройства, чтобы обмануть родителя, который следит за своим ребёнком.

Йохен Хоманн, президент Федерального сетевого агентства Германии, отметил, что такие устройства следует рассматривать как несанкционированную передающую систему. Он также заявил, что некоторые родители использовали смарт-часы для слежения за работой учителей в классе, что противоречит немецкому законодательству: запись или прослушивание частного разговора незаконны без разрешения всех участвующих в нём людей.

***

22.11.2017

Журналиста в Турции приговорили к трем годам тюрьмы за пост в Twitter

Суд приговорил редактора сайта турецкой оппозиционной газеты Cumhurriyet Огуза Гювена к трем годам лишения свободы за опубликованное на странице издания в Twitter сообщение о гибели прокурора Мустафы Альпера (InternetUA).

Гювена обвинили в пропаганде терроризма и попытке создать в турецком обществе негативное восприятие борьбы с организацией оппозиционного исламского проповедника Фетхуллаха Гюлена FETO.

Эту организацию турецкое правительство считает причастной к организации попытки государственного переворота в июле 2016 года.

Альпер, занимавшийся расследованием роли FETO в попытке госпереворота, погиб в мае текущего года, после того как его сбил грузовик.

На странице газеты Cumhurriyet в Twitter об этом происшествии первоначально сообщили с использованием выражения «грузовик переехал прокурора».

Спустя минуту после публикации, эта запись была удалена и заменена на другую, в которой говорилось о «трагической гибели прокурора в страшном ДТП».

Как отмечает агентство, Гювен утверждал, что первое сообщение разместил не он, а другой журналист. Суд, несмотря на это, объявил Гювена виновным, так как именно он был ответственным за аккаунт газеты в Twitter.

***

22.11.2017

СБУ пресекла деятельность трех антиукраинских администраторов в соцсетях

Сотрудники Службы безопасности Украины в ноябре прекратили деятельность трех антиукраинских администраторов в соцсетях, которые размещали материалы по указанию кураторов из российских спецслужб (InternetUA).

Во время реализации комплекса мер по обеспечению информационной безопасности страны сотрудники СБУ обнаружили новые доказательства использования спецслужбами РФ социальных сетей в интернете для нанесения ущерба государственной безопасности Украины. Правоохранители задокументировали противоправную деятельность жителей Киева, Тернополя и Черкасс, которые были администраторами антиукраинских сообществ в российской социальной сети «ВКонтакте».

Оперативники спецслужбы установили, что модераторы по указанию из России размещали в соцсети материалы с призывами к изменению границ территории Украины и в поддержку террористических организаций «Л/ДНР».

В рамках открытых уголовных производств сотрудники СБ Украины изъяли у администраторов компьютеры и мобильные телефоны с доказательствами подготовки и размещения антиукраинских материалов.

***

23.11.2017

Нацполиция и Microsoft подписали меморандум о сотрудничестве в сфере кибербезопасности

Национальная полиция и Microsoft Ukraine 22 ноября подписали меморандум о сотрудничестве в сфере информационной и кибербезопасности. Заключение соглашения стало результатом встречи заместителя главы Национальной полиции Украины Константина Бушуева и генерального директора Microsoft Ukraine Надежды Васильевой, передает пресс-служба полиции (InternetUA).

Сообщается, что в ходе встречи участники обсудили вопросы сотрудничества в области информационных технологий, информационной и кибербезопасности. Также обсуждалось о создание и модернизация

информационной инфраструктуры, обеспечение автоматизации, прозрачности и контролируемости внутренних процессов.

«Такое сотрудничество поможет нам в вопросах построения комплексных решений технического обеспечения нашей деятельности в масштабах государства, применение инноваций в сфере государственного управления, а также оптимизации имеющегося ресурса с целью уменьшения влияния человеческого фактора на деятельность полиции», – отметил Бушуев.

Кроме того, участники встречи обсудили перспективу развития взаимоотношений между Национальной полицией и компанией-производителем программного обеспечения, частности, речь идет о формировании с помощью Microsoft Ukraine своеобразного «ядра» из числа работников Национальной полиции, отвечающих за обеспечение информационной и кибербезопасности ведомства.

Проблема захисту даних. DDOS та вірусні атаки

15.11.2017

Центробанк Нидерландов задействует хакеров для атак на банки страны

Центральный банк Нидерландов (De Nederlandsche Bank, DNB) создаст команду из хакеров и экспертов в области кибербезопасности для атак на финансовую инфраструктуру страны. Таким образом регулятор намерен протестировать и улучшить киберзащиту финучреждений, сообщает издание Financieele Dagblad.

Докладніше

***

15.11.2017

Карта будущего: изобретена платежная карта с временным ПИН-кодом и экраном

Инновационная карта Da Vinci Choice представляет собой целый компьютер, обещает полностью устранить необходимость в паролях и трансформировать сферу платежей.

Докладніше

***

15.11.2017

Создана система, которая защитит бизнес от популярных паролей

Компания Shape Security запустила систему Blackfish, предназначенную для профилактики использования хакерами похищенных или утекших паролей. Пользователи часто обходятся одной-двумя комбинациями логинов и паролей на десятках разных ресурсов, поэтому утечка логинов с одного может представлять угрозу сразу для многих других.

Докладніше

***

15.11.2017

В полиции рассказали о новых уловках интернет-мошенников

Украинцам стоит помнить о мошенниках, которые идут в ногу со временем, активно осваивают интернет, пользуются излишней доверчивостью сограждан, а потому, чтобы избежать потерь, людям не стоит сообщать секретные сведения о себе незнакомцам (InternetUA).

Об этом предупредили в пресс-службе Национальной полиции.

Стражи порядка напомнили, что украинцам нужно быть осторожными при выполнении денежных операций, особенно через интернет.

Также украинцам советуют для расчетов в интернете использовать отдельные платежные карты с ограниченным лимитом, которые предусмотрены только для этого и не дают возможности использовать карту для операций в торговых сетях или снятия наличных.

Отдельно полицейские посоветовали использовать сайты только известных и проверенных интернет-магазинов, а в случае возникновения сомнений – отказаться от предложения и поискать другие варианты.

***

15.11.2017

Дмитрий Малышко

Шпионская угроза:Google Play удалит приложения, которые используют API

Google удалит из Play Store все приложения, предоставляющие специальные возможности (InternetUA).

Изменения не коснутся программ, предназначенных для людей с ограниченными возможностями, сообщает Корбин Девенпорт, разработчик софта, в том числе расширений для браузера Chrome.

Докладніше

***

15.11.2017

Британское правительство обвинило РФ в атаках на свои энергосети

За последний год «русские хакеры» атаковали британские электроэнергетические, телекоммуникационные и медиакомпании. Такое заявление сделал глава британского Национального центра по борьбе с киберпреступностью (National Cyber Security Centre, NCSC) Киаран Мартин (Ciaran Martin) на саммите Times Tech Summit в Лондоне (InternetUA).

«Я не могу вдаваться в подробности в делах разведки, но я могу подтвердить, что вмешательство России, фиксированное Национальным центром по борьбе с киберпреступностью в течение года, включает атаки на британские организации медиа, телекоммуникационного и энергетического секторов», – приводит слова Мартина издание The Telegraph.

По словам главы NCSC, для борьбы с угрозой ведомство активно привлекает к сотрудничеству международных партнеров, а также промышленное и гражданское общество. За год своего существования NCSC заблокировал десятки миллионов кибератак и отреагировал на 590 инцидентов, в том числе на атаки с использованием вымогательского ПО WannaCry. Данные атаки связываются с Северной Кореей, однако правительство Великобритании более всего обеспокоено по поводу именно «русских хакеров».

***

15.11.2017

Из подключенных к интернету банкоматов можно создать ботнет

Подключенные к интернету банкоматы могут быть обнаружены по ключевым словам с помощью специальных поисковых сервисов, а затем включены в ботнет.

По словам исследователей, многие банкоматы работают на базе устаревшей версии ОС Windows XP, что делает их уязвимыми по умолчанию.

Докладніше

***

15.11.2017

Хакеры помогли Пентагону исправить тысячи уязвимостей

Спустя почти год после того, как Пентагон запустил программу раскрытия уязвимостей, ведомство получило 2837 достоверных отчетов об уязвимостях от примерно 650 хакеров из 50 стран по всему миру, указывается в пресс-релизе на портале HackerOne (InternetUA).

Более 100 обнаруженных уязвимостей были критическими или представляли серьезную опасность для систем ведомства.

Докладніше

***

16.11.2017

Расширение для Chrome собирает данные пользователей из Facebook и LinkedIn

Эксперт в области кибербезопасности Лоуренс Абрамс (Lawrence Abrams) обнаружил в каталоге Chrome Web Store подозрительное расширение Browse-Secure, позиционируемое как инструмент, гарантирующий пользователям безопасный поиск. В действительности программа собирает данные (имя, адрес электронной почты, информацию о поле, номере мобильного телефона и адресе) из учетных записей пользователей в Facebook и LinkedIn и отправляет их на удаленный сервер.

Докладніше

***

16.11.2017

Пользователи Telegram манипулируют курсами криптовалют по своему желанию

Telegram стал рассадником криптовалютных трейдеров, которые организуют в мессенджере группы с десятками тысяч участников. Распространяя рекламу в Telegram, они искусственно повышают стоимость криптовалют благодаря активной покупке, а потом сбывают их ничего не подозревающим подписчикам других каналов.

Докладніше

***

18.11.2017

Россия оказалась главной целью китайских хакеров

Эксперты в области интернет-безопасности заметили активизацию китайскоговорящих хакеров и их нацеленность на Россию. Об этом говорится в отчете «Лаборатории Касперского» (InternetUA).

Согласно информации, предоставленной в отчете «Лаборатории глобальных исследований и анализа» (GReAT) за третий квартал 2017 года, 10 из 24 спланированных атак связаны с группировками, говорящими на китайском языке.

Кроме того, специалисты заметили, что таргетированные нападения связаны с государственными проектами России. Так, в июле была обнаружена атака IronHusky на российские и монгольские авиакомпании. Перед этим страны договорились о сотрудничестве по нескольким проектам, касающимся воздушной обороны Монголии.

Другая кибератака была зафиксирована во время переговоров России и Индии в атомном секторе. Еще одно нападение, в ходе которого были скомпрометированы популярные программы Netsarang и CCleaner, специалисты

связывают с попыткой злоумышленников проникнуть в корпоративные сети российских компаний.

В октябре правительство США опубликовало совместный отчет ФБР и министерства внутренней безопасности, в котором рассказало об увеличении числа хакерских атак в отношении энергетических компаний и промышленных предприятий.

***

18.11.2017

Хакеры похитили персональные данные участников АТО

Хакеры похитили персональные данные участников АТО, взломав компьютер подразделения Государственной службы Украины по делам ветеранов войны и участников антитеррористической операции, сообщает пресс-служба Киберполиции (InternetUA).

«Мы установили компьютер, взломав который, хакеры получили доступ ко всей информации, которая была размещена не только на данном устройстве, но и во всей локальной сети подразделения. Сейчас мы проводим тщательный осмотр пораженной техники», – заявил начальник департамента киберполиции Сергей Демедюк.

По его словам, пользователь соцсети под вымышленным именем предлагал загрузить архивы с персональной информацией участников АТО.

Киберполиция определяет пути поражения компьютера вирусом и устанавливает причастных к хакерству.

***

19.11.2017

Блокчейн вместо отпечатков пальцев – новый способ идентификации личности в Канаде

Чтобы пройти стопроцентную идентификацию личности необходимо выполнить множество процедур, начиная от сравнения отпечатков пальцев и заканчивая измерением диафрагмы (InternetUA).

Однако большинство биометрических систем нуждаются в сложной и дорогостоящей инфраструктуре. Более простые и дешевые методы зачастую оказываются ненадежными и даже небезопасными.

Канада нашла креативное решение с оптимальным соотношением стоимости и надежности. Новая система, основанная на технологии блокчейн позволит идентифицировать граждан Канады мгновенно и со 100 % точностью.

Сила блокчейна

Основой для этого эффективного с экономической точки зрения решения стала технология блокчейн. Система позволяет гражданам Канады хранить свои персональные данные на одном устройстве, например, смартфоне.

Когда государственные структуры либо банковские учреждения запросят личную информацию, гражданину достаточно будет предоставить секретный ключ, который откроет доступ ко всем персональным данным.

Система предлагает простое решение для жителей Канады, которые не хотят, чтобы их данные хранились в нескольких базах данных и были уязвимы для хакерских атак. Для граждан других государств некоторые частные компании, такие как SelfKey, предлагают аналогичные решения.

С помощью данной системы пользователи смогут подтвердить свою личность используя специальное приложение на смартфоне или девайсе с операционной системой Windows. Система будет открыта для пользователей, начиная с первой половины 2018 года.

***

20.11.2017

Илья Кабачинский

Авиакомпании владеют вашими личными данными. И постоянно их используют

Данные о своих пользователях собирают не только интернет-сервисы. Издание Bloomberg подготовило материал на тему сбора и дальнейшего использованния информации о своих пассажирах авиакомпаниями. Оказывается, они знают о своих клиентах почти все: что вы любите есть, пить, и даже, когда у вас день рождения.

Докладніше

***

20.11.2017

Крипто-мафия: хакеры нашли новый способ взлома биткоин-кошельков

По мере роста интереса пользователей, в том числе и украинских, к майнингу и криптовалютам, пропорционально увеличилась и заинтересованность мошенников к крипто-кошелькам. Все чаще целью хакеров становятся на только отдельные аккаунты, но и целые криптобиржи.

Докладніше

***

20.11.2017

Золото оператора. Как мобильщики превращают наши данные в деньги

Big Data стала новой валютой. Все говорят, что Facebook и Google бесплатны. Но мы, пользователи, за их сервисы расплачиваемся нашими

данными. Компании их пакуют и продают тем, кому это интересно. Эти слова в числе прочих были адресованы выпускникам Big Data School от Киевстар.

Докладніше

***

21.11.2017

Google втайне следит за местоположением пользователей всех Android-устройств

Google может по своему желанию отследить местоположение пользователей устройств на Android, даже если те предпочли вручную отключить службы геолокации, выяснили журналисты Quartz. Сбор данных происходит в периоды, когда смартфон или планшет подключен к Интернету, чтобы иметь возможность отправлять информацию о наших перемещениях прямиком на сервера компании (InternetUA).

В Google подтвердили факт сбора данных, уточнив при этом, что все полученные сведения не подлежат долгосрочному использованию, а потому не сохраняются. После обращения журналистов Quartz представители компании пообещали, что предпримут все необходимые меры по предотвращению дальнейшей слежки за пользователями Android-устройств, отключивших службы геолокации.

По словам сотрудника пресс-службы Google, отслеживая местоположение своих клиентов, компания всего-навсего рассчитывала повысить скорость передачи сообщений. Первые опыты в этой области в Маунтин-Вью начали проводить еще в январе 2017 года. Как именно информация о нахождении пользователей могла ускорить работу службы текстовых сообщений, неизвестно.

***

22.11.2017

«Доктор Веб» обнаружил новый бэкдор для Linux

Специалисты компании «Доктор Веб» обнаружили новый Linux-бэкдор, что косвенно свидетельствует о неослабевающем интересе к операционным системам семейства Linux со стороны вирусописателей (ITnews).

Троянец, получивший наименование Linux.BackDoor.Hook.1, был обнаружен вирусными аналитиками в библиотеке libz, которая используется некоторыми программами для функций сжатия и распаковки. Он работает только с бинарными файлами, обеспечивающими обмен данными по протоколу SSH. Весьма необычен способ подключения злоумышленников к бэкдору: в отличие от других похожих программ, Linux.BackDoor.Hook.1 вместо текущего открытого сокета использует первый открытый сокет из 1024, а остальные 1023 закрывает.

Бэкдор Linux.BackDoor.Hook.1 может скачивать заданные в поступившей от злоумышленников команде файлы, запускать приложения или подключаться к определенному удаленному узлу. Этот троянец не представляет опасности для наших пользователей – его сигнатура добавлена в базы Антивируса Dr.Web для Linux.

***

22.11.2017

Хакери вкрали персональні дані 57 млн клієнтів і водіїв Uber. У компанії приховували це рік

У 2016 році хакери вкрали дані 57 млн клієнтів і водіїв онлайн-сервісу замовлення таксі Uber (Espreso.tv).

Компанія приховала інцидент, заплативши хакерам $100 тис., щоб видалити дані.

Під час зламу були вкрадені імена, електронні адреси та номери мобільних телефонів 50 млн користувачів Uber по всьому світу. Також в розпорядження хакерів потрапили особисті дані 7 млн водіїв, включаючи 600 тис. номерів водійських посвідчень в США.

При цьому компанія зазначає, що дані про кредитні картки, маршрути поїздок та інша інформація не потрапила до хакерів.

«Хоча ми не бачили доказів шахрайства або зловживання, пов'язані з інцидентом, ми стежимо за порушеними рахунками і позначили їх для додаткового захисту від шахрайства», – коментує виконавчий директор Uber Дарі Хосровшахи.

Він заявив, що не збирається виправдовуватися за те, що сталося.

***

22.11.2017

Библия заразила пользователей опасным вирусом

Специалисты обнаружили в Google Play вредоносное программное обеспечение, замаскированное под приложение для чтения Библии. Об этом сообщает The Next Web со ссылкой на отчеты компаний McAfee и Palo Alto Networks, специализирующихся на информационной безопасности (InternetUA).

По данным экспертов, в действительности сервис не только позволял читать Библию на корейском языке, но и превращал устройство на базе Andriod в часть бот-сети. При этом сотрудники Palo Alto Networks утверждают, что приложение находилось в официальном магазине Play Store и было одобрено модераторами, но McAfee опровергает эту информацию.

Вредоносное ПО было загружено более 1,3 тысячи раз. Специалисты полагают, что атака была направлена в первую очередь на владельцев устройств компании Samsung. Подобное заражение обычно приводит к замедлению работы смартфонов и появлению многочисленных сбоев.

Вероятным распространителем называют хакерскую группировку Lazarus. Некоторые специалисты полагают, что за ними стоят злоумышленники из Северной Кореи.

***

21.11.2017

Хакеры украли более 10 млн грн с банковских карт украинцев

Сотрудники Службы безопасности Украины (СБУ) совместно с прокуратурой разоблачили в Киеве хакерскую группировку, участники которой похищали средства с банковских карт клиентов банков, в том числе государственных. По предварительной информации, злоумышленники успели украсть более 10 млн грн с карт граждан (InternetUA).

Как установили правоохранители, используя вредоносное ПО хакеры инфицировали банковские сети для получения доступа к данным, дублировали реквизиты платежных карточек с помощью специальных технических средств негласного получения информации. Согласно сообщению СБУ, злоумышленники сняли деньги с более чем 1,5 тыс. банковских карт.

В ходе обысков правоохранители обнаружили компьютерную технику с установленным вредоносным ПО и перепиской хакеров, специальное оборудование для считывания и записи поддельных банковских карт, мобильные телефоны и банковские карты, подтверждающие проведение нелегальных сделок. Также полиция изъяла 1,2 млн грн, пистолеты Макарова, «ТТ», автомат Калашникова з глушителями и большое количество патронов к ним.

В настоящее время четверым злоумышленникам объявлено о подозрении в совершении преступлений. Они задержаны согласно ст. 208 Уголовно-процессуального кодекса Украины. Для всех избрана мера пресечения в виде содержания под стражей.

***

21.11.2017

Эксперты предупредили пользователей Tinder об угрозе шантажа со стороны «русских» хакеров

Национальный центр кибербезопасности Великобритании (National Cyber Security Centre, NCSC) предупредил о возможности взлома профилей пользователей в Facebook и других социальных сетях через приложение Tinder (InternetUA).

Эксперты центра выявили уязвимость в защите популярного сервиса для знакомств, которая проявляется в процессе загрузки пользователем новых фотографий в папку Tinder. В этот момент хакер удаленно может получить коды доступа к Facebook, так как многие пользователи авторизуются в сервисе через свою учетную запись на соцресурсе.

По словам исследователей, наибольшей угрозе подвергаются владельцы Android-устройств, работающих на базе устаревшего программного обеспечения.

Как отметил эксперт Энтони Глис (Anthony Glees), публикуя личную информацию в интернете, пользователи раскрывают важные и конфиденциальные подробности о себе, которые могут попасть в руки хакеров.

«Это чистое золото для русских, китайцев и всех, кто хочет проэксплуатировать эти факты», – отметил Глис. Исследователь порекомендовал пользователям не публиковать в Facebook, Tinder и других подобных сервисах персональную информацию, например, о привычках и предпочтениях, «о которых не хотели бы, чтобы узнала мама».

***

23.11.2017

ПриватБанк застерігає від нового шахрайства в Instagram

У соціальній мережі Instagram з'явився новий вид шахрайства. ПриватБанк закликав користувачів цієї соцмережі бути обачними, не переходити за сумнівними посиланнями, не реєструватися на невідомих сайтах та не передавати шахраям персональні дані (InternetUA).

Про це повідомляє прес-служба ПриватБанк.

У стрічці новин Instagram почали з'являтися рекламні повідомлення, в яких йдеться, що кожен громадянин України відтепер може отримати 3800 гривень. У коментарях фейкові акаунти користувачів розповідають, що їм буцімто вже зарахували ці гроші на картку ПриватБанку.

У разі переходу за рекламним посиланням користувачу пропонують зареєструватися й отримати гроші, продавши частину свого інтернет-трафіку. Під час реєстрації в користувачів просять ввести особисті дані та інформацію про рахунки в ПриватБанку.

***

22.11.2017

Хакеры атаковали покупателей AliExpress

Эксперты специализирующейся на IT-безопасности компании Check Point Software Technologies в результате проведенного исследования обнаружили уязвимость на сайте популярной торговой площадки. Она могла автоматически перенаправлять покупателей, зашедших на AliExpress, на сайт злоумышленников (InternetUA).

Там вредоносный код, вероятно, похищал ценную информацию. Также пользователям могли демонстрировать поддельное всплывающее окно с предложением указать данные банковской карты. В крайнем случае, ресурс мог быть зараженным вредоносной программой.

Уязвимость была обнаружена еще полтора месяца назад, но про нее стало известно только сейчас. Администрация площадки AliExpress оперативно отреагировала и устранила проблему.

***

22.11.2017

100 % организаций по всему миру подверглись мобильным атакам - Check Point

Компания Check Point представила результаты первого исследования атак на мобильные устройства в корпоративных средах.

Согласно данным, полученным от 850 компаний на четырех континентах, мобильные устройства, используемые в организациях, уязвимы для атак вне зависимости от операционной системы – Android или iOS.

Докладніше

***

26.11.2017

Раскрыты подробности деятельности хакерской группировки Fancy Bear

Хакерская группировка Fancy Bear, которую связывают с российскими спецслужбами, в течение трех лет арендовала серверы у британской компании Crookservers, которые использовались для кибератаки на компьютерную сеть немецкого парламента, перехвата трафика сайта нигерийского правительства и взлома устройств Apple, пишет BBC. Как предполагают эксперты, Fancy Bear, также известная как APT28, Sofacy, Iron Twilight и Pawn Storm, также причастна ко взлому серверов Национального комитета демократической партии США во время избирательной кампании в 2016 году.

Докладніше

***

27.11.2017

Сеть Bitcoin Gold снова оказалась под прицелом хакеров

26 ноября команда Bitcoin Gold сообщила пользователям сети о критической киберугрозе, связанной с заменой хакерами установочного файла Windows-кошелька в репозитории проекта на GitHub (InternetUA).

В период с с 21 по 25 ноября установочный файл Windows-кошелька на странице загрузки на официальном сайте и на странице проекта на GitHub были предположительно заменены на вредоносное программное обеспечение с целью кражи средств и личной информации пользователей.

Как отметила команда, антивирусные программы не реагируют на угрозу, но пользователям рекомендуется немедленно удалить файл и проверить компьютер на наличие скрытого вредоносного ПО.

Представители проекта утверждают, что угроза устранена, но напомним, что на прошлой неделе ForkLog стало известно о масштабной уязвимости в электронном кошельке Mybtgwallet, в результате которой злоумышленники похитили от $2,5 млн до $3,3 млн, несмотря на то, что изначально команда Bitcoin Gold заверила, что кошелек безопасный.

Стоит отметить, что после официального запуска работа основной сети Bitcoin Gold саботировалась BTG-пулом Suprnova, который не добавил поддержку протокола Segregated Witness, заблокировав подтверждения блоков других пулов.

***

26.11.2017

Мошенники требуют от киевлян погасить несуществующие долги

Аферисты требуют от киевлян погасить несуществующие долги и ведут рассылку от ПАО «Киевэнерго». Об этом сообщили в пресс-службе компании (InternetUA).

Злоумышленники рассылают электронные письма с бесплатных почтовых сервисов от имени «Киевэнерго» и требуют погасить задолженность.

В компании отметили, что «Киевэнерго» информирует о наличии задолженности с помощью операторов контакт-центра, по смс и рассылает письма на официальных бланках.

***

27.11.2017

«Доктор Веб» исследовал нового банковского троянца

Троянцы, предназначенные для хищения денег с банковских счетов, представляют серьезную угрозу. Новый банковский троянец, получивший наименование Trojan.Gozi.64, основывается на исходном коде предшествующих версий Trojan.Gozi, который уже долгое время находится в свободном доступе. Как и другие представители этого семейства, Trojan.Gozi.64 может заражать компьютеры под управлением 32- и 64-разрядных версий Windows.

Докладніше

***

27.11.2017

Представители Imgur подтвердили факт взлома базы данных их сервиса

Владельцы одного из самых крупных хостингов для обмена изображениями подтвердили тот факт, что их базу данных взломали в 2014 году (InternetUA).

В ходе взлома 1,7 миллиона e-mail-адресов и паролей, пусть и зашифрованных SHA-2-алгоритмом, были украдены. Несмотря на то, что помимо адресов электронной почты и паролей, никаких других персональных данных клиентской базы не пострадало, это всё ещё часть информации от общего числа 150 миллионов ежемесячных посетителей ресурса.

Информация об утечке была скрыта до тех пор, пока не попала в руки Троя Ханта (Troy Hunt), владельца сервиса оповещаний о попытках взлома «Have I been Pwned». Сам Хант, получив эти данные, незамедлительно проинформировал представителей ресурса Imgur о событии, после чего работники сервиса запустили кампанию по сбросу паролей взломанных учётных записей с просьбой к владельцам обновить их персональные данные.

На данный момент на сервисе Imgur проводится расследование данного дела и подводится общее количество пострадавших пользователей. Однако, по заверениям представителей сервиса, система безопасности Imgur на данный момент значительно надёжнее, чем три года назад, и теперь база данных паролей и электронных адресов шифруется с использованием алгоритма bcrypt, признанного более надёжным, чем хеширование данных алгоритмом SHA-2.

Все пострадавшие уже получают письма с просьбой сменить свой электронный адрес и пароль от учётных записей Imgur и на других ресурсах, в том случае, если пострадавший использует те же данные для других сервисов.

***

28.11.2017
Сколько стоит взломать Face ID?

Ранее в этом месяце экспертам вьетнамской компании Bkav, специализирующейся на исследованиях в области кибербезопасности, удалось обойти защиту Face ID. Для этой цели на 3D-принтере была напечатана маска, в подробностях повторяющая лицо условного владельца. К сожалению авторов эксперимента, далеко не все поверили в их честность с первого раза. Чтобы уверить всех в своей правоте, Bkav сняли новое, более детальное видео (Украинский телекоммуникационный портал).

Судя по всему, новый ролик был снят одним кадром, либо – нужно отдать монтажерам Bkav должное – смонтирован настолько гладко, что разглядеть склейки попросту нереально. По ходу этого видео уже знакомый нам ведущий опровергает предположения зрителей о том, что в первом эксперименте он за кадром позволил Face ID записать в память маску, вручную введя пароль доступа, а также отключил функцию «Смотреть в камеру».

На этот раз он демонстративно обнуляет память Face ID и заново регистрирует свое лицо, после чего разблокирует смартфон. Следующим этапом эксперимента стала попытка заставить интерфейс идентифицировать

маску вместо владельца. Защиту удалось обойти спустя всего несколько мгновений, а распознать подмену Face ID не помогла даже активная функция «Смотреть в камеру», благодаря которой в теории снижается вероятность ложного срабатывания.

Объясняя, как Bkav удалось создать такую маску, в пресс-службе компании заявили, что для «снятия» трехмерного слепка с лица условного владельца была задействована установка, опоясанная несколькими камерами. Получив снимки, сделанные с разных ракурсов, специалисты вручную сформировали объемное изображение, которое было напечатано с использованием 3D-принтера. Впоследствии готовая маска подверглась ручной обработке для имитации естественного человеческого взгляда.

ДОДАТКИ

Додаток 1

15.11.2017
Skype запускает аккаунты нового типа

Microsoft вскоре намерен начать тестирование нового типа аккаунта Skype, ориентированного на индивидуальное удаленное предпринимательство: репетиторство, онлайн-консультации и пр. (InternetUA).

Skype для репетиторов

В Skype появится специализированный тип аккаунта – Skype Professional Account – для людей, которые используют этот мессенджер для индивидуального предпринимательства: удаленного репетиторства, проведения мастер-классов, консалтинга, инструктажа и пр.

Новый тип аккаунтов объединит в себе классические опции непосредственного общения с календарем, почтой и платежной системой.

В дополнение к этому в аккаунте будет предусмотрено создание расширенного профиля его владельца с подробной информацией о его услугах, что, по сути, станет самостоятельным микросайтом.

Пользователи нового типа аккаунта смогут импортировать в него весь контакт-лист из своей учетной записи, в то время как для его оппонентов при общении с ним через его новый аккаунт не произойдет никаких изменений.

На данный момент в официальном блоге Skype говорится, что новый тип аккаунта изначально рассчитан только на десктопную версию мессенджера. В тестовом режиме новый сервис планируется запустить в США. Как минимум во время этого периода он будет бесплатным. Воспользоваться им сможет ограниченное число энтузиастов. Для этого им потребуется заполнить анкету в своей учетной записи.

Недавние изменения в судьбе Skype

Отметим, что данный анонс фактически происходит на фоне недавнего сообщения владельца мессенджера – компании Microsof, которая в конце

сентября 2017 г. объявила о том, что намерена заменить корпоративный мессенджер Skype for Business другим сервисом для бизнес-коммуникации – Microsoft Teams, запущенным менее года назад.

Skype for Business был создан в 2015 г. на основе предыдущего корпоративного мессенджера Microsoft – Lync. Запуск Microsoft Teams сам по себе являлся признаком того, что Skype for Business осталось жить недолго, писало в сентябре издание The Verge. В настоящий момент Teams уже может использовать большую часть его функциональности.

(вгору)

Додаток 2

17.11.2017
Facebook обновила сервис Stories

Компания Facebook выпустила крупное обновление в рамках сервиса Facebook Stories, который позволяет людям обмениваться разными событиями жизни друг с другом (InternetUA).

В рамках обновления данный сервис имеет общее название Stories и доступен в рамках непосредственно Facebook и стороннего клиента Messenger Day.

Теперь неважно, где именно размещена история – пользователи могут просмотреть её с любого из двух сервисов, и после этого она будет отмечена как увиденная для вашей учётной записи в целом, а не для конкретно взятого приложения, как раньше.

Но, несмотря на это, использование камеры в обоих приложениях всё ещё работает по-разному. В случае с Messenger она ориентирована на создание текстовых сообщений поверх видеоряда, в то время как камера в мобильном приложении Facebook эксплуатирует технологии дополненной реальности, используя возможности накладывания цветовых фильтров и масок на отснятый сюжет. В обозримом будущем эти функции также намерены объединить в рамках обеих программ.

Помимо этого также было принято решение отказаться от Facebook Direct, который предоставлял возможность отправлять сообщения с предустановленным сроком, по истечении которого оно удаляется. Сама возможность отправлять подобные сообщения остаётся, но не в рамках отдельного сервиса, а как дополнительная возможность для приложения Messenger.

Отдельным и, пожалуй, самым приятным пунктом стала возможность создавать коллективные истории в рамках различных мероприятий, концертов и прочих подобных событий, где каждый отдельный человек может внести свой вклад в общий сюжет. Для этого необходимо выбрать модератора истории, который будет фильтровать добавляемый контент и редактировать его, согласовывая свои действия с остальными участниками события.

(вгору)

Додаток 3

21.11.2017

Facebook добавит маркер отличия для проверенных издательств

Компания Facebook ввела новую отметку, которой будут награждаться новостные посты издательств, прошедших дополнительную проверку на подлинность информации (InternetUA).

Здесь надо сделать оговорку для пояснения терминологии. «Издательства» в рамках Facebook являются очень условной аналогией «пабликов» в «ВКонтакте» с той поправкой, что, как правило, за издательствами в Facebook гораздо чаще стоят настоящие предприятия, книжные издательства и реально существующие новостные ресурсы, которым важна своя репутация и которые заинтересованы в том, чтобы пользователи доверяли им.

Данный маркер называется индикатором доверия, или же Trust Indicator, с помощью которого пользователь может получить информацию по издательству, которое поделилось данной информацией, и тем фактом, насколько факты в ней являются достоверными. Благодаря индикатору доверия пользователи могут ознакомиться с их политикой в отношении подачи фактов, их содержательности и добросовестности в рамках обращения с преподнесённым материалом.

Таким образом представители компании Facebook надеются помочь пользователям отфильтровывать недобросовестные новостные ленты и находить наиболее актуальный и полезный материал – с одной стороны, а с другой – уменьшить общий уровень дезинформации в рамках хотя бы своей платформы и мотивировать издателей тщательнее следить за материалом, который публикуется под их именем.

Помимо этого к публикуемому материалу также планируется добавить вкладку со статьями схожего содержания и подробную информацию по издательству. Данное нововведение реализуется в рамках общего проекта Trust Project, работа над которым началась ещё в прошлом месяце.

(вгору)

Додаток 4

20.11.2017

Twitter будет следить за поведением проверенных пользователей за пределами собственного ресурса

Не так давно представителей всех крупных компаний и социальных сетей США вызвали в Конгресс для обсуждения проблем проверки пользователей и того, какой материал допускается к распространению в рамках предоставляемых сервисов. Ответная реакция с посылом ужесточить процедуру верификации не заставила себя ждать. Отныне лишиться значков

подтверждения учётной записи в рамках Twitter можно не только за неправомерные действия на просторах самого ресурса, но и за его пределами (Центр информационной безопасности).

Эта поправка к общему своду правил Twitter была добавлена совсем недавно, уже после изначального пересмотра пунктов, касающихся подтверждения личности. Теперь это звучит как «Причины лишения подтверждения учётной записи могут касаться действий как в рамках Twitter, так и за его пределами». Если совсем простыми словами – в рамках Twitter пользователь всё ещё может поддерживать свою репутацию честного и порядочного гражданина, но если представители компании обнаружат на его стене «ВКонтакте» или в Facebook неожиданные посты с материалом экстремистского характера, любой другой оскорбительный или подозрительный контент – значок подтверждения тут же снимается, а сам пользователь берётся на заметку в соответствующих службах. Дальнейшие санкции, соответственно, о чём не говорится прямо, но что подразумевается – в зависимости от поведения самого пользователя – могут быть самыми разными, от простого удаления учётной записи до донесения о нём властям.

На фоне новой поправки службы поддержки Twitter намерены провести повторную проверку ранее подтверждённых учётных записей общим количеством в 287 тысяч пользователей. Каким именно образом будет происходить данная проверка, тем не менее, не разглашается.

Общая цель нового пункта правил – сделать значок подтверждения о проверке учётной записи не только фактом того, что за ней стоит реальная личность, но и прямым доказательством её правомерности и порядочного поведения как в рамках непосредственно пользователей Twitter, так и хотя бы на просторах мировой Сети.

(вгору)

Додаток 5

27.11.2017
Telegram-каналов об образовании, науке и криптовалюте

10 Telegram – отличная альтернатива социальным сетям. Здесь нет умной ленты, которая показывает новости только по известному ей алгоритму. Новости от друзей не смешиваются с постами от групп. Многие паблики из социальных сетей уже давно перекочевали в Telegram. Плюс множество авторских каналов, которые есть только внутри мессенджера (AIN).

Сегодня @themarfa отобрали десятку крутых каналов об образовании, науке и криптовалюте.

«Темная Сторона Интернета» – канал с авторскими статьями об анонимности и безопасности, чёрных рынках и тёмном интернете. Качественные переводы с английского и эксклюзивные материалы.

In Crypt We Trust – первый мейнстримовый канал о блокчейне и альтернативной валюте. Если вы всегда хотели заиметь биткоины, но даже не

знаете, где их купить, этот канал для вас. Авторы легко и популярно рассказывают о новостях из мира криптовалют, делятся аналитикой и прогнозами.

Название канала говорит само за себя. Здесь собраны статьи про технологии, гаджеты, науку и космос со всего интернета. Авторы вручную отбирают только самое лучшее и предоставляют научную картину дня своим читателям в удобном формате.

Официальный канал научно-популярного журнала Naked Science. СМИ из «большого» интернета редко добиваются успеха в Telegram. Но каналу Naked Science это удалось. В первую очередь, благодаря качественному авторскому материалу из мира науки, аналитическим статьям, интервью с учёными и познавательным видео.

«Фактопедия» – канал-энциклопедия интересных фактов. Где находятся самые большие запасы воды в Солнечной системе? Какой вклад в разоружение СССР внесла компания Pepsi? Какое произведение Стивена Кинга вызывает у читателей сомнения в его авторстве?

Ответы на самые неожиданные вопросы вы найдёте в этом канале, у которого очень удобный мобильный формат.

Есть вопрос? Узнай Ответ! В канале публикуются посты в формате вопрос-ответ. Что позволяет легко и с пользой провести время в дороге или на скучном мероприятии. Вам ведь интересно узнать – скрещиваются ли заяц и кролик?

Автор канала Елена Фонина – профессиональный преподаватель английского языка. На страницах канала она в лёгкой и доступной форме объясняет грамматические правила английского языка, а также делится своим опытом подготовки учеников к международным экзаменам (IELTS, TOEFL, FCE), прохождению собеседований в посольстве, эмиграции в Канаду, США и Великобританию. Здесь вы найдёте уроки по деловой переписке и телефонным переговорам, аудио-упражнения, практические задания и прочее.

Весь контент разработан автором специально для подписчиков канала. В чате канала Елена проводит бесплатные аудио-уроки для всех желающих.

«Мир Путешествий» – авторский канал о путешествиях. Статьи и фотографии о красивых, необычных и интересных уголках нашей планеты. Есть полезные статьи для путешественников. Любите помечтать или планируете отдых? Зайдите в «Мир Путешествий».

Конечно, иногда хочется просто отдохнуть и отвлечься от науки, технологий и, главное, работы. Канал «Чёрный Юморист» поможет в этом. Смешные картинки (без котиков) с перчинкой чёрного юмора.

Если вы уже не первый день в Telegram, то наверняка сталкивались с каталогами. Фишка «Каталог Telegram» в том, что это структурированный каталог каналов, чатов и ботов. Здесь нет той обычной свалки каналов. Выбираете категорию и получаете только нужные вам каналы. Если мало того, что в этой статье, то добро пожаловать в «Каталог Telegram».

(вгору)

Додаток 6

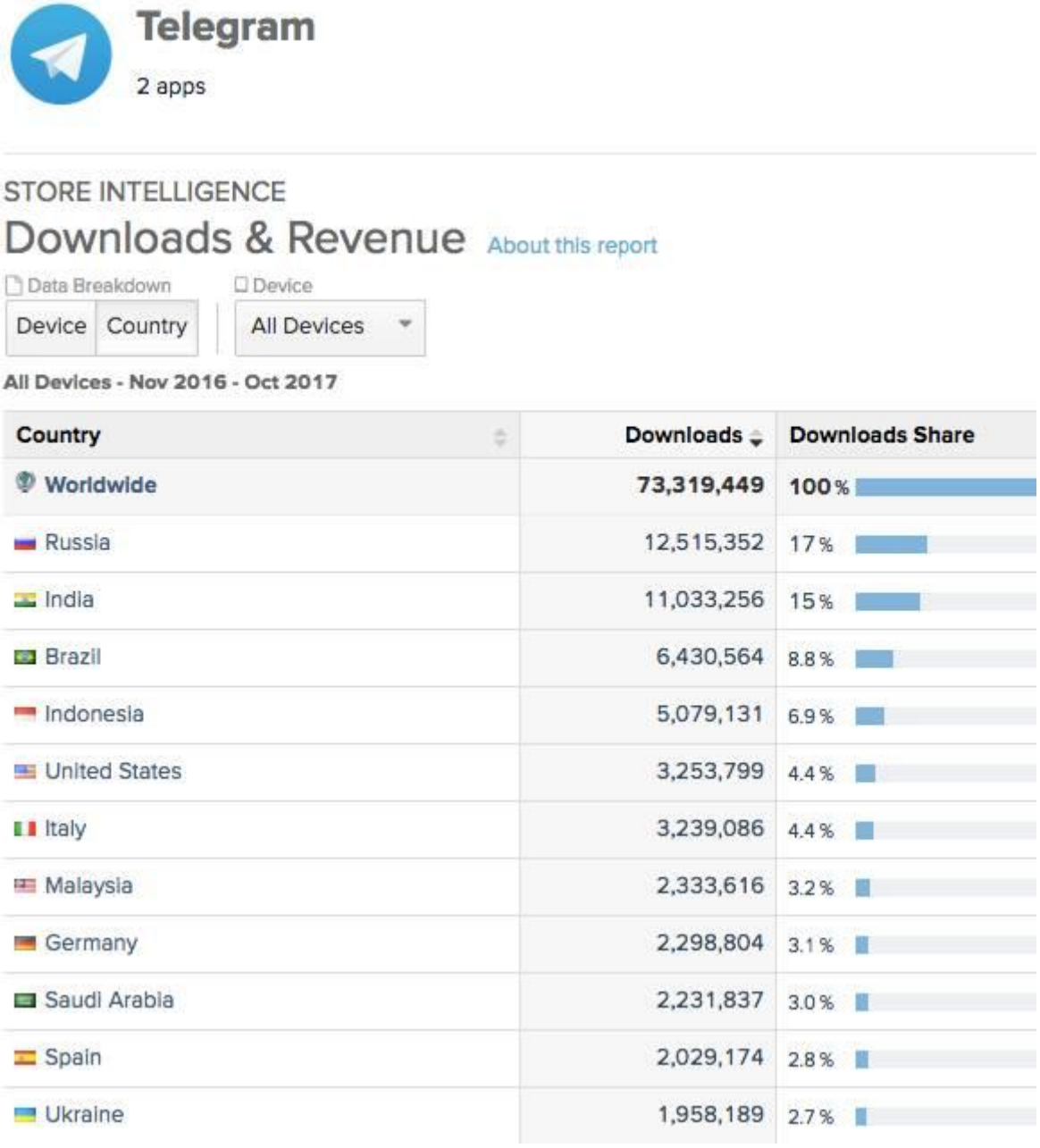
27.11.2017

Олег Дмитренко

За останні 12 місяців українці завантажили додаток Telegram майже 2 млн разів

За останні 12 місяців Telegram завантажили понад 74 мільйонів разів (дані за листопад 2016 – жовтень 2017). Про це свідчать дані App Annie (Watcher).

За кількістю завантажень Україна перебуває на 11 місці з майже 2 мільйонами завантажень. На першому місці – Росія. Там месенджер завантажили понад 12 млн разів.



Telegram

2 apps

STORE INTELLIGENCE

Downloads & Revenue About this report

Data Breakdown Device

Device Country | All Devices

All Devices - Nov 2016 - Oct 2017

Country	Downloads	Downloads Share
Worldwide	73,319,449	100%
Russia	12,515,352	17%
India	11,033,256	15%
Brazil	6,430,564	8.8%
Indonesia	5,079,131	6.9%
United States	3,253,799	4.4%
Italy	3,239,086	4.4%
Malaysia	2,333,616	3.2%
Germany	2,298,804	3.1%
Saudi Arabia	2,231,837	3.0%
Spain	2,029,174	2.8%
Ukraine	1,958,189	2.7%

Минулого року лідером за кількістю завантажень була Бразилія.

Протягом останніх 30 днів Telegram стабільно займає 2-5 місце серед найпопулярніших додатків в українському App Store та 9-14 в Google Play.

В Україні протягом останнього року активно розвиваються тематичні канали в Телеграмі. Наприклад, канал Digitaliziren – про цифровий маркетинг.

(вгору)

Додаток 7

15.11.2017

«Мені не заплатили»: Швачки Zara додавали до одягу прохання допомогти

Майстрині з Туреччини вкладали у кишені пошитого одягу бірки, у яких ішлося, що їм не дають зарплату (Українська правда).

Працівниці турецької компанії Bravo Tekstil виготовляли одяг для Zara, Mango та кількох інших відомих брендів, повідомляє BBC.

«Я пошила цю річ для вас, але мені за неї не заплатили!» – такими були написи на бірках, які кравчині вкладали до кишень одягу, що продавався у Стамбулі.

Компанія Bravo Tekstil збанкрутувала у липні 2016 року. Її працівникам заборгували зарплату за три місяці та додаткову компенсацію за втрату робочого місця.

Швачка Філіз Тутья розповіла, що керівництво компанії зникло, тож у неї та її колег не було іншого виходу, крім як привернути увагу громадськості.

Їм це вдалося, оскільки користувачі соцмереж, які знайшли записки в одязі, започаткували флешмоб #BravoIscileriIcinAdalet (#СправедливістьДляПрацівниківBravo).

Онлайн-петицію, де небайдужі вимагають сплатити всі борги швачкам, підтримали понад 270 тисяч людей.

Zara, у свою чергу, заявила, що борги Bravo погашені, а для тих, кому досі потрібна фінансова допомога, діє фонд із 210 тисячами євро.

У профспілці компанії заявили, що фонд здатен покрити тільки 25 % збитків, тож протести можуть тривати й далі.

Раніше повідомлялося, що на фабриці Berry Apparel у Камбоджі, яка належить шведському модному гіганту H&M, швачки масово втрачали свідомість.

(вгору)

Додаток 8

27.11.2017

У соцмережах запустили флешмоб, присвячений праці волонтерів

У соціальних мережах 27 листопада дали старт флешмобу, присвяченому Всесвітньому дню волонтера, який відзначатимуть 5 грудня (ZIK).

Користувачам пропонують під хештехом #ivolunteer розповісти власну історію волонтерства, чому варто допомагати іншим та прикріпити фото з місця волонтерсва. Якщо такого немає, то сфотографуватися з листком А4, на якому буде напис #ivolunteer.

«Це може бути не такий масштабний досвід, як літо в Африці. Адже волонтерство – це коли ви десь безкоштовно працювали чи взяли під опіку тварину, або ж допомагали комусь здійснити добру справу Або можна написати про те, чому волонтерство важливе. Про те, що волонтерство буває різним. Чи про те, яка користь від нього», – йдеться в умовах акції.

Для того, аби про добро, яке безкорисливо творять небайдужі люди, та їхні вражаючі історії дізналося якомога більше людей, окрім хештегу слід позначити трьох друзів, таким чином передавши їм естафету.

До флешмобу уже почали долучатися відомі українці.

«Це модне слово увійшло в наше життя зовсім нещодавно разом з тривожним дзвінком війни. Добровольці були першими, хто відправився на фронт; за ними вирушили невидимі колони медиків, юристів, підприємців, які кинули свої родини, віддали свій час, здоров'я, а іноді і життя тому, у що вірили. І все це безкорисливо. Я знаю сотні світлих хлопців, з якими ще на початку війни як журналіст ми відвозили одяг і продукти під Слов'янськ, в Билбасівку, в тоді ще Красноармійськ, Артемівськ і Авдіївку», – підписав свою фото Мустафа Найєм.

Флешмоб триватиме до 5 грудня.

(вгору)

Додаток 9

16.11.2017

YouTube блокирует блоггеров с обзорами iPhone X

Видеоролики, посвященные iPhone X и выложенные на YouTube, не могут заработать на рекламе, потому что видеохостинг ограничивает их сотрудничество с рекламодателями. При этом ролики не содержат никакого контента, нарушающего правила YouTube. Возможные причины – сбой в алгоритме оценки контента или его неадекватная реакция на букву «X» (InternetUA).

YouTube запрещает рекламу

YouTube по неизвестной причине ограничивает размещение рекламы в видеороликах, посвященных iPhone X, сообщает издание The Verge. На это, в частности, пожаловался видеоблоггер Бен Шманке (Ben Schmanke), который в начале ноября разместил на YouTube обзор, где сравнивает камеры iPhone X, Samsung S8 и LG V30.

Изначально YouTube классифицировал видео Шманке как доступное всем рекламодателям, отметив его значком зеленого доллара. Однако уже на следующий день блоггер увидел, что доллар стал желтым – это значит, что ролик может заработать деньги только от ограниченного числа рекламодателей.

По словам Шманке, никаких причин для ограничения заработка его ролика нет. За ночь он успел набрать порядка 10-20 тыс. просмотров. Напомним, с апреля 2017 г. зарабатывать на YouTube могут только те видео, которые преодолели порог в 10 тыс. просмотров.

Представитель YouTube сообщил The Verge, что проблема возникла далеко не со всеми роликами об iPhone X, поэтому о тенденции говорить нельзя. У компании и раньше наблюдались сбои алгоритма оценки и маркирования видео. YouTube борется с этим, но из-за большого потока контента, который обрабатывает этот алгоритм, устранить проблему до конца не удается. Шманке предполагает, что алгоритм мог отреагировать на присутствие буквы «X» в названии смартфона.

Похожие случаи

Похожие случаи произошли и с другими блоггерами, которые также выкладывали на YouTube ролики об iPhone X. Например, Дилан Хонг (Dylan Hong), автор небольшого технического канала, сообщил, что его ролик об аксессуарах для iPhone X тоже получил желтый значок, ограничивающий размещение рекламы. Хонг говорит, что не очень переживает о потере выручки – гораздо сильнее было удивление, вызванное неожиданной маркировкой.

«Я делаю супер-дружественные по отношению к рекламодателям и к семейной аудитории видео. Это просто какой-то просчет в алгоритме, из-за которого некоторые видео об iPhone X от именитых блоггеров и каналов помельче автоматически получили такую маркировку с самого начала», – отметил Хонг.

История вопроса

Несколько дней назад технические YouTube-канлы MKBHD, TLD и SuperSaf первые пожаловались в соцсети Twitter, что видеохостинг запрещает монетизацию их роликов об iPhone X. Все три обзора были посвящены извлечению iPhone X из коробки и проверке работоспособности. Для некоторых блоггеров это был первый желтый доллар – до этого YouTube никогда не ограничивал их в заработке.

Похожий случай произошел с блоггером Кейси Нейстатом (Casey Neistat). Его ролик был посвящен длинным очередям возле нью-йоркских Apple Store, в которых люди ждали возможности купить iPhone X. Несмотря на специфический авторский стиль, видео Нейстата не содержало нецензурной лексики, эротического или неприемлемого для рекламодателей контента, не разжигало ненависти и не использовало непозволительным образом популярных у семейной аудитории персонажей – то есть не делало всего того, за что YouTube может ограничить размещение рекламы в ролике.

Другие из перечисленных обзоров также не содержали этих элементов. В связи с этим некоторые пользователи Twitter начали высказывать предположения, что действия YouTube – это способ компании Google, владеющей видеохостингом, бойкотировать Apple.

Действия компании

О жалобах блоггеров в Twitter первым написал ресурс TechnoBuffalo. Через пару дней издание выяснило, что его собственный ролик о технологии Face ID в iPhone X также был демонетизирован на YouTube. В ответ на запрос видеохостинг сообщил, что в ролике использован сторонний контент. Проведя собственное расследование, TechnoBuffalo обнаружил, что у YouTube имеются претензии к музыкальному провайдеру, к услугам которого издание прибегло как раз для того, чтобы избежать подобных проблем. YouTube согласился изменить статус ролика TechnoBuffalo, но ущерб уже был нанесен.

(вгору)

Додаток 10

16.11.2017

Як соціальні мережі виявляють психологічні потреби особистості

Валерія Цихоня, практикуючий психолог

Уявіть ситуацію: ще сто років тому люди особисто або листуванням домовлялися про зустрічі за тиждень або навіть місяць. І не було ніяких смс «я затримаюся на 15 хв.». Вони приходили на призначене місце і чекали. Звичайно, ритм життя був більш спокійним. Сьогодні ми можемо робити дива – швидко корегувати свої плани та погоджувати їх з іншими. Ми можемо за лічені хвилини знайти будь-яку інформацію і для цього нам не обов'язково йти до бібліотеки. За допомогою Інтернету та мобільного пристрою можна вести прямі трансляції на весь світ. Це безумовно відкриває нові можливості, але у будь-яких інновацій є зворотний бік.

За якихось неповних 20 років людство перейшло на новий формат спілкування та передачі інформації. Це має свої зручності, але часто в новому контексті знаходять своє втілення й індивідуальні психологічні проблеми.

Де межа між простим спілкуванням, відкритістю та демонстративністю? Чим керуються такі люди, які постійно звітують про своє життя іншим в Інтернеті? Може, вони хочуть щось комусь довести? А може прагнуть переконати себе, що їх життя дійсно цікаве. Та що казати? Звичайно, якоїсь універсальної відповіді ми не знайдемо на це питання. Також ми не будемо розглядати випадки, коли люди просувають свій бізнес в мережах. Ми всі дуже індивідуальні, але у сучасній науці є спроби узагальнити причини активності та надмірної відвертості у соціальних мережах. Спробуємо проаналізувати окремі з них. Виділяють такі потреби, що складають підґрунтя надмірної активності у соціальних мережах. Це – потреба у стимуляції, потреба в подіях, потреба в упізнаванні, потреба у визнанні досягнень, потреба у структуруванні часу. Розглянемо їх більш детально.

Потреба у стимуляції

Полягає в тому, що протягом життя людина отримує численні стимули з оточуючого середовища. Найбільш значущими є стимули, які ми отримуємо від інших людей. Соціальна стимуляція є особливо важливою, коли зворотний зв'язок ми отримуємо від авторитетних осіб, або людей, які викликають повагу,

симпатію. Окремо можна виділити стимуляцію від незнайомих осіб, яких ви раптом зацікавили. Наприклад, як користувач мережі, ви написали статус стосовно актуального політичного становища у країні і в таких спосіб озвучили свою громадянську позицію. Соціальна стимуляція в даному випадку буде вимірюватися кількістю позитивних оцінок публікації, так званими лайками та цитуванням – ревітами. З одного боку, наше сучасне життя – стрімке, насичене подіями, з іншого, більшість з нас вважає його нудним.

«Як часто я чую від своїх клієнтів про те, що гортаючи чийсь фейсбук, контакт або інстаграм в них виникає відчуття того, що порівняно з іншими їх життя – нецікаве».

Люди потребують певної динаміки, строкатості навколо себе та розмаїття подій. Життя середньостатистичної людини буденне – дім, робота, коли є час і сили — зустрічі, відпочинок. Контакт з іншими через соціальні мережі – це отримання новин. Заходиш в інтернет і бачиш: хтось ходив на концерт, хтось змінив роботу, хтось імідж, хтось потовстішав, хтось одружився тощо. При нагоді ці новини можна обговорити з іншими людьми, адже коли тобі немає чого розповісти про себе завжди можна розповісти про іншого. Така часто пасивна споглядацька активність є квазіспілкуванням, яке з одного боку задовольняє потребу у подіях, а з іншого – все більше пробуджує власний голод до них. І так можна не зчутися як одного разу, цікаво проводячи час, ви почнете ділитися цим з вашими підписниками у соціальних мережах, адже цікава зустріч, відвідування театру, виставки, пікнік, відпустка — це підтвердження іншим того, що твоє життя також цікаве.

Потреба в упізнаванні

Пов’язана з нашим бажанням не випадати з соціального контексту. Серед сучасних людей багато кому знайомий страх того, що одного разу їх зв’язки втратять свою актуальність, про них забудуть, важливі події будуть проходити без них. Бажання «тримати руку на пульсі» або іншими словами «контролювати» оточення та події, які в ньому відбуваються і є реалізацією так званої потреби в упізнанні. Упізнання в даному випадку – це самоідентифікація, якоюсь мірою ми визначаємося і через наше оточення, яке боїмося втратити. Особливо яскраво це проявляється в тих випадах, коли люди змінюють роботу, місто або країну. Взаємодія через соціальні мережі – це спроба подолання соціальної деривації, це компенсація. Тому спілкування в мережі може видатися в окремих випадках достатньо корисним для подолання внутрішньої невпевненості, ізоляції.

Потреба у визнанні

Це одна із найактуальніших потреб сучасного покоління. Ще кілька років тому навіть офіційна державна політика базувалась на засадах спільності та рівності. Тепер ми знаємо, що світ належить кращим. І для того, щоб щось мати треба щось із себе представляти, або хоча б удавати. Пригадайте статуси дівчат, які цитують компліменти своїх бойфрендів на власну адресу, які фотографують свої вечері в ресторанах, коштовні подарунки або пишаються тим, що отримали підвищення. Вони наче намагаються сказати всьому світу «заздріть мені». Для

кожної людини є важливим, щоб оточуючі розуміли, що вона гарна, розумна, професійна. Але у когось це менш виражена потреба, а у більшої частини дана потреба є більш актуальною. Проголошуючи про свої досягнення, пишаючись своїм особистим життям, фаховими успіхами, стилем у інших складається враження, що такі особи в більшій мірі намагаються переконати себе в своїй успішності. В цьому є правда. От вам і баланс. Де межа між тим, що ти хочеш поділитися своєю радістю з іншими, а де отримати визнання та побавити власне нарцистичне его? До речі, дослідження взаємозв'язку між, так званою, самозакоханістю та активністю у соціальних мережах є достатньо популярними.

Як зазначає Лора Буффаді, нарцистичні особи активні в соціальних мережах, вони частіше за інших відмічають себе на фото, мають велику кількість «друзів»-підписників.

Звичайно, є і зворотній бій активності – повна її відсутність. Але ізоляція та відмежування від спілкування в інтернеті, на думку німецького дослідника Кристофа Мюллера, є підтвердженням наявності проблем із психічним здоров'ям людини.

Мюллер вважає низьку активність у соціальних мережах – небезпечним симптомом.

Газета Der Tagesspiegel, посилаючись на автора теорії, зазначає, що перевірка активності в інтернеті є інструментом для виявлення асоціальних особистостей. Дедалі частіше, і в Україні зокрема, кадрові агенції під часу пошуку спеціалістів на вакантні посади моніторять персональні сторінки претендентів в соціальних мережах. Часто зміст профілю може надати вичерпну інформацію про користувача. Німецьке видання пише, що у разі відсутності профайлу у соціальній мережі, компанії-рекрутери з більшою вірогідністю відмовляють претендентам на посаду, адже вважають, що таким людям є що приховувати, вони мають складнощі у спілкуванні з іншими особами, а відповідно, їм буде важко працювати в колективі.

Потреба у структуруванні часу

Повернемось до потреб, які можна задовольнити спілкуванням у соціальній мережі. Таке спілкування в певній мірі задовольняє і потребу у структуруванні часу. Ерік Берн виділяв різні види структурування часу: ритуали, процедури, розваги, близькість та гру. Ритуали в соціальних мережах представлені у вигляді нагадувань привітати підписника із днем народження. Процедури ми виконуємо, коли створюємо відео конференції та обговорюємо робочі та організаційні моменти нашого життя. Розваги — це коли ми спілкуємося на теми хобі та інтересів. Близькість в мережах реалізується у позначенні статусів на кшталт «у стосунках», налаштуваннях приватності сторінки. До гри часто відносять спілкування із маніпулятивним відтінком. Таким чином, можна підсумувати, що контекст спілкування для людей новий, а от психологічні спонукачі до нього — старі, як світ. І коли сьогодні до психологів приходять люди зі скаргою на те, що вони мають залежність від соціальних мереж, за цим стоїть одна із зазначених потреб. А що означає

потреба? Потреба – це дефіцит, це нестача у чомусь. Потреба не виникає на порожньому місці, вона часто може дуже влучно описати свого носія. Якщо ви читаєте цей текст і розумієте, що частіше, ніж потрібно заглядаєте на фейсбук або вконтакт, або навіть просто автоматично та бездумно оновлюєте стрічку новин без особливої на це потреби, подумайте, що саме або кого ви очікуєте там побачити?

(вгору)

Додаток 11

20.11.2017

Исследование: пользователи осознали опасность смартфонозависимости

Тревожность, депрессия, проблемы со сном, неспособность сконцентрироваться на значительное время – вот далеко не полный список проблем, с которыми могут столкнуться люди в результате чрезмерного использования смартфонов. Как показывает недавно проведенное в США исследование, пользователи, раньше, как правило, не догадывавшиеся о «смартфонозависимости» и ее последствиях, начинают осознавать всю серьезность ситуации (InternetUA).

Как выявило исследование Global Mobile Consumer Survey, проведенное компанией Deloitte, 47 % опрошенных (репрезентативная выборка американцев в возрасте от 18 до 75 лет) сознательно прилагают усилия, чтобы снизить или ограничить продолжительность и частоту использования мобильников. Обычно для этого стараются либо убрать аппарат с глаз долой, либо отключить оповещения, или хотя бы их звуковые сигналы. Еще любопытно, что голосовые звонки начали отвоевывать утраченные позиции – их использование, падавшее четыре года подряд, в 2017-м подросло на 9 %. Тем не менее, 14 % опрошенных совершают со своих телефонов менее 1 звонка в неделю.

При этом эксперты Deloitte выявили еще один интересный факт: если в начале текущего десятилетия частота использования смартфонов постоянно росла, то в последние годы график ее роста вышел на плато. Уже три года подряд среднестатистический американец обращается к смартфону примерно 47 раз в день. Однако частота использования продолжает расти среди самых молодых пользователей (18-124 года): она увеличилась за минувший год с 82 до 86 раз в день.

На то, что активность использования смартфонов американцами близка к пределу возможного, указывает и среднее количество скачиваемых и используемых приложений. Оно за последний год выросло незначительно: с 22 до 23 штук. Почти не растет и доля людей, обращающихся к смартфону в первый час после утреннего пробуждения: за год она изменилась с 88 до 89 %. Доля использующих смартфон в час перед отходом ко сну не изменилась с 2016-го: 81 %.

К настоящему времени в США смартфонами успели обзавестись 82 % населения, а в возрастной категории 18-24 года – 93 %. При этом средний возраст пользователя растет: быстрее всего теперь доля пользователей смартфонов увеличивается среди американцев старше 55 лет.

При этом производителям смартфонов пока волноваться особенно не о чем: хотя все больше людей замечают «изнанку» активного использования карманных гаджетов, отказываться от устоявшейся привычки приобретать новый телефон каждые два года американцы не собираются – такого «графика» придерживаются 2/3 опрошенных.

(вгору)

Додаток 12

20.11.2017

Facebook и другие социальные сети могут продлевать жизнь

В течение 6 месяцев сотрудники Калифорнийского университета мониторили активность 12 миллионов пользователей Facebook (Телеграф).

Дружба необходима нам для психологического благополучия, но преимуществами обладает не только офлайн-общение. Новое исследование ученых из Калифорнийского университета в Сан Диего показало, что социальные сети могут продлить жизнь, если мы будем использовать их правильно.

Наличие близких друзей связали с долголетием еще в конце 1970-х. Девятилетнее исследование продемонстрировало, что отсутствие прочных социальных связей повышает риск преждевременной смерти до 2,8 раз. В 2010 году мета-анализ 148 аналогичных научных работ подтвердил, что регулярное общение с друзьями повышает шансы стать долгожителем на целых 50 %, а в 2016 одиночество причислили к вредным привычкам, назвав таким же значимым фактором смертности, как курение и употребление алкоголя.

В нашем глобализованном мире все больше людей живут вдали от своей семьи и родины, что иногда приводит к разрыву социальных связей, чувству одиночества, изоляции и депрессии. Благо, выживать помогают современные технологии и социальные сети.

Новое исследование американских ученых во главе с Уильямом Хоббсом и Джеймсом Фаулером предполагает, что Facebook увеличивает продолжительность жизни. Тем не менее, работает это только в том случае, когда Facebook используется для поддержания и улучшения реальных социальных связей. Результаты исследования опубликованы в журнале «Труды Национальной академии наук США».

Facebook увеличивает продолжительность жизни, но работает это только в том случае, когда социальную сеть используют для поддержания и улучшения реальных социальных связей.

В течение 6 месяцев сотрудники Калифорнийского университета мониторили активность 12 миллионов пользователей Facebook, родившихся в

период с 1945 по 1989 год, а затем сравнили их уровень смертности с аналогичными данными людей, которые не пользуются интернетом для общения. Оказалось, что риск преждевременной смерти у среднего пользователя Facebook на 12 % ниже.

Исследователи изучили списки друзей, обновления статусов и фотографии пользователей, и пришли к выводу, что высокая активность в Facebook коррелирует не только с реальной социальной активностью, но и с более крепким здоровьем.

– Умеренная онлайн-активность дополняет взаимодействие между людьми, повышая их психологическое благополучие и физическое здоровье, – уверен Уильям Хоббс, ведущий автор исследования. – Впрочем, наши выводы просто указывают на корреляцию, и не должны интерпретироваться как причинно-следственная связь. В любом случае, Facebook и другие социальные сети позволяют побороть изоляцию и одиночество, способствуют снижению стресса и рисков развития реальных заболеваний.

(вгору)

Додаток 13

25.11.2017

По лайкам в Facebook можно узнать сексуальную ориентацию и IQ

Всего пара лайков в Facebook могут определить сексуальную ориентацию, а также политические или религиозные предпочтения пользователя, считают исследователи нескольких американских вузов, опубликовавшие свое исследование в журнале Big Data. И лучше иметь возможность скрыть эту информацию от рекламодателей (InternetUA).

Исследователи обнаружили, что 3 лайка в социальной сети дают достаточно материала рекламодателям, чтобы понять, можно ли отнести пользователя к группе геев и строить на этом рекламную политику. При этом не важно, указывает ли он эту информацию на своей странице или нет. Ученые предложили также, чтобы Facebook и другие соцсети создали какую-нибудь «систему маскировки» для тех, кто не готов раскрывать о себе эти сведения, даже если они соответствуют действительности, пишет The Telegraph.

Помимо личной информации, местоположении и истории поисков о пользователе Facebook многое можно узнать по тем страницам, которые им нравятся. Как выяснилось, в среднем требуется менее восьми лайков, чтобы определить не только сексуальную ориентацию, но и IQ, религиозные или политические взгляды, а также отношение к курению и алкоголю. Например, если пользователю нравятся страницы Леди Гаги, кампании по защите прав человека, сериала «Настоящая кровь» и Гарри Поттер, то, скорее всего, он гей.

Исследователи обнаружили также, что если скрыть небольшое число лайков, этот алгоритм перестает работать, и информация, которую пользователи Facebook хотели бы скрыть, останется конфиденциальной. Количество лайков, которые необходимо скрыть, зависит от типа информации:

3,5, если речь идет о сексуальной ориентации; 12,2 – о наркозависимости; 11,7 – о приверженности исламу. Число скрытых лайков для получения ложно положительного результата – чтобы пользователя отнесли к группе, к которой он на самом деле не относится – обычно меньше.

«Одним пользователям возможность определения их предпочтений в точки зрения рекламы окажется полезной, но у других такое заключения могут вызвать беспокойство, – пишут исследователи. – Эти выводы могут не только оказаться ложными из-за нехватки данных или неадекватности модели, некоторые пользователи вообще не хотят, чтобы определенные характеристики всплывали. Для многих вторжение в частную жизнь с помощью статистических методов вызывает не меньшее опасение, чем раскрытие персональных данных».

Помимо лайков, личную информацию о пользователе может выдать другая его активность в сети: по выбору лексики можно узнать возраст и пол, черты личности и род занятий, даже шанс смерти от сердечных заболеваний.

(вгору)

Додаток 14

16.11.2017

Як у соціальних мережах маніпулюють українцями: розкрито схеми

У соціальних мережах останнім часом точаться справжні бої: “порохоботи” зчепилися із “зрадофілами”, “білі хакери” воюють з кремлівськими “ботами” і “тролями”. З території спілкування соцмережі перетворилися на місце, де політтехнологи і пропагандисти різного ґатунку маніпулюють суспільною свідомістю. Згідно зі звітом міжнародної правозахисної організації Freedom House, уряди по цілому світу не лише підтримують, а часто й ініціюють подібні маніпуляції, що загрожує укріпленням авторитарних режимів (Народна правда).

Маніпуляції онлайн-контентом досить складно виявити, а боротися з ними ще складніше, визнають фахівці Freedom House. Лише цього року тактика маніпуляції та дезінформації зіграла чималу роль у виборах у щонайменше 17 країнах світу. А влада у близько 30 державах світу використовувала соцмережі для поширення проурядової думки або ж для придушення критиків усередині своєї країни. Такі ж країни, як Росія, за допомогою маніпуляцій поширювали свій вплив на інші держави, зазначає президент Freedom House Майкл Абрамович.

«Використання платних коментаторів і політичних ботів для поширення державної пропаганди було започатковано Китаєм та Росією, але тепер стало глобальним», – зауважує Абрамович.

Однією з жертв проросійських маніпуляцій і пропаганди у соціальних мережах стала Україна. У відповідь, Київ заблокував деякі інтернет-сервіси російського походження, в тому числі соціальні мережі «Одноклассники», «ВКонтакте» та пошукову систему Yandex.

Як заявив президент Петро Порошенко, Київ може переглянути це рішення тоді, «коли останній російський солдат покине суверенну і незалежну територію України».

Як зазначає публіцист Сергій Грабовський, ще з часу першого президентства Володимира Путіна ФСБ перетворювало інтернет, соціальні мережі на «місце дислокації» проросійських пропагандистів.

«У Росії, тільки-но Путін став президентом, в інтернеті з'явились фсбшні "бригади", які "завалювали" інтернет не те що фейками, а шумовинням – щоб там губилась нормальна інформація. Вони тероризували всіх, хто відхилявся від "генеральної лінії". Все це мало колосальні наслідки: інтернет у Росії повністю перейшов не тільки під контроль ФСБ, а і під контроль відповідно частини пропутінського суспільства», – зазначав експерт в інтерв'ю для Радіо Свобода.

Дослідник медійних комунікацій, один з керівників інформаційного проекту «Майдан Прес Центр» Алекс Беккер нарікає на брак контролю за повідомленнями на рекламних платформах у соцмережах. Ці платформи перетворені на агітаційні платформи, окремі держави використовують їх як місця для поширення пропаганди та політичної реклами. Негативний вплив таких маніпулятивних дій показали вибори президента США минулого року, цьогорічні вибори у Німеччині та Франції, каже експерт.

А у 2014-15 роках проросійські «тролі», маніпулюючи правилами соцмережі Facebook, блокували українських волонтерів та громадських активістів за нібито розпалювання ворожнечі, а фактично – за поширення інформації про бойові дії на сході України, про вторгнення російських військ тощо. Відтак, вважає Беккер, необхідно аналізувати контент соціальних мереж і не допускати поширення пропаганди, брехні тощо.

«Це гібридна війна, і застосування соціальних мереж є критичним з огляду на це, тож необхідно взагалі врегульовувати цю ситуацію», – пояснює Беккер у розмові з Радіо Свобода.

Українські політики: від «джинси» – до «ботів»

На сьогодні в Україні різні політичні сили також активно використовують соціальні мережі для поширення своїх заходів, проектів, меседжів. Як наголошено у звіті Freedom House, для поширення і пропаганди політики влади у соцмережах використовують проплачених провладних коментаторів та політичних ботів. Також в Україні, хоч і незначною мірою, під цензуру потрапляють критика влади, а також у значній мірі теми, пов'язані зі збройним конфліктом на сході.

У розмові з Радіо Свобода медіа-експерт, представник міжнародної організації «Репортери без кордонів» Оксана Романюк зауважила: якщо ще кілька років тому окремі політики і партії інвестували у медійну «джинсу», то тепер вони платять «ботам».

«Насправді у нас в інтернеті різні політичні сили використовують так званих "ботів" або проплачених коментаторів, і так само це використовують й економічні компанії. І це не є суто українською особливістю: це – ознака

нашого часу, це риса, яка буде притаманна соцмережам у найближчі кілька років. Що з цим можна зробити? Це – підвищувати медіа-грамотність населення, розвивати критичне мислення», – каже Романюк.

У цілому, спроби окремих українських політиків маніпулювати суспільною свідомістю у час гібридної війни Росії проти України українські експерти називають вкрай небезпечним явищем, оскільки результатом можуть бути розкол українського суспільства та відволікання уваги українців від важливих проблем.

(вгору)

Додаток 15

18.11.2017

Сотрудник рассказал о работе российской «фабрики троллей»

Сотрудник российской «фабрики троллей» рассказал о работе секретного агентства по производству контента, который видели миллионы американцев в преддверии президентских выборов в США 2016 года. Об этом он рассказал NBC News, передает УНН (InternetUA).

26-летний Виталий Беспалов сообщил, что в агентстве интернет-исследований в Санкт-Петербурге в России ежедневно работали сотни сотрудников для создания политической пропаганды во время выборов в США.

С его слов, блоггеры и бывшие журналисты штамповали «ложь... карусель лжи».

В. Беспалов сказал, что он «абсолютно» верит в то, что агентство интернет-исследований связано с Кремлем.

В январском отчете американского разведывательного сообщества указывается на близкого союзника президента России Владимира Путина как на «вероятного финансиста» этого агентства.

Как отмечается, в агентстве В.Беспалов работал в подразделении, которое занималось написанием фальшивых новостных статей, которые публиковались в социальных сетях. В.Беспалов рассказал о том, как его собственная работа сосредоточилась на дискредитации Украины, но другие сотрудники были сосредоточены исключительно на США.

С его слов, при написании таких статей факты должны были оставаться неизменными, но с некоторыми «правками». Сообщется, что «террорист» становился «ополченцем», «украинская армия» становилась «национальной гвардией», а Россию нельзя было критиковать.

В прошлом месяце Facebook сообщил, что агентство приобрело 3000 рекламных объявлений за 100 тысяч долларов, которые могли видеть до 126 миллионов американцев во время выборов в 2016 году.

Facebook позже сообщил, что до 146 миллионов американцев могли видеть контент, связаный с Россией, в Facebook и Instagram.

(вгору)

Додаток 16

20.11.2017

Солдаты информационной войны. Как Ольгинские и другие тролли завоевывают интернет

Мощная и высокобюджетная фабрика интернет-троллей в России становится серьезной силой, существенно влияющей на ситуацию в собственной стране и способной расшатать мир, пишет журнал Новое Время (InternetUA).

Вмешательство в выборы в США

В последние годы на интернет-площадках Facebook, Twitter и Google орудовали сотни российских троллей. Там они под видом американских активистов распространяли пропаганду и организовывали митинги, стремясь к расколу общества в США, а также пытались повлиять на недавние президентские выборы.

Еще в начале сентября, Facebook сообщил о выявлении 470 поддельных российских аккаунтов, которые в течение двух лет купили 3 тыс. платных объявлений об иммиграции, расе и равных правах общей стоимостью $ 100 тыс. Затем о блокировке 2752 управляемых из России аккаунтов заявил Twitter. Пропагандистские учетные записи были обнаружены и в Instagram. А Google насчитал десятки тысяч долларов, потраченных российскими агентами на рекламу с целью повлиять на ход выборов в США.

Однако Кремль открестился от вмешательства в выборы за океаном. «Мы никогда об этом не слышали, мы ничего об этом не знаем и тем более не имеем никакого отношения к этим делам», – заявил пресс-секретарь российского президента Дмитрий Песков.

Следы интернет-троллей привели американских расследователей в Санкт-Петербург, где, как оказалось, работает целая фабрика манипуляторов общественным мнением. Впервые о ней заговорили после публикации расследования журналиста Андрея Сошникова, который в 2013 году внедрился туда под видом сотрудника. Тогда фабрика базировалась в пригородном районе Ольгино, и с тех пор российских троллей называют ольгинскими.

Затем компания сменила несколько юридических названий и переехала из пригорода в Петербург. Здесь в доме № 55 по улице Савушкина фабрика работает до сих пор, подтверждает в беседе с НВ Сошников, ныне журналист Русской службы ВВС.

Как устроена фабрика троллей

По рассказам экс-троллей, вакансии на фабрике они нашли через сайты поиска работы, и особых требований – как, например, грамотность либо осведомленность в политике – к ним не предъявляли. Зато зарплаты предложили выше рыночных – 40–50 тыс. руб. ($ 700–870) в месяц, а для англоязычных сотрудников и вовсе 65 тыс. руб. (более $ 1 тыс.).

Как удалось выяснить журналистам, на фабрике посменно в круглосуточном режиме работают несколько сотен сотрудников. Свое рабочее

место они иронично называют министерством правды с отсылкой на роман-антиутопию Джорджа Оруэлла 1984.

Трудятся тролли в нескольких отделах, каждый из которых возглавляет тим-лидер. Одни занимаются подготовкой технических заданий, другие пишут блоги, третьи – комментарии к новостям в российских и зарубежных СМИ. Отдельная группа монтирует фотографии известных западных политиков, превращая их в саркастические демотиваторы и фотожабы.

Работа тролля заключается в написании постов и комментариев в соответствии с конкретными техзаданиями – информационными подборками, которые состоят из темы, нескольких тезисов, ссылок на материалы для ознакомления и вывода, к которому должен прийти автор. Выполнить техзадание сотрудник должен из нескольких аккаунтов от имени разных лиц.

Так в рунете формируется положительный облик кремлевской верхушки и негативный образ российской оппозиции, а также целого ряда государств, в первую очередь – Украины, США и стран Европейского союза.

Российские тролли в рунете

Изначально команды своих троллей Кремль направлял в первую очередь на россиян. Впервые организованный политический троллинг появился в России на фоне протестов 2012 года, когда после четырех лет президентства Дмитрия Медведева главный пост страны вновь занял Владимир Путин. Тогда рунет в значительной степени контролировали оппозиционеры, вспоминает Арик Толер, специализирующийся на Восточной Европе аналитик сайта для взаимодействия журналистов-расследователей Bellingcat.

«Провластные силы не могли владеть информационным пространством, но попытались сделать его мутным и максимально размыть антипутинские голоса», – считает он.

Задача троллей – загадить информационную площадку, убедить, что все врут, считает российский политолог Дмитрий Орешкин. «Украина вот-вот рухнет, Запад гниет и разлагается, Россия поднимается с колен, и все это на фоне “а мы ничему не верим”», – описывает он создаваемую ими информационную картину.

По данным специалистов, эффект от такой пропаганды уже есть. «Для значительного количества людей интернет – это большая помойка, источник, к которому они не относятся с большим доверием», – подтверждает Степан Гончаров, социолог российского Левада-центра, который проводит исследования о поведении в соцсетях и регулярно организует фокус-группы с молодежью и жителями больших городов по этой теме.

В такой ситуации пользователи более охотно принимают за правду мнения, близкие их собственным убеждениям. «В эпоху постправды в соцсетях люди склонны дружить, верить и репостить мнение тех, кто с ними согласен», – формулирует Ник Белогорский, эксперт по кибербезопасности, который ранее работал в Microsoft и Фейсбуке. Это создает благоприятную почву для эффективного распространения фейков и одновременно препятствует развитию демократического общества.

«Россия благодаря этим “усилиям” возвращается в первобытное состояние, когда люди верят только членам своего племени или группы – тем, кого знают лично», – констатирует Орешкин.

Не только в России

Россия – не единственная страна, где интернет-троллинг организован на высшем уровне. Согласно свежему отчету американской исследовательской организации Freedom House, проправительственные фабрики троллей действуют в 30 странах. Например, в Китае правительство платит блогерам и участникам интернет-форумов за формирование в сети положительного мнения о руководстве страны. За год армия так называемых умаоданов публикует в интернете почти 450 млн фейковых комментариев, подсчитали в 2016 году исследователи Гарвардского университета.

«В Турции платные государственные тролли называются aktroller, их около 6 тыс., они атакуют курдов и поддерживают [президента] Эрдогана», – рассказывает Белогорский. Российский троллинг эксперт называет «высокобюджетным, изощренным и непрямым», признавая его лидером среди аналогичных проектов в мире.

(вгору)

Додаток 17

21.11.2017

Ольга Карпенко

От лайков к шантажу: как работает индустрия фейковых профилей на Facebook

Один подозрительный пост на Facebook порой может привести к раскрытию работы целой подпольной сети, чья цель – обманом заставлять пользователей делиться приватными изображениями и затем – шантажировать их. Тому, как устроен бизнес сети фейковых профилей, которые паразитируют на мужчинах, заинтересованных в сексе, посвящено недавнее расследование Radio Canada. Публикуем его перевод (AIN.UA).

Вы получаете запрос на добавление в друзья на Facebook. Судя по фото, это девушка. Вы с ней незнакомы, но она симпатичная и вы заинтригованы. Почему бы и нет? Принимаете запрос. Только что вы, сами того не зная, запустили в работу механизм ловушки sextortion (шантаж разоблачением подробностей личной жизни).

Расследуя мир фейковых Facebook-профилей, мы с коллегой Мари-Эвой Трембли раскрыли масштабную сеть мошеннических аккаунтов, которые ловят жертв-мужчин, используя украденные фото молодых женщин и юных девушек. Это история расследования, которое длилось месяцы, и которое позволило нам узнать детали о работе этой сети.

«Я принимаю в друзей всех»

Существует множество способов, чтобы достичь успеха в социальных сетях. Я пишу о фейковых новостях и онлайн-дезинформации уже третий год, и

думал, что видел все. Но Facebook-профиль на имя Беатрис Бустар заставил меня задуматься.

Она шикарно выглядела, она была таинственной, ей удалось собрать аудиторию из нескольких сотен тысяч пользователей. Нюанс в том, что она крала данные больных людей или людей с инвалидностью, чтобы добиться этого.

Впервые я познакомился с профилем Беатрис в феврале 2016 года. Она регулярно постила фото облысевших людей, людей с ампутациями, и просила написать «аминь» в комментариях. Зачем? Потому что «с тех пор, как я заболела раком, меня никто не любит» или «муж бросил меня после того, как мне ампутировали ноги».

Подобные посты неизбежно собирали тысячи лайков, комментариев и репостов. Неудивительно, что ей удалось собрать базу фанатов из 671 000 пользователей – это намного больше, чем у ведущих канадских СМИ вроде National Post или Toronto Star, и почти столько же, сколько у Globe и Mail.

Было несложно понять, что фото – украдены, и что люди на фотографиях не больны раком либо же живут вполне счастливой жизнью, несмотря на инвалидность.

В то время мне казалось, что это обычная схема «лайк-фарминга». Это стратегия создания Facebook-страницы, наполнения ее вирусным контентом и затем продажи на «черном рынке» или использования ее для продвижения чего-либо.

Мне стало интересно и я решил понаблюдать за Беатрис и ее страницей. Если бы она превратилась в страницу компании-производителя напитков-энергетиков, из этого вышел бы занятный новостной сюжет.

Но однажды Беатрис перестала постить фото больных людей, вместо этого на странице начали появляться сексуальные фото девушек. Очень юных девушек.

Возникновение сети

Все фото сопровождались однотипными сообщениями. «Она ищет парня. Напишите в комментарии и она ответит вам в личку. Не стесняйтесь, добавляйте ее!». Затем она тегала 4-5 «друзей» в посте.

Ее друзья также были фейковыми аккаунтами, украшенными украденными фотографиями красивых женщин. Каждый аккаунт в свою очередь перепечатывал эти фото, добавляя в теги еще друзей-фейков.

Наблюдая за этими взаимодействиями между фейковыми профилями, я выстроил базу данных из примерно 40 профилей. Они все действовали по одной формуле: публикация украденной фото сексуальной девушки, поощрение мужчинам написать коммент, тегирование других фейков.

Уже тогда было понятно, что это все делается для наращивания аудитории. Более того, на многих фото девушки были очень юными, и в то же время – снятыми явно в сексуальном контексте, в соблазнительных позах. Несколько фейковых профилей утверждали, что принадлежат 15-16-летним девушкам.

Мне не удалось отследить каждую использованную фотографию. Говоря о тех, которые я проверил: они все принадлежали различным аккаунтам, и скорее всего, были украдены с единственной целью – привлекать мужчин. Именно это подтолкнуло меня исследовать вопрос глубже. Как минимум, сеть крала фото девушек и девочек, и помещала их в сексуальный контекст без их согласия.

В реальности кроличья нора оказалась намного глубже.

Как устроена сеть

Искать фейковые профили и устанавливать связи между ними – все равно, что собирать паззл. Часто непонятно – подходит сюда этот кусок мозаики или это случайный элемент.

Многие молодые люди тегали эти фейки у себя в постах. Что, конечно же, не означало, что они тоже – часть сети. Возможно, они всего лишь хотели выехать на популярности этих аккаунтов. Они знали о том, что тегают фейки?

Чтобы лучше понять, как устроена сеть, я проанализировал около 200 Facebook-постов от 40 фейковых аккаунтов. Каждый раз, когда один фейк тегал другого, я записывал источник и цель.

Используя софт для анализа, я создал карту и организовал аккаунты в соответствии с отношениями между ними. Софт распознавал более активные аккаунты как «узлы» и окружал их аккаунтами, с которыми они чаще всего взаимодействуют.

Также я использовал алгоритм, определяющий, какой профиль взаимодействует с каждым другим профилем чаще, чем с остальными: их он определяет как «подсети» – они на графике обозначены голубым и желтым. Возможно, это – различные сети, которые сотрудничают друг с другом для продвижения. Также это может означать, что эти подсети управляются различными людьми.

Как можно заметить, в сети связаны все аккаунты, но некоторые из них служат узлами, как правило, у них больше всех фолловеров, и они продвигают остальные аккаунты в сети. Отсюда вопрос: зачем так напрягаться? Кроме продвижения друг друга, фейковые аккаунты часто еще и вступают в дискуссии между собой в комментариях, чтобы создать иллюзию того, что они – настоящие люди. Никто бы не стал заниматься таким просто для развлечения.

Это точно связано с деньгами, думал я. Некоторые посты участников сети размещали ссылки на мошеннические сайты, которые просили данные кредитки. Но мне казалось, эти аккаунты вовлечены в какое-то sextortion-мошенничество.

Оказалось, что разные аккаунты играют разные роли. Но все – сотрудничают, чтобы эффективней завлечь будущую жертву. Из того, что нам удалось выяснить: часть сети физически находится в северной Франции и Бельги. Другая – расположена в Испании. Но крупнейшая часть находится в южной Франции, в окраинах Марселя.

Как работает сеть

Фейковые профили делятся на несколько категорий: фидеры, аккаунты-приманки и аккаунты-охотники.

Фидеры работают «воротами» в сеть. У этих профилей – как правило, сотни тысяч фолловеров, но они сами не публикуют сексуальные фото. Скорее, кликбейтный контент, вроде тупых IQ или бесполезных лайфхаков. Эти посты получают сотни и тысячи лайков, комментов и перепостов.

В посте фидер тегает другие фейки, уже из категории «приманок». Эти очень популярные посты служат рекламой для «приманок». Любопытствующие пользователи-мужчины кликнут по отмеченным профилям и, увидев, что они принадлежат красивым женщинам, зафоловят их. Уже на этом этапе сеть отфильтровывает пользователей, которые не хотят фоловить профили девушек и женщин с ярко выраженным сексуальным контекстом. Чтобы эти профили казались реальными, им добавляют детализации. Часто в рамках одного профиля используется фото одной и той же девушки, добавляются детали вроде даты рождения или города проживания.

Эти аккаунты – не интерактивны. Они не принимают запросы в друзья и никогда не отвечают на личные сообщения. Аккаунты-приманки часто делятся линками, которые, как они обещают, дадут пользователям возможность посмотреть порно (иногда это порно с участием несовершеннолетних). Эти линки всегда ведут на мошеннические сайты, где пользователя просят поделиться данными кредитки. Но аккаунты-приманки никогда не участвуют непосредственно в sextortion. Подобные незаконные линки никогда не публикуются напрямую на Facebook.

Иногда «приманки» исчезают – либо на них жалуются другие пользователи, либо же сами владельцы сети деактивируют их. Но даже в этом случае структура сети остается целостной. Фидеров это никак не задевает, ведь они никогда не делятся подозрительным материалом. За счет многослойной структуры сеть защищает себя.

Основная функция «приманок» – постить интригующие фото и тегать другие аккаунты-фейки. Посты всегда поощряют мужчин писать комментарии (в стиле «Как думаете, я – горячая штучка?» или же обещают выслать личные фото каждому мужчине, который напишет свой возраст в комментариях. Это – важная часть процесса, которая служит для работы третьего слоя сети.

Аккаунты-охотники

Здесь и начинается мошенничество.

В классической схеме мошенник представляется как привлекательная девушка и мотивирует пользователя-мужчину мастурбировать на камеру. Затем у жертвы вымогают крупную сумму денег. Если жертва не соглашается, мошенник угрожает опубликовать скриншоты или видео процесса в социальных сетях (нечто подобное, кстати, мы видели в «Черном зеркале» – ред.). Иногда мошенники доходят до обвинений в том, что по ту сторону камеры находилась несовершеннолетняя девушка.

Аккаунты-приманки уже создали идеальную среду для sextortion-схемы. Пользователи, которые оставляют комментарии, не боятся сообщить

общественности о своем интересе к юным девушкам, плюс им не хватает соображения понять, что они общаются с фейками. Они – идеальная целевая аудитория для «охотников». Такие пользователи начинают получать от «охотников» десятки запросов на дружбу.

Когда пользователь принимает запрос, ему приходит личное сообщение. Фейковый аккаунт шлет ему линк на мошеннический сайт с порно или же дейтинговый сайт, или же пытается начать общение. Буквально за секунды пользователю предлагают продолжить разговор в видеочате, к примеру, в Google Hangouts или Skype.

Аккаунты-«охотники» как правило недолговечны, и часто исчезают спустя минуты после установленного контакта с жертвой. Скорее всего, добавляя так много друзей за короткий период времени, они вызывают подозрительность алгоритмов Facebook, которые охотятся на фейки. Поэтому «охотники» стараются очень быстро перевести разговор в другой чат.

Запись разговора, который с «охотником» провела редакция радио – на скриншоте видно, как аккаунт пытается пригласить пользователя побеседовать в видеочате, ясно виден сексуальный контекст и желание побудить пользователя включить свою веб-камеру.

Как только общение продолжается в видеочате, «охотник» просит пользователя раздеться и заняться мастурбацией – ему нужно сделать запись и фото для последующего шантажа.

Кто за этим стоит?

Франция, среда, 6 сентября, около 15:00 по местному времени.

Мы только что получили один из важных элементов расследования. Это – фото группы друзей на Facebook, на первый взгляд – ничего особенного. Однако это фото и комментарии под ним позволяют нам наконец-то идентифицировать одного из организаторов сети.

Затем, как в фильме, спустя секунды после того, как мы сделали скриншот, все исчезает из сети. Около дюжины самых популярных аккаунтов сети уходят в офлайн.

Назовем его «Мехди». Его имя несколько раз всплывало в моих заметках на протяжении месяцев. Он – модератор закрытой Facebook-группы, в которой 600 000 участников и которая часто используется сетью фейков, чтобы получать трафик. Другие модераторы группы – тоже фейки. Все указывает на него. И затем мы находим фото, где он допустил серьезную ошибку. Одна из друзей Мехди запостила групповое фото и затегала знакомых, включая его. Я узнаю его по фото, но когда навожу курсор, вижу, что он затеган не под собственным именем, а под именем Amandine Ponticaud – одним из крупнейших фейковых профилей сети. В комментариях парень начал высмеивать Мехди, тот отвечал на насмешки, но из-под профиля Amandine.

После чего идет обмен оскорблениями между двумя пользователями, Мехди находит фото матери парня на Facebook и угрожает, что использует его в следующем порнопосте. А ведь «приманки» часто используют порнолинки, чтобы заманивать жертв. Парень блокирует профиль Amandine, но Мехди не

успокаивается и возвращается к дискуссии уже под ником Léa Pierné — это еще один фейковый аккаунт сети. После блокировки оказывается, что у Мехди есть доступ к еще одному фейку – Isabelle Bekaert. Понятно, что по крайней мере, в сентябре 2016 года он контролировал минимум три крупных фейковых аккаунта – ключевых для сети. Он даже признался в публикации порноконтента.

Банда из Марселя

Все стало еще интересней, когда мы поискали Мехди в Google. Его имя не раз всплывало на геймерских форумах Франции. Еще с 2012 года пользователи форума хотели, чтобы его заблокировали в Facebook – по причине того, что он постит украденные фото девушек. В этих старых постах на форуме фигурирует также парень, представляющийся партнером Мехди. Назовем его «Пабло». Он дружит с теми пользователями, которые вовлечены в работу сети. Пабло и Мехди – родом из южной Франции, живут в районе Марселя.

Порывшись в интернете еще немного, я наткнулся на два рекламных объявления – от Пабло и от Мехди, опубликованные на сайте Webfrance в апреле 2015 года. В обоих случаях они пытаются продать одну и ту же Facebook-страницу, ныне уже недоступную, на тот момент – с 280 000 подписчиков. В комментариях некто жалуется, что уже «три раза пострадал от мошенничества Пабло», который пытался продать ему фейковые аккаунты.

Во втором объявлении Пабло рассказывает о том, что хочет уйти из соцсетей, чтобы жить реальной жизнью. Он продает три страницы, с 280 000, 129 000 и 70 000 активных пользователей, при этом адрес почты включает имя Мехди.

Здесь у истории намечается неожиданный поворот. Пока я искал Пабло в Facebook, я наткнулся на очень странный профиль – от его имени, с его фотографией. 10 июля 2013 года этот аккаунт опубликовал альбом с 373 фото, в общем доступе. Фото выглядят как скриншоты с компьютеров и мобильных телефонов. На этих скриншотах видна «внутренняя кухня» этой сети.

Здесь есть фото девушек, созданных для завлекания пользователей, статистика фейковых профилей, статистика вовлечения, скриншот чата, где Мехди просит друга сделать его администратором страницы. «Хочу облапошить чувака, и только что сказал ему, что я – админ». Спустя пару минут он уже хвастается, что обман удался. В этом же альбоме – платеж по PayPal на сумму в 500 евро. Есть скриншоты того, как собственно проходит sextortion-мошенничество – в процессе используются порнографические видео, чтобы вынудить пользователя перейти к более решительным действиям, сам же мошенник занят записью доказательств для дальнейшего шантажа.

Мы не можем быть точно уверены о происхождении этих фото. Маловероятно, чтобы кто-то подделал 373 фото, чтобы испортить репутацию Пабло. Может, это – последствия взлома? Возможно, их по ошибке загрузил кто-то, кто работает в сети?

«Пабло» и «Мехди» проигнорировали наши попытки с ними связаться. Однако моя коллега Мари-Эва пообщалась с двумя реальными молодыми

женщинами, которые участвовали в работе сети, перепощивая посты с фейковых-аккаунтов. Обе подтвердили, что таким образом зарабатывают деньги. По словам одной из них, за репосты она заработала около 10 000 евро в месяц. Обе женщины сначала согласились на детальное интервью, потом внезапно исчезли. После этого стали исчезать и фейковые профили.

Мы также проанализировали коды мошеннических страниц, линки на которые публиковала сеть. Оказалось, что сеть использует один из CPA-сервисов. Исходя из данных на сайте, которая управляет CPA, сеть может зарабатывать до 28 евро каждый раз, когда пользователь, переходя по линку, авторизуется на сайте. Учитывая сотни тысяч подписчиков этой сети, она должна зарабатывать более, чем достаточно денег.

Возможно, сеть передает своих пользователей мошенникам за долю в прибыли. Или же мошенники выявили, что внутри сети их ожидают идеальные охотничьи угодья. Что мы знаем точно – так это то, что в целом процесс отлажен почти безупречно.

А что же случилось с Беатрис? Мы не выяснили, кто стоит за ее профилем. Но недавно она перестала публиковать сексуальные фото и вернулась к старой практике – фото больных людей или людей с инвалидностью.

(вгору)

Додаток 18

15.11.2017

Владимир Кондрашов

Провайдеры заявляют о подмене понятий в законодательстве о кибербезопасности

Операторы и провайдеры – члены ИнАУ 14 ноября призвали экспертов Совета Европы помочь в «противодействии мошеннической практике подмены понятий в законодательстве о кибербезопасности» (InternetUA).

Об этом сообщает InternetUA со ссылкой на ИнАУ.

Недовольство операторов и провайдеров вызвали законодательные инициативы, где «суть предлагаемого законопроекта противоположная его декларируемой цели и названию, когда привлекательным и «проходным» названием прикрывается диктаторская и антирыночная суть».

Речь идет о трех документах – законопроекте об имплементации Конвенции о киберпреступности, правительственном законопроекте №7275 и уже принятом законе «О государственной поддержке кинематографии в Украине».

В законе о господдержке кинематографии в Украине, по мнению провайдеров, медиагруппы пролоббировали чрезмерные обязанности датацентров по досудебной блокировке контента:

– В Специальном докладе 301 2017 года Торгового представительства США отмечено беспокойство из-за того, что в этом законе некоторые

обязанности являются слишком неоднозначными и тяжелыми, чтобы облегчить и эффективно реагировать на интернет-пиратство, – считают в ИнАУ.

В законопроект об имплементации Конвенции о киберпреступности, отметили во время вчерашней встречи, «представители силовых структур планируют добавить блокировки интернет-контента провайдерами, о чем в Конвенции нет и речи».

Правительственный законопроект №7275, о котором InternetUA писал 15 ноября, по мнению провайдеров, несмотря на декларируемое противодействие безосновательному изъятию органами досудебного расследования компьютерной техники у субъектов хозяйствования, фактически отменяет даже те механизмы противодействия изъятию серверов, что действуют сегодня. Законопроект также «создает коррупционный механизм, когда правоохранители будут сами решать, удалять серверы, или копировать с них информацию».

Отдельно Интернет Ассоциация огласила собственную позицию по блокировке интернет-контента. Она состоит в том, что технически блокировка и удаление интернет-контента возможно только в случае выполнения такого требования владельцем сайта или дата-центром, где размещен этот контент, ведь корректная блокировка интернет-контента провайдерами доступа технически невозможна. Сама же блокировка контента, по мнению операторов и провайдеров, должна осуществляться только по решению суда, а в случае иностранной юрисдикции собственника вебсайта или дата-центра – с применением международных правовых механизмов.

(вгору)

Додаток 19

20.11.2017

Парламент ЕС рассматривает возможность блокировки веб-сайтов в рамках защиты прав пользователей

Согласно новому закону, принятому на днях в парламенте Евросоюза, теперь появится возможность заблокировать неугодные веб-сайты, которые по тем или иным причинам нарушают права пользователей (InternetUA).

Эта мера была принята в рамках обсуждения защиты прав потребителя и касается недобросовестных веб-сервисов, ориентированных в основном на торговлю и применения компенсационных санкций в том случае, если пользователь понёс материальные убытки в ходе сделки с тем или иным поставщиком услуг. Однако итоговый вердикт звучит как возможность отсудить право владения доменного имени у владельца сайта в том случае, если в принципе само содержание данного ресурса посчитается как нечто вызывающее, оскорбительное или же неправомерное и, разумеется, подлежит устранению.

Блокировка может осуществляться несколькими способами. Первый и наиболее очевидный – владелец ресурса добровольно удаляет незаконный

контент, или обязан продемонстрировать пользователям предупреждение об оном. Второй – обратиться к провайдеру ресурса с просьбой удалить контент, из-за которого возник конфликт. Третий – разделегировать доменное имя, после чего, разумеется, владелец ресурса потеряет доступ к своему сайту.

Разумеется, мнение самих пользователей в данном случае не учитывается, и отказаться от подобной навязчивой защиты прав нельзя. Зато уже сейчас прогнозируют всплеск повышенной цензуры и целенаправленное устранение веб-ресурсов, которые до этого вполне мирно существовали на просторах всемирной Сети.

На данном этапе закон принят, но никаких активных действий по блокировке тех или иных сайтов ещё не предпринималось.

(вгору)

Додаток 20

15.11.2017

Центробанк Нидерландов задействует хакеров для атак на банки страны

Центральный банк Нидерландов (De Nederlandsche Bank, DNB) создаст команду из хакеров и экспертов в области кибербезопасности для атак на финансовую инфраструктуру страны. Таким образом регулятор намерен протестировать и улучшить киберзащиту финучреждений, сообщает издание Financieele Dagblad (InternetUA).

Как рассказала в интервью газете представитель Центробанка Петра Хиелкема (Petra Hielkema), команда будет проводить тайные атаки на банки, акционерные компании и клиринговые дома. В настоящее время проект, получивший название Tiber (Threat Intelligence Based Ethical Red Teaming), находится в пилотной фазе. Регулятор не раскрывает информацию о том, в каком состоянии с точки зрения кибербезопасности находится финансовая инфраструктура Нидерландов. Чуть позже Центробанк намерен опубликовать руководство для финучреждений по организации взломов.

Предполагается, что банки будут самостоятельно нанимать хакеров (так называемая «красная команда»), а попытки компрометации систем осуществляться под наблюдением DNB. О готовящейся атаке на финорганизацию проинформируют лишь небольшую группу экспертов («белая команда»). Остальные сотрудники («синяя команда») должны будут отразить атаку, не подозревая, что она тестовая. По данным газеты, в рамках проекта Tiber будут имитироваться известные потенциальные сценарии кибератак. Длительность фальшивых атак составит от 6 до 9 месяцев.

(вгору)

Додаток 21

15.11.2017

Карта будущего: изобретена платежная карта с временным ПИН-кодом и экраном

Инновационная карта Da Vinci Choice представляет собой целый компьютер, обещает полностью устранить необходимость в паролях и трансформировать сферу платежей (InternetUA).

В современном мире, полном хакеров, низкого уровня кибербезопасности и слабых паролей, нам необходимы более надежные банковские карты, чтобы быть уверенными в сохранности наших денег.

Инновационную карту будущего, Da Vinci Choice, изобрел Саймон Хьюитт, бывший начальник отдела безопасности крупнейших банковских групп Австралии.

Новая карта представляет собой целый компьютер, обещает полностью устранить необходимость в паролях и трансформировать сферу платежей.

Как работает Da Vinci Choice

На первый взгляд Da Vinci Choice ничем не отличается от любой другой банковской карты в нашем кошельке – она такая же тонкая и сделана из пластика.

Но стоит только перевернуть ее, как становится очевидно, в чем ее особенность и ценность: карта представляет собой мини-компьютер с маленьким экраном и клавиатурой.

Чтобы воспользоваться картой, необходимо ввести пароль Da Vinci PIN – единственный пароль, который Вам потребуется – и выбрать карту, с которой будут списаны средства, так как пользователь может привязать к карте Da Vinci все уже имеющиеся у него платежные карты.

Как только карта AMEX, MSTRCARD, или любая другая карта, которую вы выберете, появится на мини-экране, карту Da Vinci нужно поднести к бесконтактному считывающему устройству, чтобы совершить транзакцию.

Нет ПИН-кода, нет проблем

Для оплаты крупного счета (или снятия большой суммы в банкомате) на экране карты Da Vinci появится временный одноразовый ПИН-код, благодаря которому снижается риск мошенничества: после того, как клиент использует его для совершения транзакции, одноразовый ПИН-код перестает действовать.

Da Vinci Choice поступит в продажу в начале 2018 года и будет стоить около 75 фунтов стерлингов.

(вгору)

Додаток 22

15.11.2017

Создана система, которая защитит бизнес от популярных паролей

Компания Shape Security запустила систему Blackfish, предназначенную для профилактики использования хакерами похищенных или утекших паролей. Пользователи часто обходятся одной-двумя комбинациями логинов и паролей

на десятках разных ресурсов, поэтому утечка логинов с одного может представлять угрозу сразу для многих других (InternetUA).

До того, как станет известно всем

Компания Shape Security разработала систему Blackfish, предназначенную для идентификации украденных логинов и паролей в Сети еще до того, как об утечке становится известно. Технология призвана помочь бизнесменам блокировать использование их паролей, украденных на некорпоративных ресурсах, и тем самым пресекать попытки захватов корпоративных аккаунтов.

Это связано с тем, что киберпреступники регулярно автоматизируют процесс тестирования украденных или утекших паролей на сторонних сайтах, исходя из того, что юзеры часто используют одни и те же комбинации на нескольких разных ресурсах.

При этом мошенники нередко используют утекшие пароли также для того, чтобы делать покупки в Сети за чужой счет. По оценкам Shape Security, во многих отраслях, в том числе в ритейле, более 90 % попыток входа в онлайновые системы так или иначе связаны с попытками воспользоваться чужими логинами и паролями.

На сегодняшний день клиентами Shape Security являются топовые банки, авиалинии, ведущие гостиничные сети и два министерства в США.

Как это работает

Описание принципов работы системы Blackfish довольно скупо. На сайте разработчиков указывается лишь, что Blackfish задействует искусственный интеллект для идентификации атак с использованием угнанных паролей. В первую очередь, система смотрит, откуда именно злоумышленники пытаются получить доступ к интересующим их ресурсам.

То есть, например, если тот или иной пользователь регулярно подключается к одному и тому же банку из нескольких точек (из дома или с работы), а затем вдруг происходит попытка залогиниться из совершенно другого места, располагающегося на большом удалении от прежних точек, то система на это среагирует. Особенно систему насторожит, если подозрительная попытка входа имела место спустя слишком короткое время для физического преодоления этого расстояния.

По каким еще признакам Blackfish определяет, произошел ли угон паролей, остается неизвестным.

В случае, если система убеждена, что пара логин-пароль скомпрометирована, то эта комбинация получает соответствующую пометку и деактивируется для всех клиентов Blackfish. Вдобавок система собирает информацию о возможных утечках и попытках эксплуатации краденых паролей своих клиентов, ускоряя обмен такой информацией и тем самым повышая общий уровень защищенности.

Примечательно, что информация о самих скомпрометированных паролях хранится в системе Blackfish исключительно в виде хэшей, пропущенных через так называемый фильтр Блума, – так что даже если злоумышленники взломают

саму систему, получить из нее какую-либо полезную информацию о паролях не удастся.

(вгору)

Додаток 23

15.11.2017

Дмитрий Малышко

Шпионская угроза:Google Play удалит приложения, которые используют API

Google удалит из Play Store все приложения, предоставляющие специальные возможности (InternetUA).

Изменения не коснутся программ, предназначенных для людей с ограниченными возможностями, сообщает Корбин Девенпорт, разработчик софта, в том числе расширений для браузера Chrome.

В течение многих лет Android позволял приложениям влиять на поведение других приложений, используя Accessibility Services – специальные возможности. Хотя у разработчиков этих программ была цель создать приложения для пользователей с ограниченными возможностями, API часто используются для других функций. Среди них – наложение содержимого, заполнения текстовых полей и т. д.). LastPass, Universal Copy, Clipboard Actions, Cerberus, Signal Spy, Tasker и Network Monitor Mini – и еще многие другие приложения используют API во всю прыть.

Хотя службы специальных возможностей могут значительно расширить функциональность приложений, они потенциально могут создать угрозу безопасности. Если приложения получают необходимые разрешения, они могут при помощи API считывать данные из других приложений и пересылать их третьим лицам. Вероятно, по этой причине Google отправил электронные письма разработчикам приложений относительно использования служб доступности.

Разработчик BatterySaver получил следующее сообщение:

«Мы обращаемся к вам, потому что ваше приложение, BatterySaver System Shortcut, с именем пакета com.floriandraschbacher.batterysaver.free запрашивает android.permission.BIND_ACCESSIBILITY_SERVICE .

Приложения, запрашивающие специальные возможности, должны использоваться только для предоставления помощи пользователям с ограниченными возможностями, которые используют устройства и приложения Android. Ваше приложение должно соответствовать нашей политике разрешений и требованиям раскрытия пользовательских данных.

Что нужно сделать: если вы еще этого не сделали, объясните пользователям, как ваше приложение использует «android.permission.BIND_ACCESSIBILITY_SERVICE». Это поможет пользователям с ограниченными возможностями использовать устройства и приложения Android. Приложения, которые не могут выполнить это требование

в течение 30 дней, могут быть удалены из Google Play. Кроме того, вы можете удалить любые запросы на службы доступности в своем приложении.

Вы также можете отказаться от публикации своего приложения.

Все нарушения отслеживаются. Серьезные или неоднократные нарушения любого характера приведут к удалению вашей учетной записи разработчика, а также к расследованию и возможному удалению связанных аккаунтов Google.

Если вы пересмотрели политику и считаете, что, мы, возможно, допустили ошибку, обратитесь в нашу службу поддержки. Один из моих коллег свяжется с вами в течение 2 рабочих дней.

С Уважением, Группа оценки Google Play»

Подобное письмо получили многие разработчики – от них много постов на форуме Reddit. Это означает, что в ближайшее время функциональность многие приложений очень сильно ухудшится, если их разработчики захотят остаться в Play Store или не смогут убедить Google, что их приложения полезны для людей с ограниченными возможностями.

Если кратко резюмировать сегодняшнюю «открытость» Андроида для разработчиков, можно уверенно предположить, что доход разработчиков от загрузки, разработанных ими бесплатных приложений, состоит именно в получении конфиденциальной информации или от деятельности гаджета-зомби, о которой законному владельцу может быть ничего не известно.

Новая политика может иметь серьезные последствия для сотен приложений, особенно тех, которые предназначены для костумизации или для опытных пользователей. Google пока не дал комментариев.

Что касается самих Андроид-пользователей, то, скорее всего – вредоностный софт останется их личной проблемой.

(вгору)

Додаток 24

15.11.2017

Из подключенных к интернету банкоматов можно создать ботнет

Подключенные к интернету банкоматы могут быть обнаружены по ключевым словам с помощью специальных поисковых сервисов, а затем включены в ботнет. Об этом сообщили исследователи безопасности Ольга Кочетова и Алексей Осипов из «Лаборатории Касперского» журналистам издания Security Week на конференции DefCamp 2017 (InternetUA).

По словам исследователей, многие банкоматы работают на базе устаревшей версии ОС Windows XP, что делает их уязвимыми по умолчанию. Также в банкоматах могут быть установлены некоторые ненужные приложения, позволяющие взломать устройство, например, программа TeamViewer или уязвимая версия Adobe Acrobat Reader.

Часто банки не обновляют программное обеспечение банкоматов, подвергая их риску атак с использованием вредоносного ПО и пр. Как правило,

компоненты банкоматов, обеспечивающие сохранность наличных, не имеют отдельных систем защиты. Таким образом, скомпрометировав один элемент, злоумышленники могут взять под контроль все устройство, отметили исследователи. Более того, получив доступ к устройству какого-либо банка, преступники потенциально могут взломать все принадлежащие ему банкоматы.

Как заявили исследователи, существует множество способов взлома банкоматов: физическая установка вредоносного устройства, компрометация компьютеров, контролирующих работу банкоматов, и даже кибератака на компанию, поставляющую прошивку для устройств.

Получив доступ к одному банкомату, злоумышленник способен отправлять команды всем устройствам в сети. После этого преступник может использовать любую карту для вывода наличных в любом банкомате банка, пояснили исследователи.

Все банкоматы банка обычно подключены таким образом, что каждый компьютер в сети может видеть все подключенные устройства. Если злоумышленник внедрит свое устройство в банкомат, подключенный к сетевому кабелю, то получит возможность удаленно им управлять. Как отметили специалисты, это классический пример атаки «человек посередине» (Man-in-the-Middle, MitM). После извлечения устройства исчезнут все следы пребывания злоумышленника в системе. В настоящее время исследователи не зафиксировали случаи создания подобного ботнета, однако злоумышленникам удавалось инфицировать целые сети банков вредоносным ПО для хищения информации.

«Это тоже можно рассматривать как своего рода ботнет, поскольку все устройства были заражены, а злоумышленник дистанционно собирал данные с них», – пояснила Кочетова.

Злоумышленники также могут изъять драйвер VPN из устройства и подключиться к сети банка через него. Подобные VPN-устройства способны работать вне зависимости от хоста, позволяя злоумышленнику использовать их на своем компьютере.

Еще один эффективный метод проникновения в сети банкоматов – поиск устройств через специализированные поисковые системы, такие как Shodan. Банкоматы можно с легкостью найти, если использовать правильные ключевые слова и фразы в поиске, отметили специалисты. Осуществив поиск, злоумышленник может начать проверку открытых портов, а затем попытаться скомпрометировать устройства с помощью эксплоитов. В случае успеха преступники могут похитить информацию клиентов банка или включить устройства в ботнет.

(вгору)

Додаток 25

15.11.2017

Хакеры помогли Пентагону исправить тысячи уязвимостей

Спустя почти год после того, как Пентагон запустил программу раскрытия уязвимостей, ведомство получило 2837 достоверных отчетов об уязвимостях от примерно 650 хакеров из 50 стран по всему миру, указывается в пресс-релизе на портале HackerOne (InternetUA).

Более 100 обнаруженных уязвимостей были критическими или представляли серьезную опасность для систем ведомства. Проблемы в почти 40 компонентах систем Минобороны США позволяли удаленно выполнить код, осуществить SQL-инъекцию и обойти аутентификацию.

Большинство отчетов были представлены исследователями из США, Индии, Великобритании, Пакистана, Филиппин, Египта, России, Франции, Австралии и Канады.

Программа раскрытия уязвимостей Минобороны США не предполагает денежного вознаграждения – она предоставляет только канал для сообщения о проблемах безопасности без возможных юридических последствий. Однако в рамках инициативы Пентагона было запущено несколько временных программ, предлагавших денежные вознаграждения. Исследователи, принявшие участие в данных программах, заработали более $300 тыс. за обнаружение в системах ведомства почти 500 уязвимостей.

Первой такой инициативой была программа Hack the Pentagon («Взломай Пентагон»), в рамках которой исследователи заработали порядка $75 тыс. за 138 сообщений об уязвимостях. Далее ведомство запустило программы Hack the Army («Взломай армию»), в рамках которой было выплачено около $100 тыс. за 118 уязвимостей и Hack the Air Force («Взломай ВВС»), в рамках которой участники обнаружили 207 уязвимостей, заработав в общей сложности $130 тыс.

После успеха данных программ правительственные организации и законодательные учреждения США проявили усиленный интерес к программам выплаты вознаграждений за обнаруженные уязвимости.

Администрация общих служб (General Services Administration, GSA) запустила программу поиска уязвимостей, предлагающую вознаграждение в размере от $300 до $5 тыс. Министерство юстиции США также разработало механизм, призванный помочь организациям в запуске программ по поиску уязвимостей.

(вгору)

Додаток 26

16.11.2017

Расширение для Chrome собирает данные пользователей из Facebook и LinkedIn

Эксперт в области кибербезопасности Лоуренс Абрамс (Lawrence Abrams) обнаружил в каталоге Chrome Web Store подозрительное расширение Browse-Secure, позиционируемое как инструмент, гарантирующий пользователям безопасный поиск. В действительности программа собирает

данные (имя, адрес электронной почты, информацию о поле, номере мобильного телефона и адресе) из учетных записей пользователей в Facebook и LinkedIn и отправляет их на удаленный сервер (InternetUA).

Страница Browse-Secure в Chrome Web Store не вызывает особых подозрений, за исключением отсутствия иллюстраций. По словам Абрамса, расширение также предлагается на сторонних мошеннических сайтах, которые отображают фальшивые уведомления об угрозе безопасности и рекомендуют загрузить плагин для устранения проблем.

После установки Browse-Secure подключается к серверу по адресу backend.chupashop.com/getuid4search и пользователю присваивается идентификатор, который затем используется для определения данного конкретного браузера. Затем расширение обращается к содержащему в нем файлу crawl.json, включающему список правил и URL, которые Browse-Secure использует для извлечения данных. Получив нужную информацию, расширение загружает сведения на сервер. В каких целях разработчики Browse-Secure используют похищенные персональные данные в настоящее время неизвестно, отмечает Абрамс.

В аннотации к расширению разработчики заявляют, что Browse-Secure сделает поиск более безопасным, однако исследователь не уверен в правдивости данного утверждения. После установки расширения в поисковой строке действительно появляется значок с изображение замка, а запросы к поисковым системам Google, MyWebSearch, Bing, MSN, Ask, WoW, MyWay, AOL и SearchLock проходят переадресацию. При поисковом запросе расширение формирует ссылку browse-secure.com/search?a=[id_расширения]&q=[поисковый запрос], затем пользователь перенаправляется в Google или другую поисковую систему. Таким образом, авторы расширения отслеживают еще и IP-адреса пользователей.

Месяцем ранее Абрамс обнаружил плагин для Chrome под названием Ldi, выводящий вредоносную активность расширений на новый уровень. Ldi не только устанавливает в браузере майнер Coinhive, но также использует учетную запись Gmail жертвы для регистрации бесплатных доменов с помощью сервиса Freenom.

(вгору)

Додаток 27

16.11.2017

Пользователи Telegram манипулируют курсами криптовалют по своему желанию

Telegram стал рассадником криптовалютных трейдеров, которые организуют в мессенджере группы с десятками тысяч участников. Распространяя рекламу в Telegram, они искусственно повышают стоимость

криптовалют благодаря активной покупке, а потом сбывают их ничего не подозревающим подписчикам других каналов (InternetUA).

Трейдеры в Telegram

В мессенджере Telegram в большом количестве замечены сообщества, члены которых зарабатывают деньги на «накачке» криптовалют, то есть искусственном повышении их курса с последующей продажей. Эта техника носит название «pump and dump» – «накачай и сбрось». В частности, ее использует Telegram-группа PumpKing Community, насчитывающая около 17 тыс. подписчиков, отмечает издание Business Insider. Помимо нее в мессенджере существуют и другие крупные сообщества криптовалютных трейдеров, в том числе Pump.im, Crypto4Pumps, We Pump и AltTheWay.

Поскольку рынок криптовалют по большей части не регулируется на законодательном уровне, деятельность этих групп пока что не является незаконной. Однако на других рынках – например, на бирже – такие схемы расцениваются как мошеннические, полагает Business Insider.

Telegram стал излюбленным приложением криптовалютных трейдеров благодаря сильному шифрованию и возможности соблюдать анонимность, несмотря на привязку к телефонному номеру. Сообщества трейдеров привлекают внимание потенциальных подписчиков броскими рекламными объявлениями, в которых обещают помочь «сделать деньги». В PumpKing Community такие объявления публикует администратор под псевдонимом Ton Montana.

Как это работает

В определенное время участникам группы сообщают название «накачиваемой» криптовалюты и дают ссылку на ресурс, где они должны начать ее скупать. Всего в PumpKing Community насчитывается более 14 тыс. пользователей, но благодаря перекрестной рекламе, распространяемой по азиатским каналам, в реализацию схемы может быть включено до 60 тыс. человек, утверждает Ton Montana.

На левом скриншоте PumpKing Community обещает пользователям помочь «сделать деньги», на втором – сообщает об охвате аудитории в 60 тыс. человек, на третьем – дает ссылку на криптовалюту, которую нужно скупать

Как демонстрирует Business Insider, после того, как администратор группы отдал распоряжение о скупке криптовалюты Magi, ее курс на бирже Bittrex стремительно пошел вверх, поскольку объемы продажи монет резко возросли. По мере увеличения стоимости монет, множество пользователей в других каналах получают сообщение, что Magi пошла в рост, и что ее нужно как можно быстрее покупать. Эти пользователи не подозревают, что стали жертвой мошеннической схемы. При этом участники PumpKing Community всячески подогревают интерес новых покупателей сообщениями, что это долгосрочный рост, или какими-нибудь новостями.

Например, когда похожее сообщество проводило такую же операцию с криптовалютой VCash, оно использовало новость об открытии создателями валюты нового сайта, что должно было убедить сторонних инвесторов

покупать монеты. Во время «накачки» стоимость монет VCash выросла на 35% за пять минут, отмечает Business Insider.

PumpKing Community предлагает своим пользователям ссылку на «Инструкцию по «накачке» на Bittrex», а также ссылки на группы в Facebook и каналы в Telegram, где можно найти доверчивых инвесторов. Сообщество предупредило, что вся схема с Magi будет проходить в четыре этапа, поэтому средства лучше разделить на три части, чтобы получить максимальную выгоду.

Фаза «дампа»

По достижении монетами Magi пиковой стоимости пользователи PumpKing Community начали продавать их новым покупателям – по цене выше той, по которой они их купили. Волна продаж, как правило, приводит к тому, что курс валюты снова падает, часто ниже той отметки, на которой он был в начале реализации схемы. Трейдеров, «сбросивших» монеты, это уже не беспокоит, зато очень расстраивает пользователей, купивших их по высокой цене.

Нельзя сказать точно, всегда ли трейдеры возвращают потраченные средства и получают прибыль – для этого наплыв сторонних покупателей должен быть достаточно велик. Трейдеры рискуют остаться держателями бесполезных для них монет, если не смогут привлечь инвесторов. Однако их действия в любом случае, независимо от полученной выгоды, были бы признаны незаконными на других рынках.

Мошеннические схемы

За время своего расследования Business Insider отследил реализацию пяти подобных схем в Telegram, но, судя по частоте появления рекламы, их реальное количество гораздо больше, считает издание. Изученные схемы затрагивали криптовалюты UBQ, VCash, Chill Coin, Magi Coin и Indorse. Все они были реализованы или на бирже Bittrex в Лас-Вегасе, или на российской бирже Yobit.

В течение 2017 г. посредством первичного предложения монет (ICO) в мире было собрано более $3 млрд инвестиций. В результате, по данным сайта CoinMarketCap.com, в настоящий момент количество криптовалют в мире превышает 1,2 тыс. Несмотря на предупреждения регуляторов о возможности реализации мошеннических схем, рынок криптовалют дорос в этом году до $200 млрд. Около 80 % его стоимости составляют известные криптовалюты, такие как биткоин или эфир.

(вгору)

Додаток 28

20.11.2017

Илья Кабачинский

Авиакомпании владеют вашими личными данными. И постоянно их используют

Данные о своих пользователях собирают не только интернет-сервисы. Издание Bloomberg подготовило материал на тему сбора и дальнейшего

использованния информации о своих пассажирах авиакомпаниями. Оказывается, они знают о своих клиентах почти все: что вы любите есть, пить, и даже, когда у вас день рождения. Редакция подготовила адаптированный перевод материала (AIN.UA).

Авиакомпании действительно хороши в некоторых вещах: в перемещении людей, обслуживании самолетов и безопасности пассажиров. Кроме этого, они также являются экспертами сбора данных о клиентах: о том, какие типы кредитных карт и компьютеров вы используете, как часто летаете, и где и сколько вы тратите на все дополнительные услуги, в том числе.

Если у вас вдруг исчезла связь, бортпроводники скажут вам, к каким воротам нужно бежать, сколько времени у вас есть, и будет ли ваш следующий рейс вовремя. Но кроме этого, они также могут знать, что на прошлой неделе вы застряли в Буффало на шесть часов из-за задержки рейса и лично извиниться. Они даже могут использовать свой запас ваших данных, чтобы удостовериться, что на борту есть вдоволь красного для владельцев специальных бонусных программ, которые пьют только каберне.

Самые престижные отели давно используют эту стратегию: если вы чувствуете себя особенным и любимым, возможно, вы вернетесь. Теперь к ним примкнули еще и авиакомпании.

«У нас достаточно данных о том, кто вы, куда вы летите, и, что более важно, у нас есть информация о том, когда мы задержали вас, отменили ваш рейс, заставили сменить место или пролили кофе на вас – у нас есть все моменты наших неудач и успеха», – сказал 9 ноября Оскар Муньос – исполнительный директор United Continental Holdings Inc., на конференции, организованной New York Times. «Я думаю, что наши клиенты сегодня нуждаются в более качественном обслуживании и лучшей персонализации. И это то, на чем мы фокусируемся».

В апреле 23 000 работников Delta Air Lines Inc. начали использовать новое программное обеспечение под названием SkyPro на своих мобильных устройствах, чтобы следить за некоторыми основными сведениями о клиентах. Вы получите извинения, если ваш рейс на прошлой неделе был задержан, например. Или благодарность, если вы пролетели 200 000 миль за год. На устройствах Nokia каждое место полета обозначено цветом. Зеленый палец верх для пассажиров Delta – поблагодарить или поздравить, красный – если авиакомпания хочет извиниться за недавнюю неудачу в обслуживании.

American Airlines Group Inc., крупнейший перевозчик в мире, оснащает 24000 бортпроводников устройствами Samsung Galaxy Note. В начале следующего года American выпустит новое приложение iSolve, которое будет решать проблемы обслуживания клиентов на борту.

Как и другие перевозчики, обсуждающие, как использовать «big data» с помощью новых цифровых инструментов, Delta исследует, где находится пугающий фактор во всем этом в понимании клиента. Например, должна ли стюардесса поздравлять вас с днем рождения? Как насчет появления с Кровавой Мэри в руках, потому что вы заказали этот напиток на 9 из ваших

последних 10 рейсов? Что, если на этот раз вы сядете возле вашего босса? А нужно ли обновлять и распространять данные о ценных клиентах во всей компании? Конкретно сейчас ситуация другая, но то, что началось как использование информации, которая есть у авиакомпаний, так или иначе, вскоре может стать целенаправленным накоплением данных о путешественниках.

«Клиент это воспринимает хорошо, но он задается вопросом: «Если они знают, когда у меня день рождения, что еще они знают обо мне?»», – говорит Джон Ромэнтик, управляющий директор службы обеспечения полетов American.

На рейсах Delta нет никаких поздравлений с днем рождения или непрошеных коктейлей. Перевозчик «постепенно увеличивает количество элементов данных, с которыми клиенту, с которым мы взаимодействуем, комфортно», – сказала Аусбанд. Более крупная, ближайшая цель: «Убедиться, что они знают, что они имеют для нас значение, независимо от того, сидят они на месте 32B или 1A».

Мэллори Браун, стюардесса Delta с 10-летним стажем, сказала, что клиенты хорошо реагируют на извинения и благодарности. «Они были впечатлены этим», – рассказала Браун, которая также помогает разработать учебную программу бортового обслуживания для перевозчика. «Все прошло так хорошо, что пассажиры начали говорить об этом».

Delta считает, что знание предпочтений клиентов является «стратегическим преимуществом», – сказала Аусбанд. Это не единственная авиакомпания, когда речь идет об использования клиентской информации, ведь каждая крупная международная авиакомпания изучает, как лучше адаптировать свой подход.

British Airways, которая входит в международную группу Consolidated Airlines Group SA, использовала планшеты iPad с 2011 года. Авиакомпания разработала более 40 приложений для различных аспектов обслуживания клиентов, в том числе таких, которые позволяют бортпроводникам узнавать «топ-клиентов», – заявила пресс-секретарь Кэролайн Титмусс. С помощью iPad стюардесса может также отметить проблемы. Например, если не был принесен конкретный заказ, авиакомпания предложит дополнительные извинения после полета.

В этом сервисном ландшафте многие авиакомпании также будут сталкиваться с тем, как широко распространять такое цифровое взаимодействие. Не мудрее ли будет сосредоточиться на «ценных» клиентах в самолетах премиум-класса или лучше попытаться вовлечь весь самолет? В конце концов, время бортпроводника – очень ограниченный ресурс.

«Мы не думаем, чтобы или одни, или другие», – сказал Дейв О’Фланаган, исполнительный директор Boxever Ltd., который продает программное обеспечение для обслуживания клиентов и услуги для индустрии туризма. «Так люди думали раньше. Мы очень заинтересованы в лояльности для всех».

Одна авиакомпания из Азии, которая использует Boxever, даже планирует предлагать немедленное повышение класса обслуживания, если ваш багаж потерян, сказал О'Фланаган, ссылаясь на быструю эволюцию технологий отслеживания багажа. Поскольку перевозчики развивают более высокий уровень координации данных клиентов, ожидается увеличение количества личных извинений, бесплатных напитков или бонусных миль. Вы сможете получить пожелание счастливого дня рождения, без упоминания вашего возраста, конечно.

(вгору)

Додаток 29

20.11.2017

Крипто-мафия: хакеры нашли новый способ взлома биткоин-кошельков

По мере роста интереса пользователей, в том числе и украинских, к майнингу и криптовалютам, пропорционально увеличилась и заинтересованность мошенников к крипто-кошелькам. Все чаще целью хакеров становятся на только отдельные аккаунты, но и целые криптобиржи (InternetUA).

Для виртуальных взломщиков электронные кошельки, как правило, менее интересны: взломать их не так просто, а добыча оказывается не такой солидной. Другое дело взлом криптобиржи, который позволяет получить доступ сразу ко многим счетам. Именно поэтому атаки на криптобиржи более заметны и вызывают резонанс на рынке.

«Для взлома криптокошелька нужно быть уверенным, что сумма на нем покроет расходы, связанные с его взломом. «Холодный» кошелек (флешка с паролем) более защищена от хакерских атак, но может быть предметом прямого нападения, если злоумышленники знают о такой ценности», – отметил в разговоре с UBR.ua старший аналитик Forex Club Андрей Шевчишин.

Все популярные биткоин-кошельки примерно одинаковы по безопасности, говорят эксперты. К примеру, наиболее популярные сейчас Electrum, Copay и пр., представленные на сайте Bitcoin.org.

А вот малоизвестные кошельки могут оказаться мошенническими проектами. Прецеденты, когда сервисы исчезали вместе со средствами пользователей, уже случались.

Дорогая безопасность

Также стоит обратить внимание на то, предоставляет кошелек приватные ключи от ваших биткоин-адресов или нет. Стоит выбирать кошелек, в котором можно сделать резервную копию приватного ключа с помощью сид-фразы, чтоб в случае утери доступа или сбоев вы могли восстановить доступ к средствам через другие сервисы.

«Не стоит полагаться на кошельки, не предоставляющие такой возможности, так как в этом случае ваши риски значительно возрастают.

Удобства и преференции, которые могут предоставлять подобные сервисы, того не стоят», – заметил в беседе с UBR.ua маркетолог биткоин-агентства Kuna Вадим Попов.

Кошельки делятся на два типа: Software и Hardware. Последний – это фактически отдельная флешка, без которой деньги с кошелька не спишутся. Самые лучшие и защищенные, по мнению экспертов, – это Hardware. А из них наилучшим образом себя зарекомендовал Ledger. Также надежен и популярен Trezor. Если оперируете значительными сумами – придется потратиться на дорогой кошелек.

«Чем больше безопасности, тем меньше гибкости и удобства в использовании. Поэтому, если у вас незначительное количество монет, то не имеет смысла заморачиваться покупкой дорогого Hardware кошелька. Что касается Software – выбирайте проверенного разработчика. А там уже ориентируйтесь на удобство интерфейса. Самые популярные – Jaxx и Electrum», – рассказал UBR.ua финансист, управляющий партнер компании «ЭСКА Капитал» Сергей Васьков.

Слабое звено биткоина

Надежными считаются те кошельки, которые хранят ключи на устройстве. Соответственно, небезопасные те, что хранят ключи где-то еще, то есть не на вашем устройстве, например, в облаке. Существует риск, что ключи оттуда могут уплыть в чужие руки, а потеря ключа равносильна потере криптоактива.

«Лично пользуюсь bread wallet. Рекомендации очень простые: как только завели секьюрный правильный кошелек, обязательно выпишите и сохраните мнемоническую фразу (набор слов) — фактически это и есть ваш ключ. С ее помощью в любой момент можно полностью восстановить доступ к криптоактиву. Эту фразу надо хранить в безопасном месте. Любой, кто узнает ее, автоматически получит доступ к средствам», – подметил UBR.ua основатель plugandmine.com Сергей Козлов.

По словам экспертов, желательно предпочесть кошельки-приложения, а не онлайн-сервисы. Поскольку последние всегда находятся в сети, и вероятность их взлома потенциально выше.

(вгору)

Додаток 30

20.11.2017

Золото оператора. Как мобильщики превращают наши данные в деньги

Big Data стала новой валютой. Все говорят, что Facebook и Google бесплатны. Но мы, пользователи, за их сервисы расплачиваемся нашими данными. Компании их пакуют и продают тем, кому это интересно (Центр информационной безопасности).

Эти слова в числе прочих были адресованы выпускникам Big Data School от Киевстар. В скором будущем часть из них пополнит ряды сотрудников оператора, чтобы как раз превращать анализ данных его абонентов в дополнительную прибыль.

Такой специфический хантинг специалистов Киевстар провел уже во второй раз. И на этом не останавливается.

LIGA.net выяснила, зачем операторы продают обезличенную информацию о собственных абонентах и как решают проблему с нехваткой дата-специалистов.

Ничего личного – только бизнес

Данные мобильных операторов – лакомый кусочек для множества бизнесов. Ни у кого другого в Украине нет настолько детальной информации о перемещениях, частоте звонков и потреблении трафика. Да и совокупная аудитория украинских мобильщиков уже давно превысила население страны.

Одно это позволяет понять, где ходит нужная аудитория и в какой момент ей лучше направить рекламное предложение, чтобы оно не улетело в спам.

«Раньше все думали, что big data = big money. От внедрения технологии в бизнес наивно ожидали, что она умножит прибыли на 10. Постепенно лихорадка проходит, и все думают, как же это все-таки нормально применить. Не глобально, а в конкретных кейсах», – говорит Сергей Марин, основатель Студии данных и Школы данных, один из менторов Big Data School.

Для самого оператора это способ заработка. Во-первых, анализ поведения абонента и потребления им услуг подсказывает, кому какой тариф предложить, кому направить спецпредложение или подсказку о новом офисе. Если все попало в цель, абонент становится более лояльным и продолжает приносить деньги компании.

Во-вторых, есть внешние запросы.

«Мы уже активно реализуем проекты для внешних заказчиков. Одна сфера – скоринг, в частности банковский, где мы предсказываем вероятность дефолта заемщика. Вторая – так называемые хитмэпы (тепловые карты), когда мы показываем вероятное местоположение групп клиентов», – говорит диджитал-директор Киевстар Виталий Султан.

Абонентов успокаивают: никто не передает «сырую» личную информацию. Никто не дает слушать звонки, читать SMS или список сайтов, на которых проводит время абонент с конкретным номером. Внешнему заказчику передается только анонимизированная и зашифрованная информация.

Например, в случае кредитного скоринга банк отправляет оператору запрос по конкретному номеру заемщика, а в ответ получает только абстрактную цифру «благонадежности». За ней стоят модели, которые опираются на десятки и сотни данных об абоненте.

Для получения «тепловой карты» расположения целевой аудитории заказчика (того же банка или ритейл-сети) оператор разрабатывает предсказательную модель. По ключевым характеристикам она помогает выделить из всей базы абонентов нужный сегмент.

Таких проектов, по словам Digital-директора Киевстар, уже «двузначное число». Среди них и тепловые карты для Киева и Одессы, где оператор помог городским властям проанализировать транспортные потоки и скорректировать маркетинговую политику по развитию туризма в регионе. Новые направления тоже открываются, но для них не хватает людей.

Не учат в школе. И в университетах тоже

По словам дата-архитектора SoftServe Родиона Миронова, технология big data уже состоялась. Но data science только набирает силу, и хайпа вокруг нее пока еще больше, чем реальных приложений. Однако те приложения, которые будут менять бизнес, страну или мир, будут создаваться в том числе теми, кто сейчас учится.

Но в Украине готового механизма обучения специалистов нет. Государственные и коммерческие вузы пока не предложили ничего, что могло бы закрыть дыру по Big Data. Онлайн-курсы по большей части касаются машинного обучения и создания моделей.

Другой момент – у технически подкованных дата-аналитиков есть оторванность от бизнеса. Строя модели, они не видят конечной цели для заказчика, из-за чего эффективность внедрения методов big data падает.

Так мобильные операторы пришли к мысли, что проще научить специалистов самим, чем ждать, пока рынок образования дорастет до спроса.

Недавно Vodafone объявил об отборе в Big Data Lab, в рамках которой впервые откроет массив своих реальных данных о 100 000 абонентах из Западной Украины всем заинтересованным дата-аналитикам и разработчикам. Доступ открывают на 3 месяца. За это время участники программы должны разработать свои проекты с помощью больших данных. Не исключено, что финалисты получат предложение о работе.

Киевстар уже более двух лет идет другим маршрутом. Big Data School – это бесплатная программа обучения по направлениям big data и machine learning. Кандидаты проходят двухуровневый отбор – тестовое задание и собеседование. После этого с помощью экспертов они изучают последние тренды в big data и тренируются, решая реальные бизнес-кейсы. На время обучения Киевстар открывает для них доступ ко всей базе анонимизированных данных об абонентах.

Первая школа состояла из обзорных модулей, разбитых на несколько месяцев. В 2016 году по ее результатам Big Data команда Киевстар увеличилась на трех человек.

При отборе на курс этого года компания сделала упор на ребят с глубоким знанием аналитики и пропустила их через 10-дневный интенсив, а в качестве менторов пригласила практикующих дата-инженеров, дата-сайнтистов и дата-архитекторов.

«На курсовом проекте мы искали определенные признаки, по которым можно было бы сказать, что абонент руководит компанией или входит в правление. Мы строили гипотезы и искали им подтверждение в данных», –

рассказывает Юлия, математик-программист, выпускница второй Big Data School.

Кирилл, тоже выпускник школы Киевстар, отметил комплексность: «Нам дали полный рабочий набор - не просто анализ данных, непонятно откуда взятых, но и инструменты хранилища, концепции, которые используются в обработке больших данных, аналитику. До школы были обрывочные понимания, а к последним дням занятий пазл сложился».

С момента выпуска и до окончательного вхождения студента в команду оператора может пройти не один месяц. «Мы не строим иллюзии, что все ребята будут работать в нашей компании. Многим из них мы сделаем предложение. “Но многие уйдут в другие компании и создадут там дата-продукты, которые принесут новую ценность клиентам и доходы бизнесу. Это постепенно увеличит интеллектуальную составляющую в украинской экономике», – отмечает Виталий Султан.

Если планы мобильных операторов сбудутся, в ближайший год-два big data поменяет восприятие их на рынке: помимо простых поставщиков связи, они станут поставщиками бизнес-решений. А за внимание и деньги украинского потребителя теперь будут сражаться куда более технологично.

(вгору)

Додаток 31

22.11.2017

100 % организаций по всему миру подверглись мобильным атакам - Check Point

Компания Check Point представила результаты первого исследования атак на мобильные устройства в корпоративных средах.

Согласно данным, полученным от 850 компаний на четырех континентах, мобильные устройства, используемые в организациях, уязвимы для атак вне зависимости от операционной системы – Android или iOS (ITnews).

Мобильные угрозы способны скомпрометировать любое устройство и предоставить злоумышленникам доступ к ценным данным в любое время. Любой бизнес может стать жертвой этих угроз – от финансовых организаций до государственных структур или промышленных компаний.

Ключевые результаты исследования:

100 % организаций подверглись атакам мобильного вредоносного ПО;

54 – среднее число атак на мобильные платформы одной компании;

89 % компаний столкнулись хотя бы с одной атакой «Человек посередине» (Man-in-the-middle, MitM) на сеть Wi-Fi;

75 % организаций имеют в среднем 35 взломанных устройств, которые, в зависимости от платформы, подверглись операции jailbreak (iOS) или root (Android).

Чтобы дать отпор мобильным угрозам, Check Point представил улучшенную версию SandBlast Mobile – ведущего в отрасли решения для

предотвращения продвинутых кибератак на корпоративные мобильные устройства. Check Point SandBlast Mobile защищает от угроз для мобильных устройств и приложений, а также сетевых атак, и обеспечивает самый высокий уровень отслеживания угроз. Check Point расширил возможности SandBlast Mobile, которые позволят организациям и пользователям быть на шаг впереди угроз:

Система обнаружения угроз на базе искусственного интеллекта, чтобы останавливать вредоносное ПО «нулевого дня»;

Блокирование таргетированного SMS-фишинга на устройствах iOS и Android;

Новое приложение, которое позволяет пользователям отслеживать и контролировать безопасность устройств.

«Финансовая выгода и частота атак на мобильные устройства превысили аналогичные показатели для ПК в 2017 г. Этот факт объясняет результаты исследования Check Point, – говорит Василий Дягилев, глава представительства компании Check Point Software Technologies в России и СНГ. – По сути, мобильные устройства – это новый бэкдор для киберпреступников, и мы рады предоставить усовершенствованное решение SandBlast Mobile для защиты компаний и пользователей».

По независимой оценке Miercom Mobile Threat Defense Industry Assessment 2017, Check Point достиг наивысших результатов по обнаружению угроз среди ИБ-вендоров, принявших участие в тестировании. Check Point смог отследить новые векторы атак на мобильные устройства – от известного ПО, сетевых и операционных эксплойт-китов до угроз нулевого дня, SMS-атак и Bluetooth эксплойтов. В ответ на эти угрозы Check Point разработал комплексное решение для корпоративных заказчиков в рамках архитектуры безопасности Check Point Infinity. Infinity производит постоянный обмен показателями между сетевыми устройствами, конечными ПК, облаком и мобильными устройствами. Для заказчиков и пользователей ZoneAlarm существует специальное предложение.

(вгору)

Додаток 32

26.11.2017

Раскрыты подробности деятельности хакерской группировки Fancy Bear

Хакерская группировка Fancy Bear, которую связывают с российскими спецслужбами, в течение трех лет арендовала серверы у британской компании Crookservers, выяснили журналисты BBC в результате проведенного расследования (InternetUA).

Арендованные серверы использовались для кибератаки на компьютерную сеть немецкого парламента, перехвата трафика сайта нигерийского правительства и взлома устройств Apple, пишет BBC. Как предполагают

эксперты, Fancy Bear, также известная как APT28, Sofacy, Iron Twilight и Pawn Storm, также причастна ко взлому серверов Национального комитета демократической партии США во время избирательной кампании в 2016 году. IP-адрес, привязанный к арендованному у Crookservers серверу, был обнаружен во вредоносном коде, использовавшемуся в данной атаке, отмечает BBC.

Crookservers специализируется на перепродаже доступа к серверам. Подобный бизнес целиком и полностью ведется online. Сами сдававшиеся серверы принадлежали другой компании и физически располагались во Франции и Канаде. Журналистам удалось выяснить имя управляющего компанией. Им оказался некто по имени Усман Ашраф (Usman Ashraf). Согласно информации из социальных сетей и других интернет-источников, в период с 2010 года по середину 2014 Ашраф находился в Олдеме (городе, где была зарегистрирована Crookservers). Сейчас он, судя по всему, проживает в Пакистане.

Журналисты связались с Ашрафом. По его словам, в компании не знали, что предоставляют услуги хакерам. После того, как в 2015 году Ашрафу сообщили о деятельности злоумышленников, Crookservers аннулировала их аккаунты.

«Мы никогда не знаем, каким образом клиент использует сервер», – отметил Ашраф.

Согласно техническим и финансовым документам Crookservers, с которыми ознакомились журналисты, Fancy Bear располагала значительными финансовыми средствами и проводила платежи через online-сервисы, часть которых впоследствии была закрыта в ходе операции по пресечению отмывания денег.

Fancy Bear арендовала серверы у Crookservers более трех лет, скрывая следы своей деятельности с помощью фальшивых удостоверений личности, виртуальных частных сетей (VPN) и платежных систем, использование которых трудно отследить. С помощью серверов компании хакеры провели ряд своих операций.

Хакеры связывались с компанией, используя псевдонимы, например, Роман Бреческу (Roman Brecesku) или Николай Младенов (Nikolay Mladenov). Последний арендовал у Crookservers сервер, который затем связали с атакой на Бундестаг. За услуги компании Младенов расплатился биткойнами через систему Perfect Money. Сервер он использовал до июня 2015 года, пока СМИ не сообщили об инциденте и Crookservers потребовала прекратить аренду. IP-адрес того же сервера фигурировал и во вредоносной программе, использовавшейся для взлома учетных записей ряда посетителей авиасалона в Фарнборо в 2014 году, а также содержался в черве, который Fancy Bear применила в кибератаках на одну из британских телекомпаний и Национальный комитет демократической партии США, хотя к тому времени у группировки уже не было доступа к данному серверу.

Финансовая учетная запись Младенова использовалась и другим хакером, который под псевдонимом Клаус Вернер (Klaus Werner) арендовал у

Crookservers дополнительные серверы. На один из них поступал перенаправленный трафик с официального правительственного сайта Нигерии.

Один из серверов Crookservers и электронный адрес, с которого поступил запрос на его аренду, могут быть связаны с вредоносной программой, использовавшейся для взлома устройств на базе iOS, пишет BBC. Функционал вредоноса включает возможность аудиозаписи разговоров и хищения текстовых сообщений.

В общей сложности группировка потратила на услуги Crookservers $6 тыс. Перевод платежей осуществлялся через финансовые сервисы, обеспечивающие высокий уровень анонимности. В их числе Bitcoin, Liberty Reserve и Perfect Money. Британская компания Elliptic, специализирующаяся на выявлении незаконного использования биткойнов, проанализировала выплаты Fancy Bear и обнаружила электронный кошелек, содержавших биткойны на сумму $100 тыс. Некоторые средства в кошельке были приобретены через биржу BTC-e. Напомним, американские правоохранители прекратили деятельность площадки в июле нынешнего года, а ее предполагаемый основатель Александр Винник был арестован в Греции по обвинению в отмывании не менее $4 млрд.

(вгору)

Додаток 33

27.11.2017

«Доктор Веб» исследовал нового банковского троянца

Троянцы, предназначенные для хищения денег с банковских счетов, представляют серьезную угрозу (ITnews).

Обычно это довольно сложные многокомпонентные вредоносные программы, поэтому банковские троянцы появляются на свет нечасто. Вирусные аналитики компании «Доктор Веб» исследовали новую версию вредоносной программы, относящейся к широко известному семейству Trojan.Gozi.

Новый банковский троянец, получивший наименование Trojan.Gozi.64, основывается на исходном коде предшествующих версий Trojan.Gozi, который уже долгое время находится в свободном доступе. Как и другие представители этого семейства, Trojan.Gozi.64 может заражать компьютеры под управлением 32- и 64-разрядных версий Windows. Троянец имеет модульную архитектуру, но, в отличие от предыдущих модификаций, он полностью состоит из отдельных загружаемых плагинов. Также Trojan.Gozi.64 не имеет алгоритмов для генерации имен управляющих серверов – их адреса «зашиты» в его конфигурации, в то время как одна из первых версий Gozi использовала в качестве словаря текстовый файл, загружаемый с сервера NASA.

Создатели троянца заложили в него ограничение, благодаря которому он способен работать с операционными системами Microsoft Windows 7 и выше, в более ранних версиях Windows вредоносная программа не запускается.

Дополнительные модули скачиваются с управляющего сервера специальной библиотекой-лоадером, при этом протокол обмена данными использует шифрование. Лоадер Trojan.Gozi.64 может выполнять на зараженной машине следующие вредоносные функции:

– проверка обновлений троянца;

– загрузка с удаленного сервера плагинов для браузеров, с помощью которых выполняются веб-инжекты;

– загрузка с удаленного сервера конфигурации веб-инжектов;

– получение персональных заданий, в том числе для загрузки дополнительных плагинов;

– удаленное управление компьютером.

Для осуществления веб-инжектов в каждом браузере Trojan.Gozi.64 использует собственный настраиваемый плагин. В настоящий момент вирусным аналитикам известны плагины для Microsoft Internet Explorer, Microsoft Edge, Google Chrome и Mozilla Firefox. Установив соответствующий модуль, троянец получает с управляющего сервера ZIP-архив с конфигурацией для выполнения веб-инжектов. В результате Trojan.Gozi.64 может встраивать в просматриваемые пользователем веб-страницы произвольное содержимое – например, поддельные формы авторизации на банковских сайтах и в системах банк-клиент. При этом, поскольку модификация веб-страниц происходит непосредственно на зараженном компьютере, URL такого сайта в адресной строке браузера остается корректным, что может ввести пользователя в заблуждение и усыпить его бдительность. Введенные в поддельную форму данные передаются злоумышленникам, в результате чего учетная запись жертвы троянца может быть скомпрометирована.

Помимо этого на зараженный компьютер могут быть загружены и установлены дополнительные модули – в частности, плагин, фиксирующий нажатие пользователем клавиш (кейлоггер), модуль для удаленного доступа к инфицированной машине (VNC), компонент SOCKS-proxy-сервера, плагин для хищения учетных данных из почтовых клиентов и некоторые другие.

Банковский троянец Trojan.Gozi.64 не представляет опасности для пользователей антивирусных продуктов Dr.Web, поскольку сигнатуры вредоносной программы и ее модулей добавлены в вирусные базы.

(вгору)

Соціальні мережі

як чинник інформаційної безпеки

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

Упорядник **Терещенко** Ірина Юріївна

Редактор О. Федоренко

Свідоцтво про державну реєстрацію КВ № 5358 від 03.08.2001 р.

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