СОЦІАЛЬНІ МЕРЕЖІ ЯК ЧИННИК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Огляд інтернет-ресурсів
(7.06–20.06)

2018 № 12

Соціальні мережі
як чинник інформаційної безпеки

Інформаційно-аналітичний бюлетень
Додаток до журналу «Україна: події, факти, коментарі»
Огляд інтернет-ресурсів
(7.06–20.06)
№ 12

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

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

Упорядник
І. Терещенко

Заснований у 2011 році
Виходить двічі на місяць

Київ 2018

ЗМІСТ

Орфографія та стилістика матеріалів – авторські

РОЗВИТОК І ПЕРСПЕКТИВИ СОЦІАЛЬНИХ МЕРЕЖ

7.06.2018

Instagram может разрешить пользователям публиковать 60-минутные видео

Недавно стало известно, что пользователи Instagram вскоре смогут публиковать видео, длинной в час. Администрация социальной сети решила пересмотреть правила, которые определяют длину видеороликов (IGate).

Нововведение будет направлено на вертикальный формат видео, поскольку именно он используется в Instagram Stories. Остается неясным, можно ли будет публиковать такие видео в основную ленту сети. На сегодняшний день для Stories в Instagram действует ограничение в 15 секунд, тогда как клипы в ленте могут длиться не больше 60 секунд.

В ноябре прошлого года сервис Stories насчитывал более чем 300 млн активных аккаунтов, а в самой сети Instagram уже зарегистрировано более 800 млн пользователей.

Руководство социальной сети считает, что нововведение может открыть пользователям новые творческие возможности. Помимо этого, Instagram составит более серьезную конкуренцию YouTube и даже Facebook. Окончательного решения об этом изменении еще нет, поэтому ограничение на длину видеороликов может остаться прежним.

***

8.06.2018

Владимир Кондрашов

Две российские соцсети остаются в десятке самых популярных в Украине сайтов

На заседании Комитета Интернет Ассоциации Украины по вопросам интернет-рекламы оглашены данные исследования интернет-аудитории Украины за май, которое выполняется по заказу ИнАУ компанией Factum Group Ukraine (InternetUA).

По итогам мая 2018 года на базе медиа-панели численностью 5 тыс. человек определен список популярных доменов, посещаемых украинскими пользователями.

Согласно обнародованным данным, российская соцсеть vkontakte (vk.com) остается на четвертом месте, а «Яндекс» и «Одноклассники» за май потеряли по одной позиции и заняли восьмую и девятую строчки рейтинга соответственно. Растерял в популярности и почтовик из РФ mail.ru – 15 позиция против 13-ой в апреле.

В лидерах рейтинга остаются Google, Youtube и Facebook.

***

10.06.2018
Facebook запустила страницу с игровыми стримами

В январе Facebook запустила программу Gaming Creator, призванную помогать создателям игрового видеоконтента наращивать аудиторию в социальной сети. Теперь компания анонсировала программу Level Up, направленную на помощь авторам-новичкам.

Докладніше

***

10.06.2018
Миллионы людей остались без популярного приложения

Официальный клиент Twitter с первого июня этого года перестал работать на мобильных гаджетах под управлением Windows Phone 8.1. Ранее разработчики официально сообщили об окончании поддержки приложением Twitter операционной системы Windows 10 Mobile, сообщает MSPowerUser (InternetUA).

Помимо этого, пользователи гаджетов на этих платформах не могут использовать новый сервис Twitter lite – он не работает должным образом в Internet Explorer или Edge в старых версиях Windows, перенаправляя браузер на старый мобильный сайт Twitter, который не позволяет публиковать твиты.

Согласно данным StatCounter, по состоянию на май 2018 года доля мобильных версий Windows на рынке карманных устройств составляет менее одного процента. С учетом того, что в мире используется несколько миллиардов активных смартфонов, речь может идти о миллионах человек.

***

10.06.2018
Facebook Messenger перестанет навязывать друзей

Одна из самых раздражающих вещей в социальной сети Facebook – когда вы принимаете запрос на добавление в друзья или принимают ваш запрос, в Facebook Messenger также появляется оповещение, что вы с эти пользователем на связи ещё и в мессенджере (InternetUA).

В результате, требуется выйти из приложения Facebook, зайти в приложение Messenger и открыть этот созданный автоматически диалог, чтобы очистить его. Некоторым пользователям приходится проходить через этот ритуал кучу раз на дню. Теперь разработчики Facebook признали, что это может оказаться немного утомительно.

Конечно, просто отметить такие оповещения было бы слишком просто. Вместо этого, в Facebook использовали машинное обучение, чтобы отследить

реакции пользователя на них – пользуется ли он возможностью поприветствовать новый контакт. Если пользователь всегда отвергает их, то такие оповещения перестанут ему присылать.

***

10.06.2018
Facebook выпустил таблицу для модераторов

Издание Motherboard опубликовало внутренний документ для модераторов социальной сети Facebook, которую используют для определений нарушения этики в сообщениях с эмодзи (InternetUA).

В документе отмечается, что коммуникации с помощью эмодзи постоянно расширяются, поэтому команде модераторов Facebook нужно понимать, какой новый смысл приобретают те или иные высказывания. По словам создателей таблицы, в каждом случае использования эмодзи необходимо понимать контекст, в котором пользователь прибегнул к его использованию.

В различном контексте нейтральные эмодзи могут означать абсолютно разные вещи – особенно если это комбинация картинок. При этом модераторы в каждом случае должны принимать решение, ориентируясь на собственную моральную позицию.

***

12.06.2018
Facebook открыла средство отладки мобильных приложений

Компания Facebook анонсировала релиз с открытым кодом на GitHub инструмента мобильной отладки Sonar. Он базируется на платформе разработки Google Chrome, предоставляет возможность добавлять подключаемые модули, создавать новые функции, анализировать ошибки и оптимизировать приложения для Android и iOS (Компьютерное Обозрение).

Эта инициатива стартовала более трех лет назад с выходом Stetho, отладочного «моста» Android, построенного на инструментарии Chrome.

«С Sonar мы хотели использовать то, чему мы научились со Stetho, для разработки инструмента с более расширяемым функционалом, более богатым пользовательским интерфейсом, и который бы работал как на iOS, так и на Android», – написал в анонсе программный инженер Facebook, Эмиль Шолендер (Emil Sjölander).

Sonar доступен для сообщества разработчиков на GitHub вместе с множеством подключаемых модулей, созданных инженерами Facebook. Он состоит из двух компонентов: настольного клиента и наборов SDK, устанавливаемых на мобильных устройствах. Десктопный клиент создан на основе кросс-платформенной open source библиотеки GitHub – Electron и открытых проектов Facebook, таких как React.js, Flow, Metro, RSocket и Yarn.

***

13.06.2018
Ирина Фоменко
Yahoo Messenger закроется в следующем месяце

После двадцати лет работы во всем мире Yahoo Messenger «попрощается» со своими поклонниками в следующем месяце. Об этом сообщает The Star Online (InternetUA).

Согласно информации на веб-сайте Yahoo, до 17 июля пользователи еще смогут пользоваться мессенджером, но после этой даты чаты уже будут не доступны.

Как объясняют в компании, поскольку Yahoo постоянно экспериментирует с новыми услугами и приложениями, в настоящее время пока нет альтернативы Yahoo Messenger.

Тем не менее, Yahoo рекомендует пользователям попробовать мессенджер Yahoo Squirrel, который в настоящее время находится в статусе бета-тестирования и доступен только по приглашениям.

Yahoo напоминает пользователям, что они могут загрузить свою историю чата на персональный компьютер или мобильное устройство до конца ноября этого года.

Сперва нужно перейти на указанный сайт и войти в систему. После выбора верификационного метода пользователю необходимо ввести ключ учетной записи. Затем нажать «загрузить» и дождаться, когда файл будет отправлен на электронную почту.

Отметим, закрытие мессенджера Yahoo Messenger не повлияет на такие услуги, как Yahoo Mail, Yahoo Fantasy и другие.

***

13.06.2018
Google выпустила «убийцу» Viber и WhatsApp

Новое приложение «корпорации добра» обладает достаточными функциональностью и удобством для того, чтобы полностью затмить именитых конкурентов (InternetUA).

Компания Google выпустила программу под названием Android Messages, которая должна стать полноценным «убийцей» таких популярных мессенджеров как Viber и WhatsApp. В данный момент функционал данного приложения несколько скуден, так как в планах специалистов из Google доработать мессенджер и представить его полную версию уже до конца 2018 года. Представители корпорации заявили о том, что Android Messages в скором будущем сможет объединить абсолютно все платформы, включая мобильные системы и стационарные компьютеры.

Разработкой приложения занимаются эксперты из Chromium Gerrit, которые рассказали о том, что Android Messages будет работать в рамках браузера, поэтому для пользования мессенджером можно будет попросту установить необходимое расширение или добавить любимый сервис в закладку.

***

14.06.2018
Роман Черный
Как изменятся социальные сети в будущем

Социальные сети кардинально изменились за последнее десятилетие. Сегодня они превратились в невероятно мощный социальный институт, оказывающий колоссальное влияние на облик мира. Очевидно, в будущем соцсети никуда не исчезнут. А вот как они будут развиваться – весьма интересный вопрос.

Докладніше

***

16.06.2018
Роман Черный
Как формируется новостная лента Instagram

После скандала с Facebook и Cambridge Analytica все большее количество пользователей начинает интересоваться внутренними механизмами работы соцсетей. Людей интересует не только то, какую информацию о них собирают компании, но и то, по каким принципам соцсеть формирует ленту для пользователя.

Докладніше

***

16.06.2018
В Instagram отказались от одной из функций

Разработчики Instagram отключили в соцсети функцию, которая была доступна в тестовом режиме несколько месяцев (InternetUA).

Зимой 2018 года пользователи Instagram получили возможность протестировать новую возможность на ресурсе. Приложение отправляло уведомления владельцам аккаунтов, если кто-то сделал скриншот их фото или видео из Stories. Автор получал сообщение с никнеймом человека, сохранившего картинку.

14 июня 2018 года представители Instagram заявили изданию Buzzfeed, что решили отказаться от это функции. Теперь пользователи смогут скрыто делиться чужими Stories.

***

17.06.2018

По фотографиям из социальных сетей можно будет предсказать счастье соседей

По фотографиям в социальных сетях, будь то обедающие люди или массовые мероприятия, можно реально предугадать благополучие района и уровень джентрификации (реконструкции строений в прежде не фешенебельных местах) (InternetUA).

Сайт Frontiers in Physics опубликовал интересное исследование. Учёные изучили миллионы фотографий культурных мероприятий в Лондоне и Нью-Йорке из социальных сетей. Их целью было создание модели, которая может прогнозировать высокий уровень благосостояния и определить планы на реконструкцию районов на 5 лет вперед.

Идея основана на концепции «культурного капитала» в социологии. Например, если в определённом месте проводится много интересных событий, то в будущем можно ожидать более высокий уровень благополучия жителей это района. Исследователи также предполагают, что инвестиции в искусство и культуру будут активно улучшать состояние жилых районов.

Команда исследователей хочет изучить здоровье граждан, используя такой же метод. Фотографии мест с едой будут наложены на карту города с целью выяснить, в каких точках кафе и другие заведения пользуются спросом.

***

16.06.2018

Исследование: использование соцсетей в качестве новостных агрегаторов падает

Традиционно институт журналистики Reuters выпустил отчет о потреблении онлайн-новостей на основе опроса YouGov более 74 тыс. потребителей в 37 странах, включая США и Великобританию. В докладе основное внимание уделяется вопросам доверия и дезинформации, новым онлайн-бизнес-моделям, влиянию изменения алгоритмов Facebook и появлению новых платформ и приложений для обмена сообщениями (Телекритика).

В докладе говорится, что пользование Facebook в качестве источника новостей упало на 9 % с 2017 года по 2018 в США и на 6 % по всему миру. А среди молодого поколения и вовсе упало на целых 20 %.

Подчеркивается, что изменение алгоритма Facebook вредит новостям. Примечательно, что в других соцсетях такого не наблюдается.

Использование мессенджера WhatsApp выросло на 4 % за этот период времени. А потребление новостей в Instagram и Snapchat выросло на 3 % и 2 % соответственно за два года. Как отмечает Reuters Institute, пользователи охотнее обращались к более приватным сервисам, таким как WhatsApp и делились новостным контентом.

***

18.06.2018
Facebook научился открывать глаза на фото

Разработчики социальной сети Facebook создали алгоритм на базе нейросетей, способный исправлять неудачные фото, где модель моргнула и представлена с закрытыми глазами. Алгоритм может «открыть» глаза на основании одного такого неудачного фото (IGate).

Разработчики натренировали нейросеть не только распознавать закрытые глаза на фотографиях, но и заменять их подходящими открытыми глазами, а затем ретушировать результат. В процессе учитываются такие параметры, как ракурс, освещение, макияж и так далее.

Подобные алгоритмы часто далеки от совершенства. Как можно заметить на иллюстрации, искусственный интеллект не понимает многих важных вещей, например, что открытие глаз не должно изменять цвет кожи вокруг, или что ресниц не должно вдруг оказаться слишком много.

На иллюстрации слева направо представлены фото человека с открытыми глазами, неудачное фото, с которым работают, результат алгоритма Photoshop и результат нового алгоритма. Разработка Facebook выдаёт заметно более реалистичный результат, чем Photoshop – глаза не выглядят вырезанными из другого изображения, без очевидных сшивок и несовпадения цветов.

***

18.06.2018
WhatsApp прекратит поддержку iOS 7

Команда разработчиков мессенджера WhatsApp объявила о своих планах отказаться от поддержки устаревших платформ в ближайшем будущем. По заверениям компании, это позволит сосредоточить все свои усилия на актуальных операционных системах (InternetUA).

Согласно анонсу в блоге WhatsApp, мессенджер перестанет поддерживать iOS 7 с 1 февраля 2020 года. Такая же участь постигнет и владельцев Android 2.3.7 Gingerbread. Пользователям будет предложено обновиться на актуальное ПО, а в том случае, если это невозможно – приобрести новый смартфон.

Для вышеперечисленных платформ команда WhatsApp сможет лишь гарантировать доставку и получение сообщений вплоть до начала 2020 года. Все остальные функции могут перестать работать в любой момент. Кроме того, приложение с этого момента больше не будет получать обновления с новыми опциями на неактуальных версиях ПО.

Согласно статистике, на iOS 7 сейчас работает около 10,7 миллиона устройств, что составляет около 5 % iPhone по всему миру. Что касается Android, то на Gingerbread работает лишь 0,3 % смартфонов от общего числа, что составляет около 3,9 миллиона устройств.

***

19.06.2018

Twitter начнёт присылать персонализированные новостные уведомления

Twitter сообщила, что её мобильные приложения начнут рекомендовать пользователям новости на основе их интересов. В сервисе и сейчас есть возможность подписываться на уведомления с новостями, но скоро последние станут персонализированными (InternetUA).

Сервис начнёт присылать новости на основе того, на какие аккаунты вы подписаны и на какую тему обычно отправляете твиты. При нажатии на уведомление будет открываться страница с похожими публикациями и тематическими видеороликами – точно так же, как если бы вы нашли какой-то материал во вкладке Explore.

Вверху ленты станут отображаться мероприятия, которые могут вас заинтересовать. Twitter уже использует панель Happening Now для показа спортивных событий в прямом эфире, однако скоро на ней будут отображаться и новости из упомянутых выше уведомлений. «В верхней части ленты вы увидите новости, которые могут быть вам интересны, а также относящиеся к ним твиты и видео», – рассказала компания.

В ближайшие месяцы Twitter ждут и другие обновления, связанные с новостями. Также компания обновит вкладку Explore: вместо типов контента в ней появятся разные темы. Это позволит по отдельности просматривать публикации о развлечениях, науке, технологиях и так далее.

На данный момент главным недостатком ленты Twitter является невозможность сортировать твиты по категориям. Если вы подписаны на одни аккаунты ради новостей, а на другие – ради шуток, то вы не можете нормально разделить этот контент. Вероятно, обновление вкладки Explore исправит эту проблему.

***

19.06.2018

Звезды «Барселоны» запускают соцсеть для футбольных фанатов на блокчейне

Команда разработчиков совместно с бывшими игроками испанского футбольного клуба «Барселона» Карлесом Пуйолем, Андресом Иньестой и Иваном де ла Пенья заявила о запуске социальной сети Olyseum, предназначенной для общения поклонников футбола с их кумирам.

Докладніше

СОЦІАЛЬНІ МЕРЕЖІ ЯК ВИЯВ ФОРМУВАННЯ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА

8.06.2018
У соцмережах почали другий етап акції на підтримку Сенцова
Марія Леонова

Організатори акцій на підтримку українського режисера, політв'язня Кремля Олега Сенцова оголосили другий етап глобальної кампанії #SaveOlegSentsov (hromadske).

Про це йдеться у Facebook акції.

Організатори закликають 8 та 9 червня долучатися до ініціативи, яку пропонують провести в онлайн-режимі.

Охочим підтримати Сенцова пропонують писати коментарі на публічних сторінках політиків та ключових осіб міжнародних переговорів із закликом звільнити Сенцова.

«8-9 червня лідери G7 («Великої сімки») зберуться у Мальбе (Квебек, Канада), щоб обговорити найважливіші проблеми світу. Ми переконані, що звільнення Олега Сенцова та всіх 70 заручників Кремля має бути одним із ключових питань саміту. Спільними зусиллями ми зможемо цього досягти!», – заявили організатори.

***

11.06.2018
#коліржиття: ДонорUA запускает флешмоб в поддержку донорства крови

14 июня 2018 в Международный день Донора всеукраинская платформа рекрутинга доноров и поиска доноров для реципиентов, нуждающихся в крови, ДонорUA запускает социальную кампанию в Facebook и Insragram с хэштегом #коліржиття. На один день платформа просит бренды заменить свой логотип на бесцветный с сообщением: колір має значення. Отметим, в Украине втрое меньше доноров, чем рекомендует ВООЗ. Основатель проекта ДонорUA Ирина Славинская отмечает: «Недостаточно просто говорить, что донорство – это круто, модно и нужно. Мы должны показать насколько важна кровь здесь и сейчас, для каждого человека! Мы призываем: подари #коліржиття другому – зарегистрируйся на donor.ua. Наша команда хочет привлечь внимание миллионов людей, ведь донорство – касается каждого» (Marketing Media Review).

***

12.06.2018

«Ніжної ночі у СІЗО»: У соцмережі радіють арешту догхантера Святогора

Шевченківський районний суд Києва ухвалив рішення взяти під варту на два місяці догхантера Олексія Святогора. За словами прокурора, Святогора підозрюють у виготовленні творів, що пропагують культ насильства та жорстокості (Інформатор).

«Знаєте, шо в ситуації із арештом догхантера Святогором тішить найбільше?

В Лук'янівському СІЗО, на жаль, купа нормальних хлопців, особливо з добровольців, багатьох з них знаю особисто.

А нормальні люди тваринок уважають. На відміну від тварин на кшталт Святогора.

Тому, знаю напевне, вказаній вище сволоті сидітиметься дуже больно. ночь нєжна…», – написав з цього приводу у Facebook народний депутат Андрій Лозовий.

«Сподіваюсь, він там своє отримає, цей Святогор, побільше йому ніжних ночей» – іронізують у коментарях.

Не зважаючи на те, що Святогора вже взяли під варту, деякі користувачі соцмереж не впевнені в правосудді у цій справі. «Засудили б його на більший строк! Хоча наступний суддя ще і відпустить!»

***

13.06.2018

#BoycottWorldCup2018: в сетях бойкотируют ЧМ-2018

В социальный сетях пользователи призывают бойкотировать Чемпионат мира по футболу, который пройдет в России с 14 июня 2018 года по 15 июля 2018. Многие используют «убийственные плакаты» украинского художника Андрея Ермоленко, как и страница Министерства иностранных дел Украины в Facebook (Marketing Media Review).

***

14.06.2018

«І не повертайтеся!» – у соцмережах бурхливо відреагували на українців, які поїхали на ЧС-2018

Сьогодні – відкриття чемпіонату світу 2018 у Росії. І, попри масовий бойкот і заклики не відвідувати мундіаль під час війни з РФ, 5 тисяч українців так купили квитки до Росії. У соцмережах активно обговорюють таке рішення. Засуджують вболівальників, які поїхали до Росії, і відомі українці. До прикладу, Юрій Винничук. У мережі розглядають можливі варіанти розвитку поїздки 5 тисяч українців до Росії. Дехто пропонує альтернативні варіанти.

Відомий комік та шоумен Володимир Андрєєв звернувся віршем до українців, які поїхали на ЧС в Росію (expres.ua).

***

14.06.2018

Забий Путіну: В соцмережах стартує акція до ЧС-2018

14 червня, у день відкриття чемпіонату світу з футболу в Росії, українські правозахисники розпочинають акцію в соцмережах, в якій пропонують «грати за політв'язнів» і «забити перший гол Путіну» (Depo).

Про це повідомила голова громадської організації «Центр громадянських свобод», координатор «Євромайдан SOS» Олександра Матвійчук.

«Наша перша мета – прийняття термінової резолюції Європейського парламенту про Олега Сенцова та інших заручників Кремля. Ми зробили всю підготовчу роботу. У фінальний текст резолюції завдяки друзям України в Європарламенті увійшли наші рекомендації. Сьогодні о 9 ранку відкриється пленарна сесія. Ми ведемо гру проти потужного російського лобі в ЄС. Нам важливо зіграти командою», – каже Матвійчук.

Правозахисники пропонують такий алгоритм дій: натиснути автоматичний твіт про вступ в гру, написати в своєму Facebook і Twitter – #EuropeanParliament Act Now! Vote for resolution! Save Ukrainian Jailed-70 #SaveOlegSentsov #FreeSentsov # WorldCup # WorldCup2018, тегнути у Facebook https://www.facebook.com/europeanparliament/, тегнути у Twitter @Europarl_EN.

БІЗНЕС І СОЦІАЛЬНІ МЕРЕЖІ

7.06.2018

Крупнейшие телеканалы США будут создавать передачи специально для Facebook

В США несколько телеканалов, среди которых CNN, ABC, Fox News и Univision, будут снимать новостные передачи специально для показа в Facebook. Об этом говорится в официальном блоге соцсети. В сообщении говорится, что перечень СМИ может быть расширен (IGate).

Программы, выпускаемые каналами специально для Facebook, будут располагаться в особой секции в разделе, посвященном поиску новостей. В Facebook считают, что нововведение поможет пользователям получить доступ к «высококачественному и своевременному новостному контенту». Передачи будут вести «как удостоенные премий журналисты, так и новички». Показ первых программ ожидается уже этим летом.

***

13.06.2018
В Instagram Stories появилась функция покупок

Бренды могут рекламировать продукты в Instagram Stories с помощью иконки с сумкой. По данным сети, Adidas, Aritzia и Louis Vuitton среди брендов, которые будут использовать эту функцию. И хотя тэг для покупок был давно доступен в ленте Instagram, этот шаг является преимуществом для брендов, которые хотят зарабатывать на пользователях Stories. По данным сети, 300 млн из 500 млн ежедневных пользователей взаимодействуют со Stories каждый день (InternetUA).

***

13.06.2018
Ирина Фоменко
Facebook наносит удар по китайской электронной коммерции

Facebook принимает жесткие меры в отношении китайских торговых сайтов, рекламирующих в социальной сети продукты, которые в итоге оказываются низкого качества. Facebook запускает новую функцию для электронной коммерции на панели управления Recent Ads Activity – теперь покупатели смогут оставлять отзывы о долгой доставке, странных запахах и плохих товарах.

Докладніше

***

20.06.2018
Facebook запустил автопроигрывающуюся видеорекламу в Messenger

Некоторые пользователи уже видят видеорекламу рядом с сообщениями от друзей и близких. Messenger начал продавать рекламу в мессенджере 18 месяцев тому назад, но это была статичная реклама, а не видео. Преимущество видеорекламы в том, что она более дорогая, поэтому и более ценная для сети. Вопрос в том, будут пользователи считать рекламу рядом с приватными сообщениями назойливой. В компании отметили, что будут следить за поведением пользователей, чтобы узнать, как это повлияет на их пользование сервисами сети (Marketing Media Review).

СОЦІАЛЬНІ МЕРЕЖІ І ПРОБЛЕМИ СУСПІЛЬНОЇ БЕЗПЕКИ

Інформаційно-психологічний вплив мережевого спілкування на особистість

8.06.2018
Ирина Фоменко
Люди с низким доходом стали больше сидеть в сети

Уровень использования Интернета американцами значительно вырос в 2017 из-за людей с низким доходом. Об этом сообщает Reuters (InternetUA).

Национальное управление по телекоммуникациям и информации (NTIA) также заявило, что впервые планшеты оказались более популярными, чем компьютеры, а у большинства домохозяйств зафиксировано использование мобильных данных, а не проводного широкополосного доступа в Интернет.

Результаты правительственного исследования демонстрируют растущее значение Интернета в повседневном общении, поскольку меняется доступ потребителей к контенту.

Так, опрос показал, что среди американцев в сельских районах с семейным доходом ниже 25 000 долларов в год использование Интернета увеличилось до 62 % в 2017 с 57 % в 2015, в то же время в семьях с ежегодной прибылью в 100 000 долларов и более использование сети осталось на прежнем уровне – 86 %.

Прирост в 13,5 миллионов человек обусловлен более частым использованием Интернета семьями с низким доходом, пожилыми людьми, афроамериканцами, латиноамериканцами и другими группами. «Хотя тенденция обнадеживающая, американцы с низким доходом все еще не хотят выходить в сеть», – заявил глава NTIA Дэвид Редл.

***

7.06.2018
Полина Лисовец
4 признака того, что социальные сети вызывают у вас депрессию

Социальные сети стали частью нашей жизни, но они не только облегчают общение, но и могут усугубить депрессивное состояния.

Докладніше

Маніпулятивні технології

10.06.2018

Техніка маніпуляції. Вісім брудних прийомів, які використовують пропагандисти в соцмережах

Данило Малуха, Сергій Клімович

Як у Фейсбуці від «вашого імені» поширюють певну інформацію? Чому ваші друзі вважають, що ви залайкали сайт із поганою репутацією? Люди, котрі створили розважальні групи, заробляють на політичній пропаганді. Ми визначили 8 найпоширеніших прийомів маніпуляції та обману, які використовують українські політичні штаби, комерційні компанії та російські пропагандисти.

Докладніше

***

11.06.2018

Заяви про «мінування» львівських бізнес-центрів генерують російські програми-боти

Численні повідомлення про фальшиві замінування бізнес-центрів у Львові надсилають з території Росії – про це під час апаратної наради в ЛОДА повідомив 11 червня начальник обласного управління СБУ у Львівській області Олександр Ткачук (ZAXID.NET).

«Спочатку повідомлення про замінування надходили з електронних адрес, зареєстрованих на анонімних серверах електронної пошти на території Російської Федерації. Всі ці повідомлення генерував робот. Було прийнято рішення про блокування цих серверів», – заявив керівник СБУ Львівщини.

Він також повідомив, що після блокування повідомлення почали надсилати з міжнародного сервісу електронної пошти.

«Цей сервіс ми заблокувати не можемо, але вдалося встановити, що адреса користувача знаходиться на території Російської Федерації в місті Омську. Зараз ми приймаємо рішення, як саме реагувати на повідомлення, що надходять по три рази на день», – заявив Олександр Ткачук.

***

11.06.2018

ПриватБанк не проводить грошових «опитувань» у соцмережах

ПриватБанк ніколи не проводив опитувань із розіграшем грошових призів через соціальні мережі чи сторонні сайти (Діловий регіон).

Як повідомила прес-служба ПриватБанку, «опитування» GIVEAWAY 2018 від імені банку або держорганів з обіцянками виплат грошових призів, що днями з'явилися в Instagram, є фейковими та проводяться шахраями з російських акаунтів.

Під приводом отримання грошового виграшу шахраї пропонують довірливим громадянам переказати певну суму грошей для «підтвердження» виграшу, після чого зібрані гроші виводяться на особисті рахунки шахраїв. Шахраї збирають такі платежі, як правило, через російські платіжні агрегатори, такі, як SimplePay або WalletOne, зазначають банкіри.

За даними служби безпеки банку, перші звернення постраждалих від шахраїв клієнтів було зафіксовані у червні. Для запобігання дій шахраїв банк звернувся до всіх платіжних сервісів, за допомогою яких шахраї збирають гроші, з вимогою блокування незаконних операцій і використання карток українських банків у шахрайських схемах. Також Приватбанк звернувся з відповідною заявою до кіберполіції.

Спецслужби і технології «соціального контролю»

7.06.2018

Facebook забанил украинского художника за плакаты к ЧМ-2018, напоминающие о преступлениях Кремля

Социальная сеть Facebook забанила украинского художника Андрея Ермоленко за плакаты к Чемпионату мира по футболу 2018 в РФ, напоминающие о преступлениях кремлевского режима (InternetUA).

Их тематика касается, в частности, оккупации Россией чужих территорий, бомбардировок мирных жителей в Сирии, терактов, убийств российских граждан за границей и политических репрессий в самой стране.

По словам Ермоленко, в Facebook ему объяснили такой шаг «нарушением принципов сообщества».

Впрочем, благодаря массовым обращениям пользователей к руководству соцсети по этому поводу страницу художника все же разбанили.

***

11.06.2018

Ирина Фоменко

Мюллер проверит мессенджеры на безопасность

Команда специального прокурора Роберта С. Мюллера III проверит зашифрованные мессенджеры на безопасность в ходе российского расследования.

Докладніше

***

12.06.2018

СБУ викрила члена російського руху, який розпалював за криптовалюту міжнаціональну ворожнечу

Співробітники Служби безпеки України викрили на Хмельниччині учасника російської політичної організації «Национальное освободительное движение» на інспіруванні міжнаціональної ворожнечі та антиукраїнській пропаганді в інтересах країни-агресора (InternetUA).

Правоохоронці встановили, що мешканець Кам'янець-Подільського, перебуваючи в складі вищезгаданої організації, був завербований представниками ФСБ під час періодичних виїздів до Росії. За завданням «кураторів» агітатор виготовляв листівки нібито від українських націоналістів із закликами до агресивних дій стосовно поляків, які проживають на території України. Вказані матеріали він отримував від «замовників» через Інтернет. Потім зловмисник поширював агітки у популярних серед іноземних туристів історичних та культурних місцях регіону.

Оперативники спецслужби зафіксували, що агітатор також адмініструв спільноту в одній із соціальних мереж, через яку поширював матеріали щодо підтримки терористичних організацій «Л/ДНР» та виправдовував російську військову агресію проти нашої держави.

Фінансування злочинної діяльності зловмисника здійснювалось представниками спецслужб РФ з використанням криптовалют.

Під час санкціонованого обшуку у помешканні фігуранта справи співробітники СБУ виявили матеріали з антипольською та проросійською пропагандою, а також комп'ютерну техніку із доказами протиправних дій.

У рамках відкритого кримінального провадження за ст. 110 Кримінального кодексу України тривають слідчі дії.

***

13.06.2018

Жителя Сміли судитимуть за пости в соціальних мережах

Прокуратура Черкаської області та слідчий відділ управління Служби безпеки України в Черкаській області завершили досудове розслідування у кримінальному провадженні стосовно жителя міста Сміли, який обвинувачується у вчиненні кримінального правопорушення, передбаченого ч. 2 ст. 109 (дії, спрямовані на насильницьку зміну чи повалення конституційного ладу або на захоплення державної влади) Кримінального кодексу України (InternetUA).

Використовуючи особисту комп'ютерну техніку, вказаний громадянин за допомогою персонального акаунту в одній із соціальних мереж, упродовж 2015 – 2017 років розміщував на своїй сторінці статті з закликами до насильницької зміни чи повалення конституційного ладу, що підтверджено висновками експертів.

Зараз обвинувальний акт у кримінальному провадженні скеровано для розгляду до суду.

Зловмиснику загрожує покарання у вигляді обмеження або позбавлення волі на строк до 3 років.

***

12.06.2018

Канцлеру Австрии начали угрожать через соцсети

В Австрии приняли решение об усилении охраны канцлера Себастьяна Курца и министров, так как после сообщения о закрытии семи мечетей на территории страны и высылке имамов через соцсети стали поступать угрозы в их адрес. Об этом сообщает OE24 (InternetUA).

Отмечается, что угрозы поступили через Facebook и Instagram. После поступления подобных сообщений угрозами стало заниматься австрийское Федеральное ведомство по защите Конституции и борьбе с терроризмом.

***

7.06.2018

«Не треба доводити до абсурду»: Путін прокоментував арешти за публікації в соцмережах

За його словами, варто чітко визначити поняття, які вартують арешту.

Президент Росії Володимир Путін заявив, що «не потрібно доводити до абсурду» арешти росіян за публікації у соцмережах, однак все одно підтримав затримання за так звані «поширення екстремістської інформації».

Про це він розповів під час «Прямої лінії з президентом» 7 червня (ТСН)

«Якщо йдеться про поширення саме такої інформації, яка є екстремістською, то звичайно, я вже про це говорив, повинні застосовуватися загальні правила: порушив – відповідай», – заявив Путін.

Однак, він також зазначив, що не варто доводити все до маразму та абсурду та потрібно чітко визначити поняття, які потребують арешту.

«Хіба хтось буде проти того, що потрібно поставити заслін пропаганді суїцидів в соцмережах або поширенню фашистських ідей», – підкреслив президент РФ.

***

17.06.2018

Адміністратора сайту з Рівненщини засудили за поширення піратської продукції

Рівненською місцевою прокуратурою за участі Департаменту кіберполіції Національної поліції України організовано досудове розслідування, відповідно до заяви Української антипіратської асоціації, за фактом умисного порушення

авторського права шляхом розповсюдження аудіовізуальних творів, що завдало матеріальної шкоди в особливо великому розмірі (за ознаками кримінального правопорушення, передбаченого ч. 3 ст.176 КК України) (InternetUA).

В результаті зібраних доказів виявлено та припинено діяльність міжнародного Інтернет-ресурсу, у зв'язку із протиправною трансляцією як популярних українських, так і значної кількості іноземних фільмів.

У ході санкціонованого обшуку зафіксовано причетність 31-річного чоловіка, який адміністрував вказаний ресурс, дії якого пов'язані з протиправним відтворенням та розповсюдженням аудіовізуальних творів, що спричинило матеріальну шкоду правовласникам в особливо великому розмірі на суму понад 2,5 млн. грн.

Санкція статті передбачає покарання у вигляді штрафу від двох до трьох тисяч неоподатковуваних мінімумів доходів громадян або позбавленням волі на строк від трьох до шести років, з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років.

***

20.06.2018

Вот и сказочке конец: Европарламент проголосовал за законопроект, который убьет интернет

Новый закон, называемый Директивой об авторском праве ЕС, поддерживается несколькими гигантами медиа-индустрии. Однако лоббистская группа CCIA, куда входят Google, Facebook, eBay, Amazon и Netflix, критикуют закон. Основатель Wikipedia Джимми Уэллс и изобретатель Всемирной паутины Тим Бернерс-Ли заявляют, что с принятием нового закона интернет просто не сможет существовать (Телекритика).

Комитет депутатов Европарламента проголосовал за принятие серьезных изменений в европейском законодательстве об авторском праве. Они проголосовали за утверждение спорных статей: 13-ой, которая фактически положит конец мемам, ремиксам и другому контенту, создаваемому обычными пользователями сети, а также 11-ой, требующей, чтобы онлайн-платформы оплачивали издателям комиссионные за отсылки на их новостной контент.

Комитет Европарламента по юридическим вопросам проголосовал 15 голосами (против 10) за 13 статью и 13 голосами (против 12) за 11 статью нового закона.

Теперь законопроекту предстоит отправиться на рассмотрение более широкого заседания Европейского парламента в июле.

Проблема захисту даних. DDOS та вірусні атаки

7.06.2018

Мошенники завладели камерами наивных пользователей

Десятки австралийцев стали жертвами мошенников, замаскировавшихся под службу поддержки клиентов популярного сервиса и завладевших веб-камерами пользователей, пишет ABC Australia (InternetUA).

Злоумышленники обманным путем заманили жертв на ресурс, стилизованный под страницу поддержки пользователей Adobe Flash. Один из пострадавших рассказал, что набрел на страницу Support for Adobe Australia, когда искал советы по самостоятельной установке программного обеспечения. Он позвонил по бесплатному номеру, указанному на сайте, где ему заявили, что на его компьютере обнаружена вредоносная программа и посоветовали установить нейтрализующее ее программное обеспечение.

Однако рекомендуемая программа и оказалась вредоносной. Она позволила мошенникам удаленно управлять веб-камерой скачавших ее абонентов. В результате злоумышленники начали записывать видео из их жизни и загружать на YouTube.

На видео попадало происходящее в спальнях, гостиных, кабинетах и кухнях. На одном из них резвились дети, на другом – мужчина без рубашки сидел за компьютером. ABC связалась с некоторыми из попавших на видео. Они признались, что были шокированы, узнав, что ролики с ними публиковались в сети.

***

7.06.2018

Пограничная полиция Китая загружает вирусы в Android-смартфоны

Ранее США обвинили Китай во встраивании вредоносного софта в смартфоны ZTE и Huawei в целях слежения за жителями Америки. В этот раз о слежке заговорили обычные люди.

Докладніше

***

7.06.2018

Кибертеррористы наступают: как украинские компании «укрепляют» свои позиции

«Самое точное определение того, что сейчас происходит в Украине, – кибертерроризм», – подчеркнул директор по работе с партнерами и клиентами представительства Cisco в Украине и странах СНГ Сергей Мартынчук на недавнем Cyber Defence Congress 2K18.

Докладніше

***

7.06.2018

Amazon прекращает продажу умных игрушек из-за проблем с безопасностью

Мягкие плюшевые медвежата кажутся безобидными – ровно до тех пор, пока хакеры не используют их для слежения за детьми. Amazon сообщила, что убрала из своего онлайн-магазина CloudPets, умную игрушку с проблемами безопасности. На прошлой неделе это сделали также Walmart и Target. С утра их уже не было в каталогах Amazon. Решение было принято через сутки после того, как Mozilla связалась с Amazon и продемонстрировала новые уязвимости CloudPets (InternetUA).

«В мире, в котором утечки данных становятся все более рутинными, и такие продукты, как CloudPets, все еще находятся на полках магазинов, я все больше беспокоюсь о конфиденциальности и безопасности своих детей», говорит Эшли Бойд, вице-президент по безопасности Mozilla.

Amazon прекращает продажу продуктов из-за опасений безопасности не впервые. В прошлом июле онлайн-ритейлер заморозил продажу телефонов Blu – на тот момент они продавались очень хорошо – потому что исследователи нашли вирус на популярных устройствах.

Подключенные устройства открыты для атак по множеству причин, независимо от того, стоят ли на них пароли по умолчанию, обновляют ли их разработчики или что с ними делают владельцы.

***

8.06.2018

Facebook по ошибке рассекретила личные публикации 14 миллионов пользователей

Приватные публикации 14 миллионов пользователей Facebook стали общедоступными. Об этом сообщает The Verge со ссылкой на официальных представителей компании (InternetUA).

Они рассказали, что в результате программной ошибки настройки публикаций без ведома хозяев изменились на «публичные». Сбой произошел с 18 по 27 мая. Сотрудники компании устранили ошибку 22 мая, однако изменить настройки уже опубликованных сообщений удалось лишь через пять дней.

Компания высылает уведомления о произошедшем всем пользователям, которых затронул сбой.

***

9.06.2018

Facebook предоставлял доступ к данным пользователей некоторым компаниям

Социальная сеть Facebook предоставляла доступ к личным данным пользователей некоторым компаниям, несмотря на обещание в 2015 году остановить передачу данных разработчикам приложений. Об этом сообщает The Wall Street Journal со ссылкой на собственные источники, судебные документы и представителей компании (InternetUA).

По данным издания, Facebook заключал соглашения о предоставлении данных с разработчиками приложений определенных компаний. В этот «белый список» входили, например, Royal Bank of Canada и Nissan Motor. В числе предоставляемых данных были, например, номера телефонов и статистика по метрике «дружеская связь», которая позволяет определить степень знакомства между двумя пользователями соцсети.

В компании заявили, что соглашения с разработчиками приложений необходимы для того, чтобы тестировать новые функции и улучшить интерфейс для пользователей.

***

10.06.2018

Вирус BabaYaga обновился и стал еще опаснее

Эксперты по кибербезопасности выявили активность вируса, имеющего название BabaYaga (iLenta.com).

Точнее говоря, данный вирус орудует в Сети уже достаточно давно, но последнее обновление сделало его действительно опасным. Задачей вредоносного ПО является взлом сайтов на базе WordPress.

Зараженные страницы перенаправляют пользователей на маркетинговые ссылки. Злоумышленники получают процент, если перешедший по ссылке пользователь что-то купит.

Эксперты отмечают, что BabaYaga состоит из двух модулей: один внедряет спам в уязвимые сайты, другой служит для постоянного контроля зараженной страницы.

Отличительная особенность «Бабы Яги» состоит в том, что она может самостоятельно обновлять зараженный сайт и удалять другие вредоносные программы.

***

10.06.2018

Ущерб от хакеров за 2017 год оценили в 172 млрд долларов

Производитель антивирусного программного обеспечения Symantec опубликовал результаты исследования, посвященного киберпреступности. В 2017 году ущерб интернет-пользователей от хакеров составил 172 млрд долларов.

Докладніше

***

10.06.2018
Дмитрий Демченко
Как увеличить безопасность своих данных в интернете. Инструкция

На фоне скандала с утечкой данных Facebook мы начали осознавать, сколько сведений о себе раскрываем онлайн-ресурсам. Некоторую информацию мы отдаем сознательно, но это не всегда так. Мы непроизвольно оставляем данные о сайтах, на которых побывали, а рекламные сети используют их для более точного таргетинга. Иногда это полезно, но чаще всего – неприятно и навязчиво. С другой стороны, есть много способов, чтобы повысить конфиденциальность своей информации в интернете.

Докладніше

***

11.06.2018
Самі винні: чому небезпечно розповідати про проблеми з банком у соцмережах
Крістіна Левчук

Клієнти банків, які розповідають про проблеми з банківським обслуговуванням у соціальних мережах, ризикують стати наступними жертвами шахраїв. Такого висновку дійшов Reuters з посиланням на співробітників правоохоронних органів та інших представників галузі.

Докланіше

***

11.06.2018
ESET обнаружила в Украине сверхсложное шпионское программное обеспечение

Компания ESET сообщает об обнаружении шпионского программного обеспечения InvisiMole, которое способно следить за деятельностью жертв и похищать их конфиденциальную информацию.

Докладніше

***

11.06.2018
Прослушка по сигналу: зачем смартфоны шпионят за нами

Смартфоны прослушивают своих владельцев, и это легко проверить – к такому выводу пришел австралийский исследователь, который утверждает, что запись разговоров передается в социальные сети, использующие эти данные

для контекстной рекламы. Мы выяснили, как узнать, что за вами следят, и что нужно делать, чтобы минимизировать этот риск.

Докладніше

***

12.06.2018

Хакеры могут получить доступ к финансовым приложениям 58% банков

Производитель решений информационной безопасности (ИБ) Positive Technologies представил исследование, посвященное вопросам киберзащиты банков (IGate).

По данным экспертов, хакеры имеют возможность получить доступ к финансовым приложениям 58 % банков. В 25 % кредитных организаций могут быть скомпрометированы узлы, с которых осуществляется управление банкоматами, а значит, из этих банков смогли бы вывести деньги последователи группировки Cobalt, использующие аналогичные методы взлома. Перевести средства на собственные счета через системы межбанковских переводов, на которые нацелены группировки Lazarus и MoneyTaker, было бы возможно в 17 % банков.

Из доклада также следует, что в 17 % банков недостаточно защищены системы карточного процессинга, что позволяет мошенникам манипулировать балансом на своих карточных счетах.

По словам ИБ-специалистов, уровень защиты сетевого периметра в банках значительно выше, чем в других компаниях: за три года в рамках внешнего тестирования на проникновение доступ ко внутренней сети был получен в 58 % систем, а для банков этот показатель составил лишь 22 %.

***

13.06.2018

Украинский хакер «положил» охранную систему нескольких предприятий

Сотрудники Приднепровского управления киберполиции разоблачили хакера, который совершал несанкционированное вмешательство в работу компьютерных систем охраны, функционирующих на частных предприятиях Запорожья и Мариуполя.

Докладніше

***

13.06.2018

Миллионы футбольных фанатов оказались под угрозой слежки

В популярном приложении для футбольных болельщиков La Liga обнаружили инструменты для скрытой слежки за пользователями. Об этом сообщает El Pais (InternetUA).

В ходе установки на смартфоны под управлением Android программа запрашивала доступ к микрофону и датчику GPS. Это значит, что La Liga может в любой момент прослушать все разговоры пользователя, а вместе с тем определить его точное местоположение.

Юзеры заметили эти спорные пункты в пользовательском соглашении приложения, после чего обратились к разработчикам с претензиями в социальных сетях.

Создатели La Liga подтвердили факт записи разговоров: они отметили, что таким образом пытаются найти бары, которые транслируют футбольные матчи без лицензии. То есть разработчики пытались защитить футбольные клубы от несанкционированных трансляций. Они утверждают, что из-за незаконной деятельности мошенников испанская лига теряет около 150 миллионов евро в год.

Судя по всему, запись разговоров включается только в определенные промежутки времени, когда в стране проходят матчи чемпионата Ла Лиги. В остальное же время шпионская функция неактивна.

Согласно статистике магазина Google Play, приложение La Liga скачали более 10 миллионов раз.

***

13.06.2018

Специалисты по безопасности показали главный недостаток Siri

Специализирующаяся на кибербезопасности компания продемонстрировала как «поумневшую» Siri могут использовать мошенники для обмана пользователей (InternetUA).

В момент, когда на iPhone поступает вызов с отсутствующего в книге контактов номера, голосовой ассистент пытается выяснить, кто же это звонит. Алгоритм берет во внимание сообщения, электронную почту, просмотренные сайты и прочие данные, так или иначе связанные с айфоном пользователя.

Если злоумышленники предварительно отправят письмо или сообщение на номер жертвы с подписью «Банк такой-то» или «Кредитная организация N» и указанием номера телефона, во время анализа неизвестного номера Siri подумает, что это и есть тот самый «банк» или «кредиторская фирма».

Проще говоря, предварительно отправив сообщение с указанием номера телефона и желаемым именем, любой пользователь может обмануть Siri.

В результате, многие пользователи iOS могут подумать, что им звонят из банка и, ничего не подозревая, ответить на телефонный звонок. Дальше уже включаются классические схемы развода на деньги.

Такая дыра в безопасности Siri была обнаружена еще в iOS 9. Несмотря на попытки Apple блокировать данный вариант мошенничества, с тех пор ничего так и не изменилось.

***

13.06.2018

Facebook записывает движение ваших губ и многую другую информацию

В ответ на запрос Конгресса США после апрельского скандала с Cambridge Analytica, компания Facebook раскрыла все свои способы сбора информации о пользователях социальной сети. Для этого потребовалось составить документ из 222 страниц. Он описывает разные способы сбора данных, от тех, о которых мы догадывались, до тех, о которых мы даже не подозревали.

Докладніше

***

14.06.2018

Розпочала роботу Рада з питань інтелектуальної власності під головуванням Степана Кубіва

14 червня під головуванням Першого віце-прем'єр-міністра – Міністра економічного розвитку і торгівлі України Степана Кубіва відбулося перше засідання Ради з питань інтелектуальної власності, яка створена для посилення захисту прав інтелектуальної власності в Україні, протидії «патентному троллінгу», боротьби з інтернет піратством, легалізації програмного забезпечення в органах державної влади, організації функціонування Центрів підтримки технологій та інновацій та взаємодії з Вищим спеціалізованим судом з питань інтелектуальної власності (Урядовий портал).

«Український винахідник та науковець має право на захист своїх розробок, а Україна зацікавлена у стимулюванні та впровадженні результатів інтелектуальної діяльності у реальний сектор економіки. Ми створюємо взаємовигідну, ефективну систему і сьогодні зробили великий крок у цьому напрямку – розпочали роботу Ради з питань інтелектуальної власності. Вона є майданчиком для напрацювання пропозицій щодо реформи у цій сфері», – підкреслив Степан Кубів.

За підсумками першого засідання Ради Степан Кубів дав низку доручень центральним органам виконавчої влади.

***

17.06.2018

Telegram рассылает требование обновить старые версии мессенджера

Сервисный аккаунт Telegram проводит массовую рассылку сообщений среди пользователей десктопной версии приложения. Главное требования мессенджера – установить обновление (InternetUA).

К сожалению, у Вас старая версия приложения Telegram Desktop, которая плохо работает из-за блокировок и не может обновляться автоматически. Чтобы обновить приложение, скачайте и установите одну из следующих версий, в зависимости от вашей системы. После этого Telegram Desktop снова сможет автоматически обновляться.

Внимание! Никогда не открывайте файлы из незнакомых источников. Обратите внимание, что это сообщение прислано верифицированным аккаунтом Telegram Notigficiations.

Если вы используете Telegram Desktop на других платформах, Вы можете найти необходимые файлы в канале Telegram Desktop.

В сообщений есть ссылка для загрузки нужной версии. Разработчики призывают обращать внимание рассылку только от верифицированных каналов. Загружать версии мессенджера из каналов, которые не содержат соответствующую галочку возле аватарки очень рискованно.

***

18.06.2018

Найден баг PGP, уже 20 лет позволявший подделывать цифровые подписи

Цифровые подписи используются для аутентификации источника зашифрованного сообщения, программного обновления или резервной копии. Обычно они защищены частным ключом, однако серия уязвимостей в популярных инструментах шифрования электронной почты позволяет в ряде случаев подделывать подпись с помощью публичного ключа или Key ID, которые часто публикуются в открытой сети.

Докладніше

***

18.06.2018

Все сети 4G уязвимы для атак, которые приводят к отказу в обслуживании абонентов

Согласно отчету Positive Technologies, используя недостатки протокола Diameter, злоумышленник может лишить абонентов основных преимуществ 4G – высокой скорости и качества связи.

Докладніше

***

18.06.2018

Пять лет в тени: эксперты нашли в Украине и России шпионское ПО

ESET обнаружила новую вредоносную программу, которая используется для кибершпионажа. InvisiMole открывает атакующим удаленный доступ к зараженному устройству, позволяет следить за действиями жертвы и перехватывать конфиденциальные данные (InternetUA).

По данным телеметрии ESET, кибергруппа, использующая InvisiMole, активна с 2013 года. Тем не менее, вредоносная программа не была изучена и не детектировалась до момента обнаружения продуктами ESET на зараженных компьютерах в России и Украине. InvisiMole предположительно применялась только в целевых атаках на высокопоставленные объекты (несколько десятков устройств), что позволяло избегать обнаружения на протяжении пяти лет.

InvisiMole имеет модульную архитектуру. Заражение начинается с модифицированной DLL, далее действуют два модуля – RC2FM и RC2CL, собирающие информацию о жертве.

Модуль RC2FM поддерживает 15 команд. В частности, он может удаленно включать микрофон, записывать аудио, делать снимки экрана, создавать списки файлов на встроенных и внешних дисках, а также передавать собранную информацию своим операторам. Получив соответствующую команду, модуль может вносить изменения в систему.

Второй модуль, RC2CL, оснащен еще более широким списком инструментов шпионажа – 84 команды. Он изучает зараженный компьютер и передает атакующим исчерпывающие данные: системную и сетевую информацию, список установленных и используемых программ, недавно открытых документов и других интересующих файлов. Операторы InvisiMole могут удаленно включать веб-камеру и микрофон, делать снимки экрана и каждого открытого окна. Спайварь позволяет просматривать определенные директории и внешние устройства, отслеживать изменения документов и похищать файлы, выбранные атакующими.

Вектор заражения InvisiMole пока не установлен. В настоящее время рассматриваются все варианты, включая установку вручную при наличии у злоумышленников физического доступа к компьютеру.

***

18.06.2018

Киберполиция расследует утечку данных из батальона Нацгвардии в Кривом Роге

Департамент киберполиции расследует нарушения правил пользования компьютерами, что привело к утечке данных 21-й бригады охраны общественного порядка Нацгвардии в Интернет. Об этом редакция 368.media узнала из материалов уголовного производства по ст.363 УК (InternetUA).

Правоохранители считают, что неизвестные лица открыли доступ пользователям к рабочим документам, архивам, папкам должностных лиц, которые, возможно, имели гриф «ДСП», «Секретно», «Совершенно секретно».

Данные выложили в сеть. Для установления типов открытой информации полицейские назначили экспертизу. Поручили исследование командиру НГУ и его заместителю.

Кроме того, правоохранители установили IP-адрес, с которого, вероятно, и произошла утечка. В настоящее время подозрение никому пока не предъявлено.

***

19.06.2018
Обнаружен крайне живучий вирус на Windows

Хакерская группировка Zacinlo обнаружила способ обойти защиту в Windows 10 и распространяет вирус, заставляющий жертв просматривать рекламу. Об этом сообщает ZD Net (Компьютерное Обозрение).

По данным исследователей, 90 процентов зараженных устройств работают на Windows 10. При этом именно в этой версии операционной системы с момента ее релиза содержалась устойчивая защита, не позволяющая подобному вредоносному ПО проникать в корневые папки.

Специалисты предупреждают, что вирус способен функционировать незамеченным. В основном он направлен на показ жертве рекламы, а также имитации пользовательских кликов на объявлениях. Таким образом злоумышленники зарабатывают на рекламе. Кроме того, мошенники могут делать скриншоты всего, что происходит на рабочем столе зараженного устройства.

***

19.06.2018
Европол обезвредил хакерскую группировку Rex Mundi

В мае текущего года Королевская полиция Таиланда арестовала 25-летнего хакера по выданному французскими властями международному ордеру. Арест мужчины стал восьмым по счету в рамках международной операции, начавшейся год назад при поддержке Европола и Объединенной группой по борьбе с киберпреступностью (J-CAT) (InternetUA).

В мае 2017 года одна из британских компаний стала жертвой кибератаки, в ходе которой был похищен большой объем данных ее клиентов. Ответственность за инцидент незамедлительно взяла на себя группировка Rex Mundi (в переводе с латыни означает «Король мира»).

Спустя несколько дней после атаки с компанией по телефону связался франкоговорящий мужчина, представившийся как участник Rex Mundi. В подтверждение своих слов мужчина переслал компании большую часть похищенных данных ее клиентов. За неразглашение данных преступник потребовал выкуп в размере 580 тыс. евро в перерасчете на биткойны. Еще 825 тыс. евро он потребовал за раскрытие используемой в атаке уязвимости и совет

по ее исправлению. За каждый день неуплаты сумма выкупа увеличивалась на 210 тыс. евро.

Получив материалы дела от британских и французских властей, Европол начал операцию. В течение одного часа правоохранителям удалось установить личность вымогателя, которым оказался гражданин Франции.

С июня 2017 года французские власти арестовали пять участников Rex Mundi. Согласно признанию главного подозреваемого, он занимался вымогательством, но для осуществления кибератаки нанял хакеров, предлагавших свои услуги в даркнете. В октябре 2017 года во Франции были арестованы еще два человека, а в мае текущего года в Таиланде был произведен восьмой арест.

***

19.06.2018

Найден опасный способ распространения вирусов на Android-смартфонах

Эксперт по безопасности ESET Лукас Стефанко (Lukas Stefanko) обнаружил, что разработчики мобильных приложений обманывают пользователей, подделывая количество загрузок в магазинах. Об этом способе продвижения опасных программ сообщается в блоге компании (InternetUA).

Создатели программного обеспечения вписывают в поле для имени разработчика фальшивое количество загрузок. Таким образом рядовые пользователи видят имя приложения, а ниже – огромные цифры, которые якобы указывают на популярность программы. Псевдорейтинг может исчисляться миллиардами ненастоящих установок.

Однако эксперт проанализировал большинство алгоритмов, использующих подобный трюк «накрутки», и пришел к выводу, что большинство из них являются рекламными и не несут никакого полезного функционала.

При этом простой метод оказался очень эффективным: пользователи, как правило, склонны доверять очень популярным программам, так как считают их безопасными. Потенциально их доверчивостью могут воспользоваться злоумышленники (сейчас данный метод продвижения киберпреступниками не используется).

Чтобы обезопасить свой гаджет от вредных алгоритмов, специалисты рекомендуют обращать внимание на дополнительную информацию о приложениях, предоставляемую Google, и отзывы юзеров. Если реальное число скачиваний невелико, то эксперты не рекомендуют доверять программе. Также следует обратить внимание на то, что Google Play не раздает значки верификации: программы, выдаваемые за «лицензионные», являются фальшивыми.

***

19.06.2018

Эксперты предупредили о «Франкенштейне» среди вирусов для Android

Данное вредоносное ПО сочетает в себе многочисленные характеристики различных известных программ, которые могут представлять собой серьезную угрозу (InternetUA).

Называется данный «Франкенштейн» среди вирусов MysteryBot. Объединяет она в себе функции вымогательства, «клавиатурных шпионов» и различных банковских троянов. Таким образом новый вирус для Android может атаковать сразу на нескольких фронтах.

Исследователи безопасности из ThreatFabric обнаружили вредоносное ПО и заявили, что оно напрямую связано с известным трояном LokiBot для Android.

MysteryBot способен контролировать заряженные устройства и умеет читать сообщения, а также занимается сбором конкретной информации. Помимо этого, он атакует незащищенные электронные почтовые ящики, получая доступ ко всей переписке.

Пока что «Франкенштейн» ничем не грозит владельцам последних версий Android, ведь специализируется на более старых вариациях. Однако эксперты советуют не расслабляться, ведь вскоре данное «упущение» хакеров наверняка будет исправлено.

Вирус открывает дополнительную вредоносную ссылку для отображения поддельных страниц входа поверх приложений для Android, поэтому киберпреступники могут украсть конфиденциальные учетные данные пользователя.

***

20.06.2018

Викрито хакера, який зламував облікові записи користувачів соцмереж

Працівники Карпатського управління Департаменту кіберполіції Національної поліції України, за процесуального керівництва Львівської місцевої прокуратури №1, виявили факти несанкціонованого втручання в роботу облікових записів соціальних мереж та розповсюдження шкідливого програмного забезпечення.

Докладніше

***

20.06.2018

Михаил Сапитон

Хакеры, саботировавшие Олимпиаду-2018, вернулись. В списке целей есть и Украина

Вредоносный червь Olympic Destroyer, с помощью которого саботировали проведение зимней Олимпиады в Пхёнчхане, вернулся за новыми жертвами, пишет издание ArsTechica со ссылкой на экспертов Kaspersky Lab.

Докладніше

ДОДАТКИ

Додаток 1

10.06.2018
Facebook запустила страницу с игровыми стримами

В январе Facebook запустила программу Gaming Creator, призванную помогать создателям игрового видеоконтента наращивать аудиторию в социальной сети. Теперь компания анонсировала программу Level Up, направленную на помощь авторам-новичкам (Украинский телекоммуникационный портал).

Джон Има (John Imah), руководитель Gaming Creator, и Ник Миллер (Nick Miller), менеджер по продукту Facebook, рассказали, что компания запустит программу Level Up в ближайшие несколько месяцев.

Одной из главных её особенностей станет система монетизации Facebook Stars, которая позволит фанатам покупать и передавать виртуальные предметы и таким образом поддерживать любимых стримеров. О тестировании нововведения Facebook сообщила в январе. Также компания запустила экспериментальную ежемесячную подписку, которая пока доступна ограниченному кругу стримеров-партнёров.

Level Up даст авторам контента ранний доступ к новым функциям Gaming Creator, а также позволит получать рекомендации от опытных стримеров. Помимо этого, участники программы смогут обращаться за специализированной поддержкой.

Facebook будет приглашать пользователей к участию в Level Up группами. Позже в этом году программа станет доступна всем желающим. Подписаться на тестирование можно на специальной странице социальной сети.

Также компания хочет, чтобы пользователям было проще искать в Facebook игровые трансляции и записи. Для этого она запустила страницу с простым адресом fb.gg.

«Люди смогут искать на новой странице игровые видео по интересующим их авторам, играм, страницам и группам, – написали Има и Миллер. – Также на fb.gg мы будем продвигать стримеров, киберспортивные турниры и контент с игровых мероприятий.

Сейчас мы находимся в экспериментальной фазе и продолжим тестировать новые возможности, включая ленту для поиска интересного игрового контента, улучшения рекомендаций, расширенный каталог видео на

разных языках и интеграцию вкладки Instant Games с мобильной версией игровой страницы, чтобы люди могли и смотреть, и играть в игры».

(вгору)

Додаток 2

14.06.2018
Роман Черный
Как изменятся социальные сети в будущем

Социальные сети кардинально изменились за последнее десятилетие. Еще в середине нулевых они выглядели эдакой перспективной диковинкой, игрушкой для молодежи. Сегодня же они превратились в невероятно мощный социальный институт, оказывающий колоссальное влияние на облик мира. Очевидно, в будущем соцсети никуда не исчезнут. А вот как они будут развиваться – весьма интересный вопрос (IGate).

Фокус на межличностных отношениях

Одна из первых социальных сетей называлась Friendster и была сфокусирована на том, чтобы знакомить людей между собой. Ее цель декларировалась как создание и поддержание дружбы. Примерно так же начинали и MySpace с Facebook. Со временем фокус сместился на обслуживание личных интересов пользователя.

Современная социальная сеть напоминает скорее персонализированное СМИ, сообщающее человеку новости из сферы его интересов. Также соцсети стали чем-то вроде общественных трибун для компаний и частных лиц. Любой, кому есть что сказать, может вещать на весь мир.

Но, похоже, такая ситуация разрушила ту «теплую ламповую» атмосферу, которая была присуща соцсетям середины нулевых. Сеть больше не воспринимается людьми как инструмент для дружбы и общения с близкими. И это попытаются исправить.

Вероятнее всего, руководство соцсетей снова попытается сместить фокус в сторону межличностных отношений. Первые признаки этого мы можем видеть уже сейчас, когда Facebook стимулирует пользователей делиться личными воспоминаниями и всячески пытается вызвать ностальгию.

Больше инструментов самовыражения

До сих пор средства выражения в соцсетях довольно ограничены. Вы можете разместить в посте текст, картинку, аудио или видео и ссылку на внешнюю статью. Эксперты полагают, что в будущем инструментарий значительно расширится новыми, более интерактивными возможностями. К примеру, пользователь сможет конструировать на базе соцсети виртуальные пространства и приглашать в них других людей.

Платные опции

Конечно же, социальные сети будут оставаться бесплатными. Но в них, наверняка, появятся платные опции. Российская соцсеть «ВКонтакте» уже предлагает пользователям платную подписку на музыку. Но в будущем стоит

ждать появления в соцсетях «премиумных» пакетов, к примеру, отключающих назойливую рекламу. Также плата может взиматься за хранение архива фотографий и видео пользователя без сжатия и потери качества.

Много видеоконтента

Несколько лет назад текстовые посты стали практически повсеместно вытесняться постами с картинками. Сегодня картинки вытесняются видеороликами. Пользователи социальных сетей будущего будут общаться с виртуальным миром, в основном, при помощи камеры, а не при помощи клавиатуры.

Социальные маски и роли

С родственниками мы ведем себя иначе, чем с друзьями, а с коллегами – иначе чем с родственниками. Увы, поскольку современные соцсети становятся всеобъемлющими, они разом охватывают практически весь круг общения пользователя. Это может вызывать неприятные ситуации. Например, вы можете захотеть скрыть от чересчур верующих родственников свое увлечение блэк-металом или не афишировать увлечение охотой перед пацифистами-веганами с работы.

Отписка и отказ от активности в интересующих вас сообществах – не выход. Стоит ожидать, что в будущем в соцсетях появятся функции, позволяющие в той или иной форме имитировать социальные маски, которые все мы носим в реальной жизни. Например, пользователь сможет распределять друзей по группам, для которых будет блокироваться тот или иной контент.

Аполитичные друзья не узнают о вашем участии в политических баталиях, а бабушка не увидит пост, в котором вы хвастаетесь очередной татуировкой.

Больше приватности

Учитывая последние скандалы с Facebook, стоит ожидать, что социальные сети будут уделять гораздо больше внимания приватности. Пользователи будут точно знать, какая информация о них собирается и куда передается. По крайней мере, компании приложат максимум усилий, чтобы создать у людей иллюзию безопасности, приватности и контроля над личной информацией.

Цифровое наследие

Что попало в интернет, остается в интернете. Со временем социальные сети превратятся в огромные архивы, хранящие информацию о жизни прошлых десятилетий. По мере того, как будут меняться поколения, соцсети превратятся в своеобразные «цифровые кладбища», станут уникальным учебником истории для тех, кто придет в них после нас.

(вгору)

Додаток 3

16.06.2018
Роман Черный
Как формируется новостная лента Instagram

После скандала с Facebook и Cambridge Analytica все большее количество пользователей начинает интересоваться внутренними механизмами работы соцсетей. Людей интересует не только то, какую информацию о них собирают компании, но и то, по каким принципам соцсеть формирует ленту для пользователя. Чтобы удовлетворить это любопытство, представители Instagram рассказали об умных алгоритмах, которые формируют ленту для каждого из пользователей (IGate).

Алгоритмы VS хронологическая выдача

Напомним, еще пару лет назад Instagram выдавал пользователю посты в простом хронологическом порядке. Пользователь видел все сообщения от всех своих подписок. Соответственно, чем больше подписок было у пользователя, тем больше новых постов накапливалось в ленте за определенный промежуток времени.

Такой способ подачи может быть удобным, если вы подписаны да два-три аккаунта. Но для тех, кто подписан на сотни аккаунтов, хронологическая выдача совершенно неудобна. Новых постов становится слишком много, пользователь не прокручивает ленту до конца и пропускает много интересного.

Чтобы исправить ситуацию, разработчики Instagram внедрили интеллектуальный алгоритм выдачи, основанный на технологии машинного обучения. По статистике, до этой “реформы” среднестатистический пользователь упускал из виду около 70% постов от общего числа своих подписок и половину постов друзей. После внедрения умного алгоритма пользователь видит примерно 90% постов своих друзей и, в целом, взаимодействует с приложением Instagram дольше, чем в начале 2016.

Как работает алгоритм

Вот какие параметры учитываются социальной сетью при формировании вашей индивидуальной ленты:

Интерес

Instagram запоминает интересы пользователя и выводит на поверхность посты, которые, с большой долей вероятности, понравятся конкретному человеку. Если пользователь в прошлом лайкал, комментировал или долгое время рассматривал определенный контент, в будущем в его ленте появится больше подобных фото. К примеру, если вы долго рассматривали фотографии горячей пиццы, ждите наплыва постов на кулинарную тематику.

Новизна

Хотя от хронологической выдачи Instagram отказался, более свежие посты считаются приоритетными. У пользователя больше шансов увидеть фото, размещенное пару минут назад, чем то, что было загружено на прошлой неделе.

Отношения

Если вы часто взаимодействуете с определенным человеком – лайкаете, комментируете его посты, просматриваете профиль – его сообщения вы будете видеть чаще.

Также на формирование ленты влияют такие показатели:

Частота

Чем чаще вы запускаете приложение Instagram, тем чаще алгоритм формирует для вас новую ленту.

Разнообразие

Если вы подписаны на большое количество разных аккаунтов, алгоритм попытается выстроить ленту таким образом, чтобы посты разной тематики чередовали друг друга.

Продолжительность сессий

Алгоритм учитывает, как долго конкретный пользователь работает с приложением Instagram. Если вы запускаете приложение на пару минут, вам постараются показать самые «сливки». Но если вы имеете манеру задерживаться в Instagram подольше, алгоритм выдаст вам больше разнообразных фото.

В первое время после запуска алгоритма многие пользователи были недовольны. Новшество породило множество слухов. Представители Instagram решили опровергнуть их.

Во-первых, Instagram не скрывает непопулярные посты. Ни один пост никогда не был преднамеренно спрятан от глаз пользователей. Если вы будете листать ленту достаточно долго, то увидите каждое сообщение. Разница лишь в том, что теперь посты выводятся не в хронологическом порядке.

Соцсеть не продвигает определенные типы контента. Если вы подолгу рассматриваете фотографии, алгоритм отдает приоритет фотографиям а не видеороликам. То же происходит, если вы пролистываете видеоролики, не просматривая их. В этом случае фотографии будут отображаться первыми.

Если человек использует сервисы Stories или трансляции Live, Instagram не продвигает его контент и вносит его в список «суперпользователей». По словам представителей соцсети, такого VIP-списка попросту не существует.

Точно так же Instagram не «понижает рейтинг» тех, кто постит слишком часто. Как уже говорилось, соцсеть не присваивает пользователям никаких рейтингов. Просто, учитывая вышеописанные особенности алгоритма, частые посты от одного и того же человека могут «разбавляться» другими сообщениями в лентах его подписчиков.

(вгору)

Додаток 4

19.06.2018

Звезды «Барселоны» запускают соцсеть для футбольных фанатов на блокчейне

Команда разработчиков совместно с бывшими игроками испанского футбольного клуба «Барселона» Карлесом Пуйолем, Андресом Иньестой и Иваном де ла Пенья заявила о запуске социальной сети Olyseum,

предназначенной для общения поклонников футбола с их кумирам. Об этом сообщает Bankless Times (InternetUA).

«На протяжении всей моей карьеры в «Барселоне» я пользовался неизменной поддержкой миллионов болельщиков по всему миру. Андрес, Иван и я объединились, чтобы создать пространство для любителей футбола и теснее взаимодействовать с ними», – сказал Карлес Пуйоль.

Созданная с помощью технологии блокчейн сеть Olyseum появилась благодаря желанию футболистов наладить более тесные отношения с собственными поклонниками. Проект создаст универсальную платформу для общения, взаимодействия и вознаграждения спортсменов и их фанатов с помощью передовых технологий.

В дополнение к блокчейну, Olyseum будет иметь основанную на смарт-контрактах программу стимулирования пользователей, которые участвуют в развитии комьюнити. В качестве вознаграждения они будут получать эксклюзивные товары, VIP-билеты и уникальный опыт общения со звездами футбола.

Тестирование соцсети будет проводиться во время проходящего в эти дни в России Чемпионата мира по футболу. В 2016 году при первом запуске на испанском языке Olyseum возглавил списки самых популярных приложений App Store в шести странах. Официальный запуск проекта намечен на конец 2018 года.

CEO проекта Карлос Грегуар имеет степень магистра в области информационной безопасности и неврологии и пишет кандидатскую диссертацию в области компьютерных наук и телекоммуникаций. Он является создателем компании Quantum Fields Technologies, которая специализируется на проектах в области безопасности и искусственного интеллекта. Его партнер по Olyseum, разработчик Кевин Митник, известен по работе в компаниях из списка Fortune 500 и ФБР.

«Слишком долго между кумирами и их поклонниками существовала пропасть. Olyseum создан, чтобы преодолеть ее через социальную сеть, которая дает фанатам новые возможности и, самое главное, вознаграждает их за участие. Меня всегда увлекало улучшение отношений между людьми за счет компьютеров и технологий. Когда Карлос, Андрес и Иван пришли ко мне с проблемой ограниченного участия фанатов, я почувствовал, что нужно использовать свои знания и навыки, чтобы предложить решение», – заявил Грегуар.

(вгору)

Додаток 5

13.06.2018
Ирина Фоменко
Facebook наносит удар по китайской электронной коммерции

Facebook принимает жесткие меры в отношении китайских торговых сайтов, рекламирующих в социальной сети продукты, которые в итоге оказываются низкого качества. Сегодня Facebook запускает новую функцию для электронной коммерции на панели управления Recent Ads Activity – теперь покупатели смогут оставлять отзывы о долгой доставке, странных запахах и плохих товарах. Об этом сообщает TechCrunch (InternetUA).

Пользователи могут получить доступ к объявлениям, нажав на них, и оставить отзыв, кликнув на Ads Activity. Facebook также расширяет возможности обратной связи для тех, кто приобрел товар благодаря рекламе: например, через подсказки в уведомлениях.

Существует две основных причины новой тактики медиа-платформы. Во-первых, так рекламодателям проще получить больше информации о предпочтениях клиентов, чтобы впоследствии внести изменения в свою работу. Во-вторых, при большом количестве негативных отзывов Facebook ставит ультиматум бизнесу – исправить ситуацию. В случае если этого не будет сделано, социальная сеть откажется рекламировать товар.

На прошлой неделе Facebook дал возможность публикующим на Marketplace рекламировать свои услуги в ленте новостей. В мае социальная сеть расширила своего конкурента Craigslist, добавив в него уборщиков. Таким образом, чтобы убедиться, что реклама в области электронной коммерции не «сойдет на нет», Facebook должен повысить уровень доверия потребителя, иначе 2,2 млрд пользователей перестанут кликать на торговые объявления, опасаясь быть обманутыми.

«У большинства из нас был негативный клиентский опыт. А плохой шоппинг стоит денег и приносит массу дискомфорта. Такая электронная коммерция не подходит ни клиентам, ни Facebook», – заявила директор по маркетингу Facebook Сара Эппс.

Существует еще одна причина для повышения эффективности работы как пользователей, так и рекламодателей: по данным некоторых исследований, компании, которые выросли в целые предприятия благодаря продаже товаров через рекламу в Facebook, теперь ищут альтернативные платформы, поскольку объявления стали слишком дорогостоящими.

Хоть и полный контроль за любым продавцом невозможен, новая стратегия Facebook позволит, по крайней мере, использовать негативные отзывы для защиты клиентов от мошенничества. В этом отношении она похож на метод Facebook, который компания применяет касательно агрессивных публикаций и фейковых новостей: социальная сеть полагается не только на алгоритмы – платформа пытается анализировать комментарии, а также сотрудничает с третьими сторонами для проверки фактов и новостей.

Впервые эту проблему на Facebook выявила новостная компания Buzzfeed два года назад: оказалась, что полученные товары не соответствуют ожиданиям. Как заявляют в социальной сети, Facebook понадобилось несколько лет, чтобы решить эту проблему.

«Мы изучали этот вопрос до того, как его начали обсуждать в СМИ. Самая большая проблема заключается в том, что эта деятельность происходила вне Facebook – мы не знаем, что вы делаете, когда покидаете социальную сеть из-за рекламы. Поэтому нам потребовалось время для разработки надлежащего механизма обратной связи, и мы хотели убедиться, что это справедливо и в отношении бизнеса, и клиента», – прокомментировали в пресс-службе компании. – «Теперь мы хотим получить обратную связь от общественности. Иногда реклама полностью соответствует нашим правилам, но в реальности товары этих компаний не соответствуют ожиданиям».

Важно отметить, что негативные отзывы не означают моментальный отказ социальной сети рекламировать продукт. В компании утверждают, что рекламодатели тоже могут делать ошибки, ненамеренно вводя в заблуждение потребителя. Основная часть объявлений, анализированных BuzzFeed, как оказалось, поступает от китайских компаний, где главные проблемы – логистика и язык.

«Мы даем предприятиям время исправить ситуацию. Из сотен компаний, которыми мы были недовольны, многие предприняли меры. До сих пор реакция предприятий была положительной», – заявила Сара Эппс.

(вгору)

Додаток 6

7.06.2018
Полина Лисовец
4 признака того, что социальные сети вызывают у вас депрессию

Социальные сети стали частью нашей жизни, но они не только облегчают общение, но и могут усугубить депрессивное состояния.

Мы знаем, что существует связь между социальными сетями и проблемами психического здоровья, поскольку использование онлайновых платформ может усугубить депрессивное состояние. Но новое углубленное исследование подтвердило эту корреляцию и установило, что определенные привычки в отношении социальных сетей имеют прямую связь с депрессией (Marie Claire).

Исследователи Техасского государственного университета проанализировали онлайн-поведение 500 студентов, которые часто использовали Facebook, Twitter, Instagram и Snapchat. Кроме того, они опросили участников о том, были ли у них какие-либо симптомы депрессивного расстройства, и то, что они обнаружили, нас поразило.

Ученые определили, что у тех, у кого прослеживались признаки депрессии, вели себя в социальных сетях следующим образом:

Признак 1: Они используют социальные медиа, чтобы сравнивать себя с другими, «лучшими», чем они сами. Чаще всего такая тенденция прослеживается в Instagram, когда пользователи выкладывают только удачные фото и демонстрируют успешную жизнь, оставляя реальность за кадром;

Признак 2: Они регулярно используют социальные сети и это доходит до уровня «наркомании» (такое состояние было определено посредством опроса, в котором студенты отвечали «да» на следующие утверждения: «вы пытались максимально сократить использование социальных сетей», «вы очень часто используете социальные сети, что это негативно отразилось на вашей работе / учебе»)

Признак 3: Они чувствовали себя обеспокоенными после того, как их отметили на неудачных фотографиях в социальных сетях. Часто это вызывало у студентов тревогу и даже агрессию.

Признак 4: Эти студенты редко публикуют фотографии с другими людьми. Причина, по которой люди с депрессией, меньше публикуют снимки с другими, считают авторы исследования, состоит в том, что индивидуумы с этой психологической проблемой часто склонны изолировать себя от других.

Хотя исследование, которое еще не было официально опубликовано, но уже представлено в прошлом месяце на ежегодном собрании Ассоциации психологических наук в Сан-Франциско, дает большое представление о моделях поведения людей, у которых наблюдается депрессия, ученые не утверждают со сто процентной вероятностью, что симптомы депрессии могут быть вызваны социальными сетями.

Так что задумайтесь, если вы замечаете за собой хотя бы один из наведенных выше признаков, возможно, стоит немного ограничить время пребывания в социальных сетях.

(вгору)

Додаток 7

10.06.2018

Техніка маніпуляції. Вісім брудних прийомів, які використовують пропагандисти в соцмережах

Данило Малуха, Сергій Клімович

Як у Фейсбуці від «вашого імені» поширюють певну інформацію? Чому ваші друзі вважають, що ви залайкали сайт із поганою репутацією? Люди, котрі створили розважальні групи, заробляють на політичній пропаганді. Ми визначили 8 найпоширеніших прийомів маніпуляції та обману, які використовують українські політичні штаби, комерційні компанії та російські пропагандисти (Детектор медіа).

1. Мимовільний лайк ФБ-сторінки

Ваші друзі у Фейсбуці бачать, що ви залайкали якийсь сайт-помийку, яка пропагує зраду чи, навпаки, неадекватну перемогу. Ви про це дізнаєтеся, тільки коли вам напишуть у приват щось типу: «Чувак, ти що здурів? Чому переметнувся до них?»

Як так сталось? Вас обдурили і використали. Колись ви клікнули на якийсь крикливий заголовок у тому ж ФБ і потрапили на сайт, який опублікував цей заголовок. Тоді вам на екран вискочило нав'язливе вікно

«Дізнавайтесь новини сайту на нашій ФБ-сторінці». І ви роздратовано клікаєте по ньому і навколо нього, аби закрити.

Це вікно зроблено не маленьким, як ви бачите, а на весь екран. Просто 80 % його – прозоре поле. А налаштування даної програмки таке, що будь-який клік мишкою зараховується як лайк. Подібний прийом дозволяє відносно швидко набрати аудиторію, але, звісно, порушує правила Facebook.

2. Поширення від вашого імені

Ваші друзі вам пишуть, що ви виправдовуєте забудовника. А ви про нього взагалі не чули.

Все почалося з того, що до вас у друзі попросилася незнайомка із надзвичайно звабливою аватаркою. Хто ж такій відмовить? Значить, майже напевно дали доступ до свого списку друзів. В налаштуваннях можна заборонити цей доступ, але як це зробити, мало хто знає. Тепер ваша нова віртуальна подруга пише пропагандистський пост (світлина з рекламою, запис, який розганяється Мережею, якась подія-івент, гра тощо), тегає вас – і чимало ваших друзів побачать це. Частина подумає, що це ваш допис.

Проста математика. Нехай у вас 1000 френдів. Спамер затегав сотню таких, як ви. Якщо цей контент побачить хоч 5 % «ваших друзів», то це вийде аудиторія до 5000 фейсбукерів. А якщо таких спам-інтервентів з десяток? А потім ще по всій цій купі людей є можливість замовити таргетовану рекламу.

3. Купівля мережі популярних груп/спільнот

У 2014 році один з авторів цієї статті на власні очі бачив, як за одну годину десь з півтора десятка груп на кшталт «Цікава Вінниця» стали набором груп «Цікава Волинь». Бо їх модератори хотіли отримати замовлення на поширення політичної агітації, спрямованої на мешканців Волині. Зрозуміло, що реального ефекту на результати виборів це не справило.

4. Забанити топа

Ви не можете знайти акаунт вашого знайомого у Фейсбуці, або пишете йому листи в месенджер, а він вперто не відповідає, хоча завжди був пунктуальною людиною? Його забанили. Ймовірно, він написав щось, що не сподобалося російським тролям, і вони масово почали на нього скаржитися.

Подібну тактику й досі дуже широко використовують ольгінці.

Існує «антидот» у вигляді резервних профілів. Втім, шкоди від бану на, наприклад, 30 діб, достатньо для передвиборчої кампанії, щоб займатися таким «під ключ».

5. Спам-коментарі

Ви хочете почитати всю дискусію під постом, але бачите тільки півдесятка коментарі, вирваних з контексту. Це алгоритм Фейсбуку, який пропонує усім найбільш цікаві чи резонансні (на його машинну думку) коменти. І цим користуються. «Анти-троль», який захищає свого клієнта від навали тролів, приходить в дискусію з кількох акаунтів і лишає свої «нейтральні» думки. Але в його роботі важливо не користуватися функцією «Відповісти», а робити начебто нові коменти – їх сервіс і пропонуватиме свіжим читачам. А справжній негатив ховатиметься десь нижче.

6. Боти і тролі

Незнайомі люди починають вам писати в особисті повідомлення і щось доводити, або ображати вас та вашу затишну компанію в коментах. Розслабтесь, вас атакують боти. Як правило вони – жіночої статі. Є тут щось від підсвідомої фрейдистської довіри до жінки. Зазвичай, минає кілька днів або й навіть тижнів після додавання «в друзі», коли бот починає «працювати».

Власне, тролів тому так і назвали, що вони приходили на якийсь сайт чи форму без премодерації коментарів, і там своїми образливими і занадто емоційними коментарями припиняли будь-яку конструктивну дискусію. Звісно, профіль бота є максимально загальним – не більше півдесятка світлин, вкрадених зазвичай десь на американських іміджбордах.

Боти і тролі – це гарматне м'ясо на полях гібридної війни, на бото-фермах таких виробляють у промислових масштабах. Якщо вірити телеграм-каналу «Исповедь кремлебота», в Ольгіно для цього навіть існує спеціальний виробничий відділ.

Боти – найпримітивніший, проте, внаслідок величезного обсягу таких профілів, ефективний інструмент.

Причому, ботів застосовують не тільки для війн між країнами, а навіть на рівні розборок у міськраді. Боти – це масовість, примітивні образи і тролінг. З боку ольгінців пішла мода створювати акаунти від імені українців. Деякі пишуть українською. Можуть навіть причепитися, якщо опонент пише російською.

– Коментування ботами [при цьому] завжди було і залишається головним способом взяти гроші з замовника, – говорить фахівець з перевиборчих інтернет-комунікацій Микола Малуха. – Найбільш прибутковий бізнес, а ефекту – нуль. Він будується на ірраціональних бажаннях замовника бачити, як його хвалить аудиторія, і прибирати будь-який негатив.

7. Елітарна спільнота

Ви долучилися до якоїсь групи у ФБ і вважаєте, що тут зібралися однодумці? Будьте обережні.

Задовго до часу Х (передостанній тиждень передвиборчої кампанії) створюється «напівзакритий», «елітарний» тематичний майданчик для дискусій. У тих, хто потрапить сюди, складатиметься враження причетності, допущеності до певного кола обраних. Слово Миколі Малусі: «Запуск такої групи у ФБ не особливо затратний і цілком дієвий. Реальні факти можна змішувати з чутками, чорнухою і навіть «трешняком». Грамотна робота доведе аудиторію до того рівня, коли буде сприйматися будь-яка інформація».

Як людині, яка попала в таку пропагандистську спільноту, вирахувати, що нею хочуть маніпулювати?

Для цього необхідно критично мислити і перевіряти бодай поверхнево факти, з якими стикаєтеся. Гугл багато чого може розповісти.

8. Реклама у Facebook

У США багато дискутують з того приводу, як політична реклама у ФБ, за яку платила Росія, вплинула на вибори. Пропонується, щоб соцмережа

вказувала, хто оплатив політичну рекламу. В Україні політична реклама у ФБ використовується на повну котушку.

Адже ФБ толком не перевіряє фейкову інформацію. Тому можна побачити, як через рекламу поширюють відверту чорнуху. Створюється паблік (тематична публічна сторінка, наприклад, «Не надто типова Шепетівка»), через який йде атака на конкурента, публікації ставляться на рекламу. Причому, нерідко трапляється, що сторінки мають розважальний характер, але на них поширюється політична агітація. Такими є майже всі великі (у десятки, сотні тисячі фоловерів) столичні міські пабліки, які регулярно «продаються» політичним замовникам.

Facebook часто пропускає треш-рекламу і без жодних маніпуляцій. Є низка стоп-слів, за якими ФБ визначає тематику оголошень і те, чи не порушує така реклама правила. Наприклад, після заборони реклами Initial Coin Offering (криптовалюти), спритні рекламники або прибирали це слово з текстів, або змінювали букву «О» на цифру «0»… і ФБ дозволяв публікувати рекламу.

Як цьому протистояти? Дуже просто – не вірте тому, що пишуть у соцмережах незнайомі люди. Перед тим, як поширити пост навіть свого знайомого, перевірте основні факти через гугл. Тоді ви не станете корисним ідіотом, якого використовують інші для досягнення своїх цілей.

(вгору)

Додаток 8

11.06.2018
Ирина Фоменко
Мюллер проверит мессенджеры на безопасность

Команда специального прокурора Роберта С. Мюллера III проверит зашифрованные мессенджеры на безопасность в ходе российского расследования. Об этом сообщает The Washington Post (InternetUA).

Группа Мюллера изучает рекомендации экспертов относительно «лучших мессенджеров». Благодаря сквозному шифрованию только отправитель и получатель могу прочитать сообщения: такие мессенджеры популярны среди активистов, журналистов, специалистов в области безопасности и правительственных чиновников.

На этой неделе команда Мюллера обвинила бывшего председателя президентской кампании Трампа Пола Манафорта в подкупе свидетелей – он пытался связаться с ними по телефону и через зашифрованные мессенджеры.

Итак, как команда Мюллера сможет просматривать содержимое таких приложений? Представитель аппарата специального прокурора отказался комментировать ход расследования. The Washington Post рассказал, как работают 4 приложения, которые сейчас проверяет команда Мюллера.

Signal

Среди экспертов Signal считается одним из лучших безопасных мессенджеров. Пользователи могут настроить сообщения так, чтобы они

удалялись через 5 секунд или до одной недели. Их можно также удалять вручную. Сообщения сохраняются только на устройстве.

В ходе расследования свидетели «сдали» телефоны добровольно. Если они оставили устройства разблокированными, команда Мюллера могла просмотреть всю переписку. Чтобы гарантированно сохранить доказательства, группа могла извлечь сообщения, сделать резервную копию и записать на новое устройство.

WhatsApp

WhatsApp, используемый 1,5 миллиардами человек ежемесячно, принадлежит Facebook. В нем пользователи могут звонить, отправлять текстовые сообщения, изображения и видео. Шифрование WhatsApp построено на той же технологии, что и Signal, а содержимое сообщений хранится только на устройстве. Однако, имея доступ к телефону, агенты смогут увидеть историю сообщений WhatsApp пользователя. В WhatsApp нет функции автоматического удаления, но пользователи могут вручную удалять сообщения или целые чаты.

В отличие от Signal, у WhatsApp есть резервное копирование сообщений. По словам экспертов, так пользователям удобнее сохранять истории чатов при потере телефона или покупке нового. Но существует и риск, что неавторизованный пользователь получит доступ к сообщениям. При резервном копировании чатов медиа и переписки больше не защищены сквозным шифрованием.

Dust

В Dust пользователи могут настроить мессенджер так, чтобы он автоматически удалял сообщения через 24 часа или сразу же после прочтения. Приложение предупреждает пользователей, когда кто-то делает скриншот; а для тех, у кого ОС Android и Windows, Dust отключает эту функцию. В Dust нельзя сохранять сообщения: человек не сможет прочитать старую переписку.

Confide

Сообщения в Confide автоматически удаляются сразу же после прочтения. Они не сохраняются ни на телефоне, ни на серверах. В мессенджере нельзя делать скриншоты переписок.

По мнению большинства экспертов, удаление сообщений зависит от телефона, безопасности приложения и тщательности поисков.

«Гипотетически, это возможно. Но это очень сложно сделать, если приложение действительно хорошо разработано», – заявил профессор Университета Джонса Хопкинса Мэтью Грин.

С другой стороны, утверждают аналитики, не только сообщения могут стать ценным источником информации. «Мне может быть интересно не содержание разговора, а то, с кем общается пользователь», – прокомментировал технолог Американского союза защиты гражданских свобод Дэниел Кан Гиллмор.

(вгору)

Додаток 9

7.06.2018

Пограничная полиция Китая загружает вирусы в Android-смартфоны

Ранее США обвинили Китай во встраивании вредоносного софта в смартфоны ZTE и Huawei в целях слежения за жителями Америки. В этот раз о слежке заговорили обычные люди. Если быть более точными, речь идет о пользователе популярного форума «Reddit» под ником «BigTyPB», который поделился интересным случаем на границе Китая (InternetUA).

Случай этот произошел, по словам автора поста, совсем недавно:

«Моя жена и я недавно пересекли границу Китая, на которой полиция установила на наши Android-смартфоны (Moto X4 и мой Huawei Mate 9) программное обеспечение.

Я видел процесс установки, на рабочем столе появилась иконка приложения, полицейский запустил приложение, после чего иконка сама по себе исчезла. Не уверен, пытался ли он получить root-права или что-то подобное. Я знаю, что-то было запущено на моём телефоне до того, как они отпустили нас, потому что они использовали портативное устройство для проверки соединения наших телефонов с их системой.

У кого-нибудь есть какие-либо идеи для проверки устройства на отсутствие какого-либо ПО слежения на моём телефоне?»

Данный пост получил много отзывов (около 314 комментариев на момент написания статьи). Некоторые пользователи всерьез предложили автору новые смартфоны взамен на их собственные с китайским ПО слежения. Пользователи посчитали, что данные устройства высоко оценят специалисты по безопасности, которые бы с радостью изучили заражённые аппараты.

(вгору)

Додаток 10

7.06.2018

Кибертеррористы наступают: как украинские компании «укрепляют» свои позиции

Почему киберугрозы взлетели на второе место в рейтинге самых опасных рисков для бизнеса (InternetUA).

«Самое точное определение того, что сейчас происходит в Украине, – кибертерроризм», – подчеркнул директор по работе с партнерами и клиентами представительства Cisco в Украине и странах СНГ Сергей Мартынчук на недавнем Cyber Defence Congress 2K18. Спикеры отмечали, что большинство крупных кибератак выполняли не экономические, а политические и военные задачи. Вместе с тем жертвами профессиональных хакерских ОПГ становится все большее число частных компаний.

Как бизнесу продержаться в этой войне с наименьшим числом потерь? Почему лучше стать случайной жертвой, а не инструментом кибератаки? На эти и другие вопросы отвечали спикеры конгресса. Mind выбрал наиболее интересные факты и мнения.

Масштаб ущерба. CEO и соучредитель страхового брокера «Инсарт» Александра Гладышевская констатирует, в 2017 году потери мировой экономики от кибератак оценены в $600 млрд. К 2020 году аналитики «оптимистично» прогнозируют рост ущерба до $2 трлн.

«Только от вируса Petya украинская экономика потеряла $466 млн, или 0,5% ВВП. Это лишь белые цифры. Оценить весь размер ущерба не может никто», – сообщила Александра Гладышевская.

Сергей Мартынчук отметил: до 2017 года многие украинские компании надеялись, что их «хата с краю». Но масштабные атаки прошлого года, особенно Petya, произвели отрезвляющий эффект. Спикер напомнил о недавно выявленном вирусе VPN Filter. «Им инфицировано более 500 000 устройств в 54 странах. Специалисты Cisco Talos пришли к выводу, что Украина – цель данной атаки. Самое важное, что атака еще не приведена в действие. Пока прошел только первый этап инфицирования. А судя по числу зараженных устройств, масштаб может быть огромным», – считает Сергей Мартынчук. Те, кто не успел «очиститься» от вируса, могут найти детальные рекомендации в блоге CiscoTalos.

Президент Киевского отделения международной неприбыльной профессиональной ассоциации ISACA Алексей Янковский сообщил, что в ближайшее время нас ожидает кибератака, мировой ущерб от которой может достичь $50 млрд.

В одной лодке. Спикеры иронизировали, что все компании можно поделить на две категории: те, кто знает, что их хакнули, и те, кто еще не в курсе. Третьего, увы, не дано. По словам Алексея Янковского, в последнее время уровень угроз существенно возрос. «Если ранее мы имели дело с хакерами-одиночками, то сейчас – с профессиональными, структурированными ОПГ, в состав которых входит по 10-30 человек. Они отлично разбираются в различных сферах бизнеса, имеют неограниченные ресурсы и время. Могут позволить себе годами пытаться взломать систему», – рассказывает спикер.

«Согласно данным отчета Allianz Global Corporate&Specialty, киберугрозы уже переместились на второе место в рейтинге самых опасных рисков для бизнеса. Еще три года назад они были на 15-м», – рассказала Александра Гладышевская.

По словам Сергея Мартынчука, в условиях кибертерроризма компаниям отведена роль «мирных жителей», как в игре «Мафия». «У них есть два варианта – стать случайной жертвой или инструментом атаки. Участь вторых (например, компании M.E.Doc) не завидна. Если компания становится инструментом – ее страдания умножаются в десятки раз, потому что потеря имиджа просто сумасшедшая и порой непоправимая», – считает спикер.

Как компании «укрепляют» позиции? Пока общая картина «строевой подготовки» не впечатляет. «По данным отчета об инфорбезопасности Cisco, 66 % инцидентов не обнаруживается месяцами и даже годами, до выявления проникновения в среднем проходит 229 дней, в 60 % случаев данные утекают в первые 24 часа, и только 33 % организаций узнают об атаках с помощью своего мониторинга», – подчеркивает Сергей Мартынчук.

Алексей Янковский из ISACA сообщил: их недавний аудит украинских компаний выявил, что многие пока не осознают риски, не знают о правилах, инструментах и подходах к противодействию. «После вируса Petya компании стали строить службы информационной безопасности (СИБ). Но даже крупные предприятия формируют СИБ из 2-3 человек. Кроме того, мы выявляем недостаточный уровень компетенции специалистов как IT–департаментов, так и СИБ, неотлаженные коммуникации между этими подразделениями», – рассказал Алексей Янковский.

Глава правления ИнАУ Александр Федиенко провел маленький эксперимент на конгрессе: попросил отозваться тех, у кого на предприятиях внедрены правила безопасности. Руку никто не поднял. «Можно нанять самых крутых специалистов, но без правил по кибербезопасности ничего не будет работать!» – отметил Александр Федиенко. Он уверен: правила должны знать все – как новые, так и старые сотрудники. Важно тестировать персонал и не бояться штрафовать тех, кто нарушает регламенты.

Александра Гладышевская привела показательный пример: «Наши клиенты заполняют опросники и сообщают, какие системы кибербезопасности у них работают. Иногда очень удивляют. К примеру, представители одной из украинских страховых компаний написали, что у них на рабочих станцияхнет антивируса. Эта компания входит в ТОП-10 на своем рынке и вообще никак не защищают данные своих клиентов».

Алексей Янковский сообщил, что пока лишь некоторые украинские компании стали строить центры мониторинга и управления безопасностью (Security Operation Center, SOC). Хотя многие начали интересоваться сейчас модными SOC.

Волшебная палочка. Помимо трех китов – внедрения инструкций, обучения сотрудников и использования разнообразных инструментов защиты – бизнесу помогает и киберстрахование», – полагает Александра Гладышевская. В случае ЧП (фишинга, кибервымогательства, кражи и уничтожения данных, получения контроля над IT-ситемами, атак на POS-терминалы и т.п.) компаниям могут выплатить по страховке до $1 млн. Страховой тариф – от 1 %. К примеру, $10 000 в год, если компания страхуется на $1 млн.

По словам CEO «Инсарт», застрахованным могут возместить убытки (упущенную прибыль, претензии третьих лиц, штрафы государства) и расходы (реагирование на кибератаку, восстановление данных и репутации, юридическую поддержку, проведение расследования).

Присутствовавшие на конгрессе сотрудники компаний после выступления спикера иронизировали, что страховщики начали отбирать у них

работу: бизнесу проще заплатить $10 000 в год, чем оплачивать труд хотя бы нескольких специалистов по безопасности.

(вгору)

Додаток 11

10.06.2018

Ущерб от хакеров за 2017 год оценили в 172 млрд долларов

Производитель антивирусного программного обеспечения Symantec опубликовал результаты исследования, посвященного киберпреступности. В 2017 году ущерб интернет-пользователей от хакеров составил 172 млрд долларов (InternetUA).

В общей сложности от кибермошенников пострадали 978 млн человек из 20 стран мира (Австралия, Бразилия, Великобритания, Германия, Гонконг, Индия, Индонезия, Испания, Италия, Канада, Китай, Мексика, Нидерланды, Новая Зеландия, ОАЭ, Сингапур, США, Швеция, Франция и Япония).

Больше половины (53 %) от этого количества столкнулись с вирусами. 38 % пострадали от мошенничества с банковскими картами, а 34 % – от кражи данных к персональным аккаунтам.

Наибольший объем атак пришелся на Китай, где пострадали 352 млн человек. В Индии таковых насчитывалось 186,5 млн, в США – почти 144 млн. Следом расположились Бразилия (62,2 млн), Индонезия (59,5 млн), Мексика (33,2 млн), Германия (23,4 млн), Франция (19,3 млн), Япония (17,7 млн). В десятку стран с самым большим количеством киберпреступлений вошла Великобритания – там было 17,4 млн пострадавших.

Средний урон от киберпреступлений в 2017 году составил 142 доллара. На ликвидацию последствий атак пользователи тратили около суток. 58 % жертв киберпреступности так или иначе поделились, как минимум, одним паролем от любой своей учетной записи с третьими лицами, а 20 % использовали один и тот же пароль во всех аккаунтах.

По данным IBM, в 2017 году у потребителей и компаний по всему миру было похищено более 2,9 млрд записей против 4 млрд годом ранее.

Почти 70 % данных, которые были похищены в 2017 году, появились у злоумышленников в результате неправильно настроенных облачных серверов. Относительно 2016 года объем утечек по этой причине подскочил на 424 %. Таким образом, хакеры продолжают активно пользоваться человеческими ошибками в ИТ-инфраструктурах.

Каждый третий киберинцидент в 2017 году возник вследствие фишинговой атаки, когда пользователи проходят по ссылке на вредоносный сайт или загружают вирусные файлы в электронных письмах. Чаще всего этот метод используется в кампаниях по рассылке спама, отмечают в IBM.

Ранее IBM и организация Ponemon Institute провели исследование, показавшее, что в 2017 году одна утечка информации наносит мировым компаниям убытки в среднем в 3,62 млн долларов против 4 млн долларов годом

ранее. Средняя стоимость потерянной или украденной записи составляет 141 доллар, в здравоохранении этот показатель является самым высоким – 380 долларов.

(вгору)

Додаток 12

10.06.2018
Дмитрий Демченко
Как увеличить безопасность своих данных в интернете. Инструкция

На фоне скандала с утечкой данных Facebook мы начали осознавать, сколько сведений о себе раскрываем онлайн-ресурсам. Некоторую информацию мы отдаем сознательно, но это не всегда так. Мы непроизвольно оставляем данные о сайтах, на которых побывали, а рекламные сети используют их для более точного таргетинга. Иногда это полезно, но чаще всего – неприятно и навязчиво. С другой стороны, есть много способов, чтобы повысить конфиденциальность своей информации в интернете (AIN.UA).

Что не поможет: режим инкогнито

Во всех популярных браузерах есть режим, где не сохраняется история посещенных сайтов. В некоторых моментах он действительно полезен. Но он не подходит для долгосрочного использования. Скорее всего, вы хотите, чтобы некоторые вещи браузер запоминал: например, не хотите каждый раз вводить пароль, чтобы заходить в Facebook. Режим инкогнито не предусматривает такой возможности. Более того – он не блокирует «слежку» за вами в интернете со стороны рекламодателей.

Измените настройки вашего браузера

Самый простой шаг – запретить сторонним сайтам сохранять файлы cookie. Это небольшой объем информации, которые сайты хранят на компьютерах пользователей. Они могут быть полезны, например, для того, чтобы оставаться залогиненым на сервисах. Но с их помощью сайты могут отслеживать ваше поведение.

Запрещая сторонним сайтам сохранять cookie, ваш браузер запретит делать это ресурсам, которые вы на самом деле не посещаете. К ним можно отнести, например, сайты рекламных компаний, объявления которые вы видите на посещаемых страницах. Это не отключит все отслеживание, но приведет к уменьшению и снижению персонализации рекламы, которая вам отображается.

Chrome: перейдите в дополнительные настройки, вкладку «Настройки контента», «Файлы cookie» и включите блокировку сторонних файлов cookie.

Edge: перейдите в дополнительные настройки, «Файлы cookie» и выберите блокировку сторонних файлов cookie.

Firefox: зайдите в настройки, «Приватность и защита», и поставьте «Никогда» напротив графы «Принимать куки и данные сайтов со сторонних веб-сайтов».

Safari: Apple активирует эту функцию по умолчанию.

Блокируйте еще больше с расширениями

Методы выше блокируют передачу не всех данных. Чтобы добиться полной блокировки, нужно воспользоваться расширениями. Есть много браузерных надстроек, но стоит обратить внимание на Privacy Badger. Это расширение не полагается на чужие базы трекеров. Вместо этого, оно само определяет, какие трекеры ведут себя не так, как нужно и блокирует их.

При использовании подобных расширений, некоторые сайты могут некорректно работать. Но настройку можно отключать конкретно для каждого ресурса. Privacy Badger работает в Chrome, Firefox, и Opera. Пользователям Safari и Edge стоит обратить внимание на расширение Ghostery (оно также работает и в вышеперечисленных браузерах).

Такие расширения можно поставить и на смартфон

Правила, приведенные в материале, можно применять и на смартфонах. На iOS Safari разрешает устанавливать расширение, которые блокируют сторонние трекеры. Одно из самых популярных – 1Blocker. На Android придется загружать отдельный браузер. Например, Firefox Focus, который блокирует трекеры и предоставляет возможность быстро удалить все свои данные.

Проверьте настройки в Facebook, Google и других сервисах

В популярных сервисах также стоит воспользоваться некоторыми функциями. Facebook, Google и другие крупные компании, занимающиеся рекламой, часто дают возможность отказаться от некоторых отслеживаний и персонализации. Это не полностью заблокирует сбор информации, но тоже может помочь повысить безопасность данных пользователя.

Facebook, например, в этом разделе позволяет отключить персонализацию рекламы. Google предлагает аналогичное решение – его можно включить здесь. Нужно понимать, что эти шаги не предоставят полную безопасность информации. Но это важные и первоочередные способы, чтобы сделать интернет более комфортным.

(вгору)

Додаток 13

11.06.2018

Самі винні: чому небезпечно розповідати про проблеми з банком у соцмережах

Крістіна Левчук

Клієнти банків, які розповідають про проблеми з банківським обслуговуванням у соціальних мережах, ризикують стати наступними жертвами шахраїв. Такого висновку дійшов Reuters з посиланням на співробітників правоохоронних органів та інших представників галузі (K.Fund Media).

Клієнти британського банку TSB масово публікували пости зі скаргами на банківське обслуговування в соціальних мережах, коли через збій у системі заблокували тисячі облікових записів банківських клієнтів.

У результаті показник щоденних спроб кібератаки на облікові записи клієнтів зріс у 70 разів, а понад 1,3 тис. клієнтів вивели гроші зі своїх рахунків у банку, повідомив глава TSB.

Шахраї отримують інформацію про акаунти клієнтів через соціальні мережі, де користувачі можуть неусвідомлено розповісти важливі деталі про банківські дані.

«Що більше інформації публікується в соціальних мережах, тим простіше шахраям вкрасти вашу особистість», – нагадує прес-секретар TSB Супріт Томас (Supreet Thomas).

Як варіант, шахраї представляються співробітниками банку й повідомляють, що виявили підозрілу активність щодо акаунту, тому для уточнення деталей власнику необхідно перейти за таким-то посиланням. Усі комунікації відбуваються за допомогою дзвінків, листів електронної пошти і СМС-повідомлень з номерів, які видають за номери банку.

Загалом за травень клієнти TSB повідомили про 749 спроб фішингу – на 30 випадків більше в порівнянні з попереднім місяцем, за даними британського центру звітності кіберзлочинності Action Fraud.

(вгору)

Додаток 14

11.06.2018

ESET обнаружила в Украине сверхсложное шпионское программное обеспечение

Компания ESET сообщает об обнаружении шпионского программного обеспечения InvisiMole, которое способно следить за деятельностью жертв и похищать их конфиденциальную информацию (Компьютерное Обозрение).

По данным телеметрии ESET, угроза была активной минимум с 2013 г., однако инструмент для осуществления кибершпионажа оставался незамеченным до момента обнаружения системами ESET на инфицированных компьютерах в Украине и России.

Поскольку угроза является целенаправленной, вредоносное программное обеспечение имеет низкий уровень инфицирования с несколькими десятками зараженных компьютеров.

Угроза InvisiMole имеет модульную архитектуру, начиная свое распространение с модифицированной DLL и двух встроенных модулей. Оба модуля – многофункциональные бэкдоры, которые вместе собирают как можно больше информации об инфицированной цели.

Первый, меньший модуль RC2FM, содержит бэкдор, предназначенный для внесения различных изменений в систему и выполнения нескольких шпионских команд. В частности, модуль способен дистанционно активировать

микрофон на инфицированном компьютере и записывать звук по запросу злоумышленников. Также вредоносная программа может делать снимки экрана и отслеживать все фиксированные и переменные диски в локальной системе.

Второй модуль RC2CL также бэкдор с широкими возможностями шпионажа. В частности, вредоносная программа может проверять инфицированный компьютер и предоставлять различные данные – от системной информации, такой как список активных процессов, запущенных служб, загруженных драйверов или доступных дисков, до информации о сети.

Вредоносная программа также может дистанционно активировать веб-камеру и микрофон жертвы и шпионить за жертвой путем съемки и звукозаписи. Деятельность экрана контролируется с помощью снимков экрана не только всего дисплея, но и каждого окна по отдельности.

Кроме этого, вредоносное программное обеспечение InvisiMole способно сканировать доступные беспроводные сети в инфицированной системе, записывая такую информацию, как идентификатор службы и MAC-адрес видимых точек доступа Wi-Fi. Затем эти данные могут быть объединены с публичными базами данных, позволяя преступникам отслеживать географическое положение жертвы.

Другие команды могут предоставлять информацию о пользователях инфицированного компьютера, информацию об их учетных записях и предыдущие сеансы.

Итак, угроза InvisiMole представляет собой хорошо оснащенное шпионское программное обеспечение, возможности которого могут конкурировать с другими шпионскими инструментами в реальной среде. Вредоносная программа использует только несколько методов, чтобы избежать обнаружения и анализа, однако, благодаря развертыванию на очень малое количество высоко профильных целей, она оставалась не выявленной не менее пяти лет.

(вгору)

Додаток 15

11.06.2018

Прослушка по сигналу: зачем смартфоны шпионят за нами

Смартфоны прослушивают своих владельцев, и это легко проверить – к такому выводу пришел австралийский исследователь, который утверждает, что запись разговоров передается в социальные сети, использующие эти данные для контекстной рекламы. Мы выяснили, как узнать, что за вами следят, и что нужно делать, чтобы минимизировать этот риск (InternetUA).

Пользователи гаджетов и интернета все чаще жалуются на то, что многие называют либо мистикой, либо паранойей – контекстная реклама онлайн как будто читает мысли. Стоит в реальной жизни обсудить какую-либо проблему с близким человеком, как в жизни виртуальной рекламодатели уже предлагают доступное решение по привлекательной цене. Возникает вопрос, которым в том

числе задаются конгрессмены в США и мировая пресса: может ли смартфон каким-то образом подслушивать и записывать бытовые разговоры?

В ожидании сигнала

Эксперт по кибербезопасности и бывший лектор Университета Эдит Коуэн доктор Питер Ханнэй полагает, что так оно и есть. В своем исследовании он описывает некие слова-триггеры, которые могут «пробудить» телефон по аналогии с фразами «окей, Google» или «привет, Siri». Как только гаджет фиксирует такой аудио-триггер, он записывает фрагмент разговора, а потом отправляет его тем приложениям, которые установлены на смартфон, например, Facebook или Instagram.

«Периодически аудиофрагменты ваших разговоров отправляются на серверы других компаний, но пока нет точного понимания, на какие именно триггеры реагирует смартфон», – заявил Ханнэй.

Он добавил, что приложения, принадлежащие этим компаниям, выпрашивают у пользователя разрешение на использование микрофона и периодически его включают. То аудио, которое пересылается третьим лицам, находится в зашифрованном виде, поэтому список слов-триггеров до сих пор не установлен.

Исследователь допускает, что у Facebook или Instagram могут быть тысячи триггеров, а рядовой разговор с другом о покупке новых джинсов может вызвать целый шквал рекламных объявлений о продаже изделий из денима в этих приложениях.

Facebook опровергает любые инсинуации о неправомерном использовании микрофона. В официальном блоге компании есть отдельная запись, в которой сообщается, что компания не использует микрофоны для таргетирования рекламы.

«В прессе появляются сообщения о том, что мы слушаем разговоры людей, чтобы потом показывать им релевантные объявления. Это не так», – утверждается в публикации.

Об этом говорил и глава Facebook Марк Цукерберг на слушаниях в конгрессе США. Один из политиков задал вопрос, имеет ли социальная сеть отношение к загадочным случаям, когда друзья между собой устно обсуждают какую-то тему, а потом заходят в Facebook и видят соответствующую рекламу.

«Facebook этим не занимается, и не знаю, кто еще мог бы такое сделать. Возможно, это просто совпадение», – ответил Цукерберг.

Американский журналист портала Vice Сэм Николс решил проверить это заявление и устроил собственный эксперимент. В течение пяти дней он произносил вслух фразы, которые могли бы быть потенциальными триггерами – «я хочу вернуться в университет» и «мне нужны дешевые рубашки для работы».

Затем Николс проверил свою ленту в Facebook на предмет рекламных публикаций. Результат не заставил себя ждать – там появились объявления с разными учебными курсами, а также бренды, предлагающие одежду по бюджетным ценам. Также Николс пообщался со своим другом, рассказав ему о

нехватке места на жестком диске, после чего в ленте неожиданно возникло выгодное предложение о покупке новой флеш-карты.

Конечно, для рекламодателей имеет смысл записывать аудио, поскольку информация, полученная от прослушивания в разговорах, позволит им лучше таргетировать рекламу, рассказал старший инженер-программист Avast Войтех Бочек.

Тем не менее, это является серьезным нарушением конфиденциальности, поскольку частные разговоры передаются третьей стороне без ведома пользователя.

«Пока мы сталкивались только с отдельными случаями, которые не подтверждены каким-либо техническим анализом приложения Facebook и других мобильных приложений. Например, если пользователь использует Android, он может достаточно легко определить, что какое-то приложение записывает аудио: батарея будет садиться быстрее, а на смартфоне с ОС Android 8.0 или выше появится уведомление о работе фонового сервиса. Чтобы быть абсолютно уверенными, что никто не слушает ваши личные разговоры, нужно отключить все мобильные и смарт-устройства вокруг», – посоветовал эксперт.

Соцсети знают наперед

Сайт «Би-би-си» также проявил скепсис к заявлению Facebook, которая отрицает любую причастность к загадочной контекстной рекламе, и попросил читателей рассказать свои истории, когда последствия разговора в жизни настигали героев онлайн.

Американец по имени Нейт сообщил, что он и его невеста решили спонтанно пожениться, купили кольцо в магазине, а уже на следующее утро в социальных сетях появилась тематическая «свадебная» реклама. Нейт уточнил, что они так и не успели никому рассказать о свадьбе, но интернет как будто бы знал о ней заранее.

Линдси из Линкольна рассказала о том, как бросила свою работу и решила обсудить с другом, куда ей двигаться дальше.

Она предположила, что можно устроиться на работу в кофейню, чтобы пить бесплатный кофе, и спустя несколько часов в ленте Facebook появилось объявление о том, что популярная сеть кофеен неподалеку ищет новых сотрудников.

Мужчина по имени Майкл заявил, что начал видеть большое количество рекламы на испанском сразу после того, как начал учить этот язык. С одной стороны, это даже помогло ему в обучении, но ощущение слежки «было весьма пугающим».

По словам эксперта по информационной безопасности КРОК Анастасии Федоровой, в современном мире часто случаются ситуации, когда для продвижения товаров и услуг используются механизмы негласного сбора информации. Однако зачастую производители «умных» устройств предлагают меры по борьбе с подобными действиями: в настройках устройств мы можем

запретить или разрешить доступ к микрофону, контактам, камере или геолокации.

Эксперт добавила, что механизмы поиска контекстной рекламы срабатывают и по безобидным действиям пользователей, например, «лайкам» в социальных сетях, запросам в поисковых системах, ответам на тесты в развлекательных сайтах и т. п.

«На текущий момент пользователю необходимо быть более внимательным к своим данным, максимально использовать настройки приватности «умных» устройств, а также соблюдать правила безопасности при работе в сети. Это значительно минимизирует риски по распространению личной информации», – порекомендовала собеседница «Газеты.Ru».

(вгору)

Додаток 16

13.06.2018

Украинский хакер «положил» охранную систему нескольких предприятий

Сотрудники Приднепровского управления киберполиции разоблачили хакера, который совершал несанкционированное вмешательство в работу компьютерных систем охраны, функционирующих на частных предприятиях Запорожья и Мариуполя. Об этом говорится на официальном сайте Национальной полиции Украине (InternetUA).

Преступником оказался 29-летний житель Мариуполя. Злоумышленник владел техническими знаниями, а также имел навыки программирования.

Сообщается, что хакер с помощью вредоносного программного обеспечения осуществлял целенаправленное незаконное вмешательство (DDOS-атаку) на маршрутизаторы частных предприятий. Он воспользовался уязвимостью функционала роутеров и атаковал открытые порты.

Совершая большую нагрузку на роутер, злоумышленник блокировал доступ оборудования предприятий к интернету и не позволял управлять удаленными устройствами около 3 тысяч абонентов компаний.

Таким образом, информация к центральному пульту охраны от оборудования абонентов в момент совершения атаки не поступала. В результате частные предприятия теряли своих клиентов, потому как не могли реагировать на оставленные сигналы о помощи.

Сотрудники киберполиции Запорожской и Донецкой областей совместно со следователями полиции Запорожской области выяснили, что хакер совершал DDOS-атаки из квартиры в Мариуполе, в которой он временно проживал.

По результатам обыска, проведенного правоохранителями в квартире преступника, было изъято несколько ноутбуков, флэш-накопителей и мобильный телефон.

Полиция начала уголовное производство по ч.1 ст.361 (Несанкционированное вмешательство в работу компьютеров,

автоматизированных систем, компьютерных сетей или сетей электросвязи) УК Украины. В настоящее время устанавливаются убытки, причиненные предприятиями в результате кибератак.

(вгору)

Додаток 17

13.06.2018

Facebook записывает движение ваших губ и многую другую информацию

В ответ на запрос Конгресса США после апрельского скандала с Cambridge Analytica, компания Facebook раскрыла все свои способы сбора информации о пользователях социальной сети. Для этого потребовалось составить документ из 222 страниц. Он описывает разные способы сбора данных, от тех, о которых мы догадывались, до тех, о которых мы даже не подозревали (IGate).

Разумеется, вы могли подозревать, что компания Facebook следит за тем, сколько времени вы проводите на страницах социальной сети. Она следит за покупками, которые вы совершаете. Ниже представлены действительно удивительные вещи из документа компании.

- Facebook записывает движение ваших губ. Это помогает компании убедиться в том, что вы не робот.
- Еще один способ, который помогает компании Facebook убедиться в том, что вы человек, – это распознавание того, находится ли окно браузера поверх других окон или же за ними.
- Facebook собирает информацию о ваших устройствах. Но это не только информация о модели устройства и версии операционной системы. Компании интересно знать уровень заряда вашей батареи, уровень сигнала сотовой сети и объем доступной памяти.
- Разумеется, собирается информация не только об операционной системе, но и о браузере, установленных плагинах и даже названиях файлов.
- Еще компании известна информация о вашем сотовом операторе, интернет-провайдере, IP-адресах, cookie, часовом поясе и скорости соединения.
- В некоторых случаях компания собирает информацию не только о вашем устройстве, но и о тех устройствах, что находятся в одной сети или поблизости.
- Facebook известны доступные вашему устройству Bluetooth-устройства, точки доступа Wi-Fi и сотовые вышки, которые находятся в радиусе приема.
- Помимо информации с GPS, камеры и галереи фото, на Android Facebook может получать список вызовов и историю SMS.
- Наконец, компания Facebook знает о приложениях, которые вы используете, и учетных записях.

(вгору)

Додаток 18

18.06.2018

Найден баг PGP, уже 20 лет позволявший подделывать цифровые подписи

Цифровые подписи используются для аутентификации источника зашифрованного сообщения, программного обновления или резервной копии. Обычно они защищены частным ключом, однако серия уязвимостей в популярных инструментах шифрования электронной почты позволяет в ряде случаев подделывать подпись с помощью публичного ключа или Key ID, которые часто публикуются в открытой сети (Компьютерное Обозрение).

Уязвимость в GnuPGP, названная SigSpoof или CVE-2018-12020, по утверждению открывшего её Маркуса Бринкманна (Marcus Brinkmann) «глубоко укоренилась в нашей базовой инфраструктуре и может влиять на её большую часть». Конфиденциальные сообщения e-mail, на которые десятилетиями полагались многие люди, занятые в критических для экономики и безопасности отраслях, как оказалось, могли быть подделкой.

Проблемы не ограничиваются электронной почтой, под вопросом оказалась аутентичность большинства прошлых обновлений ПО, резервных копий и исходного кода в системах версионного контроля, таких как Git.

Баг CVE-2018-12020 делает возможной подделку, только если в установках уязвимого ПО задан многословный режим (verbose), используемый в отладочных целях. По умолчанию он отключен, однако в ряде рекомендуемых конфигураций, доступных онлайн, (например, cooperpair safe defaults, Ultimate GPG и Ben’s IT-Kommentare) этот режим активирован. Для этого, последнего случая, в сообщении Бринкманна описываются три концептуальных варианта спуфинговых атак, которые работают для GnuPG, Enigmail, GPGTools, python-gnupg, и, возможно, для многих других инструментов безопасности.

Всё упомянутые утилиты уже получили патч, закрывающий самую критическую уязвимость, а для Enigmail и Simple Password Store также подготовлены исправления двух связанных спуфинговых ошибок CVE-2018-12019 и CVE-2018-12356.

Бринкманн сообщил, что проблема прослеживается до версии GnuPG 0.2.2, датируемой 1998 годом.

Информация об этих трёх багах, выложенная Бринкманном в прошлую среду (после выхода патчей), углубляет кризис доверия к технологиям защиты конфиденциальности электронной переписки. Месяц назад исследователи обнародовали другой пакет уязвимостей (Efail), позволявших хакерам читать сообщения e-mail, зашифрованные с помощью PGP или S/MIME.

(вгору)

18.06.2018

Все сети 4G уязвимы для атак, которые приводят к отказу в обслуживании абонентов

Согласно отчету Positive Technologies, используя недостатки протокола Diameter, злоумышленник может лишить абонентов основных преимуществ 4G – высокой скорости и качества связи. Уязвимости протокола Diameter могут привести к блокировке работы банкоматов, POS-терминалов, приборов учета ЖКХ, автосигнализаций, а также систем видеонаблюдения. Если абонент является системой диагностики на магистральном газопроводе или GSM-контроллером утечки бытового газа, отсутствие связи может привести не только к прямому денежному ущербу, но и к опасным авариям (Компьютерное Обозрение).

Мобильные сети 4G с каждым годом получают все более широкое распространение. При этом пользователи ожидают от оператора, которому они доверяют, высокого качества связи и надежной защиты данных. Однако в протоколе Diameter, применяемом в сетях 4G для передачи служебных сообщений, эксперты Positive Technologies обнаружили ряд уязвимостей.

Например, злоумышленник может зарегистрировать абонента в несуществующей сети – и полностью оставить его без связи. Кроме того, уязвимости позволяют атакующему реализовать массовый отказ в обслуживании, что чревато серьезными финансовыми и репутационными потерями для мобильного оператора, так как сразу тысячи пользователей могут быть отключены на длительное время (до перезагрузки устройства или перехода в зону действия другого узла управления мобильностью).

Риску мошенничества в отношении оператора подвержена каждая третья сеть 4G. Киберпреступники могут пользоваться мобильной связью бесплатно и продавать подобные услуги третьим лицам. Под угрозой и приватность: все сети четвертого поколения позволяют отследить местоположение абонентов.

«В 2017 году мы уже показывали, что в сетях 4G можно реализовывать атаки, связанные с определением местоположения абонента, отказом в обслуживании и другими нелегитимными действиями. Однако пока операторы принимают лишь минимальные меры защиты в отношении уязвимостей протокола Diameter, – отмечает руководитель группы исследований безопасности телекоммуникационных систем Positive Technologies Павел Новиков. – А если посмотреть на инфраструктуру предыдущих поколений, то картина еще печальней. Злоумышленник может принудительно перевести устройство абонента в режим 3G – и проводить атаки на менее защищенную систему SS7, где прослушивать голосовые вызовы или перехватывать SMS гораздо проще. Напомню, что в сетях 2G и 3G в процессе исследования их безопасности нам удалось перехватить 9 из 10 SMS».

Большинство выявленных недостатков были связаны не только с некорректной настройкой или уязвимостями сетевого оборудования, но также с

фундаментальными проблемами протокола Diameter, для решения которых требуются дополнительные средства защиты. Эксперты Positive Technologies подчеркивают необходимость комплексного подхода к безопасности.

В исследовании Positive Technologies участвовали операторы связи стран Европы и Азии. Большую часть (80 %) составили крупные телекоммуникационные компании с объемом абонентской базы более 40 миллионов человек.

(вгору)

Додаток 20

20.06.2018

Викрито хакера, який зламував облікові записи користувачів соцмереж

Працівники Карпатського управління Департаменту кіберполіції Національної поліції України, за процесуального керівництва Львівської місцевої прокуратури №1, виявили факти несанкціонованого втручання в роботу облікових записів соціальних мереж та розповсюдження шкідливого програмного забезпечення (InternetUA).

Слідчі поліції Львівщини за даним фактом розпочали кримінальне провадження за ч. 2 ст. 361 (Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку) КК України.

Поліцейські встановили, що житель Львівської області, володіючи необхідними навичками у сфері програмування, створив Інтернет сайт xakercki-poslygu[.]hol.es. На цьому сайті зловмисник пропонував свої послуги щодо зламу облікових записів, електронних скриньок тощо. Усі листування між ним та клієнтами відбувалося за допомогою закритої спільноти, яку адміністрував зловмисник у цій же соціальній мережі. Під час спілкування з клієнтами він також надсилав їм посилання на, нібито, форму зворотнього зв’язку. Натомість – користувачі потрапляли на фішингову сторінку, за допомогою якої відбувалася компрометація логінів та паролів користувачів соціальної мережі.

Надалі, зловмисник перевіряв отримані дані авторизації по всіх соціальних мережах та популярних веб-ресурсах. Отримавши доступ до облікових записів, блокував власникам до них доступ, шляхом зміни паролю. За повернення доступу хакер вимагав гроші. Суми, які він запрошував, коливалися в залежності від платоспроможності жертви.

Крім цього, у цій же спільноті, під виглядом додатку для злому соціальних мереж, зловмисник розмістив для вільного завантаження шкідливе програмне забезпечення. Воно призначалося для несанкціонованого втручання в роботу мобільних телефонів з операційною системою «Android», у результаті чого хакер мав змогу переглядати телефонну книжку, фотографії та записи вхідних та вихідних викликів жертви.

За адресою фактичного місця проживання зловмисника поліцейські провели санкціонований обшук. За результатами, вилучено комп'ютерну техніку, яку він використовував для зайняття протиправною діяльність, а також мобільний телефон та додаткові носії інформації.

Наразі чоловіку вже оголошено про підозру у вчиненні кримінальних правопорушень, передбачених ч. 2 ст. 361 КК України та одному факту за ч.1 ст. 361-1 (Створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут) КК України.

Наразі йому вже оголошено про підозру у вчиненні більше двох десятків злочинів. Справу скеровано до суду.

(вгору)

Додаток 21

20.06.2018

Михаил Сапитон

Хакеры, саботировавшие Олимпиаду-2018, вернулись. В списке целей есть и Украина

Вредоносный червь Olympic Destroyer, с помощью которого саботировали проведение зимней Олимпиады в Пхёнчхане, вернулся за новыми жертвами, пишет издание ArsTechica со ссылкой на экспертов Kaspersky Lab. Тогда группа хакеров «положила» сайт спортивного мероприятия, воспрепятствовали получению билетов, отключила Wi-Fi. На этот раз та же группа нацелена на другие объекты — организации, которые реагируют на биологические и химические атаки, финансовые учреждения (AIN.UA).

Пока что в Kaspersky не зафиксировали каких-то разрушительных последствий. Но стоящие за Olympic Destroyer взломщики получили доступ к компьютерам во Франции, Германии, Швейцарии, России и Украине. На один и тот же источник угрозы, сообщают исследователи, указывает схожесть методик. Одна из самых популярных – рассылка email-писем на аффилированные с организацией адреса. К сообщениям прикрепляются файлы с безобидным названием вроде Korporativ и Korporativ_2018. Открыв их, на компьютере жертвы начинается исполнение вредоносного кода.

Один из фальшивых Word-файлов напоминает поддельный пресс-релиз и содержит отсылки к конференции Spiez Convergence – международной экспертной встрече по вопросам биохимических угроз. Организатором мероприятия выступает компания Spiez Laboratory, сыгравшая главную роль в расследовании отравления бывшего российского шпиона Сергея Скрипаля и его дочери Юлии. Второй документ предназначался для органов здравоохранения и ветеринарного контроля Украины.

В Kaspersky прямо не указывают страну, стоящую за подготовкой новой атаки, но указывают на сходство с группой Sofacy, которую подозревают в

работе на российское правительство. Одно из доказательств такой связи – язык написания документов, которые распространялись в Украине. Они составлены на идеальном русском, явно не благодаря машинному переводу. Sofacy также известна под именем Fancy Bear и подозревается в ряде политически мотивированных атак по всему миру. Среди них – взлом серверов Демпартии США, атака на Олимпийский комитет и немецкий Бундестаг.

То, что в числе пострадавших есть и финансовые организации из России, в Kaspersky объяснили двумя предположениями. Это могут быть соперничающие между собой группы с разными интересами, использующие одни и те же приемы. Или же таким образом злоумышленники отвлекают внимание исследователей. В атаке на Олимпиаду они провернули подобное, как писалиисследователи Cisco, оставив поддельные зацепки на происхождение вредоносного кода из Северной Кореи.

Лаборатория рекомендует организациям, занимающимся исследованием биологических и химических угроз, временно установить повышенные меры контроля за безопасностью.

(вгору)

Соціальні мережі

як чинник інформаційної безпеки

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

Упорядник **Терещенко** Ірина Юріївна

Свідоцтво про державну реєстрацію КВ № 5358 від 03.08.2001 р.

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