СОЦІАЛЬНІ МЕРЕЖІ ЯК ЧИННИК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Огляд інтернет-ресурсів
(14.02–27.02)

2018 № 4

Соціальні мережі
як чинник інформаційної безпеки

Інформаційно-аналітичний бюлетень
Додаток до журналу «Україна: події, факти, коментарі»
Огляд інтернет-ресурсів
(14.02–27.02)
№ 4

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

15.02.2018
Ольга Мінченко
Три з восьми найпопулярніших вебсайтів, якими українці користуються щодня – російські

Одразу три російських вебсайти – «Вконтакте», «Одноклассники» та «Яндекс» – потрапили до рейтингу найпопулярніших вебсайтів, якими користуються українці, за середньою денною аудиторією. Про це свідчать дані щомісячного дослідження інтернет-аудиторії компанії Factum Group (Watcher).

При цьому за місячним охопленням (якщо користувач хоча б раз на місяць заходив на вебсайт), російські сервіси перебувають значно нижче. Найвища позиція у «Вконтакте» – 9 місце. Це свідчить про те, що аудиторія російських сервісів є доволі активною, але вузькою.

***

15.02.2018
Google випустить чатбот, який відповідатиме за вас в месенджерах

Система Reply буде пропонувати кілька варіантів відповідей на стандартні запитання, щоб ви не витрачали час на їх набір. Окрім того, чатбот зможе автоматично відповідати: «Я за кермом», щоб не відволікати вас під час поїздок, і навіть розраховувати приблизний час у дорозі, орієнтуючись по геолокації телефону.

Докладніше

***

17.02.2018
Facebook выпустил Messenger Kids для Android

Приложение Facebook Messenger Kids стало доступно на Android. Оно предназначено для детей в возрасте от 6 до 12 лет (InternetUA).

В приложении отсутствуют внутренние покупки, а также есть специальные функции, чтобы родители могли больше контролировать любые сообщения.

Facebook также добавил подходящие для детей наклейки, GIF, фреймы и эмодзи, чтобы помочь детям «творчески выразить себя». Есть также индивидуальные видеозвонки с интерактивными масками AR.

В отличие от обычного приложения Messenger, версия для детей не запрашивает номер телефона или не нуждается в учетной записи Facebook. Родители и взрослые могут использовать свои профили, чтобы проверить

учетную запись Kids, а также проверить, что происходит через обычный Messenger.

Дети могут блокировать контакты и сообщать о неприемлемом контенте в приложении. Когда они это сделают, родитель будут об этом уведомлены.

***

17.02.2018

Twitter прекращает поддержку приложения для Mac

Многие годы пользователи macOS активно сидели в Twitter через одноимённое приложение. Кажется, этому настал конец (InternetUA).

Компания фокусируется на работе с разными платформами, поэтому пользователи macOS будут вынуждены использовать Twitter в веб-браузерах.

Полноценная работа с Twitter на Mac теперь возможна только в браузере.

Жалко, что компания пришла к такому решению. Twitter для Mac гораздо удобнее браузерной версии. Как минимум, потому что в ней автоматически обновляется лента и есть поддержка нескольких учетных записей.

***

17.02.2018

Facebook использует номера телефонов пользователей для рассылки спама

Пользователи Facebook, настроившие двухфакторную аутентификацию с помощью номера мобильного телефона, начали получать регулярные SMS-оповещения обо всех действиях с учетной записью. Руководство социальной сети не предоставило очевидной возможности отказаться от рассылки, чем спровоцировала целую бурю негатива (InternetUA).

«Когда я настроил двухфакторную аутентификацию на Facebook, они воспользовались этим, чтобы слать мне спам-уведомления, – негодует пользователь Гэбриэл Льюис. – [Всякий раз, когда я пытался ответить на оповещения], они отправляли мои же сообщения на мою стену».

В своем негодовании Льюиса поддержала масса пользователей, среди которых оказались весьма именитые люди. Об очевидно негативном влиянии действий Facebook написал известный социолог Зейнеп Туфекки. По его словам, то, что себе позволяет руководство социальной сети, абсолютно недопустимо и с точки зрения права, и морали.

Представители Facebook поспешили оправдать свои действия, ответив, что, оповещая пользователей обо всех действиях с учетными записями, всего лишь обеспечивают их безопасность. «Мы изучаем эту ситуацию, чтобы убедиться, что мы можем позволить пользователям управлять входящими уведомлениями», – подвели итог в Facebook.

***

19.02.2018
Skype выпустят в версии Professional

Несколько месяцев назад в Сеть просочилась информация о скором появлении профессиональных аккаунтов Skype (iLenta.com).

Теперь же новая утечка продемонстрировала установщики новой версии мессенджера Skype Professional, основная часть функций которого будет предназначаться для бизнес-клиентов.

Среди возможностей мессенджера будут подробная статистика звонков и платежей, запланированные в ближайшие дни мероприятия и много других опций.

Известно также и то, что новое профессиональное приложение будет функционировать на той же платформе, на которой работает новый десктопный клиент Skype для Windows 7/8.

***

20.02.2018
Разработчики Snapchat повторили фатальную ошибку Instagram

После смены дизайна приложения более 1 миллиона человек подписали ходатайство Change.org с требованием, чтобы Snapchat отменил новое оформление.

Докладніше

***

21.02.2018
У Facebook з'являться 3D-пости

Користувачі соцмережі Facebook тепер зможуть публікувати 3D-об'єкти в своїй стрічці новин (Економічна правда).

Про це йдеться в прес-релізі компанії, передає Liga.Net.

«Ми недавно впровадили 3D-пости, які дозволять людям бачити цифровий об'єкт з усіх боків і взаємодіяти з ним в стрічці новин Facebook», – йдеться в повідомленні.

«Він миттєво відгукується на гортання і дотик і дозволяє контенту "вискакувати" з екрану», – повідомляє компанія.

Об'єкт можна буде крутити, утримуючи лівою кнопкою миші або пальцями.

3D-пости підтримують відображення текстур, налаштувань освітлення і рендер.

***

27.02.2018

Обновления YouTube Live: автоматические титры, повтор live-чата и геотеги

26 февраля в YouTube анонсировали новые функции для улучшения live-трансляций как для блогеров, так и для зрителей. Одна из них – это возможность воспроизведения живого чата после окончания live-трансляции.

Докладніше

***

27.02.2018

Facebook анонсировал обновления Messenger для бизнеса

Компания добавила контактную информацию в быстрые ответы, расширила возможности плагина Customer Chat и улучшила пользовательские настройки (Marketing Media Review).

Быстрые ответы были доступны в Messenger с 2016 года, но обновление дает компаниям возможность получать контактную информацию через одну из кнопок быстрых ответов. Когда компания запрашивает контактную информацию, у пользователя появляется кнопка быстрого ответа с адресом электронной почты или номером телефона, связанным с учетной записью Facebook. Если у пользователя более одного адреса или номера, можно выбрать, какой из них отправить. Бизнес также может настроить текст и цвет своего приветствия в Messenger через плагин Customer Chat. Также компания представила новый инструмент настройки, помогающий компаниям быстрее запускаться, новую систему уведомлений для клиентов и постоянное меню, которое может отображаться в Messenger. Facebook даже добавил поддержку Internet Explorer, так что клиенты, которые используют этот браузер, могут пользоваться этими функциями. Кроме того, теперь компании могут видеть, сколько новых или открытых разговоров существует между их страницей и пользователями Messenger. Facebook также добавил новые теги сообщений, которые помогают компаниям знать, как отвечать клиентам.

СОЦІАЛЬНІ МЕРЕЖІ ЯК ВИЯВ ФОРМУВАННЯ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА

14.02.2018

МІП: Верифіковано понад 20 сторінок державних інституцій у Facebook

13 лютого 2018 року, на запит Міністерства інформаційної політики України до Європейського офісу Facebook, було верифіковано понад 20

сторінок центральних органів виконавчої влади та понад 10 сторінок перших осіб державних інституцій.

Докладніше

***

18.02.2018

Одесский мститель: одесситы провели флешмоб в поддержку Анатолия Мазура

Одесские активисты провели в социальных сетях флешмоб, чтобы поддержать Анатолия Мазура, которого уже называют одесский мститель (Infoport).

16 февраля 2018 года, одессит, порубил топором 13 машин на стоянке у Соломенского районного суда города Киева. По предварительным данным, Анатолий Мазур порубил автомобили в знак протеста против того, что судьи отпустили подозреваемого в хищении огромной или даже «космической» суммы, мэра Одессы Геннадия Труханова на поруки прямо из зала суда.

Одесситы выложили в социальных сетях свои фото, на которых они держат в руках таблички со словами поддержки Анатолию Мазуру и сопутствующими хештегами #суддю_на_мыло и #труханова_в_тюрму.

***

22.02.2018

В Одессе запустили соцсеть для общения с депутатами

В Одессе запустили социальную сеть для общения с депутатами горсовета. Новая муниципальная онлайн-платформа «Твой депутат Одесского городского совета» (deputat.odessa.ua) позволяет горожанам напрямую обратиться к избранникам своего округа с проблемой, просьбой или предложением.

Докладніше

***

21.02.2018

Священик з Тернопільщини благословляє вірян у Instagram

Кожен охочий може приєднатись до прямої трансляції прочитання вечірньої або вранішньої молитви отця Василя у Instagram (Espreso.tv).

Про це йдеться на сторінці у Facebook Парафії УГКЦ селища Скала-Подільська.

Священик Скали-Подільської УГКЦ Василь Германюк по неділях та святах організовує пряму трансляцію молитов і благословення у Instagram.

«Якщо молода особа прокидається вранці і першим її кроком є відкриття Instagram, щоб глянути хто що там лайкнув і кинув новенького – я пропоную,

по совісті, духовну альтернативу - помолитись разом зі мною ранішню молитву у прямій трансляції і згодом в записі на 24 години», – розповідає отець Василь.

У Instagram священик веде сторінку під ніком @hvmnew, наразі у нього 519 читачів. У своїх постах Василь розповідає про життя парафії та ділиться дотепними картинками.

***

21.02.2018

Официальные Twitter-аккаунты Украины и России снова повздорили

Российский аккаунт посмеялся над скудной аудиторией на выступлении Петра Порошенко, а украинский – над численностью атлетов из России на Олимпиаде-2018(Телекритика).

Конфликт начался с сообщения Украины, в котором Россия осуждалась за «агрессию, троллей, фейковые новости и кибератаки». Администраторы аккаунта призвали обеспечить Украину экономической, военной и дипломатической поддержкой в преддверии Мюнхенской конференции по безопасности.

Официальный аккаунт России упрекнул Украину в распространении фейков, добавив, что «с каждым годом в них верят все “больше” людей», и продемонстрировал снимок полупустого зала во время выступления Петра Порошенко на конференции.

Украина в свою очередь ответила, что в зале находится больше человек, чем атлетов из России на Олимпиаде в Пхенчхане.

Позже к конфликту подключился официальный аккаунт посольства России в Канаде.

***

23.02.2018

До акції «Врятувати Дністер …» долучилися українці з Нью-Йорка, Лондона, Парижу та Барселони

Українці організували флешмоб на підтримку Дністра та проти заборони будівництва на річці каскаду з 6 ГЕС (beztaby.te.ua).

Відтак, активісти розмістили у групі в Фейсбук «Врятуй Дністер від ГЕС» флешмоб #saveDnister_fromHPP. Щоб взяти участь у флешмобі, необхідно спершу приєднатися до групи Фейсбуку saveDnister_fromHPP, зробити фото з аркушем А4 з написом хештегу #saveDnister_fromHPP на фоні свого міста та виставити фото як пост у групі saveDnister_fromHPP на своїй сторінці, зазначивши назву міста та хештег.

23 лютого до Всеукраїнської акції порятунку Дністра долучилися активісти з Лондона, Парижу, Нью-Йорка та Барселони.

***

22.02.2018

Дякую, лікарю: закарпатці запустили у соціальних мережах новий флешмоб

У соціальній мережі Фейсбук, у популярній закарпатській групі «Порадьте, будь ласка», запустили цікавий флешмоб: люди активно дякують лікарям, які їх лікували (Закарпатський Кореспондент).

Відомо, що час від часу у цій групі з`являються пости з проханнями порадити того чи іншого лікаря. Нерідко тут можна прочитати і скарги незадоволених пацієнтів та навіть погрози лікарям. запустила у групі флешмоб:

«Запускаю флешмоб “СКАЖИ ДОКТОРУ СПАСИБО!” в ответ на посты людей, по поводу и без критикующих врачей. Если в Вашей жизни встречались доктора (один или несколько), которым Вы благодарны, не стесняйтесь сказать им прилюдное “СПАСИБО!”… ”, – написала учасниця групи Анни Кушнір.

За кілька хвилин до посту «посипався» шквал коментарів, люди почали писати прізвище лікарів, до яких зверталися і були задоволені допомогою спеціаліста. Звісно, знайшлися й ті, кому подібний флешмоб видався не дуже вдалою ідеєю. Однак більшість «мешканців» групи залишилися задоволеними.

***

27.02.2018

Івано-франківчанки просять владу збільшити кількість жіночих консультацій – соцмережі

У місті Івано-Франківськ замало жіночих консультацій, – переконані деякі користувачі соціальних мереж.

Так, користувачка Facebook Оксана Стефінів звернулася через спільноту Комуналка ІФ у соцмережі до міського голови обласного центру з проханням розглянути можливість створення додаткової жіночої консультації.

«Шановний м. Руслан Марцінків, звертаюся до вас з питанням від всіх жінок які є мамами чи планують ними бути. В нас в місті є лиш 3 жіночі консультації, місто росте розвивається. Зараз ви створили в парку кімнату матері і дитини. Чи можливий такий варіант щоб наприклад в приміщенні поліклініки №2 чи в обласній лікарні створити консультації», – зазначила О.Стефінів у своєму дописі.

***

27.02.2018

Суд оштрафував військового комісара Львівщини за публікацію у Facebook списків призовників

Військового комісара Львівської області Олександра Тіщенка оштрафували на 5,1 тис. грн за публікацію на Facebook понад 15 тис. прізвищ

осіб, які ухиляються від призову. В опублікованій 26 лютого постанові Личаківського райсуду Львова вказано, що публікація імен ухилянтів призвела до порушення прав призовників. Позов на Олександра Тіщенка подало регіональне представництво уповноваженого ВР з прав людини у Львівській області (InternetUA).

Сам Олександр Тіщенко на судове засідання двічі не з'явився, через що суддя вирішив розглядати справу без нього. Військового комісара Львівщини визнали винним у порушенні ч. 4 ст. 188-39 Кодексу України про адмінправопорушення (недодержання порядку захисту персональних даних), призначивши йому мінімальний штраф за цією статтею у 5,1 тис. грн.

Водночас львівський військкомат має ще час подати апеляцію на постанову Личаківського райсуду Львова.

БІЗНЕС І СОЦІАЛЬНІ МЕРЕЖІ

15.02.2018

Михаил Сапитон

В Google Chrome появился встроенный блокировщик рекламы. Как он будет работать?

С 15 февраля Google активировала в браузере Chrome на всех платформах встроенный блокировщик рекламы. Разработка призвана бороться с самыми назойливыми баннерами и остановить веб-мастеров от их использования.

Докладніше

***

16.02.2018

Facebook планирует выпустить две сенсорные «умные» колонки // Выход устройств запланирован на июль

Компания Facebook намерена выйти на рынок сенсорных «умных» колонок, выпустив в июле этого года два устройства под кодовыми названиями Aloha и Fiona, сообщает Digitimes (Зеркало недели. Украина).

Отмечается, что обе колонки будут оснащены 15-дюймовыми сенсорными дисплеями и «позволят друзьям и семье оставаться на связи, используя видео-чат и разнообразные социальные функции».

Модель Aloha, которая, вероятно, выйдет в продажу под официальным названием Portal, будет более сложной, чем Fiona. Она будет использовать голосовые команды, а также распознавать лица, чтобы идентифицировать пользователей для доступа к Facebook через широкоугольный объектив на передней панели устройства.

Предполагается, что Portal будет предоставлять доступ к базе медиаконтента. Facebook уже заключила соглашения с Sony и Universal Music об использовании контента в устройстве.

***

19.02.2018

Facebook ужесточит для РФ правила размещения рекламы

Facebook введет дополнительные тесты для покупателей рекламы, из-за опасений, что Россия с помощью фейковых и оплаченных новостей будет вмешиваться в процесс выборов в конгресс США в 2018 году (U-News).

Пользователям, которые захотят разместить рекламный пост с именами кандидатов выборов в конгресс США, потребуется пройти дополнительный тест – ввести с изображения автоматически генерируемый пароль, чтобы продолжить покупку рекламы, сообщает Associated Press.

Представители Facebook считают, что таким образом они смогут обезопасить социальную сеть от ботов, которые публикуют рекламные посты. Дополнительную проверку введут во время промежуточных выборов, в ноябре 2018 года.

***

21.02.2018

ИИ-решение Avaya Ava поможет при взаимодействии с клиентами через соцсети и месенджеры

Avaya представила новое решение для внедрения технологий искусственного интеллекта в контакт-центры. Avaya Ava – архитектура на основе ИИ, включающая в себя технологии естественного языкового взаимодействия, машинного обучения и аналитики, обеспечивает простоту взаимодействия с клиентами через социальные сети и платформы обмена сообщениями.

Докладніше

***

24.02.2018

Samsung может представить новую социальную сеть «Uhssup» вместе с Galaxy S9

В прошлом месяце выяснилось, что южнокорейский гигант Samsung подал заявку на товарный знак социальной сети под названием «Uhssup» (iLenta.com).

Новый отчет предполагает, что она может быть представлена в конце недели вместе с Galaxy S9 на Mobile World Congress 2018.

В докладе также говорится, что «Uhssup» – это социальная сеть, разработанная Samsung, которая позволит пользователям делиться своим местоположением в режиме реального времени, а также комментировать

местоположения других пользователей. Ожидается, что служба также предложит возможности обмена сообщениями.

В то время как компания зарегистрировала название «Uhssup» в ведомстве интеллектуальной собственности Европейского союза, в новом докладе говорится, что она также зарегистрировала «Samsung Social» на внутреннем корейском рынке.

***

24.02.2018

Facebook заключила сделку с правообладателями на 31 млн песен

В чём главное отличие Facebook от «ВКонтакте»? В созданной Марком Цукербергом социальной сети нет собственного музыкального сервиса. В ближайшее время это может измениться, потому что Facebook заключила соглашение с группой ICE Services, в базе которой насчитывается более 31 млн музыкальных произведений. Через ICE обладатели авторских прав будут получать роялти за прослушивание песен в Facebook и Instagram, а также при использовании сервисов Oculus и Messenger (InternetUA).

В ближайшем будущем договор обеспечит Facebook свободное использование музыки внутри видеороликов и других видов контента. О том, запустит ли Facebook собственный музыкальный сервис по типу Spotify пока достоверно ничего неизвестно. Недавно появились слухи, что соцсеть разрабатывает собственные смарт-динамики, которые выйдут в середине года.

Ни Facebook, ни ICE не раскрывают финансовые детали сделки.

***

27.02.2018

Глава CNN взволновался из-за могущества Facebook и Google

Глава CNN Джефф Цукер призвал власти уделить внимание Facebook и Google, так как поставщикам новостного контента все сложнее адаптироваться к современному цифровому окружению, сообщает Variety (InternetUA).

«Мне кажется, нам нужна помощь в мире рекламы и в мире технологий, чтобы найти новые способы монетизации цифрового контента, иначе хорошая журналистика исчезнет», – сказал Цукер.

По его словам, особое внимание на компании должны обратить регуляторами, так как Facebook и Google являются «монополиями».

***

27.02.2018

Майя Яровая

Facebook стал второй площадкой по видеорекламе в уанете: топ-3 рекламодателей по охватам

Видеореклама в Украине ежемесячно охватывает около 80 % всей интернет-аудитории в возрасте от 14 до 69 лет на ПК, и Facebook сейчас занимает вторую позицию по количеству показов рекламных роликов (4 % всех показов видеорекламы в месяц). Об этом свидетельствую данные исследовательской компании Gemius за январь 2018 года. Площадкой номер один в Украине остается YouTube – 47 % всех видеопоказов.

Докладніше

СОЦІАЛЬНІ МЕРЕЖІ І ПРОБЛЕМИ СУСПІЛЬНОЇ БЕЗПЕКИ

Інформаційно-психологічний вплив мережевого спілкування на особистість

25.02.2018

Как влияют социальные сети на успеваемость школьников

В журнале Educational Psychology Review были опубликованы результаты исследования относительно влияния социальных сетей на оценки школьников. Для этого был проведён метаанализ 59 научных работ о взаимосвязи социальных медиа и учебы подростков. В исследованиях приняли участие 29 337 человек.

Докладніше

***

26.02.2018

Исследование Motorola Mobility: гаджеты – лучшие друзья поколения Z

Более половины молодых людей, родившихся после 1995 года, считают свои гаджеты лучшими друзьями. Об этом говорят результаты исследования Motorola Mobility про соблюдение баланса между обыденной и цифровой жизнью людей разного возраста, представленные в рамках Mobile World Congress 2018.

Докладніше

***

27.02.2018

68 % американских родителей признали себя зависимыми от мобильных устройств

Еще одно исследование, которое в очередной раз доказало высокую степень зависимости людей от смартфонов, было проведено компанией Survey Monkey, в опросе приняли участие 4201 жителя США. Главным условиям для участия в опросе являлось наличие детей (InternetUA).

47 % заявили, что считают свои детей зависимыми от мобильных устройств. 53 % не видят никакой проблемы в том, что дети пользуются смартфонами.

Около 75 % признали, что у их детей есть доступ к смартфонам или планшетам. 60 % подтвердили, что у их детей есть личные мобильные устройства. Только 24 % родителей заявили, что у их детей нет доступа к мобильному устройству, которое имеет выход в Сеть.

Родители признают, что именно они должны контролировать, какой именно контент потребляют дети, но лишь 40 % включают родительский контроль в YouTube. Из них 60 % считают, что YouTube хорошо справляется с ограничением показа различных роликов для детей. 36 % считают, что Google может делать эту работу еще лучше.

68 % опрошенных родителей признали, что они сами зависимы от мобильных устройств. 32 % заявили, что не могут жить без смартфонов и планшетов.

***

16.02.2018

Ученые доказали, что социальные сети не смогут заменить живое общение

Сотрудники Канзасского университета опровергли гипотезу о том, что Всемирная паутина через несколько десятков лет полностью изменит социальную картину мира.

Докладніше

Маніпулятивні технології

18.02.2018

Facebook увеличит штат по безопасности из-за вмешательства россиян в выборы США

Facebook вдвое увеличит штат безопасности после расследования США по вмешательству россиян в выборах (InternetUA). Об этом сообщает CNN.

«Мы направляем на это значительные средства, включая увеличение количества людей, которые работают в сфере безопасности, с 10 тыс. до 20 тыс. в этом году. Мы также продолжаем тесно взаимодействовать с ФБР, министерством национальной безопасности и другими компаниями, чтобы

разработать методы защиты страны и людей, которые пользуются нашей соцсетью», – сказал вице-президент Facebook Джоэл Каплан.

***

19. 02.2018
Ольга Карпенко
Как кремлевская фабрика троллей влияла на выборы в США: реклама, хештеги, фейки

16 февраля американское Министерство юстиции выдвинуло обвинения в сторону 13 российских граждан и трех компаний во вмешательстве в президентские выборы в стране в 2016 году, в пользу одного из кандидатов, Дональда Трампа.
Докладніше

***

20.02.2018
Facebook разоблачит интернет-троллей с помощью почтовых открыток

Компания Марка Цукерберга придумала, как бороться с незаконной политической агитацией в социальной сети. Владельцам аккаунтов, поддерживающим или критикующим определенных кандидатов на американских выборах, по обычной почте пришлют открытки с секретным кодом. Таким образом, Facebook надеется выяснить, кто из пропагандистов находится не на территории США, а, например, в России.
Докладніше

***

21.02.2018
Андрій Пилипенко
США всерйоз взялися за російські «фабрики тролів»

У США стикається коло навколо так званих «фабрик» інтернет-тролів у рамках розслідування втручання РФ в американські президентські вибори 2016 року. За даними американських спецслужб, за атаками на сервери Демократичної партії стояло Головне розвідувальне управління (ГРУ) Генштабу Збройних сил Росії.
Докладніше

***

23.02.2018
Twitter ужесточил правила для борьбы с ботами

Twitter объявил, что ужесточает правила пользования сервисом, чтобы бороться с ботами и пропагандой. Об этом говорится в блоге компании (InternetUA).

В частности, теперь пользователям будет запрещено одновременно публиковать одинаковые или «в значительной степени похожие» твиты с разных аккаунтов, а также одновременно лайкать и ретвитить с разных учетных записей. Такая возможность пропадет из приложения TweetDeck к 23 марта.

При этом в компании добавили, что такое ужесточение правил не касается чрезвычайных ситуаций и других социально значимых событий.

Такое решение Twitter связано с необходимостью уберечь обсуждение «критически важных тем» от вмешательства со стороны, объяснили в компании.

Спецслужби і технології «соціального контролю»

14.02.2018
Михаил Сапитон
СБУ разоблачила запорожских хакеров. Они планировали атаковать банки

В Запорожье СБУ совместно с полицией задержали группу хакеров, которые планировали похищать средства с банковских счетов, сообщается на сайте пресс-службы ведомства (AIN.UA).

Трое местных жителей собирались использовать специализированное ПО для взлома процессинга банков и заражения внутренних сетей. План заключался в том, чтобы получить данные к пользовательским счетам и выводить оттуда деньги. Однако атаки удалось зафиксировать, а также идентифицировать их источник. Названия потенциальных «жертв» не раскрываются – среди учреждений были и госбанки.

В доме подозреваемых был произведен обыск. Правоохранители обнаружили вредоносное ПО, накопители, международные банковские карты, документы и другие улики, подтверждающие связь с преступлением. Оборудование направлено на экспертизу, в то время как против хакеров открыли уголовное производство по ч. 1 ст. 361 УК. Им вменяют незаконное вмешательство в работу компьютеров, систем и компьютерных сетей. В случае подтверждения обвинений, им грозит штраф и лишение свободы.

***

14.02.2018
Хвиля кібератак з Росії може зачепити Україну, – Нацрозвідка США

Протягом наступного року російські спецслужби та урядові агентства можуть посилити підривну кіберактивність проти США, країн Заходу, а також безпосередньо проти України.

Докладніше

***

14.02.2018

Власти Китая разблокировали «ВКонтакте»

Власти Китая разблокировали «ВКонтакте». Об этом «Газете.Ru» сообщили в пресс-службе социальной сети (InternetUA).

Социальная сеть полностью доступна в стране, включая web и мобильные версии сайта и приложения для смартфонов.

***

15.02.2018

В России произошел масштабный сбой YouTube

В соцсетях появилось большое количество сообщений о неполадках в работе видеохостинга YouTube. Эту информацию подтверждают данные сервиса Downdetector (InternetUA).

Некоторые зрители пожаловались, что видео на YouTube не запускаются: после включения ролика пользователи видели лишь черный квадрат, картинка и звук не появлялись.

По данным Downdetector, проблемы в работе видеохостинга начались утром 14 февраля. При этом информация о сбоях продолжает поступать спустя сутки. Судя по карте, проблема затронула только пользователей из России.

Пользователи платформы предположили, что неполадки могут быть связаны с деятельностью Роскомнадзора. 12 февраля руководители надзорного ведомства пригрозили заблокировать видеохостинг, если администрация YouTube не удалит материалы, касающиеся конфликта «охотницы за олигархами» Насти Рыбки и бизнесмена Олега Дерипаски. Роскомнадзор обязал видеохостинг заблокировать расследование Фонда борьбы с коррупцией до 14 февраля, однако по состоянию на 15 февраля материалы находятся в открытом доступе.

***

14.02.2018

Американские спецслужбы испугались китайских смартфонов

Спецслужбы США не рекомендуют американцам пользоваться китайскими смартфонами Huawei и ZTE (Телекритика).

ФБР, ЦРУ, АНБ и Национальная разведка заявили, что китайские производители гаджетов работают на правительство КНР. Отмечается, что главы спецслужб опасаются кражи информации и скрытого шпионажа.

За неделю до заседания разведывательного комитета, на котором прозвучали эти заявления, республиканцы Том Коттон и Марк Рубио предложили Сенату запретить американским властям закупать телекоммуникационное оборудование у Huawei и ZTE. Они связали это с опасениями, что компании могут следить за госслужащими США. А глава комитета по разведке Ричард Берр полагает, что Китай пытается получить доступ к американским технологиям и интеллектуальной собственности как раз через телекоммуникационные компании.

В ответ на обвинения представитель Huawei сказал, что компания представляет не большую угрозу, чем любой другой поставщик технологий.

***

19.02.2018

Бельгийский суд запретил Facebook собирать данные пользователей

Бельгийский суд принял решение в длящемся с 2015 года споре между комиссией по защите частной информации и компанией Facebook. Социальной сети предписано прекратить сбор данных пользователей. В противном случае за каждый день нарушения Facebook придется платить 250 000 евро, вплоть до 100 млн евро в сумме (InternetUA).

По мнению суда, Facebook нарушает закон, отслеживая пользователей на других сайтах. Социальная сеть не уведомляет пользователей в достаточной степени о том, что собирает персональные данные, не уточняет, какие именно данные она собирает и как долго она их хранит. Более того, она даже не получает явное согласие пользователя на сбор и хранение данных.

Компании Facebook также предписано удалить все данные о бельгийских гражданах, включая тех, кто не является пользователем социальной сети Facebook.

Представитель Facebook выразил разочарование решением суда и пообещал, что компания подаст апелляцию.

***

19.02.2018

Швеция открыла охоту на онлайн-пиратов

Правительство Швеции решило строго наказывать онлайн-пиратов. Теперь шведским борцам за «копилефт» светит до шести лет тюрьмы (Телекритика).

Согласно этому предписанию, нарушение закона об авторском праве и о торговых марках может повлечь за собой тюремное заключение. Кроме того, у

нарушителей будет конфисковываться «нефизическая» собственность. Например, домены, с которых были совершены противоправные действия.

В докладе, представленном членом Совета юстиции Дагом Маттсоном, говорится, что по новым уголовным обозначениям онлайн-преступность будет разделяться на два уровня серьезности – грубый и нормальный.

«Лицо, признанное виновным в нарушении авторских прав или копировании товарного знака нормального уровня, может быть приговорено к штрафам или тюремному заключению на срок до двух лет, – отмечает правительство. – В случаях грубых преступлений лицо может быть осуждено и отправлено в тюрьму на срок не менее шести месяцев, но не более шести лет».

Предлагаемые законодательные поправки вступают в силу с 1 июля 2019 года.

***

21.02.2018

В России предложили блокировать пиратские сайты без суда

Министерство культуры РФ разработало законопроект, который будет осуществлять блокировку сайтов, содержащих нарушающий авторские и смежные права контент, без решения суда.

Докладніше

***

23.02.2018

Співробітники СБУ викрили у Чернігові адміністратора антиукраїнських груп в російських соціальних мережах

Правоохоронці встановили, що місцевий мешканець створив у соцмережах низку акаунтів, через які здійснював адміністрування та модерування антиукраїнських спільнот. За попередньою інформацією, до створених ним Інтернет-об’єднань входило понад двадцять тисяч учасників (InternetUA).

Оперативники спецслужби задокументували, що зловмисник розміщував на сторінках матеріали із закликами до повалення конституційного ладу та державної влади, популяризував діяльність терористичних організацій «ЛНР/ДНР», поширював інформацію для дискредитації Збройних Сил України.

Під час обшуку за місцем проживання адміністратора співробітники СБ України вилучили комп’ютерну техніку та мобільні пристрої із доказами здійснення антиукраїнської діяльності.

Слідчими СБУ в Чернігівській області відкрито кримінальне провадження за ст. 109 Кримінального кодексу України. Перевіряється інформація щодо зв’язків агітатора з представниками російських спецслужб та бойовиками незаконних збройних формувань так званих «ЛНР/ДНР».

Вирішується питання про оголошення чоловіку підозри у скоєнні зазначеного злочину. Тривають невідкладні слідчі дії.

***

25.02.2018

США заподозрили Россию в хакерской атаке на компьютеры Олимпиады

Американские спецслужбы считают, что «российские военные хакеры» взломали несколько сотен компьютеров на зимних Олимпийских играх в Пчхёнхане, причем атака была произведена так, чтобы подозрение упало на Северную Корею. Об этом со ссылкой на анонимных представителей разведки сообщает Washington Post (InternetUA).

Мотивом атаки собеседники журналистов назвали месть за решения Международного олимпийского комитета, который отстранил национальную сборную России от участия в Олимпийских играх. По мнению специалистов из американских спецслужб, в начале февраля российские военные из ГРУ (Главное разведывательное управление) имели доступ к 300 компьютерам на Олимпиаде в Южной Корее.

При этом отмечается, что организаторы Игр-2018 подтвердили, что 9 февраля – в день открытия Олимпиады они действительно стали жертвой кибератаки: были перебои с доступом в Интернет и проблемы с трансляцией.

Кроме того, многие пользователи не смогли зайти на официальный сайт Игр-2018, чтобы распечатать билеты, поэтому на церемонии открытия Олимпиады было много пустых мест.

В статье американского издания также подчёркивается, что в США опасаются, что в день закрытия Игр может произойти «новая кибератака русских хакеров».

***

25.02.2018

Apple облегчила властям доступ к переписке пользователей

Власти Китая получат более легкий доступ к переписке пользователей и другим личным данным после того, как Apple перенесет китайские аккаунты iCloud в дата-центр в КНР. Об этом 24 февраля передает Reuters (InternetUA).

Переноса данных требует новое китайское законодательство. В том числе в китайский дата-центр перенесут ключи для разблокировки аккаунта iCloud, которые ранее хранились в США.

Чтобы получить эти ключи, правительству любой страны требовалось разрешение американского суда. С момента, когда аккаунты китайских пользователей сервиса перенесут в Китай, властям страны не нужно будет обращаться в суд в США для доступа к пользовательской информации.

Центр обработки данных Apple построила вместе с китайской госкомпанией Guizhou-Cloud Big Data Industry в провинции Гуйчжоу. Reuters утверждает, что фирма тесно связана с правительством КНР и китайской компартией.

Решение компании подчиниться требованиям властей КНР подчеркивает сложность работы американских технологических компаний в этой стране, отмечает агентство. В случае если та или иная корпорация откажется их выполнять, она потеряет доступ к прибыльному китайскому рынку.

К примеру, в Китае блокируются сервисы Google, поскольку компания отказалась внедрить в поисковик фильтрацию результатов поиска.

***

26.02.2018

В Австрии могут разрешить слежку за перепиской в WhatsApp и Skype

Правительством Австрии разработан законопроект, позволяющий спецслужбам тайно следить за перепиской пользователей мессенджеров WhatsApp и Skype, а также расширить возможности прослушки видеонаблюдения, сообщило Австрийское агентство печати.

Докладніше

***

27.02.2018

Спецслужбы теперь могут взломать любой iPhone

Израильский производитель инструментов для проведения криминалистической экспертизы Cellebrite уведомил своих клиентов о появившейся новой возможности взлома любого устройства под управлением iOS 11. Сюда также входит iPhone X – модель, уже успешно взломанная в ноябре 2017 года сотрудниками Министерства внутренней безопасности США, предположительно, с помощью технологии Cellebrite (InternetUA).

Компания, клиентом которой, в частности, является правительство США, не делала никаких публичных заявлений о новой возможности. Тем не менее, журналисты Forbes узнали от своих источников, пожелавших сохранить анонимность, о том, что в последние несколько месяцев Cellebrite удалось разработать ранее неизвестный метод взлома iOS 11, и теперь она предлагает эту услугу своим клиентам из правоохранительных органов и частным экспертам по всему миру.

Новая услуга также была добавлена в каталог компании. Согласно каталогу, Cellebrite может обойти механизмы защиты «Apple iOS-устройств и операционных систем, включая iPhone, iPad, iPad mini, iPad Pro и iPod touch, работающих под управлением от iOS 5 до iOS 11».

По словам одного из источников Forbes в правоохранительных органах, эксперты Cellebrite сказали ему, что могут взломать iPhone 8. Если компания способна обойти защиту iPhone 8, то наверняка может взломать и iPhone X, поскольку их механизмы безопасности практически одинаковые.

Проблема захисту даних. DDOS та вірусні атаки

14.02.2018
В Skype обнаружена серьезная уязвимость

Исследователь безопасности Стефан Кантак (Stefan Kanthak) обнаружил уязвимость в механизме обновления online-мессенджера Skype, позволяющую повысить права пользователя до уровня SYSTEM и таким образом получить полный доступ к уязвимому устройству (InternetUA).

Как пояснил Кантак в беседе с журналистами издания ZDNet, проблему можно проэксплуатировать с помощью метода подмены DLL-библиотек, что позволит атакующему обмануть установщик обновлений и «подсунуть» вредоносный код вместо правильной библиотеки. Злоумышленник может загрузить вредоносную библиотеку во временную папку и переименовать ее в соответствии с существующей DLL-библиотекой, которая может быть модифицирована непривилегированным пользователем, например, UXTheme.dll. Проблема заключается в том, что в процессе поиска приложением нужной библиотеки первой обнаруживается вредоносная библиотека. Получив полный доступ к системе, злоумышленник может выполнять различные действия, к примеру, похитить файлы, удалить данные или инфицировать устройство вымогательским ПО.

Кантак сообщил Microsoft об уязвимости в сентябре прошлого года, однако в компании заявили, что выпуск исправления потребует «пересмотра значительной части кода», поэтому уязвимость будет устранена уже в новой версии клиента.

***

14.02.2018
Check Point поддерживает запуск решения для защиты от мобильных угроз

На базе продукта Check Point Sandblast Mobile Orange Cyberdefense разработал решение для защиты от мобильных угроз Orange Mobile Threat Protection (ITnews).

Сегодня сотрудники активно используют мобильные устройства для работы, поэтому при их взломе компании рискуют потерять критические данные. Разработки Check Point и Orange позволяют защитить бизнес от любых видов мобильных угроз и обеспечить сохранность корпоративной информации.

«Бизнес точно так же полагается на мобильные устройства, как и обычные потребители. Хакеры это знают и готовы атаковать мобильные устройства, используя любую уязвимость, – говорит Майкл Шаулов (Michael Shaulov), глава отдела управления продуктами Check Point для мобильной и облачной безопасности. – Благодаря сотрудничеству с Orange Cyberdefense пользователи мобильных устройств будут защищены от любых вредоносных программ, сетевых и других видов мобильных атак».

Orange Mobile Threat Protection объединяет преимущества технологии Check Point Sandblast Mobile, ведущего в отрасли комплексного решения в области защиты от мобильных угроз, и Orange Device Management Premium. Оно включает в себя облачную административную консоль, через которую можно отслеживать весь парк мобильных устройств, а также получать аналитические данные об угрозах и поддержку 24/7 от лучших специалистов по мобильным устройствам компании Orange. Решение доступно на платформах iOS и Android.

***

14.02.2018

Facebook запускает бесплатный VPN

Приложение Facebook предлагает воспользоваться пунктом «Защита» в навигационном меню, который ведет на страницу App Store, где можно скачать бесплатное VPN-приложение. Само приложение тоже принадлежит Facebook – соцсеть собирает через него статистику для борьбы с конкурентами.

Докладніше

***

15.02.2018

0-day уязвимость в Telegram использовалась злоумышленниками для многоцелевых атак

Эксперты «Лаборатории Касперского» обнаружили 0-day уязвимость в мессенджере Telegram. Как отмечается, злоумышленники эксплуатировали брешь мессенджера для осуществления многоцелевых атак.

Докладніше

***

15.02.2018

Лондон официально обвинил Москву в атаке вируса-вымогателя NotPetya

Британский МИД официально возложил на российские власти ответственность за массированную кибератаку с использованием вируса-

вымогателя NotPetya, заразившего в июне прошлого года сотни тысяч компьютеров по всему миру.

Докладніше

***

17.02.2018

Данные 119 тыс. клиентов FedEx обнаружены в открытом доступе в Сети

Отсканированные копии паспортов, водительских удостоверений и другой документации 119 тыс. клиентов службы доставки FedEx оказались в открытом доступе в Сети из-за некорректно настроенного сервера Amazon S3. Об этом сообщили исследователи безопасности из Kromtech Security Center.

Докладніше

***

17.02.2018

Появился новый вирус, распространяющийся через Word-файлы

В Сети орудует новый компьютерный вирус, который заражает устройства при помощи файлов Word (iLenta.com).

Данный вирус распространяется путем отправки файлов Word через электронную почту. Уникальной особенностью нового зловреда стало полное отсутствие макросов.

Это означает, что при открытии зараженного файла Word пользователи не увидят никаких предупреждений или всплывающих окон. Атака имеет многоуровневую природу. Эксперты сравнивают этот вирус с «турдакеном» – праздничным блюдом, в котором цыплёнка помещают в утку, а её, в свою очередь, – в индейку.

Вирус использует комбинацию методов, которые начинаются с вложения формата .DOCX. Все обнаруженные специалистами e-mail включали вложение с именем «receipt.docx».

Специалисты отметили необычайно большое количество этапов и сценариев, используемых этим вирусом. Кроме того, файлы DOCX, RTF и HTA редко блокируются почтовыми или сетевыми шлюзами, в отличие от более очевидных, таких как VBS, JScript или WSF.

***

18.02.2018

Роман Черный

5 лучших бесплатных антивирусов начала 2018

Хороший программный продукт не обязательно дорого стоит. В сети можно найти много качественного бесплатного софта, в том числе –

бесплатные антивирусы, которые практически не уступают своим платным аналогам. Вот пятерка лучших бесплатных антивирусов начала 2018 года.

Докладніше

***

20.02.2018

Мошенники нацелились на мобильные счета украинцев

Мошенники снова активизировали попытки обчистить мобильные счета украинцев. В социальных сетях люди жалуются на странные смс, в которых их просят подтвердить перевод средств на банковские карты и интернет-игры, которых сами пользователи не инициировали.

Докладніше

***

20.02.2018

Любой желающий может стать распространителем вымогательского ПО Saturn

Разработчики вымогательского ПО Saturn позволяют любому желающему бесплатно распространять вредонос, в обмен на перечисления создателям программы часть полученных путем вымогательства средств.

Докладніше

***

19.02.2018

ESET: «полицейские» вымогатели остаются главной угрозой для Android

Вирусная лаборатория ESET представила отчет об актуальных угрозах для платформы Android.

Докладніше

***

19.02.2018

Уязвимость в Cleverence Mobile SMARTS Server используется для добычи криптовалют

В июле 2017 года специалисты компании «Доктор Веб» обнаружили в серверных приложениях Cleverence Mobile SMARTS Server уязвимость нулевого дня. Разработчики программы выпустили обновление для устранения этой уязвимости, однако ее до сих пор используют злоумышленники для добычи (майнинга) криптовалют.

Докладніше

***

19.02.2018

ПриватБанк предупредил о мошенническом приложении «мобильный банк»

ПриватБанк предупредил клиентов об опасности регистрации и использования мошеннического приложения для Android «Универсальный Мобильный Банкинг», размещенного в Google Play 14 февраля (InternetUA).

Как говорится в официальном заявлении ПриватБанка, единственным приложением, которое позволяет пользоваться услугами банка с мобильных устройств, является Приват24. Любые сторонние «мобильные банки» – фишинговые программы, созданные для воровства личных данных клиентов и воровства денег.

***

20.02.2018

ПриватБанк добился удаления фишингового приложения из Google Play

Вредоносное приложение «Универсальный мобильный банкинг» по требованию представителей ПриватБанка и ряда других украинских банков было удалено из Google Play 19 февраля в 23-00 (ITnews).

Как сообщили специалисты департамента кибербезопасности ПриватБанка, сейчас совместно с экспертами по всему миру продолжает работа по по блокированию веб-сайта мошенников и отзыве сертификата разработчиков фишингового продукта.

***

21.02.2018

Дмитрий Демченко

В uTorrent нашли уязвимость, которая позволяет сайтам получать контроль над ПК

Исследователи Google Project Zero обнаружили у одного из самых популярных торрент-приложений uTorrent уязвимости, которые позволяют мошенникам получать доступ к загруженным файлам, истории загрузок, а также выполнять действия на компьютере жертвы. Об этом сообщает ArsTechnica (AIN.UA).

Уязвимости были найдены в десктопной программе uTorrent для Windows и в приложении uTorrent Web. Согласно отчету Project Zero, сайты могут контролировать ключевые функции обоих клиентов, получать доступ к загружаемым файлам и истории загрузок. Наибольшая угроза заключается в том, что с помощью этих уязвимостей сайты могут загружать вредоносный код

в папку автозагрузок, после чего он автоматически запустится со следующим включением ПК.

В компании-производителе приложения BitTorrent отмечают, что в течение нескольких дней клиенты получат обновления, которые исправят ошибки. Обновленные версии уже можно скачать самостоятельно – как для десктопного uTorrent (после перехода по ссылке сразу начнется скачивание), так и для uTorrent Web.

ArsTechnica отмечает, что до обновления клиентов пользователям стоит приостановить их использование.

***

21.02.2018

Ольга Карпенко

Мошенники шлют спам от имени и с серверов украинских интернет-магазинов: как это исправить

Некоторые крупные украинские интернет-магазины столкнулись с необычной механикой мошенничества. Неустановленные лица используют email-базы пользователей в процессе авторизации на сайте магазина так, что в результате пользователь получает письмо от самого магазина, но со спам-ссылкой внутри.

Докладніше

***

21.02.2018

В компьютерную игру специально встроили вирусы

Создатели компьютерного симулятора включили вредоносное программное обеспечение в инсталлятор игры. Таким образом они планируют бороться с цифровыми пиратами, сообщает портал Motherboard (InternetUA).

При установке неофициальной версии игры вирус крадет пароли и имена пользователей Chrome. Этот новый эффективный способ защиты разработчики компании FSLabs вшили в аэросимулятор Flight Simulator Add-On.

Дополнения для гиперпространственной имитации полета на аэроплане от Microsoft выпускает компания FSLabs. Накануне один из пользователей имиджборда Reddit сообщил, что заметил странные проблемы с установщиком для конкретной модели самолета в симуляторе. Программное обеспечение, по словам пользователя, включало файл с именем text.exe, который фактически оказался похитителем паролей.

Сотрудники компании подтвердили гипотезу юзера. При запуске нелицензированной копии игры программа извлекает все сохраненные имена пользователей и пароли из браузера Chrome, а затем отправляет их на серверы FSLabs.

Основатель компании Fidus Information Security Эндрю Маббитт (Andrew Mabbitt) назвал этот метод защиты одним из самый экстремальных.

***

21.02.2018
В Android P появится защита от шпионов

На сайте Android Open Source Project было обнаружено упоминание одной из новых функций Android P – следующей версии мобильной операционной системы от Google. Она будет связана с безопасностью и призвана защитить владельцев смартфонов от мошенников и хакеров, использующих открытость ОС в целях слежки (InternetUA).

Как известно, Android является открытой операционной системой, которая предлагает разработчикам и пользователям много возможностей. По этой причине платформа имеет ряд уязвимостей в безопасности. Например, разработчик без проблем может создать приложение, которое будет скрытно снимать пользователя через камеру.

Google начала бороться с подобным видом слежки ещё в Android Oreo, требуя от приложений, активно использующих камеру, показывать соответствующие уведомления. Таким образом, даже если на экране устройства нет видоискателя, пользователь может узнать об этом из центра уведомлений. В Android P, как сообщается, поисковый гигант пошёл ещё дальше, запретив приложениям использовать камеру в фоновом режиме.

Стоит отметить, что данное нововведение в Android P сделает бесполезными приложения, позволяющие незаметно сфотографировать человека на фронтальную камеру смартфона, если тот был утерян или украден.

***

21.02.2018
Мобильные приложения и смартфоны несут серьезную угрозу

В результате нового расследования выяснилось, что Иран опубликовал в Google Play приложения, которые после скачивания начинают шпионить за владельцами смартфонов.

Докладніше

***

21.02.2018
Хакери зламали хмару Tesla, щоб майнити криптовалюту

Аккаунт Tesla в хмарному сервісі Amazon зламали невідомі хакери. Проте вони не стали нічого викрадати, а просто налаштували потужність хмари на видобуток криптовалюти.

Докладніше

***

22.02.2018
Хакеры скомпрометировали сервер проекта Mageia

Неизвестным хакерам удалось скомпрометировать сервер Linux-дистрибутива Mageia и похитить базу данных пользователей, после чего атакующие опубликовали ее в Сети (InternetUA).

По словам разработчиков проекта, злоумышленники получили доступ к LDAP-серверу Mageia (identity.mageia.org), на котором хранились имена пользователей, хэши паролей и электронные адреса. Несмотря на то, что пароли были модифицированы и приведены к одному регистру символов, атакующие все еще могут реконструировать учетные данные по хэшам или распространить актуальную базу в Сети.

Сразу после обнаружения утечки все пароли были сброшены, а пользователям было предложено восстановить их через интерфейс восстановления пароля. Доступ для пользователей с повышенным уровнем привилегий был восстановлен в индивидуальном порядке.

В настоящее время администраторы проекта ведут расследование инцидента и восстанавливают хронологию событий. Пока остается неясным, как именно хакерам удалось прочитать содержимое LDAP-каталога в обход настроек ограничения доступа.

***

22.02.2018
Криптомайнеры все чаще атакуют компании

Компания Check Point Software Technologies предупреждает, что вредоносное ПО для майнинга криптовалюты продолжает атаковать организации во всем мире.

Докладніше

***

22.02.2018
Пользователям торрентов угрожает серьезная опасность

Сразу в двух версиях самого популярного торрент-клиента uTorrent обнаружена опасная уязвимость. Используя ее, хакеры смогут получить доступ к истории загрузок, а также к самим загруженным файлам (InternetUA).

По словам экспертов из организации Google Project Zero, которая занимается поиском ошибок в коде различных приложений, контролировать uTorrent может любой сайт, который открывал пользователь на своем ПК.

При этом некоторые веб-страницы позволяют добавлять вредоносное ПО в папку автозагрузки Windows. Такие ресурсы представляют наибольшую опасность.

Разработчики торрент-клиента заявили, что обновление, где уязвимость будет устранена, появится в течение ближайших нескольких дней.

***

25.02.2018

Хакеры научились майнить с компьютеров жертв, использующих Microsoft Word

Хакеры, желающие разжиться криптовалютой за чужой счёт, не гнушаются любыми способами, стараясь использовать любую, даже самую сомнительную лазейку для доступа к мощностям чужих компьютеров. На этот раз злоумышленники применили новую уловку, разместив в документах Microsoft Word криптоджековый скрипт, позволяющий майнить криптовалюту, используя процессор заражённого компьютера (IGate).

Причиной уязвимости стала возможность вставить в документ видео с любого сайта без какой-либо фильтрации и предварительной проверки. После вставки embed-кода видео на страницу в документе появляется окошко с видеороликом, который можно просматривать. Одновременно с этим через Internet Explorer запускался скрипт, позволяющий майнить криптовалюту с помощью процессора компьютера, на котором запущено видео. При этом загрузка центрального процессора доходила до 90 процентов.

Из-за того, что процесс скрытой добычи криптовалюты продолжается, пока происходит просмотр видео, встраивать в документы небольшие ролики совсем невыгодно. Только с помощью видеозаписей, длящихся несколько часов, таким способом можно что-нибудь заработать, а коротенькие клипы не приносят ощутимого дохода, – сообщают специалисты из израильской компании Votiro, специализирующейся на кибербезопасности.

***

25.02.2018

Хакеры продают легитимные цифровые сертификаты для вредоносного ПО

Хакеры продают легитимные цифровые сертификаты для подписи вредоносного ПО. Об этом сообщили исследователи безопасности из команды Insikt Group компании Recorded Future.

Докладніше

***

26.02.2018

Обнаружен новый вирус-вымогатель массового поражения

В сети зарегистрированы первые доказательства работы нового массового сервиса-вымогателя Data Keeper. Об этом сообщил портал Bleeping Computer.

Первые жертвы вируса-шифровальщика появились через два дня после его официального релиза в даркнете. Вредоносное программное обеспечение шифрует файлы на компьютерах жертв и требует выкуп в криптовалюте (InternetUA).

Data Keeper – заражающий сервис, доступ к его коду выдается по запросу, это разновидность RaaS (Ransomware-as-a-Service, «вымогательство как услуга»). Зарегистрировавшись на специальном портале, любой желающий может присоединиться к киберпреступникам, достаточно лишь делиться полученной добычей с разработчиками.

По мнению экспертов компании MalwareHunter, файлы шифруются с помощью двойного алгоритма AES и RSA-4096. Data Keeper также вычисляет и пытается зашифровать все общие сети, к которым может получить доступ. При этом разработанный вирус не добавляет специальное расширение в зашифрованные документы, что лишает жертв возможности понять, какие файлы поражены.

Это уже третий «штамм» RaaS, предлагаемый киберпреступниками с начала года. Ему предшествовали разновидности, называемые Saturn и GandCrab. В отличие от «собратьев», Data Keeper не имеет фиксированного аванса в 30 процентов от выручки подписавшихся на сервис мошенников. Сумма за пользование сервисом не разглашается.

***

27.02.2018

Avast представил новое решение Smart Life для безопасности IoT-устройств

Компания Avast представила платформу Smart Life, решение для защиты цифровой информации на базе IoT (ITnews).

Smart Life использует технологию Искусственного интеллекта (Artificial Intelligence) для определения и устранения угроз. Avast предлагает заказчикам и поставщикам решение Smart Life в качестве программного обеспечения как услуги (Software-as-a-Service).

Докладніше

***

27.02.2018

Крупнейшие web-ресурсы Европы подверглись высокоскоростным DDoS-атакам

Исследователи безопасности из компании Qrator Labs зафиксировали серию высокоскоростных DDoS-атак на ряд крупнейших web-ресурсов Европы (InternetUA).

Как следует из пресс-релиза компании, с 23 по 27 февраля 2018 года по всей Европе прокатилась волна высокоскоростных DDoS-атак, с использованием техники амплификации на основе memcache (программное обеспечение, реализующее сервис кэширования данных в оперативной памяти на основе хеш-таблицы). Особенностью данной техники является отправка множества поддельных UDP-пакетов в единицу времени от широкого диапазона IP-адресов.

По словам исследователей, уязвимости в memcache существуют по меньшей мере с 2014 года, однако их наиболее активная эксплуатация пришлась на 2018 год. В частности, в ночь с 25 на 26 февраля эксперты зафиксировали серию memcache амплифицированных DDoS-атак на множество ресурсов по всему интернету.

Как выяснили специалисты, источниками атак были несколько интернет-провайдеров и хостеров, в том числе крупный провайдер OVH.

***

27.02.2018

Ольга Карпенко

Уязвимость на сайте МАУ выдавала данные о пассажирах по коду брони, сейчас она уже закрыта

На «Хабрахабре» 26 февраля появилась статья об уязвимости на сайте Международных Авиалиний Украины (МАУ). И хотя сама уязвимость уже закрыта, механизм ее работы – достаточно примечателен.

Докладніше

ДОДАТКИ

Додаток 1

15.02.2018

Google випустить чатбот, який відповідатиме за вас в месенджерах

Система Reply буде пропонувати кілька варіантів відповідей на стандартні запитання, щоб ви не витрачали час на їх набір (Espreso.tv).

Крім того, чатбот зможе автоматично відповідати: «Я за кермом», щоб не відволікати вас під час поїздок, і навіть розраховувати приблизний час у дорозі, орієнтуючись по геолокації телефону, пише Next Web.

Google працює над створенням чатбота, який буде відповідати на прості повідомлення в месенджерах замість вас. Лабораторія компанії Area 120 тестує нову систему під назвою Reply, яка поки сумісна тільки з Android, але в

кінцевому підсумку буде працювати на Hangouts, Allo, WhatsApp, Facebook Messenger, Android Messages, Skype, Twitter і Slack.

Принцип простий: щоб не відволікати вас від роботи або водіння машини, на повідомлення на кшталт: «Привіт, як справи?». Чатбот буде автоматично пропонувати заздалегідь написані варіанти відповідей, на кшталт: «Добре, дякую, ти як?».

На повідомлення: «Ти вже в ресторані?» бот запропонує відповісти: «Скоро буду», «Так, я тут», «Вже давно» і так далі. Сенс в тому, щоб не витрачати час на набір повідомлень, що не несуть особливого смислового навантаження, а відповідати на них в один дотик.

Такими примітивними функціями Reply не обмежиться. Розробники хочуть створити режим «Не турбувати», який буде автоматично вмикатися, коли ви ведете машину. Ви не будете отримувати сповіщення про повідомлення, а бот буде сам відповідати вашим співрозмовникам: «Я за кермом, напиши пізніше».

При цьому, термінові повідомлення на кшталт: «Ти де? Ми тебе чекаємо вже півгодини» будуть відображатися, навіть якщо ваш телефон на «паузі».

Ще одна цікава функція – це «розумні відповіді». Додаток, орієнтуючись на геолокацію телефону і ваш улюблений вид транспорту, зможе пропонувати відповідь на питання: «Коли ти приїдеш додому?» з точністю до хвилини.

Також в Reply можна буде поставити режим «Відпустка», щоб він автоматично відповідав на якісь нескладні повідомлення по роботі, звіряючись з вашим календарем. Дата виходу нової програми поки не розголошується – вона ще на ранніх стадіях тестування.

(вгору)

Додаток 2

20.02.2018

Разработчики Snapchat повторили фатальную ошибку Instagram

После смены дизайна приложения более 1 миллиона человек подписали ходатайство Change.org с требованием, чтобы Snapchat отменил новое оформление (Телекритика).

Snapchat сталкивается с эпическим восстанием пользователей после капитального «переоформления» приложения. На данный момент компания на недовольство пользователей никак не реагирует.

Принцип Snapchat отличается от главного конкурента Instagram – снапчатеры могут обмениваться сообщениями с прикреплёнными фото и видео, которые через определенное время исчезают. Главной особенностью приложения также является использование забавных масок при съемке селфи. Похожие технологии (Stories и маски) тот же Instagram ввел гораздо позже.

В этом месяце Snapchat представила свой глобальный редизайн, целью которого было упростить интерфейс и четко отделить «социальность» сети от «медиа».

«Твои друзья – не контент. Это отношения», – заявил генеральный директор Snapchat Эван Шпигель в рекламе обновления дизайна 2 месяца назад.

Но многие снапчатеры вышли из себя, жалуясь на то, что найти новые сообщения и друзей на обновленной странице «динамических» пользователей стало сложнее. Более 1 миллиона человек подписали ходатайство Change.org с требованием, чтобы Snap убрал дизайн. Пользователи грозятся перестать пользоваться приложением вообще. «Теперь это мусор», – заявил один из них.

Шпигель, выступая в четверг на конференции инвесторов, отметил, что Snapchat не изменит курс. «Некоторые из жалоб, которые мы видим, лишь усиливают нашу философию», – сказал он.

(вгору)

Додаток 3

27.02.2018

Обновления YouTube Live: автоматические титры, повтор live-чата и геотеги

26 февраля в YouTube анонсировали новые функции для улучшения live-трансляций как для блогеров, так и для зрителей. Одна из них – это возможность воспроизведения живого чата после окончания live-трансляции (Marketing Media Review).

Live-чат играет ключевую роль в коммуникации видеоблогера со своими подписчиками. Функция повтора чата даст возможность следить за разговором даже после того, как прямой эфир закончился. Живые чаты будут отображаться вместе с видео, точно так же, как и во время эфира.

Второе обновление – запуск автоматических титров на видео. По словам представителей YouTube, компания начала предлагать эту функцию еще в 2009 году и с тех пор добавила их к миллиарду видеороликов. Выводить субтитры во время live-трансляций сложнее, но достижения в области распознавания речи делают это возможным. В YouTube заявляют, что используют технологию автоматического распознавания речи в прямом эфире (LASR) для подачи субтитров во время live-трансляции, когда профессионально предоставленные титры недоступны. Текст на основе LASR не будет идеальным, но частота ошибок и задержка близки к отраслевым стандартам, утверждают в компании. После запуска в YouTube продолжат работу по улучшению точности титров и уменьшению задержек. Функция будет доступна в ближайшие недели, она делает YouTube одной из первых крупных видеоплатформ, которая предлагает субтитры в режиме реального времени.

Третье обновление – это возможность добавлять теги геолокации в свои live-трансляции на мобильном и загруженные видео и делиться своим местоположением со зрителями. Пользователь также сможет увидеть другие видео по одному тегу, просто нажав по нему, и использовать фильтры с

геолокациями на странице результатов поиска, чтобы найти другие видеоролики с определенного места.

(вгору)

Додаток 4

14.02.2018

МІП: Верифіковано понад 20 сторінок державних інституцій у Facebook

13 лютого 2018 року, на запит Міністерства інформаційної політики України до Європейського офісу Facebook, було верифіковано понад 20 сторінок центральних органів виконавчої влади та понад 10 сторінок перших осіб державних інституцій (Міністерство інформаційної політики).

Заступник Міністра інформаційної політики України Дмитро Золотухін зазначив: «Верифікація сторінок органів влади у Facebook створює умови для недопущення використання новітніх комунікаційних технологій для обману користувачів чи створення фейкових сторінок. Ми у Міністерстві продовжимо роботу з верифікації сторінок, тепер уже установ безпекового сектору, а також будемо захищати інтереси українців перед соцмережами».

Зокрема, було верифіковано сторінки:

– Міністерства екології та природніх ресурсів України,

– Міністерства з питань тимчасово окупованих територій та ВПО України,

– Міністерства інформаційної політики України,

– Державної міграційної служби України,

– Національної комісії з цінних паперів і фондового ринку України,

– Державної фіскальної служби України,

– Державного агентства з питань електронного урядування України,

– Державного агентства з питань кіно України,

– Державного космічного агентство України,

– Національного агентства з питань запобігання корупції України,

– Державного комітету телебачення і радіомовлення України,

– Державної авіаційної служби України,

– Державного підприємства «Національна атомна енергогенеруюча компанія «Енергоатом»,

– Вищої ради правосуддя України,

– Пенсійного фонду України,

– Державного агентства лісових ресурсів України,

– Державної архітектурно-будівельної інспекції України,

– Державного агентства України з управління зоною відчуження,

– Державної аудиторської служби України,

– Національної комісії, що здійснює державне регулювання у сферах енергетики та комунальних послуг України,

– Державного агентства автомобільних доріг України,

– Державної служби геології та надр України,

– Державної казначейської служби України.

Позначку «верифіковано» також отримали сторінки: Віце-прем'єр-міністра України В'ячеслава Кириленко, Віце-прем'єр-міністра України Володимира Кістіона, Міністра Кабінету міністрів України Олександра Саєнко, Віце-прем'єр-міністра – Міністра регіонального розвитку, будівництва та ЖКГ України Геннадія Зубко, Міністра енергетики та вугільної промисловості України Ігоря Насалика, Міністра культури України Євгена Нищука, Міністра соціальної політики України Андрія Реви, Голови Державної міграційної служби України Максима Соколюка, Голови Державної прикордонної служби України Петра Цигикала, Голови Державної служби з надзвичайних ситуацій України Миколи Чечоткіна, Голови Національної поліції України Сергія Князєва.

Зазначимо, Міністерство планує проведення тренінгів для державних службовців, присвячених правилам адміністрування офіційних сторінок у соціальних мережах.

(вгору)

Додаток 5

22.02.2018

В Одессе запустили соцсеть для общения с депутатами

В Одессе запустили социальную сеть для общения с депутатами горсовета. Новая муниципальная онлайн-платформа «Твой депутат Одесского городского совета» (deputat.odessa.ua) позволяет горожанам напрямую обратиться к избранникам своего округа с проблемой, просьбой или предложением (Сегодня).

На главной странице сайта – карта города, где разными цветами обозначены границы избирательных округов. При нажатии на тот или иной участок всплывает окошко с информацией о том, какие депутаты его представляют. Уже на странице народного избранника можно просмотреть его биографию, адреса общественных приемных, декларации, а также задать вопрос через сайт, записаться на прием или ознакомиться с поданными им запросами.

К слову, последних тут скопилось уже более 300.

Депутаты просят отремонтировать здания, привести в порядок улицы, предоставить материальную помощь тем, кто в ней нуждается. Отметим, что многие из запросов и, соответственно, ответов не являются публичными, поэтому рядовой пользователь ресурса видит лишь их заголовки.

Как и обещали разработчики, сервис интегрировали с онлайн-платформой «Единый центр обращений граждан», известной как «15-35». Народные избранники уверяют, что уже получают оповещения о проблемах своего округа с этого ресурса. Да и сам интерфейс страницы с депутатскими запросами очень

похож на сайт обращений граждан: операторы распределяют документы по исполнителям, которые отвечают в рамках своих полномочий.

Политики сетуют, что не всегда получают конструктивные ответы на свои запросы. «Депутаты получают колоссальное количество отписок, не меньше, чем граждане, – говорит нам депутат Лилия Леонидова. – В прошлом году обращалась с просьбой включить 119-ю школу в титул на ремонт 2018 года. В начале 2018-го я решила продублировать все обращения, чтобы убедиться, что работы будут выполнены в этом году, и получила ответ, что денег нет».

Тем не менее она находит сервис более удобным, чем предыдущие варианты взаимодействия. Другого мнения придерживается Алексей Еремица. «Появление такой системы – это, конечно, здорово, но я пока особой практической пользы не ощущаю», – признался нам депутат, подчеркнув, что наличие активных общественных приемных полезнее в общении с горожанами.

Одесские общественники говорят: время покажет, насколько полезен новый онлайн-ресурс.

«Чем больше возможностей задать вопросы и получить ответы, тем меньше степень коррупции. Коррупция связана с определенной недоступностью информации, и чем больше открытости со стороны горсовета – тем лучше», – говорит глава Антикоррупционного офиса Алексей Черный.

Он надеется, что городские власти создадут открытую систему электронного документооборота для доступа горожан к любым документам распределителей бюджета.

По нашим наблюдениям, платформа «Твой депутат», как и прочие муниципальные сайты, не имеет оптимизации для слабовидящих.

«Когда разрабатывались городские платформы и поднимался вопрос доступности, нас уверяли, что будет возможность для слабовидящих пользоваться этими сайтами», – рассказал нам глава Антидискриминационного комитета Дмитрий Вичик, напомнив, что люди с особыми потребностями сталкиваются с проблемой доступности не только в интернете, но в целом в городе.

(вгору)

Додаток 6

15.02.2018

Михаил Сапитон

В Google Chrome появился встроенный блокировщик рекламы. Как он будет работать?

С 15 февраля Google активировала в браузере Chrome на всех платформах встроенный блокировщик рекламы. Разработка призвана бороться с самыми назойливыми баннерами и остановить веб-мастеров от их использования. Редакция AIN.UA объясняет, как будет работать «эдблок» от компании,

которая в последнем квартале заработала 85 % дохода ($27,2 млрд) на показе интернет-рекламы (AIN.UA).

Для начала стоит уяснить – вся реклама из Chrome не пропадет. Блокировать будут объявления, нарушающие правила, установленные Коалицией за лучшую рекламу. Их разработали на основе исследований с фокус-группой в размере 40000 человек. В составе Коалиции: Google, Facebook, Procter & Gamble, газета Washington Post и другие.

Чего они хотят?

Вместе они собираются улучшить интернет, выступая против рекламных решений, которые мешают пользователям. Если обобщить, то под запрет попадает полноэкранная реклама, реклама с автоматическим воспроизведением видео или аудио, мелькающая реклама. Эти виды объявлений должен отслеживать внутренний фильтр блокировщика. Однако в Google не ограничились общими формулировками, а детально объяснили принцип его работы в корпоративном блоге.

Хотя некоторые форматы, нарушающие стандарты лучшей рекламы, являются отражением проблем самой рекламной индустрии, большинство проблемных решений контролируются владельцами сайтов.

На десктопах Google планирует блокировать всплывающую рекламу, большие рекламные «стикеры», автозапуск видеорекламы со звуком, а также рекламу, которая появляется вместе с таймером, по истечении которого вы получает доступ к контенту (такой, например, используется на сайте Forbes).

На мобильных устройствах политика Google оказалась еще более агрессивной. Помимо всех вышеперечисленных типов, блокировать будут мигающую анимированную рекламу, полноэкранную рекламу с необходимостью скроллинга, а также плотно размещенные объявления.

Я смогу нажать одну кнопку – и реклама исчезнет?

Здесь и проступает специфика. Блокировщик от Google не будет работать как сторонние решения – поначалу он выступит в роли сигнальной системы для веб-мастеров. Google разделил процесс удаления рекламы на три этапа: аудит, оповещение владельцев сайтов о проблемах, время для исправления нарушений.

Сначала автоматический парсер проанализирует страницу в поиске типичных паттернов кода, нарушающих правила Коалиции за лучшую рекламу. Они сформированы на основе правил публичного фильтра EasyList.

Затем адресу присвоят один из трех статусов: прошел проверку, получи предупреждение или провалили. Владельцы сайтов смогут использовать API для доступа к этим оценкам или инструмент Search Console для детального ознакомления с претензиями фильтра. После исправлений сайт позволят отправить на пересмотр. Однако если уведомления о нарушениях будут проигнорированы или не выполнены должным образом, после 30 дней ожидания Chrome начнет блокировать на сайте рекламу.

Отвечая на первый вопрос: нет, по одному клику назойливые баннеры не пропадут. Но в будущем вы заметите разницу.

Что еще нужно знать?

Обнаружить работу встроенного блокировщика окажется просто. На десктопе он будет отображаться в адресной строке сайта, а в мобильных версиях станет раскрывающимся предупреждением внизу экрана. Google позволит отключать его на всех платформах.

В конце концов, он ведь призван не убивать рекламу в интернете, а улучшить ее. Результаты внутреннего исследования компании показывают, что 42 % сайтов уже исправили полученные предупреждения о нарушении стандартов лучшей рекламы. Пользователи, кажется, тоже останутся в выигрыше – после попадания в «черный список» реклама на сайтах не будет даже загружаться на уровне сети, поскольку фильтр станет блокировать запросы объявлений к серверу.

(вгору)

Додаток 7

21.02.2018

ИИ-решение Avaya Ava поможет при взаимодействии с клиентами через соцсети и месенджеры

Avaya представила новое решение для внедрения технологий искусственного интеллекта в контакт-центры. Avaya Ava – архитектура на основе ИИ, включающая в себя технологии естественного языкового взаимодействия, машинного обучения и аналитики, обеспечивает простоту взаимодействия с клиентами через социальные сети и платформы обмена сообщениями (Компьютерное Обозрение).

Avaya Ava – это облачное решение, не зависящее от платформы-мессенджера, которое предлагает возможности ИИ для интеграции в сервисы обмена сообщениями и автоматизации цифрового взаимодействия. Впервые Avaya Ava была внедрена на портале онлайн-поддержки Avaya для помощи клиентам и партнерам в поисках информации по продуктам и разрешении вопросов без участия сотрудников компании.

Решение взаимодействует с клиентами посредством социальных сетей и месенджеров, не только предоставляя им быструю поддержку в форме самообслуживания, но и, при необходимости, перенаправляя их обращения к операторам. В последнем случае Ava транслирует весь предыдущий контекст взаимодействия, предотвращая необходимость повтора информации и уже выполненных действий.

Возможности ИИ по естественному распознаванию различных языков, а также анализу контекста и тональности сообщений позволяют Ava увеличить производительность и эффективность взаимодействий с клиентами. Ava уже поддерживает 34 языка и интегрирована в такие платформы, как Facebook, Twitter, WeChat, LINE и др. Список поддерживаемых платформ будет постоянно пополняться. Открытый API позволяет интегрировать решения в области ИИ от любого разработчика в рамках программы Avaya A.I. Connect.

(вгору)

Додаток 8

27.02.2018
Майя Яровая
Facebook стал второй площадкой по видеорекламе в уанете: топ-3 рекламодателей по охватам

Видеореклама в Украине ежемесячно охватывает около 80 % всей интернет-аудитории в возрасте от 14 до 69 лет на ПК, и Facebook сейчас занимает вторую позицию по количеству показов рекламных роликов (4 % всех показов видеорекламы в месяц). Об этом свидетельствую данные исследовательской компании Gemius за январь 2018 года. Площадкой номер один в Украине остается YouTube – 47 % всех видеопоказов (AIN.UA).

В январе на Facebook (ПК) было сгенерировано более 28 млн показов видеорекламы, рекламодатели охватили в социальной сети 16 % аудитории уанета. Почти 60 % видеорекламы показывались в видимой зоне экрана (viewability rate) в среднем на протяжении 8 секунд (viewability time). Магазины электроники стали лидерами по количеству показов видеорекламы, которые были отображены в социальной сети на ПК.

Топ-3 рекламодателя в украинском сегменте Facebook по видеорекламе:

1. «Розетка» – охват: 5 % интернет-аудитории страны (3,2 млн показов);
2. F.ua – 4 % (2,6 млн показов);
3. «Алло» – 3,5 % (1,7 млн показов).

Facebook с начала года укрепил свои позиции на рынке онлайн-рекламы преимущественно за счет ухода рекламодателей с заблокированных российских ресурсов («ВКонтакте», Mail.ru, «Яндекс» и др.). В апреле социальную сеть хотя бы один раз в месяц на ПК посетили 45% всех пользователей уанета, а видеореклама охватила 7 % онлайн-аудитории. Бум роста аудитории Facebook пришелся на июнь-июль 2017 года, когда более 55 % интернет-аудитории посетили социальную сеть. В июле и августе 2017 года рекламодатели сгенерировали больше всего показов и охватили аудитории на ПК (охват пользователей видеорекламой составил 20 %, на 13 % больше, чем в апреле).

В январе 2018 года Facebook посетили 60 % всей интернет-аудитории Украины на ПК и ноутбуках (11,4 млн). За месяц пользователи сгенерировали более 600 млн просмотров страниц. В среднем один посетитель провел в социальной сети более 2,5 часов в месяц, тратя на визит около 8 минут (ПК). Сейчас социальная сеть занимает третью позицию по посещаемости в месяц среди ПК-аудитории и вторую – среди мобильной аудитории (смартфоны).

(вгору)

Додаток 9

25.02.2018
Как влияют социальные сети на успеваемость школьников

В журнале Educational Psychology Review были опубликованы результаты исследования относительно влияния социальных сетей на оценки школьников. Для этого был проведён метаанализ 59 научных работ о взаимосвязи социальных медиа и учебы подростков. В исследованиях приняли участие 29 337 человек (InternetUA).

В работах учитывалось использование подростками популярных во всём мире социальных сетей, таких как Facebook, Instagram и Twitter, а также популярных в Китае сетей Weibo и Renren. Учитывалось, сколько времени подростки проводили в социальных сетях в течение дня, как часто они размещали записи или общались с кем-либо. Кроме того, психологов интересовало, часто ли школьники проверяют социальные сети, работая над домашними заданиями.

При этом было установлено, что активное использование возможностей социальных сетей, связанных с учебой (например, специализированных групп для обмена информацией) в среднем немного улучшало оценки. Однако у тех учеников, кто во время учёбы или подготовки к ней часто общался в социальных сетях в личных целях, результаты незначительно ухудшались. Также выяснилось, что немного хуже учились те, кто в принципе часто пользовался соцсетями и выкладывал много записей на протяжении дня. Однако во всех случаях улучшение или ухудшение результатов было незначительным. Время, которое школьники тратили на учебу в течение дня, оказалось примерно одинаковым вне зависимости от того, как часто они обращались к социальным медиа.

Авторы работы считают, что социальные сети не мешают эффективной учебе. По мнению психологов, родителям не стоит запрещать детям пользоваться социальными медиа. Напротив, понимание и обсуждение их использования может улучшить отношения в семье. Один из авторов работы Маркус Аппель (Markus Appel) считает: «Если родители с уважением относятся к онлайн-активности детей, они получают больше возможностей для коммуникации».

(вгору)

Додаток 10

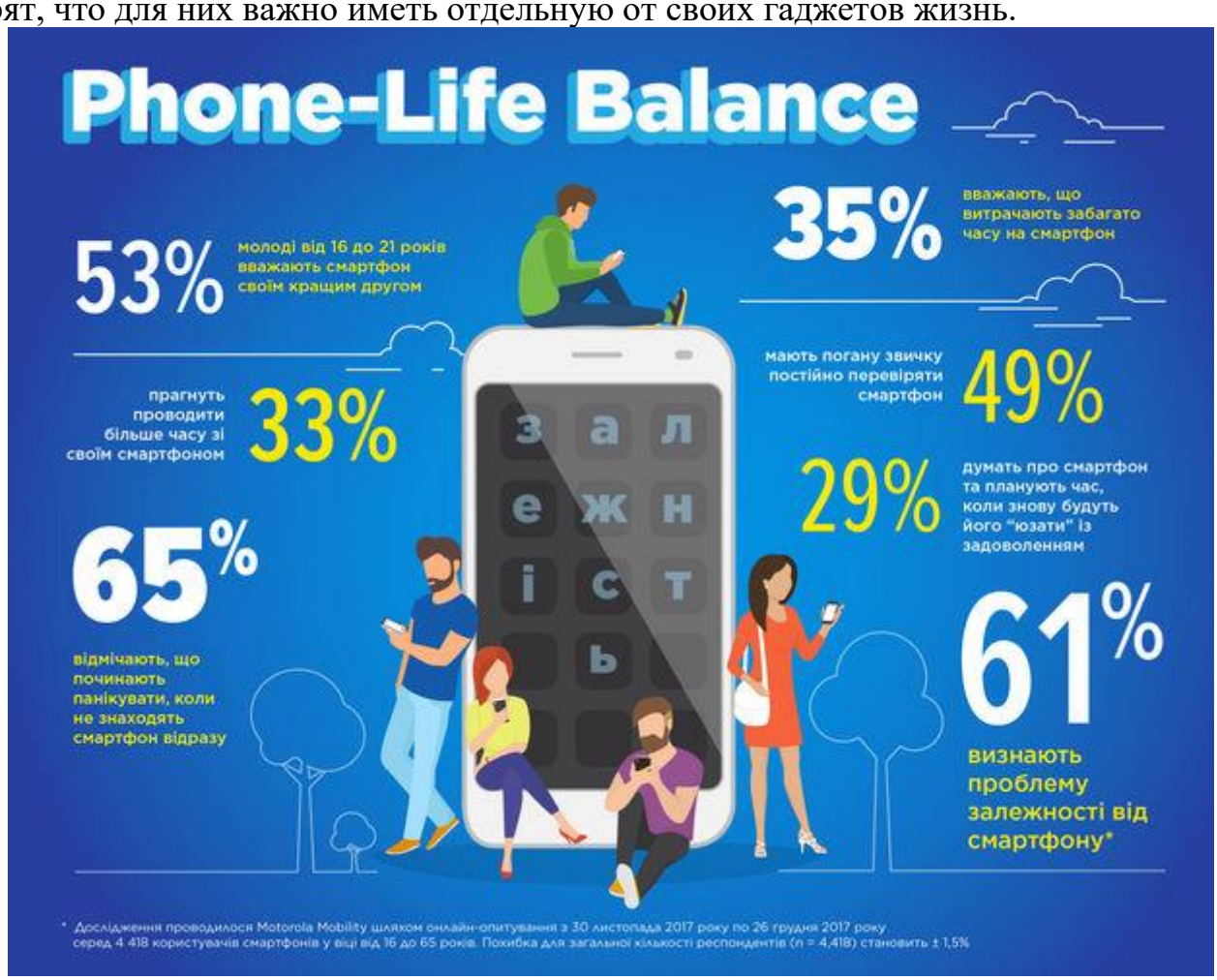
26.02.2018

Исследование Motorola Mobility: гаджеты – лучшие друзья поколения Z

Более половины молодых людей, родившихся после 1995 года, считают свои гаджеты лучшими друзьями. Об этом говорят результаты исследования Motorola Mobility про соблюдение баланса между обыденной и цифровой жизнью людей разного возраста, представленные в рамках Mobile World Congress 2018. Каждый третий опрошенный признался, что использование смартфона может быть более приоритетным, чем общение с близкими людьми.

Половина респондентов (49 %) согласны с тем, что проверяют свой телефон чаще, чем они хотели бы. Треть пользователей (35 %) признают, что тратят слишком много времени на свой гаджет (44 % среди молодежи «Поколение Z»), и считают, что они будут счастливее тратить меньше времени на телефон (34 %). При этом две трети опрошенных (65 %) признались, что паникуют, когда думают, что потеряли смартфон (Marketing Media Review).

Большинство хотели бы получить помощь для установления баланса между обыденной жизнью и смартфоном. Фактически, 60 % опрошенных говорят, что для них важно иметь отдельную от своих гаджетов жизнь.



В онлайн-опросе приняли участие 4418 человек в возрасте от 16 до 65 лет. Motorola привлекла к глобальному исследования профессора Нэнси Эткофф, известного эксперта в области поведения мозга и науки о счастье Гарвардского университета.

«Большинство пользователей смартфонов беспокоят их вредные привычки, в преодолении которых им нужна помощь», – говорит профессор Нэнси Эткофф. – Решить эти проблемы помогут положительные подкрепления поведения, контроль окружающей среды и внимательность. Широкий социальный паттерн поведения, обнаруженный в этом опросе, подчеркивает необходимость коллективного понимания проблем и последующих действий для их решения».

В рамках инициативы Phone-Life Balance каждый может пройти онлайн-опрос с 10 простыми вопросами, которые позволят пользователям лучше понять, насколько смартфон влияет на их повседневную жизнь: phone-lifebalance.com.

(вгору)

Додаток 11

16.02.2018

Ученые доказали, что социальные сети не смогут заменить живое общение

Сотрудники Канзасского университета опровергли гипотезу о том, что Всемирная паутина через несколько десятков лет полностью изменит социальную картину мира (Телеграф).

Социологи давно опасаются, что онлайн-коммуникация в скором времени придет на смену традиционному общению, и люди практически перестанут выходить из дома, предпочитая видеочаты походам в ресторан. Однако доцент кафедры коммуникаций Джеффри Холл (Jeffrey Hall) привел доказательства того, что соцсети не смогут стать полноценной заменой уютным разговорам за чашкой чая. «Я не говорю, что чрезмерное пользование социальными медиа идет нам на пользу, – пишет Холл в статье, опубликованной в журнале Information, Communication and Society, – однако все не так плохо, как мы привыкли думать».

Для того чтобы развенчать страхи ученого сообщества, Холл и его студенты-докторанты Майкл Керни (Michael Kearney) и Чонг Синг (Chong Xing) провели два уникальных исследования.

Во время первого они изучили данные двух социальных опросов молодежи, проведенных в 2009 и 2011 годах, и узнали, как менялось количество межличностных контактов в зависимости от частоты использования онлайн-мессенджеров. Годы были выбраны не случайно: считается, что именно в этот период американская молодежь повально увлекалась общением в Сети. В результате выяснилось, что использование онлайн-медиа практически не сказывалось на общении подростков с их друзьями и родственниками. Они продолжали ходить в гости, звонить по телефону и посещать различные секции и клубы, уделяя перепискам незначительное время.

Второй эксперимент разработал и провел сам автор. Он набрал группу из 116 человек, состоящую наполовину из взрослых и наполовину из студентов, и регулярно в течение пяти дней спрашивал их о том, какие контакты они совершали в последние часы: прямые или опосредованные. «Мы обнаружили, что постоянное пребывание в онлайн-режиме никак не влияло на повседневную жизнь испытуемых, − говорит Холл. – Они все также жили в реальном мире. Да, молодые люди отвлекались на то, чтобы посмотреть на экран, но делали это только тогда, когда оказывались в одиночестве».

Таким образом, можно сделать вывод о том, что теория социального перемещения в виртуальное пространство является безосновательной. Ученый

считает, что Интернет действительно вытесняет некоторые вещи из нашей жизни, но это относится в первую очередь к таким занятиям, как просмотр телевизора и чтение бумажных газет – все это мы предпочитаем делать с помощью смартфона. Но что касается взаимодействия с людьми, здесь не произошло никаких существенных изменений, разве что стало гораздо удобнее связываться с теми, кто находится за тысячи километров.

(вгору)

Додаток 12

19. 02.2018

Ольга Карпенко

Как кремлевская фабрика троллей влияла на выборы в США: реклама, хештеги, фейки

16 февраля американское Министерство юстиции выдвинуло обвинения в сторону 13 российских граждан и трех компаний во вмешательстве в президентские выборы в стране в 2016 году, в пользу одного из кандидатов, Дональда Трампа. Они крали аккаунты американских пользователей, выступали от имени политических активистов, использовали горячие темы иммиграции, религии и расы, чтобы влиять на ход кампании – говорится в 37-страничном обвинительном акте. Некоторые даже поддерживали контакты с людьми, участвовавшими в президентской кампании Трампа. Издание The New York Times опубликовало детали этого дела, редакция AIN.UA подготовила сокращенный перевод материала (AIN.UA).

Согласно документу, две компании из отмеченных в обвинении контролировал известный российский олигарх, приближенный к президенту, Евгений Пригожин («повар Путина»). Эти компании финансировали деятельность собственной фабрики троллей Internet Research Agency, созданной в 2013 году. По данным издания, там работали сотни людей, и уже к лету 2016 года ее расходы составляли порядка $1,2 млн в месяц. Месячные зарплаты составляли от $1100 младшему аналитику и $1400 блогеру, до $4200 старшему руководству.

Один из признаков связи Пригожина с фабрикой троллей, согласно документу, это компания Internet Research Agency, заплатившая обычному американцу за то, чтобы тот подержал плакат «С 55-летием, дорогой босс» перед Белым домом: считается, что так поздравляли с днем рождения самого Пригожина. В обвинительном акте фигурируют и другие должностные лица, участвовавшие в работе фабрики: CEO, блогеры, аналитики. Отдельный раздел издание посвятило конкретным пропагандистским методикам и манипуляциям, которые применяли сотрудники компании, чтобы влиять на исход выборов.

Мошеннические аккаунты в социальных сетях. Обвиняемые и их сообщники, согласно документу, создавали сотни аккаунтов в соцмедиа, которые представлялись настоящими и выдуманными американцами или организациями.

Нередкими были посты с критикой мусульман, посты на болезненные темы вроде иммиграции или Black Lives Matter, призывающие меньшинства не голосовать или рассказывающие о мошенничестве демократов. Какие-то аккаунты фокусировались на географической самоидентификации пользователей.

В письме одна из обвиняемых, Ирина Каверзина, писала родственнику: «Я писала все эти посты, постила картинки, а американцы думали, что это пишут сами американцы». Она же писала: «на работе – кризис: нас засекло ФБР(Не шутка».

Для продвижения постов использовались вирусные хештеги.

Политические митинги и марши – согласно документу, группа провела несколько политических митингов и манифестаций. Иногда они даже связывались с местными штабами Трампа и просили у них помощи. Правда, в документе не указано, сотрудничали ли американцы сознательно или нет. Группа оплачивала расходы отдельным участникам. К примеру, для одного из маршей Florida Goes Trump в августе 2016 года организация заплатила некоему лицу за изображение Хиллари Клинтон в тюремной робе. Facebook-реклама для маршей только во Флориде достигла охвата в 59 000 людей, на нее кликнуло 8300 пользователей.

Политическая реклама – группа оплачивала тематическую рекламу с апреля по ноябрь 2016 года. Эти расходы не подавались в рамках отчетов о расходах на президентскую кампанию, хотя группа самим финансированием кампании и так нарушила американские законы, поскольку в нее входили не-граждане США.

(вгору)

Додаток 13

20.02.2018

Facebook разоблачит интернет-троллей с помощью почтовых открыток

Компания Марка Цукерберга придумала, как бороться с незаконной политической агитацией в социальной сети. Владельцам аккаунтов, поддерживающим или критикующим определенных кандидатов на американских выборах, по обычной почте пришлют открытки с секретным кодом. Таким образом, Facebook надеется выяснить, кто из пропагандистов находится не на территории США, а, например, в России (InternetUA).

«Если вы запустите [в соцсети] объявление о кандидате, мы отправим вам почтовую открытку, и вам придется использовать [содержащийся в ней] код, чтобы доказать, что вы находитесь в Соединенных Штатах», – заявила Кейти Харбат, глобальный директор политических программ Facebook. Механизм верификации прост: если разместивший политическую рекламу находится не в США и использует фейковый аккаунт с указанным в нем фальшивым

американским адресом, он не получит код и не сможет размещать политическую рекламу в Facebook, сообщает Verge со ссылкой на Reuters.

Открытки с кодом будут отправляться обычной почтой любому покупателю политической рекламы в соцсети. Требование проверки личности владельца аккаунта не распространяется на тех пользователей FB, которые просто обсуждают в соцсети политические вопросы. Указывать секретный код при размещении поста придется только тем, кто агитирует за или против какого-то определенного кандидата на выборах в США любого уровня – от президентских до муниципальных. Новая система в масштабах всей страны будет опробована на предстоящих этой осенью промежуточных выборах в Конгресс.

Кейти Харбат признала, что верификация «не решит все», это всего лишь один шаг, который предпринимает Facebook, чтобы помешать иностранным гражданам вмешиваться во внутреннюю политику США.

Решение Facebook последовало вскоре после того, как спецпрокурор Роберт Мюллер предъявил обвинения 13 гражданам России, предположительно причастным к деятельности так называемой «фабрики троллей». Ее участники во время президентских выборов 2016 года в США размещали, в том числе в FB, посты с критикой кандидата от демократов Хиллари Клинтон и призывами голосовать за республиканца Дональда Трампа.

(вгору)

Додаток 14

21.02.2018
Андрій Пилипенко
США всерйоз взялися за російські «фабрики тролів»

Що відбувається?

У США стикається коло навколо так званих «фабрик» інтернет-тролів у рамках розслідування втручання РФ в американські президентські вибори 2016 року. За даними американських спецслужб, за атаками на сервери Демократичної партії стояло Головне розвідувальне управління (ГРУ) Генштабу Збройних сил Росії (Espreso.tv).

На початку серпня 2017 року спецпрокурор Роберт Мюллер скликав велику колегію присяжних для розслідування «російського сліду» у виборах. Мета – з'ясувати чи була змова штабу Дональда Трампа з Кремлем, для того, щоб підірвати позиції кандидата в президенти від Демократичної партії Хілларі Клінтон. У справах щодо втручання росіян у американські вибори також проходять екс-глава передвиборчого штабу Трампа та екс-радник Віктора Януковича Пол Манафорт та екс-радник Трампа з питань національної безпеки Майкл Флін.

У жовтні американські сенатори з Комітету з розвідки схвалили звіт спецслужб та погодилися із тим, що Росія прагнула вплинути на вибори в США

у 2016 році. Зокрема, здійснюючи хакерські атаки та розгорнувши кампанію впливу в соціальних мережах.

Чому зараз з'явилося стільки реакцій

16 лютого Мюллер висунув обвинувачення у втручанні в вибори президента Сполучених Штатів 13-тьом росіянам, які працювали у «фабриці тролів», та трьом організаціям.

Згідно опублікованих даних, російський центр втручання знаходився у Санкт-Петербурзі, за адресою вул. Савушкіна, 55. Американські спецслужби вважають, що саме там впродовж кількох років функціонувала «фабрика тролів»: вже у 2014 році в ній налічувалося не менше 80 співробітників.

З 2014-го року, за інформацією Міністерства юстиції США, на «фабриці» моніторили американський інтернет-простір за допомогою YouTube, Facebook, Instagram і Twitter. Вивчалися популярні групи, частота розміщення контенту, середня кількість коментарів та відповідей на повідомлення. Згодом почали з'являтися власні групи та сторінки, які зачіпали найбільш «болючі» для американського суспільства теми: міграцію, іслам та права мусульман, регіональний сепаратизм у Техасі, тощо.

Щомісяця у соціальних мережах з'являлися мільйони повідомлень позначених хештегами #HilIaryCIintonIsNotMyPresident, #Trump2016, #TrumpTrain, #Hillary4Prison, тобто очевидно просували ідею перемоги саме Дональда Трампа на виборах 2016-го року. Окрім дискредитації «демократичного» кандидата Хіларі Клінтон, «тролі» також використовували чорній піар проти конкурентів-республіканів Трампа – Марка Рубіо і Теда Круза. Мінюст США опублікував інструкції з електронних скриньок росіян, від лютого 2016 року, в яких вимагається використовувати будь-які можливості для критики Клінтон та підтримки її конкурента у демократичному таборі Берні Сандерса.

Буквально 20 лютого з'явилося інтерв'ю одного із росіян який працював на «фабриці тролів». 43-річний житель селища під Санкт-Петербургом Марат Міндіяров прокоментував свій досвід виданню The Washington Post: «Коли я був там, почалися санкції і рубль почав падати. Я писав, що все було навпаки: наскільки прекрасне наше життя, наскільки чудово те, що зміцнювався рубль, і подібного роду абсурд. Що ці санкції зроблять нас сильнішими і т. д. і т. п. Обсяги були колосальними – там була величезна кількість людей, від 300 до 400, і всі вони писали абсолютну неправду. Це було як у світі Орвелла".

За його словами, робоча зміна на «фабриці» тривала 12 годин. Один працівник встигав написати 135 коментарів по 200 знаків, отримуючи близько 40 тисяч рублів на місяць. Вдвічі більше сплачували у департаменті роботи з Facebook. Співробітники цього департаменту повинні знати мову ідеально, щоб користувачі не запідозрили, що мають справу з іноземцем.

В чому звинувачують тринадцятьох росіян

Росіян звинувачують у змові з метою обдурити американських виборців на передодні президентських перегонів 2016-го року, а також координації мітингів на підтримку Трампа після них. Крім того, двох росіян зі списку

обвинувачують у банківському шахрайстві. За допомогою куплених даних про номери соціального страхування або банківські рахунки вони верифікували акаунти на PayPal, для того щоб виводити зароблені гроші, або вкладати їх у «розкрутку» пропагандистських меседжів у соціальних мережах. Ще чотирьох звинувачують у крадіжці особистих даних інших людей.

Окрім безпосередньо громадян РФ, у США підозрюють три російські організації – «Агентство інтернет-досліджень» (власне це і є замаскована «фабрика тролів»), «Конкорд Менеджмент і Консалтинг» і «Concord Catering». Всіх їх пов'язують із Євгеном Пригожиним, якого вважають наближеним до Володимира Путіна та часто називають у медіа «кухарем Кремля» – за монополізацію сфери харчування та постачання продуктів для російської еліти.

Кого звинувачують

У російських медіа можна зустріти загальну інформацію про тих, хто саме став об'єктом прискіпливої уваги американських прокурорів. Окрім Пригожина, у «список тролів» потрапили:

- засновник та гендиректор організації «Агентство-інтернет досліджень», екс-поліцейський Міхаіл Бистров,
- виконавчий директор «Агенства інтернет-досліджень» Міхаіл Бурчик (він та Бистров – фігуранти минулорічного розслідування російського видання РБК про «фабрику тролів»),
- Олександра Крилова (позначена як «збирач інформації»),
- ІТ менеджер Сергій Полозов (закуповував сервери у США та здійснював іншу тех.підтримку),
- Анна Богачова, перекладач та аналітик,
- Роберт Бовда – керівник відділу перекладів,
- Марія Бовда,
- Володимир Венков,
- Ірина Каверзіна – перекладачі,
- Джейхун Асланов – керівник проектів та директор компанії «Азимут», яка за даними США, отримувала гроші за втручання у вибори,
- Вадим Подкопаєв – аналітик,
- Гліб Васильченко – експерт з моніторингу даних.

Можна відзначити те, що окрім Пригожина, який тісно пов'язаний з верхівкою російської еліти, інші фігуранти це здебільшого виконавці.

Коментарі

Президент США Дональд Трамп, який буквально кілька тижнів тому озвучував готовність піти і дати свідчення спецпрокурору (від чого його активно застерігали власні радники), відразу написав у Twitter, що звинувачення проти росіян не доводять змови його кампанії з Кремлем. 19 лютого у своїй улюбленій соцмережі він додав: «Якщо метою Росії було створення суперечностей, розколу і хаосу в США, то з усіма цими слуханнями в комітетах, розслідуваннями і партійною ненавистю вони втілили свої найсміливіші мрії. Вони в Москві сміються до упаду. Америка, будь розумніше!».

На нещодавній Мюнхенській безпековій конференції директор Нацрозвідки США Ден Коутс заявив, що на даному етапі у його відомства не має підстав сумніватися в тому, що РФ намагалася втрутитися в американські вибори 2016 року: «Близько року тому, коли я ще не займав цю посаду, американські спеслужби доповіли, що РФ справді намагалась вплинути на президентські вибори в США. Всі розслідування за цей час, а мова йде про збір інформації та розвідданих, підтвердили правильність цієї оцінки».

Зовсім відмінні реакції можна спостерігати у Росії. Якщо прес-секретар Кремля Дмитро Пєсков як завжди коротко відмахнувся від Reuters фразою: «Ми ще не ознайомилися (зі звинуваченнями – авт.)». То речниця МЗС РФ Марія Захарова пішла далі, назвавши у Facebook інформацію американського Мінюсту «абсурдом» та «поганою асоціацією із числом 13».

Яскраво виглядає коментар самого Євгенія Пригожина: «Американці дуже вразливі люди, вони бачать те, що хочуть бачити. З великою повагою ставлюся до них. Я зовсім не засмучений, що опинився в цьому списку. Якщо вони хочуть бачити диявола – хай бачать».

Висновки

Американська правова система діє неспішно, проте впевнено, як асфальтовий каток. Можна провести паралель із накладанням санкцій: рішення приймають, процедурно, впродовж тривалого часу – проте їх наслідки неможливо відмінити, ні Трампу, ні наступним президентам. Так чи інакше, вони будуть відчутними впродовж десятиліть, як славнозвісна поправка «Джексона-Вейніка», спрямована проти СРСР, а відмінена аж у 2012-му році.

Виходячи із позицій озвучених американськими урядовцями, не тільки спецслужби, а й усі органи влади США свідомі того, що кібератаки будуть продовжуватися і під час наступних виборів, що Росія буде й надалі намагатися «розхитати» демократичні процедури. І серйозно налаштовані протидіяти цьому зловживанню демократичними процедурами.

(вгору)

Додаток 15

14.02.2018

Хвиля кібератак з Росії може зачепити Україну, – Нацрозвідка США

Протягом наступного року російські спецслужби та урядові агентства можуть посилити підривну кіберактивність проти США, країн Заходу, а також безпосередньо проти України (Espreso.tv).

Про це заявив директор Національної розвідки США Деніел Коатс у своїй доповіді, представленій на слуханнях в Комітеті з питань розвідки американського Сенату.

«Ми очікуємо, що протягом наступного року Росія проводитиме більш потужні та більш руйнівні кібер-операції, очевидно, застосовуючи нові можливості проти України», – наголосив Коатс.

За прогнозами Нацрозвідки США, російський уряд розширюватиме діапазон уже реалізованих операцій, «у тому числі щодо порушення роботи енергорозподільчих мереж України, хакерських зламів з подальшим оприлюдненням інформації, збільшенні мережевих атак, а також провокацій під чужим іменем».

Крім того, у США очікують, що російські спецслужби продовжать випробувати на міцність життєво-важливу інфраструктуру США та країн-союзників, а також посилюватимуть непорозуміння між США, НАТО та іншими партнерами.

Коатс також наголосив, що Росія продовжить використовувати вибори та інші демократичні процеси в США і країнах заходу як можливість для підриву демократії.

«Як мінімум, ми очікуємо, що Росія продовжуватиме використовувати пропаганду, соціальні медіа, підставних осіб, співчутливих спікерів та інші засоби впливу, щоб спробувати посилити соціальні та політичні перепони в США», – зазначив він.

(вгору)

Додаток 16

21.02.2018

В России предложили блокировать пиратские сайты без суда

Министерство культуры РФ разработало законопроект, который будет осуществлять блокировку сайтов, содержащих нарушающий авторские и смежные права контент, без решения суда (InternetUA).

Согласно документу, опубликованному на портале regulation.gov.ru, от владельцев интернет-ресурсов потребуется указывать на сайтах контактные данные, включая название юридического лица, физический адрес и email.

В том случае если таких данных нет или связаться с владельцем правообладателю не удалось, правообладатель может обратиться к хостинг-провайдеру с требованием заблокировать ресурс.

Если хостер не ответит на запрос в течение 24 часов, аналогичное требование может быть направлено в Роскомнадзор. Ведомство, в свою очередь, попытается еще раз связаться с хостинг-провайдером или владельцем сайта-нарушителя. Если результат окажется отрицательным, пиратский ресурс в течение трех суток может быть навсегда заблокирован для пользователей из России.

Снятие ограничения на доступ к такому сайту не допускается, отмечается в тексте законопроекта.

Сейчас, согласно действующему законодательству, правообладателю необходимо обращаться в суд с требованием обеспечить предварительную блокировку сайта-нарушителя, а затем направить иск об удалении содержимого, нарушающего авторские права. Если суд вынесет решение в

пользу правообладателя, Роскомнадзор обращается к владельцу ресурса с требованием удалить контент. В случае отказа ресурс блокируется.

(вгору)

Додаток 17

26.02.2018

В Австрии могут разрешить слежку за перепиской в WhatsApp и Skype

Правительством Австрии разработан законопроект, позволяющий спецслужбам тайно следить за перепиской пользователей мессенджеров WhatsApp и Skype, а также расширить возможности прослушки видеонаблюдения, сообщило Австрийское агентство печати (InternetUA).

Законопроект призван расширить возможности правоохранительных органов и исполнительной власти, не нарушая при этом основные права граждан. Слежка будет применяться только в отношении подозреваемых в преступлениях, предусматривающих наказание от пяти и больше лет лишения свободы. В число таких преступлений входят терроризм, а также любая другая угроза жизни людей. При этом следить за лицами из круга общения подозреваемых и обычными гражданами спецслужбам будет запрещено. Для слежки будет использоваться специальное ПО, которое правоохранители будут удаленно устанавливать на устройства предполагаемых преступников.

Законопроект также предусматривает увеличение сроков хранения аудиозаписей телефонных разговоров и видеозаписей с камер наружного наблюдения, если данные материалы могут помочь в расследовании. Помимо этого, операторов связи обяжут регистрировать SIM-карты с предоплаченым тарифом на конкретное физическое лицо.

Согласно законопроекту, операторы связи должны будут хранить историю переписки и переговоров в течение 12 месяцев и предоставлять эти сведения по соответствующему запросу правоохранителей.

Законопроекту предстоит пройти обсуждение в профильных комитетах парламента, а затем голосование в Национальном совете Австрии.

(вгору)

Додаток 18

14.02.2018

Facebook запускает бесплатный VPN

Приложение Facebook предлагает воспользоваться пунктом «Защита» в навигационном меню, который ведет на страницу App Store, где можно скачать бесплатное VPN-приложение. Само приложение тоже принадлежит Facebook – соцсеть собирает через него статистику для борьбы с конкурентами (InternetUA).

Facebook предлагает VPN

Приложение Facebook стало предлагать пользователям прибегнуть к услугам бесплатной виртуальной частной сети (VPN). В его навигационном меню появился пункт «Защита», который ведет на страницу App Store, где можно установить VPN-приложение Onavo Protect. Пока что новшество работает только в iOS, сообщает ресурс TechCrunch.

К нынешнему моменту не вполне ясно, какой процент пользователей Facebook и в каких странах видит этот пункт меню. Ранее, в 2016 г. соцсеть уже пыталась дать ссылку на Onavo Protect из собственного приложения, также через пункт меню «Защита», что было замечено пользователями Великобритании. Попытки прорекламировать Onavo связаны с тем, что Facebook выкупила эту тель-авивскую компанию в 2013 г., предположительно, за сумму около $120 млн.

Что еще умеет Onavo Protect

Помимо собственно VPN, Onavo Protect располагает функционалом из сферы информационной безопасности – приложение обещает предупреждать пользователя о вредоносных сайтах и сохранять конфиденциальность таких данных, как номер банковского счета или кредитной карты, когда пользователь вводит их в интернете.

Наличие в Facebook ссылки на страницу установки Onavo Protect может привести к резкому росту количества пользователей этого сервиса. По данным ресурса Sensor Tower, на данный момент Onavo Protect был 33 млн раз установлен из App Store и Google Play, причем около 60 % установок приходится на Google Play. У приложения больше всего пользователей в США, далее следуют Индия и Бразилия.

Сбор данных в Onavo

Однако Facebook приобрела Onavo вовсе не из соображений информационной безопасности, отмечает TechCrunch. Дело в том, что этот сервис также дает Facebook возможность отслеживать активность пользователя в различных приложениях, что позволяет соцсети раньше конкурентов замечать новые тренды в мобильный экосистеме вообще.

Таким образом Facebook видит, какие приложения становятся хитами, а в каких уменьшается приток пользователей – вплоть до того, что может определить, какие новые функции тех или иных программных продуктов нравятся пользователям, а какие нет. Пользователи Onavo не знают, каким именно образом Facebook использует полученные от них данные.

Случаи использования данных

Эти данные помогают Facebook эффективнее конкурировать с другими соцсетями, в частности, со Snapchat. Например, после того, как в Instagram появились «Истории», аналог похожей функции в Snapchat, Facebook могла наблюдать замедление притока пользователей в конкурирующую соцсеть еще до того, как сама Snapchat об этом объявила. Об этом в августе 2017 г. сообщало издание Wall Street Journal.

Похожим образом статистика, собранная через Onavo, подтолкнула Facebook к покупке сервиса для проведения анонимных опросов среди друзей

Tbh в октябре 2017 г., еще до того, как он стал полноценной соцсетью. Вскоре после этого Facebook и у себя ввел похожую функцию вопросов-ответов.

Facebook и Snapchat

В 2013 г. Facebook попыталась выкупить за $3 млрд популярную соцсеть Snapchat, однако получила отказ. С тех пор Facebook стремится привлечь аудиторию Snapchat, добавляя у себя аналогичные функции. В 2014 г. компания даже выпустила «убийцу» Snapchat – приложение Slingshot, призванное подтолкнуть пользователей смартфонов делиться фотографиями и видео из повседневной жизни.

Ресурс The Guardian подсчитал, что Facebook пыталась клонировать или купить различные функции Snapchat в общей сложности 10 раз. В основном это фильтры и опции, связанные с фото- и видеоконтентом. Однако большая их часть не пользуется особой популярностью – клиенты Snapchat не спешат переходить в Facebook. В 2016 г. компания попыталась выкупить азиатский аналог Snapchat, перспективную южнокорейскую соцсеть Snow, но также получила отказ.

(вгору)

Додаток 19

15.02.2018

0-day уязвимость в Telegram использовалась злоумышленниками для многоцелевых атак

Эксперты «Лаборатории Касперского» обнаружили 0-day уязвимость в мессенджере Telegram. Как отмечается, злоумышленники эксплуатировали брешь мессенджера для осуществления многоцелевых атак (Компьютерное Обозрение).

В октябре 2017 г. экспертам стало известно об эксплуатируемой уязвимости Windows-клиента мессенджера Telegram. Она заключается в использовании классической атаки right-to-left override при отправке файлов собеседнику. Специальный непечатный символ right-to-left override (RLO) служит для изменения порядка следующих за ним в строке знаков на обратный, в таблице Unicode он представлен как ‘U+202E’. Атака подразумевает использование символа с целью введения жертвы в заблуждение, чаще всего, при отображении имени и расширения исполняемого файла: уязвимое к этой атаке ПО отображает его имя частично или в перевернутом виде.

Процесс эксплуатации такой уязвимости в Telegram выглядел следующим образом. Злоумышленник подготавливает зловред к отправке. Например, JS-файл он переименовывает следующим образом: evil.js -> photo_high_re*U+202E*gnp.js, где *U+202E* – RLO символ, который должен заставить Telegram перевернуть оставшиеся символы gnp.js. Атакующий отправляет сообщение и вместо JS-файла получатель видит PNG-картинку.

При клике по файлу появится стандартное уведомление безопасности Windows. Важно отметить, что оно отображается только в тех случаях, когда

соответствующая опция не была отключена в системных настройках. После подтверждения пользователя, вредоносный файл будет запущен.

Данная атака осуществляется с целью получить контроль над системой жертвы путем изучения окружения и установки дополнительных модулей. На первой стадии жертве отправляется загрузчик, написанный на .Net и использующий Telegram API в качестве командного протокола. После запуска прописывает себя в автозапуск и копирует свой исполняемый файл, в зависимости от окружения, в одну из директорий. Далее, с периодичностью в 2 секунды, начинает проверять наличие поступающих от управляющего бота команд. Важно отметить, что команды реализованы на русском языке. Перечень возможных команд показывает, что бот может скрытно разворачивать на целевой системе произвольные бэкдоры, логгеры и прочее вредоносное ПО. Из анализа команд видно, что средствами этого загрузчика предполагается дальнейшая установка, по крайней мере, логгера, который будет шпионить за жертвой.

Похоже, что об уязвимости было известно только злоумышленникам из России, так как все обнаруженные случаи эксплуатации происходили именно в этой стране. Кроме того, в ходе подробного изучения атак были найдены множество артефактов, указывающих на почерк киберпреступников из России.

Экспертам неизвестно, как долго и в каких версиях была открыта уязвимость, но случаи эксплуатации начались в марте 2017 г. Компания уведомила разработчиков о проблеме, и на сегодняшний день уязвимость не проявляется в продуктах Telegram.

(вгору)

Додаток 20

15.02.2018

Лондон официально обвинил Москву в атаке вируса-вымогателя NotPetya

Британский МИД официально возложил на российские власти ответственность за массированную кибератаку с использованием вируса-вымогателя NotPetya, заразившего в июне прошлого года сотни тысяч компьютеров по всему миру (InternetUA).

Всего за несколько недель до этого другой вирус-вымогатель, WannaCry, массово поразил британские больницы и другие учреждения Национальной системы здравоохранения (NHS).

«Правительство Соединенного Королевства приходит к выводу, что ответственность за разрушительную кибератаку NotPetya в июне 2017 года несут российские власти, а именно российская армия», – заявил 14 февраля вечером заместитель министра иностранных дел Великобритании Тарик Ахмад.

В Британии от вируса пострадали десятки организаций, в том числе почтовые службы, а также рекламные, юридические, логистические и

финансовые компании. Однако почти три четверти случаев заражения были зафиксированы в Украине.

Как утверждают в министерстве, кибератака была лишь обставлена как вымогательство, однако истинной целью вируса было не получение выкупа, а нарушение работы украинских госучреждений, финансового и энергетического секторов экономики.

В итоге вирус распространился дальше, заразив предприятия и организации по всей Европе, в том числе и в России.

«Эта атака показала упорное пренебрежение суверенитетом Украины. Безрассудный запуск вируса привел к нарушению работы организаций по всей Европе и нанес ущерб в сотни миллионов фунтов», – заявил британский чиновник.

«Кремль поставил Россию в прямую оппозицию к Западу, однако так быть не должно. Мы обращаемся к России с призывом стать тем самым ответственным членом международного сообщества, каким она себя позиционирует, а не пытаться втайне его разрушить», – добавил он.

Предположение о том, что за вирусом NotPetya стоят российские спецслужбы, высказывались и ранее. В частности, такие заявления делали в Службе безопасности Украины и в американской компании FireEye, занимающейся обеспечением кибербезопасности.

В том же ключе, однако не так жестко, высказывались и представители Агентства по кибербезопасности НАТО (CCDOE). Там заявили, что за созданием NotPetya стоит «государственный актор», не уточняя, что именно имеется в виду.

«Российская компания „Роснефть“ тоже была заражена, – говорится в заявлении. – Но заражение имело ограниченный эффект и нанесло мало ущерба».

С гипотезой о российском следе вируса согласны не все. Однако достоверно установить авторство вируса можно, только поймав хакера с поличным.

(вгору)

Додаток 21

17.02.2018

Данные 119 тыс. клиентов FedEx обнаружены в открытом доступе в Сети

Отсканированные копии паспортов, водительских удостоверений и другой документации 119 тыс. клиентов службы доставки FedEx оказались в открытом доступе в Сети из-за некорректно настроенного сервера Amazon S3. Об этом сообщили исследователи безопасности из Kromtech Security Center (InternetUA).

Отсканированные копии документов принадлежали клиентам из стран по всему миру, в том числе из США, Мексики, Канады, Австралии, Саудовской

Аравии, Японии, Китая и ряда европейских стран. Удостоверения личности были прикреплены к формам, содержащим персональные данные клиентов, такие как имена, домашние адреса, номера телефонов и почтовые индексы.

По данным исследователей, сервер принадлежал компании Bongo International LLC, предоставлявшей услуги по логистике и расчетах при обмене валют. Bongo была приобретена FedEx в 2014 году и переименована в FedEx Cross-Border International. В апреле 2017 года сервис прекратил работу.

«После предварительного расследования мы можем подтвердить, что некоторые архивные данные учетных записей Bongo International, расположенные на сервере стороннего поставщика облачных услуг, находятся в безопасности», – следует из заявления FedEx.

Как отметили представители компании, нет никаких свидетельств того, что информация попала в руки злоумышленников, однако расследование инцидента продолжается.

По словам исследователей, на сервере было обнаружено более 119 тыс. отсканированных копий документов. Все они были добавлены в период с 2009 по 2012 годы. В настоящее время неясно, было ли FedEx известно о существовании сервера.

(вгору)

Додаток 22

18.02.2018
Роман Черный
5 лучших бесплатных антивирусов начала 2018

Хороший программный продукт не обязательно дорого стоит. В сети можно найти много качественного бесплатного софта, в том числе – бесплатные антивирусы, которые практически не уступают своим платным аналогам. Вот пятерка лучших бесплатных антивирусов начала 2018 года (IGate).

Avast Free Antivirus

Многие компании предлагают на главной странице своих сайтов купить платные версии антивирусов, а бесплатные опции прячут куда-нибудь подальше. Avast – не из таких. Огромная оранжевая кнопка на странице загрузки антивируса предлагает пользователям скачать бесплатную версию, так что найти ее даже проще, чем платную. Но это – не единственное достоинство антивируса.

Avast предлагает стандартную антивирусную защиту, защиту от неизвестных угроз, а также имеет встроенный менеджер паролей. Согласно отчету AV-TEST, по состоянию на декабрь 2017 года Avast справлялся с абсолютно всеми известными человечеству вирусами.

AVG Free Antivirus

AVG проводит весьма спорную политику конфиденциальности. В обмен на предоставление защиты компания собирает обширную информацию о

пользователе. Но сама защита при этом остается очень качественной. Отчет AV-TEST также свидетельствует о том, что в декабре AVG Free Antivirus умел распознавать все известные человечеству угрозы.

Еще одно достоинство AVG – тихая работа в фоне. Антивирус не грузит систему и не требует внимания пользователя. При этом интерфейс программы очень дружелюбен. Если пользователь все же решит заглянуть в настройки антивируса, у него не возникнет никаких трудностей.

Bitdefender Antivirus Free Edition

Bitdefender – компания с очень хорошей репутацией в мире кибербезопасности. Ее продукты предельно просты, но вместе с тем надежны. Полные комплекты защитных программ компании стоят дорого, но базовый антивирус можно загрузить и использовать бесплатно. Его основное достоинство – очень высокая скорость работы.

Платная версия антивируса Bitdefender в конце прошлого года была названа экспертами AV-TEST одним из лучших защитных продуктов года.

Avira Free Antivirus

Avira Free Antivirus – еще один качественный бесплатный антивирус. Программа имеет удобный планировщик сканирований компьютера, по умолчанию установленный на еженедельную проверку. Также в антивирусе имеется инструмент SearchFree Toolbar, предупреждающий пользователя о потенциально опасных сайтах.

В декабре Avira также вошла в список лучших защитных продуктов года. Согласно данным AV-TEST, на тот момент антивирус распознавал 100% существующих угроз.

Microsoft Windows Defender

Microsoft Windows Defender на удивление качественная защита Microsoft, встроенная в Windows 10 и Windows 8. Она качественно оберегает пользователя от кейлоггеров, троянов, буткитов и прочей заразы, которая норовит прописаться в системе.

По данным AV-TEST, в декабре Microsoft Windows Defender справился почти со всеми вирусами, так что он вполне может использоваться в качестве основного защитного средства системы. Минус такого решения – удобство пользования. Интерфейс Windows Defender далеко не так дружелюбен и удобен, как интерфейс вышеописанных бесплатных антивирусов.

(вгору)

Додаток 23

20.02.2018

Мошенники нацелились на мобильные счета украинцев

Мошенники снова активизировали попытки обчистить мобильные счета украинцев. В социальных сетях люди жалуются на странные смс, в которых их просят подтвердить перевод средств на банковские карты и интернет-игры, которых сами пользователи не инициировали. Операторы говорят, что об этой схеме знают, и призывают абонентов к бдительности (InternetUA).

Суть мошеннической операции проста и строится на сервисе компании Киевстар «Мобильные деньги», которая позволяет оплатить с телефонного счета множество услуг или перевести деньги на банковскую карту. Причем, чтобы инициировать перевод, вовсе необязательно иметь доступ к телефону – оформить платеж можно на сайте компании, указав сумму и номер абонента, с которого будут списаны средства.

У аферистов есть только одно препятствие – чтобы компания-партнер телеком-оператора провела платеж, абонент должен подтвердить операцию, введя в специальное поле временный пароль. Его отправляют смс-сообщением на номер абонента. После нескольких инициаций, мошенник звонит жертве и под разными предлогами пытается выведать заветные 5 цифр.

В Киевстар уверяют, что временный пароль, срок действия которого ограничен 30 минутами, является надежным методом борьбы с мошенниками при соблюдении единственного условия – сообщать кому-бы то ни было этот 5-значный код категорически нельзя. Даже если об этом просит якобы сотрудник телеком-оператора, службы безопасности банка или представитель правоохранительных органов. Заодно в компании напоминают, что не стоит это делать и с прочими кодами и паролями.

(вгору)

Додаток 24

20.02.2018

Любой желающий может стать распространителем вымогательского ПО Saturn

Разработчики вымогательского ПО Saturn позволяют любому желающему бесплатно распространять вредонос, в обмен на перечисления создателям программы часть полученных путем вымогательства средств. Об этом сообщает издание Bleeping Computer (InternetUA).

Вредонос распространяется в рамках программы «вымогательское-ПО-как-услуга» (Ransomware-as-a-Service, RaaS). Для доступа к Saturn нужно зарегистрироваться на размещенном в даркнете сайте, после чего пользователь получит копию программы и сможет начать ее распространение.

В большинстве случаев RaaS-порталы требуют от пользователей сперва заплатить определенную сумму, после чего им будет предоставлен доступ к исходному коду вредоноса. Разработчики Saturn используют совершенно новый подход к данной бизнес-модели, предлагая полностью готовое к использованию ПО без необходимости платить авансом.

Пользователям, получившим доступ к коду Saturn, необходимо внедрить его в другие файлы, такие как EXE, Office, PDF и пр. Распространение осуществляется посредством спама или вредоносных рекламных сообщений.

За расшифровку данных на своих устройствах жертвам вымогателей предлагается перечислить определенную сумму на платежном портале

разработчиков Saturn, расположенном по адресу su34pwhpcafeiztt.onion. На портале указан адрес биткойн-кошелька создателей вредоноса.

В случае если файл, заразивший жертву, был создан на портале RaaS, пользователь, который сгенерировал и распространил его, получит 70 % от суммы выкупа. В свою очередь 30 % отойдут создателям Saturn.

По данным Bleeping Computer, регистрация на сайте разработчиков Saturn все еще открыта.

(вгору)

Додаток 25

19.02.2018

ESET: «полицейские» вымогатели остаются главной угрозой для Android

Вирусная лаборатория ESET представила отчет об актуальных угрозах для платформы Android (Компьютерное Обозрение).

В 2017 г. авторы вредоносных программ для Android продолжали поиск новых инструментов. Наиболее опасное нововведение вирусописателей – использование вредоносным ПО службы специальных возможностей Android Accessibility Service, облегчающей работу с устройством для людей с ограниченными возможностями. Первоначально службу взяли на вооружение авторы мобильных банковских троянов, далее – создатели программ-вымогателей.

В октябре 2017 г. специалисты ESET обнаружили DoubleLocker – первый мобильный шифратор, использующий службу специальных возможностей. Вредоносная программа оснащена сразу двумя инструментами для вымогательства: она шифрует данные в памяти устройства, а также может изменить PIN-код на произвольный.

Несмотря на внедрение новых техник атак, в 2017 г. наиболее популярным инструментом злоумышленников оставались так называемые «полицейские» вымогатели. Они блокируют экран устройства; требование выкупа как правило имитирует официальное сообщение о блокировке за распространение нелицензионного ПО и другие подобные нарушения. По данным ESET, большинство программ-вымогателей, использующих эту уловку, принадлежит к семейству Android/Locker.

Согласно телеметрии ESET, в 2017 г. доля программ-вымогателей для Android снижалась, несмотря на рост общего числа угроз для этой платформы. Тем не менее, в этом году возможны новые всплески активности вымогателей, включая DoubleLocker.

ESET рекомендует пользователям смартфонов и планшетов на Android соблюдать базовые меры предосторожности: загружать приложения только с официальных площадок, изучать отзывы и оценки, защитить устройства современным антивирусным ПО.

(вгору)

Додаток 26

19.02.2018

Уязвимость в Cleverence Mobile SMARTS Server используется для добычи криптовалют

В июле 2017 года специалисты компании «Доктор Веб» обнаружили в серверных приложениях Cleverence Mobile SMARTS Server уязвимость нулевого дня (ITnews).

Разработчики программы выпустили обновление для устранения этой уязвимости, однако ее до сих пор используют злоумышленники для добычи (майнинга) криптовалют.

Приложения семейства Cleverence Mobile SMARTS Server созданы для автоматизации магазинов, складов, различных учреждений и производств. Они предназначены для работы на ПК под управлением Microsoft Windows. В конце июля прошлого года специалисты компании "»октор Веб» обнаружили критическую уязвимость в одном из компонентов Cleverence Mobile SMARTS Server, с использованием которой злоумышленники получают несанкционированный доступ к серверам и устанавливают на них троянцев семейства Trojan.BtcMine, предназначенных для добычи (майнинга) криптовалют. Об этой уязвимости мы незамедлительно сообщили разработчикам программного комплекса.

Изначально киберпреступники использовали несколько версий майнера, детектируемых антивирусом Dr.Web как Trojan.BtcMine.1324, Trojan.BtcMine.1369 и Trojan.BtcMine.1404. На сервер, на котором работает ПО Cleverence Mobile SMARTS Server, злоумышленники отправляют специальным образом сформированный запрос, в результате чего происходит выполнение команды, содержащейся в этом запросе. Взломщики используют команду для создания в системе нового пользователя с административными привилегиями и получают от его имени несанкционированный доступ к серверу по протоколу RDP. В некоторых случаях с помощью утилиты Process Hacker киберпреступники завершают процессы работающих на сервере антивирусов. Получив доступ к системе, они устанавливают в ней троянца-майнера.

Этот троянец представляет собой динамическую библиотеку, которую киберпреступники сохраняют во временную папку и затем запускают. Вредоносная программа заменяет собой одну из легитимных системных служб Windows, выбирая «жертву» по ряду параметров, при этом файл оригинальной службы удаляется. Затем вредоносная служба получает ряд системных привилегий и устанавливает для своего процесса флаг критического. После этого троянец сохраняет на диск необходимые для своей работы файлы и приступает к майнингу криптовалюты, используя аппаратные ресурсы инфицированного сервера.

Несмотря на то, что разработчики Cleverence Mobile SMARTS Server своевременно выпустили обновление, закрывающее уязвимость в программном

комплексе, многие администраторы серверов не торопятся с его установкой, чем и пользуются злоумышленники. Киберпреступники продолжают устанавливать на взломанные ими серверы троянцев-майнеров, постоянно модифицируя их версии. Со второй половины ноября 2017 года злоумышленники начали использовать принципиально нового троянца, которого они совершенствуют и по сей день. Эта вредоносная программа получила название Trojan.BtcMine.1978, она предназначена для добычи криптовалют Monero (XMR) и Aeon.

Майнер запускается в качестве критически важного системного процесса с отображаемым именем «Plug-and-Play Service», при попытке завершить который Windows аварийно прекращает работу и демонстрирует «синий экран смерти» (BSOD). После запуска Trojan.BtcMine.1978 пытается удалить службы антивирусов Dr.Web, Windows Live OneCare, «Антивируса Касперского», ESET Nod32, Emsisoft Anti-Malware, Avira, 360 Total Security и Windows Defender. Затем майнер ищет запущенные на атакуемом компьютере процессы антивирусных программ. В случае успеха он расшифровывает, сохраняет на диск и запускает драйвер, с помощью которого пытается завершить эти процессы. Антивирус Dr.Web успешно обнаруживает и блокирует драйвер Process Hacker, который использует Trojan.BtcMine.1978, – этот драйвер был добавлен в вирусные базы Dr.Web как хакерская утилита (hacktool).

Получив из собственной конфигурации список портов, Trojan.BtcMine.1978 ищет в сетевом окружении роутер. Затем с помощью протокола UPnP он перенаправляет TCP-порт роутера на порты из полученного списка и подключается к ним в ожидании соединений по протоколу HTTP. Необходимые для своей работы настройки вредоносная программа хранит в системном реестре Windows.

В теле майнера содержится список IP-адресов управляющих серверов, которые он проверяет с целью обнаружить активный. Затем троянец настраивает на зараженной машине прокси-серверы, которые будут использоваться для добычи криптовалют. Также Trojan.BtcMine.1978 по команде злоумышленников запускает оболочку PowerShell и перенаправляет ее ввод-вывод на подключающегося к скомпрометированному узлу удаленного пользователя. Это позволяет злоумышленникам выполнять на зараженном сервере различные команды.

Выполнив эти действия, троянец встраивает во все запущенные процессы модуль, предназначенный для добычи криптовалют. Первый процесс, в котором этот модуль начинает работу, и будет использоваться для майнинга Monero (XMR) и Aeon.

(вгору)

Додаток 27

21.02.2018
Ольга Карпенко

Мошенники шлют спам от имени и с серверов украинских интернет-магазинов: как это исправить

Некоторые крупные украинские интернет-магазины столкнулись с необычной механикой мошенничества. Неустановленные лица используют email-базы пользователей в процессе авторизации на сайте магазина так, что в результате пользователь получает письмо от самого магазина, но со спам-ссылкой внутри. В деталях редакции AIN.UA подробности атаки рассказали в интернет-магазине F.ua (бывший Fotos.ua). В результате мошеннических действий письма со спам-ссылками были разосланы по примерно 17000 пользователей магазина. По данным редакции, в ходе атаки могли пострадать и другие магазины, информация сейчас уточняется (AIN.UA).

Атака использует довольно примитивную схему. Она работает в том случае, если после регистрации нового пользователя интернет-магазин шлет ему письмо с напоминанием пароля. Пользователь, имеющий базу email-адресов, регистрирует профиль на сайте магазина по этим же адресам.

Но в поле пароля вместо собственно пароля указывает спамерскую ссылку и приводит такой текст с обещанием легкого заработка: «напоминаем, у вас не израсходованный денежный бонус 1895$ www.qz.eu@pokupki.win#mr.bi. Бонус вы можете снять на банковскую карту или электронный кошелек до 23.02».

В результате пользователь-жертва атаки получает письмо-уведомление о регистрации на сайте магазина – с настоящего адреса магазина. А в поле пароля закономерно отображается спамерский текст с активным линком на другие сайты, где после перехода у пользователя могут попросить личную информацию.

В интернет-магазине сообщили, что на данный момент уязвимость уже устранена. Самый простой способ избавиться от нее: ограничить количество символов для поля пароля. Тем интернет-магазинам, которые хранят базы паролей пользователей в незашифрованном виде, будет проще проверить, попали ли они под это мошенническое действие.

На сейчас неизвестно, проходила ли рассылка по пользователям других крупных интернет-магазинов. В случае если вы получали подобное письмо от интернет-магазина, не переходите по ссылке.

(вгору)

Додаток 28

21.02.2018

Мобильные приложения и смартфоны несут серьезную угрозу

В результате нового расследования выяснилось, что Иран опубликовал в Google Play приложения, которые после скачивания начинают шпионить за владельцами смартфонов (InternetUA).

Немногие осознают, что современный смартфон опасен, так как благодаря очень быстрым процессорам, графическим ускорителям, внушительному объёму памяти и целому набору датчиков эти гаджеты по возможностям не уступают компьютерам, но при этом уязвимы к взлому.

Камеры некоторых смартфонов могут потягаться с обычными цифровыми камерами, а наличие как минимум двух микрофонов легко превращает гаджет в подслушивающее устройство, даже когда владелец полагает, что телефон выключен.

Когда батарея на месте, «шпионские» приложения способны записывать и передавать разговоры.

Некоторые шпионские приложения есть в продаже, и они требуют ручной установки, а другими смартфон оборудуется прямо на заводе.

Кроме того, шпион может проникнуть в гаджет из-за уязвимости в операционной системе или в результате фишинговой атаки.

Снизить риск прослушки практически невозможно: ради большого экрана и тонкого корпуса в некоторые смартфоны устанавливается несъёмная батарея, поэтому полностью «обесточить» такой аппарат не удастся.

Конфиденциальные встречи

Лучший выход – это отказаться от использования смартфонов на конфиденциальных встречах, и тогда разговор не будет перехвачен, однако в целом шпионские возможности девайса такая «стратегия» не ограничивает.

В Пентагоне и других организациях США участников тайных переговоров просят сдавать смартфоны на хранение.

Конечно, это полумера, так как в остальное время шпионский гаджет способен передавать ценную информацию о Пентагоне кому угодно.

Несколько недель назад сотрудникам Белого дома было запрещено пользоваться смартфонами.

Возможно, это несколько запоздалое решение, так как иностранная разведка уже успела получить доступ к телефонным книгам, звонкам, сообщениям, паролям и к другой весьма полезной информации.

Смартфон – это неисчерпаемый источник разведданных.

К примеру, благодаря смартфонам работников Ведомства по патентам и товарным знакам США иностранная разведка и преступники способны украсть идеи важнейших военных или коммерческих изобретений. Это напрямую относится к засекреченным патентам.

Америка и другие страны медленно реагируют на угрозу. Недавно ФБР, ЦРУ, и АНБ США заявили об опасности некоторых моделей смартфонов Huawei и ZTE.

Однако большая часть аппаратов собирается в Китае, и шпионское ПО может быть установлено на заводе на любую модель.

Более того, некоторые производители открыто закачивают в смартфоны приложения с постоянно выскакивающей рекламой.

Логично, что чем дешевле смартфон – тем больше в нём рекламы, однако и на дорогие модели от ведущих компаний может быть установлено «одобренное производителем» шпионское ПО.

Шпионское приложение не всегда можно отличить от рекламного, при этом некоторые из них поддаются лишь частичному удалению, либо не удаляются вовсе.

Приложения для смартфонов очень уязвимы.

Программный код приложений часто состоит из старых и новых элементов, а также из материала, полученного от третьих лиц. Особенно популярен общедоступный код, так как он бесплатен, и некоторые алгоритмы применяются в смартфонах.

Именно поэтому баг Heartbleed пробрался в смартфоны и компьютеры – в криптографическом ПО OpenSSL, которое используется для банковских операций, обнаружилась уязвимость.

Неизвестные источники

Для шифрования широко применялось ПО OpenSSL, источник которого неизвестен.

Используя общедоступный код для приложений систем безопасности, разработчики поступили крайне опрометчиво.

Большая часть приложений создаётся программистами со всего мира, и обнаружить баг или вредоносное ПО не всегда возможно.

Впрочем, недавно Пентагон назвал три безопасных смартфона: Samsung Galaxy с системой Knox, iPhone от Apple и новейший Blackberry. Какими критериями Пентагон руководствовался при выборе – неизвестно.

Пентагон оказался в трудном положении, так как дроны и другие системы часто управляются со смартфона, а сотрудникам не запрещено пользоваться гаджетами.

В магазинах приложений Google Play и Apple Store доступны тысячи приложений, которые невозможно тщательно проверить на принадлежность к шпионскому ПО.

Необходимо создать новую систему безопасности для смартфонов, и этой проблемой должно заняться государство. К сожалению, правительства тратят на шпионаж очень большие деньги, поэтому они не горят желанием бороться с угрозой.

(вгору)

Додаток 29

21.02.2018

Хакери зламали хмару Tesla, щоб майнити криптовалюту

Аккаунт Tesla в хмарному сервісі Amazon зламали невідомі хакери. Проте вони не стали нічого викрадати, а просто налаштували потужність хмари на видобуток криптовалюти (Espreso.tv).

Про це повідомила компанія Redlock, що займається кібербезпекою.

Фахівці Redlock виявили факт злому Tesla ще в січні. Вони шукали власника аккаунта Amazon Web Services, який опублікував дані для використання хмари у відкритому доступі. З'ясувалося, що витік стався з компанії Маска.

Хакери отримали доступ до Tesla завдяки консолі Kubernetes, яка призначена для оптимізації хмарних додатків. Вона була не захищена паролем, і там зберігалися дані до аккаунт компанії.

Отримавши доступ до профілю вони могли заволодіти будь-якою «хмарною» інформацією, включаючи особливо «чутливі» дані, такі як телеметрія машин. Однак компанія відразу зв'язалися з Tesla, яка швидко виправила ситуацію: дані клієнтів не постраждали.

«Ми перевірили вразливість через кілька годин після отримання інформації. Судячи з усього, атака торкнулася тільки внутрішніх тестів машини. Наше внутрішнє розслідування не виявило порушення безпеки даних клієнтів і машин», – заявив представник Tesla.

За даними RedLock, майнінг для зловмисників був цінніше, ніж будь-які дані, які зберігалися в хмарі Tesla. Проте, вони налаштували шкідливий скрипт так, щоб він працював непомітно і споживав незначні потужності обладнання. Також вони використовували нестандартний інтернет-порт, а свої IP-адреси приховали за допомогою сервісу Cloudflare.

Фахівці відзначили, що в 58 % організацій зараз використовують публічні хмарні сервіси такі як AWS, Microsoft Azure і Google Cloud і як мінімум 8 % компаній стикаються з подібними інцидентами.

«Нещодавній зліт криптовалюти зробив більш прибутковим для хакерів крадіжку потужностей, а не даних компаній. Публічні хмари є ідеальною метою, адже ефективних програм для їх захисту не існує», – каже Гура Кумар, техдиректор RedLock.

(вгору)

Додаток 30

22.02.2018
Криптомайнеры все чаще атакуют компании

Компания Check Point Software Technologies предупреждает, что вредоносное ПО для майнинга криптовалюты продолжает атаковать организации во всем мире (Компьютерное Обозрение).

В январе исследователи Check Point выявили три различных варианта вредоносных криптомайнеров, вошедших в топ-10 активных зловредов. Возглавил рейтинг CoinHive, который атаковал каждую четвертую компанию в январе. CoinHive способен в тайне от пользователя добывать криптовалюту Monero, когда тот посещает веб-сайты. CoinHive внедряет JavaScript, который затем использует мощности процессора ПК пользователя, чтобы добывать криптовалюту, таким образом сильно снижая его производительность. Также

в рейтинг попали майнеры JSEcoin и Cryptoloot, которые добывают криптовалюту без ведома жертвы.

Кроме вредоносного ПО для майнинга криптовалюты, исследователи Check Point обнаружили, что 21 % организаций до сих пор имеют зараженные Fireball рабочие станции. Fireball может использоваться как полноценный загрузчик, способный запускать любой вредоносный код на компьютере жертвы. Впервые зловред обнаружили в мае 2017 г., а летом он уже нанес серьезный удар по компаниям.

Самые активные мобильные зловреды января:

- Lokibot – банковский троян для Android, который крадет пользовательские данные и требует за них выкуп. Зловред может заблокировать телефон, если удалить его права администратора.
- Triada – модульный бэкдор для Android, который дает огромные привилегии скачанным зловредам.
- Hiddad – зловред для Android, который переупаковывает легитимные приложения и затем реализует их в магазинах сторонних производителей.

(вгору)

Додаток 31

25.02.2018

Хакеры продают легитимные цифровые сертификаты для вредоносного ПО

Хакеры продают легитимные цифровые сертификаты для подписи вредоносного ПО. Об этом сообщили исследователи безопасности из команды Insikt Group компании Recorded Future (InternetUA).

Сертификаты предназначены для цифровой подписи программного обеспечения разработчиками. Сертификат позволяет гарантировать пользователям, что код и содержимое являются безопасными для загрузки и установки. Большинство современных операционных систем по умолчанию запускают только подписанные приложения.

Приложения с цифровой подписью сложно обнаружить с помощью решений сетевой безопасности. Согласно исследованию, оборудование, использующее технологию DPI (deep packet inspection, углубленная проверка пакетов) для сканирования сетевого трафика, становится менее эффективным, если вредоносное ПО использует легитимный сертификат.

Специалисты выявили подпольный рынок по продаже легитимных сертификатов. Их стоимость варьируется от $299 до $1599 и выше за сертификаты расширенной проверки (Extended Validation Certificate, EV). Ассортимент включает сертификаты, выданные авторитетными центрами сертификации (ЦС), такими как Comodo, Symantec, Thawte и Apple.

Одним из первых сертификаты для вредоносного ПО начал предлагать хакер под псевдонимом C@T. В марте 2015 года C@T предложил для продажи сертификаты Microsoft для подписи 32/64-битных версий различных исполняемых файлов, а также Microsoft Office, Microsoft VBA, Netscape Object

Signing и Marimba Channel Signing. По его словам, сертификаты были выданы авторитетными ЦС.

Примерно через два года еще три хакера начали предлагать услуги по продаже сертификатов на русскоязычных подпольных форумах. Из них двое до сих пор активно поставляют сертификаты злоумышленникам. Стандартные сертификаты подписи кода, выпущенные Comodo, которые не включают рейтинг репутации SmartScreen стоят $295. Покупателю, заинтересованному в сертификате расширенной проверки, выпущенном Symantec, придется заплатить $1599, что на 230% процентов выше по сравнению с ценой сертификата от ЦС. Оптовые покупатели могут купить полностью аутентифицированные домены с EV SSL-сертификатами и возможностью подписи кода за $1799. При этом все сертификаты создаются для каждого покупателя индивидуально на основе данных, похищенных у различных компаний.

(вгору)

Додаток 32

27.02.2018

Avast представил новое решение Smart Life для безопасности IoT-устройств

Компания Avast представила платформу Smart Life, решение для защиты цифровой информации на базе IoT (ITnews).

Smart Life использует технологию Искусственного интеллекта (Artificial Intelligence) для определения и устранения угроз. Avast предлагает заказчикам и поставщикам решение Smart Life в качестве программного обеспечения как услуги (Software-as-a-Service). Предложение упрощает пользователям и малым предприятиям защиту IoT-устройств, сетей и конфиденциальных данных дома, в офисе и вне его.

По прогнозам, число IoT-устройств к 2025 году увеличится втрое: эксперты ожидают более 75 млрд подключенных к интернету устройств. Производители спешат выпустить умные устройства на рынок по доступной цене, однако некоторые пренебрегают защитой и системами безопасности производимых девайсов. Платформа Smart Life предназначена для защиты этих IoT-устройств от кибератак.

«Мы активно пользуемся устройствами интернета вещей дома и на работе, однако их безопасность до сих пор не идеальна. Это значит, что пользователи и сегодня остаются под угрозой, – отмечает Гаган Сингх (Gagan Singh), старший вице-президент и генеральный директор департамента мобильных разработок Avast. – Ожидания пользователей возрастают: мы хотим получать комфорт и удовольствие от использования умных гаджетов. Поэтому перед производителями встает вопрос обеспечения безопасности умных устройств».

Avast получает данные от 400 млн активных пользователей со всего мира о работе IoT-устройств. Благодаря этому механизм машинного обучения постоянно накапливает опыт, что позволяет оперативно определять и противодействовать различным нарушениям, ботнетам и другим угрозам устройств интернета вещей. При разработке платформы Smart Life одним из приоритетов стало создание защиты, которую легко использовать для обеспечения безопасности IoT-сетей и устройств.

Многие умные устройства могут быть взломаны злоумышленниками, в том числе системы регулирования отопления, умные динамики, веб-камеры и другие гаджеты, поэтому обычные пользователи и малый бизнес очень уязвимы. Один из наиболее распространенных типов атак – киберпреступники атакуют тысячи умных устройств ничего не подозревающих жертв, чтобы создать ботнет для атаки на других. И в будущем число подобных киберпреступлений будет расти наряду с хищением личных данных и угрозами физической безопасности.

Если IoT-устройство проявляет подозрительную активность и передает большие объемы данных неизвестному адресу, Smart Life незамедлительно прекращает передачу трафика и уведомляет хозяина об обнаруженной странной активности. По мере развертывания услуги, будут доступны дополнительные функции, такие как возможность приостановить доступ к интернету, ограничить время работы монитора, добавить строгую фильтрацию контента.

(вгору)

Додаток 33

27.02.2018

Ольга Карпенко

Уязвимость на сайте МАУ выдавала данные о пассажирах по коду брони, сейчас она уже закрыта

На «Хабрахабре» 26 февраля появилась статья об уязвимости на сайте Международных Авиалиний Украины (МАУ). И хотя сама уязвимость уже закрыта, механизм ее работы – достаточно примечателен. Пользователь под ником dinikin описал, как с помощью кода бронирования (PNR, passenger name record) можно было получить данные любого пассажира рейса (AIN.UA).

По словам автора статьи, попав на сайт авиакомпании, он открыл инструменты разработчика в Google Chrome, чтобы понять, почему сайт долго грузится. «Изучив запросы к серверу, я увидел, что данные о доступных местах сервером возвращаются. Опробовав несколько разных браузеров, я так и не решил проблему, однако заметил, что запрос, который возвращает список доступных мест, выполнялся во всех браузерах успешно, не смотря на то, что сессионные куки были доступны только в Google Chrome», – пишет он. Запрос к серверу выглядел так:

https://bookapi.flyuia.com/ancillary/seatmap?pnr=XXXXXX&currency=USD&flyuiacountrycode=uk&flyuialanguagecode=ru&locale=RU

XXXXXX – это и есть код бронирования или же PNR. Ответ сервера во всех браузерах содержал данные о пассажире, которому принадлежит PNR – имя, класс, номер рейса, время отлета, место прибытия и так далее.

То есть, зная только код бронирования, можно было получить практически все данные о пассажире. Автор статьи пишет, что продолжая оформлять билет, выбрал пункт заказа места для багажа. В этом случае запрос имел вид https://bookapi.flyuia.com/ancillary/luggage?pnr=XXXXXX&currency=USD&locale=RU, а ответ сервера содержал еще и дату рождения пассажира. Переходя к странице оплаты, автор заметил ту же закономерность. На запрос https://bookapi.flyuia.com/payportal/transaction/123456?flyuiacountrycode=ua&flyuialanguagecode=ru&locale=RU сервер компании отдавал данные о платеже.

По словам автора статьи, на устранение уязвимости у компании ушел примерно месяц, и на момент выхода статьи ею воспользоваться было уже нельзя.

Редакция ожидает официального комментария об уязвимости от компании МАУ.

(вгору)

Соціальні мережі

як чинник інформаційної безпеки

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

Упорядник **Терещенко** Ірина Юріївна

Редактор О. Федоренко

Свідоцтво про державну реєстрацію КВ № 5358 від 03.08.2001 р.

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