СОЦІАЛЬНІ МЕРЕЖІ ЯК ЧИННИК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Огляд інтернет-ресурсів
(24.05–6.06)

2018 № 11

Соціальні мережі
як чинник інформаційної безпеки

Інформаційно-аналітичний бюлетень
Додаток до журналу «Україна: події, факти, коментарі»
Огляд інтернет-ресурсів
(24.05–6.06)
№ 11

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

РОЗВИТОК І ПЕРСПЕКТИВИ СОЦІАЛЬНИХ МЕРЕЖ 4
СОЦІАЛЬНІ МЕРЕЖІ ЯК ВИЯВ ФОРМУВАННЯ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА 9
БІЗНЕС І СОЦІАЛЬНІ МЕРЕЖІ 11
СОЦІАЛЬНІ МЕРЕЖІ І ПРОБЛЕМИ СУСПІЛЬНОЇ БЕЗПЕКИ 14
Інформаційно-психологічний вплив мережевого спілкування на особистість 14
Маніпулятивні технології 16
Спецслужби і технології «соціального контролю» 17
Проблема захисту даних. DDOS та вірусні атаки 23
ДОДАТКИ 32

Орфографія та стилістика матеріалів – авторські

РОЗВИТОК І ПЕРСПЕКТИВИ СОЦІАЛЬНИХ МЕРЕЖ

24.05.2018

Каждую минуту в Viber регистрируются 2 тысячи новых пользователей

Представители одного из самых популярных в Украине мессенджеров Viber поделились результатами использования своего сервиса. В частности, по их данным пользователи проводят в мессенджере на 69 % времени больше по сравнению с 2017 годом. Они совершают более 7 млн действий в минуту, включая 2 тысячи новых регистраций, 7 тысяч лайков и 1,5 млн отправлений фото.

Докладніше

***

29.05.2018

Популярность мобильной версии Telegram в РФ за апрель выросла на 31 %

В апреле 2018 года российская аудитория мобильного приложения Telegram выросла на 31 % и достигла максимума с начала измерений, сообщили изданию РБК в исследовательской компании Mediascope (InternetUA).

Усредненное число россиян, хотя бы раз в день заходивших в мобильное приложение мессенджера, достигло, согласно измерениям Mediascope, более 3,7 млн человек в возрасте 12–64 лет, проживающих в городах с населением от 100 тыс. человек.

В октябре 2017 года, когда Mediascope впервые произвела подсчеты аудитории мобильного приложения Telegram, число пользователей не превышало 2,2 млн человек, в марте 2018-го – 2,8 млн.

В Москве по сравнению с мартом аудитория выросла на 45 %.

Данные Mediascope не дают представления, что делали пользователи в приложении, измеритель фиксирует лишь факт захода.

Данные по аудитории Telegram на стационарных компьютерах и ноутбуках в исследовательской компании не предоставили.

Mediascope – официальный измеритель телевизионной аудитории в России, занимается также исследованиями в сфере мобильных коммуникаций.

Аудитория мобильного приложения Telegram резко выросла в месяц, когда Роскомнадзор добивался блокировки мессенджера через суд.

***

29.05.2018

Михаил Сапитон
Как выглядит Android-аудитория украинского Telegram

Агентство TNS Ukraine провело исследование аудитории мессенджера Telegram среди украинских Android-юзеров. Данные собраны по состоянию на май 2018 года. В выборку попали города с населением более 50 000 человек и пользователи в возрасте от 16 до 55 лет (AIN.UA).

Указывается, что Telegram – третий по популярности мессенджер в стране, после Viber и Facebook Messenger. Гендерная разбивка почти равная – 51 % мужчин и 49 % женщин. Больше всего пользователей в возрасте от 16 до 25 лет – 44 %. Остальные возрастные группы менее многочисленны: 26-35 лет (31 %), 36-45 лет (21 %) и 46-55 (4 %).

Активнее всего мессенджером пользуются в Киеве – жители столицы составляют почти четверть (23 %) юзеров. Еще одна значительная группа – студенты (18 %). Также сообщается, что 17 % Android-пользователей Telegram не смотрят телевизор и еще 34 % не слушают радио. При этом они активнее других употребляют крепкий алкоголь – доля любителей виски составила 19 %, что выше показателя для мобильной аудитории в целом, объяснили в TNS.

***

30.05.2018
Пользователи WhatsApp обнаружили в мессенджере новые функции

Пользователи популярного мессенджера WhatsApp сообщают о появлении в приложении давно ожидаемых функций, анонсированных в начале этого месяца на конференции для разработчиков F8. Пока нововведения доступны лишь на некоторых устройствах под управлением iOS и Android (InternetUA).

Некоторые пользователи iOS и Android уже обнаружили в WhatsApp возможность совершения групповых аудио- и видеозвонков. Судя по всему, функция работает на стороне сервера, поэтому доступ к ней появляется даже без обновления мобильного клиента.

Во время разговора с человеком в верхнем правом углу появляется иконка добавления других участников. Нажав на неё, можно пригласить ещё двух пользователей из списка контактов. Таким образом, максимальное количество участников звонка – четыре человека.

Когда новые функции станут доступны всем пользователям WhatsApp – неизвестно.

***

29.05.2018
Немецкий разработчик «научил» YouTube останавливать видео при отводе взгляда

Чтобы Chrome начал следить за пользователем через веб-камеру, нужно установить специальные настройки (IGate).

Немецкий разработчик Маттиас Хеммингссон разработал расширение для Google Chrome, которое ставит на паузу видео на YouTube, когда пользователь отворачивается от экрана. Об этом пишет Gizmodo.

Для отслеживания лица система использует встроенный FaceDetector API браузера и веб-камеру устройства. По словам журналистов и пользователей, система не всегда точно обнаруживает лицо.

Чтобы воспользоваться расширением, нужно скачать его из магазина, зайти в раздел chrome://flags и включить экспериментальные функции веб-платформы. Для того, чтобы новые настройки вступили в силу, нужно перезапустить браузер.

При открытии видео на YouTube в правом нижнем углу должно появиться поле с переключателем, при нажатии которого браузер запросит доступ к веб-камере. После согласия в том же поле отобразится окошко с картинкой с камеры, где лицо пользователя будет выделяться зелёным квадратом. Чтобы отключить систему от веб-камеры, нужно переключить тумблер в неактивное положение.

***

1.06.2018

В Китае разрешили семьям разводиться через WeChat

В самом популярном в Китае мессенджере WeChat с активной аудиторией более 1 млрд человек и огромным количеством дополнительных инструментов можно будет официально регистрировать разводы, но пока только в провинции Гуандун. Об этом пишет The Business Insider (InternetUA).

Для того, чтобы подать заявку на развод, пользователям необходимо просто нажать на специальную кнопку в личных настройках, после чего подтвердить свою личность. Несмотря на это, китайцам пока все равно придется придти в народный суд для завершения процесса развода.

Подача на развод – лишь одна из многих новых функций WeChat. Пользователи в провинции могут хранить водительские удостоверения в мессенджере, а также использовать его как копию паспорта, или управлять своими налоговыми документами. Кроме того, жители Китая при помощи WeChat могут подать заявку на получение разрешения на свадьбу.

Похоже, что власти Китая намерены создать на базе платформы WeChat идентификационную карту, которая заменит все официальные документы, а также резко упразднит огромное количество бюрократических процедур.

***

1.06.2018

Reddit обогнал Facebook по популярности в США

Социальная платформа Reddit обогнала Facebook по популярности среди жителей США. Об этом говорится в рейтинге исследовательской компании Alexa, которая принадлежит Amazon (IGate).

Первые две строчки занимают Google и YouTube, Reddit удалось занять третью строчку, сместив Facebook на четвёртое место. Пятерку лидеров замыкает сайт Amazon.

По данным Alexa, в среднем в день пользователи проводят на Reddit 15 минут, на Facebook – почти 11 минут, на Google и YouTube – по семь и восемь минут соответственно.

В мировом рейтинге Facebook продолжает занимать третье место, а Reddit находится на шестой строчке. В апреле 2018 года соцсеть отчиталась о росте аудитории до 2,2 млрд пользователей в месяц, при этом большая часть аудитории Facebook пользуется мобильными приложениями.

Рейтинг Alexa формируется на основе ежемесячного трафика сайтов: система учитывает число просмотренных пользователями страниц и среднюю ежедневную посещаемость, говорится на сайте компании.

***

4.06.2018

Аналитики представили результаты исследования аудитории Telegram в Украине

Украинский представитель компании маркетинговых исследований TNS – ООО «Тейлор Нельсон Софрез Украина» – провел анализ украинской аудитории мессенджера Telegram и представил его результаты в формате инфографики (Телекритика).

Данные, полученные Kantar TNS CMeter, базируются на исследовании пользователей Android в возрасте 16-55 лет, проживающих в городах с населением более 50 тыс. человек (представленные ниже показатели отражают данные по состоянию на апрель 2018 года).

Выяснилось, что Telegram занимает 3 место в рейтинге мессенджеров, которыми пользуются в Украине. Его опережают Viber и Facebook Messenger. Несмотря на то, что Telegram в Украине уже успел стать нишевым мессенджером для айтишников, криптовалютчиков, представителей медиа и пиара, обычные пользователи все еще предпочитают ему привычный мессенджер в Facebook и давно завоевавший свою аудиторию Viber.

Заметной особенностью аудитории приложения Telegram в Украине является возраст – 16-25 лет (44 % от общего числа). Второй по количеству стала возрастная группа 36-45 лет. Интересно, что 46 % юзеров не состоят в браке, а 23 % пользователей Telegram в Украине проживают в Киеве.

***

4.06.2018

Instagram развенчал распространенные мифы относительно алгоритма ленты

В выходные Instagram пригласил журналистов в свой офис в Сан-Франциско, чтобы рассказать о работе алгоритма. Как объяснил глава продукта Джулиан Гутман, система на основе машинного обучения ранжирует посты исходя из поведения пользователя. Даже если вы следуете за людьми и брендами как другой пользователь, вы будете видеть другой порядок фото и видео. Приложение отдает приоритет постам на основе своих прогнозов, какие посты вас больше всего интересуют, насколько близки вы с человеком, за которым следуете, и как часто загружаете посты. Система также берет во внимание частоту захода в Instagram и длительность нахождения в сети, чтобы определить, какие посты показать первыми. Команда также развеяла некоторые мифы относительно функций алгоритма. К примеру, Instagram не отдает приоритет бизнес-аккаунтам над личными аккаунтами. Сеть также не продвигает пользователей, которые пользуются такими функциями как Stories и Live. Также она не отдает предпочтение фото или видеоформатам, она ранжирует контент в зависимости от того, с какими постами вы чаще взаимодействуете. Если в вашей ленте появилось больше видео, значит ваше поведение в браузере говорит о том, что вы смотрите много видео. Более того, Instagram не понижает аккаунты, которые размещают посты слишком часто, но может вставлять их контент между постами других пользователей. Сеть также не прячет посты с большим количеством хэштегов (Marketing Media Review).

***

5.06.2018
В Viber появились новые функции

Мессенджер Viber объявил о появлении новых дополнений для чатов: «Яркие сообщения», «Избранное» и «Местоположение». Функции станут доступны постепенно для всех пользователей в разных странах в мобильном приложении Viber для iPhone и Android.

Докладніше

***

6.06.2018
Ошибка в работе WhatsApp разозлила пользователей

Пользователи WhatsApp столкнулись с неприятной особенностью поведения программы, которая появилась, по всей видимости, после обновления мессенджера (InternetUA).

По словам владельцев iPhone, которые пользуются приложением, в уведомлениях на разблокированном экране не отображаются имена

отправителей сообщений и миниатюры. Вместо них видно лишь название мессенджера и надпись Message («Сообщение»).

Как пишет Mirror, устранить проблему достаточно просто. В настройках WhatsApp нужно открыть раздел «Уведомления», а затем передвинуть ползунок вправо напротив пункта «Показывать миниатюры». После этого в настройках уведомлений iPhone найти WhatsApp и в разделе «Показ миниатюр» выбрать параметр «Никогда».

СОЦІАЛЬНІ МЕРЕЖІ ЯК ВИЯВ ФОРМУВАННЯ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА

26.05.2018

Активист надеется отсудить у Google и Facebook до $8,8 млрд

С 25 мая в Евросоюзе вступил в силу новый регламент защиты персональных данных, известный как General Data Protection Regulation (GDPR). В первый же день работы закона австрийский юрист и борец за защиту данных Макс Шремс подал жалобы против Google, Facebook, Instagram и WhatsApp от имени некоммерческой организации None of Your Business («Не ваше дело»).

Докладніше

***

31.05.2018

У соцмережах бурхливо відреагували на «воскресіння» Аркадія Бабченка

Ірина Батюк

Інсценування убивства відомого журналіста, здається, не залишило байдужих. Президент Петро Порошенко навіть подякував українцям за небайдужість: «Сьогодні мільйони людей святкують третій день народження Аркадія Бабченко як день народження України, день народження усієї нації, яка надзвичайно класно склала іспит на державність. Дякую всім українцям, які проявили небайдужість, були готові боротися і діяти, щоби зберегти країну», – написав він.

Голова Українського інституту національної пам’яті вважає, що варто подякувати СБУ за збереження життя журналіста: «Треба вміти дякувати і нині добра нагода подякувати СБУ за роботу».

Не приховував своєї радості і лідер «Радикальної партії» Олег Ляшко.

Про те, як їх втішила новина про «воскресіння» Аркадія Бабченка, пише багато українців. А от медійників ця новина збурила. Та в основному українці жартували з новини. Соцмережі рясніють анекдотами і фотожартами.

***

30.05.2018

Гройсмана висміяли за «продуктивність» у соцмережах

У соцмережі висміяли статус прем'єр-міністра Володимира Гройсмана, в якому він зрадів новому мільярдному кредиту.

Про це повідомляє НАРОДНА ПРАВДА з посиланням на Facebook Віктора Скаршевський.

Напередодні Гройсман поставив позначку «радісно продуктивний» наступній своїй публікації: «Сьогодні орган Єврокомісії КОРЕПЕР затвердив рішення про виділення макрофінансової допомоги в розмірі 1 млрд євро для України. Цінную допомогу наших європейських партнерів».

Коментатори не зрозуміли, чому прем'єр зрадів новим кредитам, тобто боргам.

«Як ви думаєте, в яких одиницях Володимир Гройсман вимірює свою продуктивність? У мільярдах євро нових боргів. Не вірите? Подивіться скрін з його фейсбук-сторінки 40-хвилинної давності. Зверніть увагу, що він не просто продуктивний, а дуже радісно продуктивний», – пише Скаршевський.

***

28.05.2018

Фанати Ліги чемпіонів масово дякують у соцмережах киянам за безкоштовне житло

Футбольні фани, яких через неймовірне подорожчання готелів у Києві безкоштовно приймали вдома кияни, із самого ранку пишуть в соцмережах слова захоплення та вдячності (internet.ua).

Про це повідомляє телеканал «Київ».

Фани дякують за те, що їх безкоштовно прихистили у Києві, за чудові враження і навіть зізнаються у коханні Києву та його жителям.

«Дякуємо, добрі, щедрі, красиві люди!» – «Ви влаштували ідеальний прийом!» – «Ми назавжди запам'ятаємо цю поїздку!» – «Це неймовірно, Україна найкраща, дуже дякуємо!», – пишуть уболівальники «Реала» та «Ліверпуля».

***

2.06.2018

NYT рассказала, как Трамп своим твитом нарушил протокол

Президент США Дональд Трамп нарушил протокол одним своим твитом. Об этом пишет The New York Times (InternetUA).

Газета указывает, что американское Бюро трудовой статистики в первую пятницу каждого месяца выпускает отчет о занятости населения. Вечером за

день до публикации отчета с ним знакомятся официальные лица, в том числе президент США. Им запрещено раскрывать информацию до ее обнародования.

Однако утром 1 июня Трамп за час до публикации отчета написал твит, в котором сообщил, что с нетерпением ждет статистических данных по занятости в мае. Пользователи сочли, что президент таким образом сигнализировал о положительных результатах. Отчет подтвердил предположения: в мае число рабочих мест США увеличилось на 223 тыс.

Издание со ссылкой на экспертов указывает, что Трамп нарушил протокол и злоупотребил своим положением, поскольку его твит стал инсайдерской информацией и мог повлиять на фондовые рынки.

В то же время в Белом доме отметили, что Трамп никаких законов не нарушал.

***

6.06.2018

Дмитрий Демченко

В сети появился сайт, где можно «наказать» депутата, пожертвовав деньги на Facebook-рекламу его проступков

«Центр противодействия коррупции» запустил сайт «Серпом по рейтингу». Здесь можно «наказать» депутата-мажоритарщика, пожертвовав деньги на рассказ о его коррупционных схемах среди избирателей.

Докладніше

***

6.06.2018

Міська рада – у соцмережах

Відтепер дізнаватися актуальну та важливу інформацію тернополяни зможуть також на офіційних сторінках Тернопільської міської ради у соціальних мережах (Тернопільська липа).

Зокрема, акаунти можна знайти:

Twitter https://twitter.com/ternopil_rada

Facebook https://www.facebook.com/Ternopil.rada/

Instagram https://www.instagram.com/ternopil_rada/

Відеоматеріали можна переглянути на нашому YouTube-каналі https://www.youtube.com/channel/UCFf6yPT6DBb0tshW2S_aJMA

БІЗНЕС І СОЦІАЛЬНІ МЕРЕЖІ

24.05.2018

Ирина Фоменко

Через Facebook теперь можно нанимать уборщиков и сантехников

Facebook запускает новую функцию по обслуживанию на дому в разделе Marketplace для пользователей США, пишет The Verge. Marketplace – это отдельный раздел торговли на Facebook, который дает возможность пользователям связываться друг с другом для покупки, продажи и обмена товарами. В последнее время компания даже добавила функцию для поиска жилья или покупки автомобиля. С новой категорией домашних услуг пользователи теперь могут нанимать сантехников и уборщиков. Facebook будет сотрудничать с Handy, HomeAdvisor и Porch в этой сфере (InternetUA).

«Люди заинтересованы в рекомендациях по обслуживанию на дому», – заявил вице-президент Marketplace Деб Лю.

Facebook также предлагает информацию о ценах с возможностью сразу отправить запрос нескольким поставщикам услуг на Marketplace. С этой функцией можно использовать Messenger для контакта с нужными людьми.

Чтобы использовать эту функцию, просто кликните Marketplace Services в меню Marketplace на Facebook. Выберите желаемую услугу, и Facebook задаст вам несколько вопросов для сужения результатов поиска. Например, при выборе уборщика, Facebook спрашивает о регулярности уборки, сколько комнат нужно убрать, насколько большой дом и какое время вам подходит. Затем вы вводите свой почтовый индекс, а Facebook предоставляет список людей и компаний, которые могут выполнить ваш запрос. Пользователи могут просматривать профили, чтобы узнать больше о фирме или отдельном лице, включая рейтинги и обзоры.

***

30.05.2018
Услуги ПУМБ теперь можно заказать через Viber

Первый Украинский Международный Банк (ПУМБ) уже запустил для своих розничных клиентов канал коммуникации в мессенджере Viber.

Докладніше

***

30.05.2018
Ирина Фоменко
WhatsApp Pay выходит на индийский рынок

Facebook Inc. предложит платежный сервис WhatsApp жителям Индии уже в июне, сообщает Bloomberg (InternetUA).

Мессенджер будет работать вместе с HDFC Bank Ltd., ICICI Bank Ltd. и Axis Bank Ltd. для обработки переводов, а Государственный банк Индии присоединится, когда у него появятся необходимые системы. Изначально

Facebook планировал сотрудничество с четырьмя партнерами, но решил продолжить работу только с тремя из-за конкуренции.

Выход WhatsApp на индийский рынок эксперты сравнивают с WeChat, изменившим систему платежей в Китае, когда помимо обмена сообщениями у приложения появились дополнительные функции. Экспериментальная версия WhatsApp Pay – стартовавшая с 1 млн пользователей в феврале – получила восторженные отзывы, и теперь сервис является серьезной угрозой для Google Tez и Alibaba, поддерживаемых Paytm, у которых нет преимуществ социальной сети.

«У WhatsApp отличная отправная точка: монополия в чате. Это серьезный конкурент на рынке», – прокомментировал лидер в области финансовых технологий в PwC India Вивек Белгави.

Более 200 миллионов индийцев уже используют WhatsApp – количество пользователей Индии эквивалентно 60 % населения США. По оценкам Forrester Inc., WhatsApp пользуются примерно в 20 раз больше, чем Paytm.

***

29.05.2018

Конец SMM: читатели СМИ перестали заходить на свои любимые сайты через Facebook

Согласно данным Chartbeat, с октября 2017 года большая часть мобильной аудитории заходит на сайты и в приложения СМИ чаще всего напрямую, реже – через социальные платформы вроде Facebook (Телекритика).

После смены алгоритма в Facebook СМИ стало сложнее продвигать свои материалы широкому кругу читателей. И если раньше издатели пытались при помощи Facebook заставить людей переходить на свои сайты, то сейчас ситуация изменилась: показатели заходов напрямую на сайт гораздо выше, чем через соцсеть.

По данным компании Chartbeat, количество еженедельных просмотров веб-страниц выросло с 1 октября, в то время, как показатели просмотров страниц СМИ в Facebook уменьшились.

Со времени смены алгоритма в прошлом году Facebook стал предоставлять издателям меньше трафика. Эта же тенденция продолжается в 2018 году. В январе платформа заявила, что будет делать посты друзей в ленте более приоритетными, чем посты массмедиа.

Как отмечают специалисты Chartbeat, нет четкой корреляции между уменьшением трафика от Facebook и увеличением заходов на сайты напрямую.

У Chartbeat не было окончательных выводов о том, почему прямой трафик увеличился. Конечно, количество мобильных пользователей растет, и не стоит забывать, что большая часть мобильного трафика все еще связана с Facebook.

Эксперты издания Digiday пишут о том, что мобильные телефоны и устройства являются значительным фактором выработки у читателей и зрителей новых медиа-привычек.

***

5.06.2018

Генпрокурор штата Вашингтон подал иск против Facebook

В США генпрокурор штата Вашингтон Боб Фергюсон подал судебные иски в отношении компаний Facebook и Google из-за несоблюдения закона о политической рекламе. Об этом сообщается на сайте прокуратуры штата (InternetUA).

«Роберт Фергюсон подал в суд иски о финансировании избирательных кампаний, в которых говорится, что Facebook и Google не сохраняли требуемую законом информацию, касающуюся политической рекламы в штате Вашингтон», – говорится в сообщении.

По данным генпрокурора, указанные компании не предоставляли информацию об организациях, спонсировавших рекламу. А также не сообщали ее стоимость и дату размещения.

***

6.06.2018

Эксперты заподозрили Google и Facebook в недобросовестной конкуренции из-за запрета рекламы криптовалют

В марте этого года холдинг Alphabet, владеющий компанией Google, объявил, что в июне интернет-поисковик введет запрет на рекламу криптовалют и иных спекулятивных финансовых инструментов, включая бинарные опционы и финансовые пари. Аналогичные запреты также ввели сервис микроблогов Twitter и соцсеть Facebook.

Докладніше

СОЦІАЛЬНІ МЕРЕЖІ І ПРОБЛЕМИ СУСПІЛЬНОЇ БЕЗПЕКИ

Інформаційно-психологічний вплив мережевого спілкування на особистість

29.05.2018

Эксперты: люди стали проводить в Интернете больше времени, чем в реальности

Агентство Zenith выявило, что 70 % от общего времени бодрствования средний человек проводит в Интернете. Эксперты компании также спрогнозировали, что в будущем ситуация только усугубится (Телекритика).

Благодаря широкому распространению мобильных устройств время, затрачиваемое пользователями на потребление материалов медиа, растет.

По словам руководителя отдела прогнозирования Zenith Джонатана Барнарда, максимальное время, проводимое человеком в Интернете, сегодня примерно равно суммарному времени бодрствования. Однако по мере того, как развиваются новые технологии – особенно подключение 5G и интернет вещей (internet of things), «верхний предел потребления медиа», по словам Барнарда, в скором времени будет ограничен только сном.

Согласно данным Бюро статистики труда США, средний американец проводит в состоянии бодрствования 912 минут в день (примерно 15 часов). По прогнозу агентства Zenith, средний американец будет тратить на потребление медиаконтента 636,6 минуты ежедневно (70 % времени).

Барнард отметил, что уже в течение следующих двух лет люди будут тратить еще 13 дополнительных минут в сутки на медиа.

***

5.06.2018

Підлітки назвали свої улюблені соцмережі // Згідно даних, отриманих під час опитування, чіткого консенсусу серед підлітків щодо впливу соцмереж на життя немає

YouTube, Instagram та Snapchat – найпопулярніші онлайн-платформи серед підлітків. 95% з них мають доступ до смарфонів та 45% – майже постійно онлайн, – повідомляє 1NEWS.

На це вказує останнє дослідження, проведене серед підлітків Великої Британії віком 13-17 років. Згідно даних, отриманих під час опитування, чіткого консенсусу серед підлітків щодо впливу соцмереж на життя немає.

31 % з них оцінюють цей вплив позитивно. При цьому переважна більшість із них вибрали цей варіант, бо вважають, що соцмережі допомагають залишалися на зв’язку з рідними і друзями.

24 % – негативно. З них переважна більшість вважає, що у соцмережах популярне цькування і поширюється багато чуток.

Ще 45 % відповіли, що не оцінюють вплив соцмереж ані позитивно, ані негативно.

Крім того, якщо у 2014-2015 роках найбільш популярною соцмережею серед підлітків був Facebook. Ним користувалися 71 % з них, тоді як сьогодні – 51 %.

Найчастіше молоді люди Великобританії використовують Snapchat (35 %) або YouTube (32 %). Ще 15 % – Instagram.

***

6.06.2018

Смартфоны и видеоигры делают подростков грустными и нервными, – ученые

Большое количество времени, проведенного за видеоиграми и смартфоном, делают тинейджеров грустными и нервными. Новое исследование показало, что это связано с нарушением ритмов сна (News.UA).

Поскольку смартфоны и другие мобильные устройства стали вездесущими, некоторые исследователи и многие родители начали беспокоиться о рисках, связанных с психическим здоровьем детей. Новое исследование университета Стоуни-Брук охватило 3000 подростков с 2014 по 2017 год. Выводы показывают, что игры и мобильные телефоны влияют на мозг, нарушая сон и делая детей более несчастными и дерганными.

Чем больше времени проводят дети за электронными устройствами, тем сильнее симптомы депрессии, говорят авторы исследования. «Смартфоны и прочие устройства сильно влияют на сон, мешая нормальному восстановлению. Это ведет подростков к прогрессирующей депрессии», – говорит Сян Стелла Ли, ведущий автор (Xian Stella Li).

Маніпулятивні технології

4.06.2018

Ирина Фоменко

Как доверять новостям в сети после «фейковой смерти» Бабченко

Можно доверять смерти. «Альтернативные факты» и «фейковые новости», отсутствие «объективности» как «иной формы субъективности», утверждения об относительности истины… Все не имеет значения перед бесспорным, неопровержимом факте смерти, пишет The Guardian. Так было до 30 мая, когда журналист Аркадий Бабченко, официально объявленный погибшим 29 мая, оказался на самом деле жив, а его убийство было спецоперацией.

Докладніше

***

5.06.2018

«Різанина» на дитячому святі в Енергодарі: Брехню про участь нацгвардійців поширили в соцмережах

Нацгвадія спростувала свою участь в імітації перерізання горла на дитячому святі в Енергодарі Запорізької області (Depo).

Про це йдеться в прес-релізі Нацгвардії, який надійшов до редакції «Громадського».

У відомстві підтвердили, що до військової частини 3042 зверталися організатори свята – керівник Дому культури «Современник» з проханням підготувати показовий виступ на свято до Дня захисту дітей. Але керівництво частини відмовило.

«У виступу брав участь Енергодарський бійцівський клуб “Вітязь”», – повідомили в Нацгвардії.

Неправдиву інформацію про участь бійців військової частини 3042 із Енергодара у дитячому святі 1 червня поширила у Facebook місцева мешканка. Цей пост отримав резонанс і далі поширювався в Інтернеті.

Спецслужби і технології «соціального контролю»

24.05.2018

США намагаються знешкодити російських хакерів, які планують кібератаку проти України

Американська влада повідомила, що вона буде намагатися взяти під контроль сотні тисяч маршрутизаторів і пристроїв, уражених хакерами, які планували кібератаку проти України.

Докладніше

***

24.05.2018

Ирина Фоменко

Amazon и Google втихаря сотрудничают с полицией и военными

Группы защиты гражданских прав возмущены тем, что Amazon предоставляет технологии распознавания лиц правоохранительным органам США. Об этом сообщает The Fortune.

Докладніше

***

29.05.2018

В России собрались запретить Microsoft

Советник президента России по интернету Герман Клименко заявил, что Microsoft «могут попросить» покинуть Россию (InternetUA).

Как пишет РБК, об этом он сказал на конференции «Интернет после глобальности».

«Я надеюсь, что мы сможем гордиться теми, проектами, где мы действительно хороши – в искусственном интеллекте, нейронных сетях и т. д. Понятно, что в современном фрагментационном мире, когда “Касперского”

просят покинуть Америку, а мы, скорее всего, попросим покинуть нас Microsoft, за этим занятно будет наблюдать», – сказал Клименко.

«У каждого есть кого изгнать», – резюмировал он.

В сентябре 2017 года американское Министерство внутренней безопасности распорядилось, чтобы все государственные учреждения США перестали использовать продукты «Лаборатории Касперского». Власти страны полагают, что ее программное обеспечение может быть использовано российскими спецслужбами, чтобы получить доступ к правительственным документам. В российской компании эти обвинения назвали необоснованными.

В России госорганам сейчас не запрещено закупать решения Microsoft или других зарубежных компаний. Однако органы власти должны закупать в приоритетном порядке (если не доказано, что российского аналога нет) продукты, включенные в Единый реестр отечественного программного обеспечения.

***

29.05.2018

Против онлайн-СМИ открыли дело за трансляцию «парада» боевиков

СБУ расследует трансляцию псевдопарада ресурсом Корреспондент.net как пропаганду коммунистического тоталитарного режима (InternetUA).

Служба безопасности открыла уголовное производство по факту прямой трансляции на сайте интернет-издания Корреспондент.net фейкового «парада Победы», который подконтрольные Кремлю боевики провели во временно оккупированном Донецке 9 мая 2018 года. Об этом говорится в ответе СБУ на обращение народного депутата Виктории Сюмар, который парламентарий опубликовала в своем Facebook.

Как отмечается в документе, спецслужба начала досудебное расследование 24 мая. Предварительная квалификация дела – ч. 2 ст. 436-1 УК (распространение коммунистической символики и пропаганда коммунистического тоталитарного режима с использованием СМИ).

9 мая 2018 года секретарь СНБО Александр Турчинов обратился к СБУ с просьбой расследовать трансляцию некоторыми онлайн-СМИ «военного парада» террористов в оккупированном Донецке и предложил внести эти информационные ресурсы в санкционный список. В спецслужбе пообещали рассмотреть этот призыв и внести предложения по результатам проверки.

***

29.05.2018

Кенийские власти обязали граждан получать лицензии на публикацию любых видео в сети

Отныне в Кении любые видеоролики, опубликованные для общего просмотра, по закону обязаны иметь лицензию. Будь то фильмы, телепрограммы, видео на сайтах СМИ или ролики, снятые на смартфон и выложенные в социальные сети отдельными гражданами (Телекритика).

Как заявляют в Совете по классификации фильмов Кении (KFCB), отвечающем за цензуру в кино, согласно новому закону, любой человек в стране, транслирующий любые видео для публичного просмотра, должен будет иметь лицензию на съемку. Новый закон вступил в силу 28 мая 2018 года.

По словам главы KFCB Иезекиля Мутуа, это правило распространяется на любое видео, в том числе записанное с помощью мобильных телефонов, если оно предназначено для публичного показа. Мутуа также подчеркнул, что «публичный показ» подразумевает под собой публикации видеороликов в социальных сетях и на других сайтах в интернете.

В случае игнорирования нового закона и публикации видео без лицензии, преступники получат максимальный штраф в 1000 долларов США или максимальный срок тюремного заключения – 5 лет.

Кенийцы остро критикуют новое постановление, однако многие сходятся во мнении, что KFCB вряд ли удастся контролировать весь поток видеоматериалов, «нелегально» публикуемых в сети.

***

29.05.2018

Россия грозится заблокировать App Store, если Apple не удалит Telegram

Российская федеральная служба по надзору в сфере связи Роскомнадзор отправила Apple требование об удалении Telegram из местного App Store. Ведомство угрожает нарушить работу сервисов компании (IGate).

На официальном сайте Роскомнадзора появилась запись, в которой сказано, что регулятор отправил Apple письмо в котором требует прекратить рассылку сервисных уведомлений для российских пользователей. Telegram использует подобные оповещения для обхода блокировки. Ведомство также требует удалить мессенджер из российского App Store.

«Во избежание возможных действий Роскомнадзора по нарушению функционирования указанных выше сервисов Apple Inc. просим вас в кратчайшие сроки проинформировать нас о дальнейших действиях компании, направленных на решение данных проблемных вопросов», – говорится в письме.

Telegram заблокирован в России с середины апреля. На следующий день после блокировки Роскомнадзор потребовал удалить Telegram из App Store и Google Play, но обе компании проигнорировали требование ведомства. Несмотря на все попытки заблокировать мессенджер, он продолжает работать в России.

***

29.05.2018

Папуа-Новая Гвинея запретила Facebook сроком на месяц

Правительство Папуа – Новой Гвинеи запретило социальную сеть Facebook в стране на один месяц, чтобы изучить, как ее граждане используют платформу, как распространяются ложные сведения и порнография, и по возможности удалить фейковых пользователей, пишет The Guardian (InternetUA).

Число пользователей Facebook по всему миру превышает 2 млрд человек. Сколько из них являются гражданами Папуа – Новой Гвинеи, точно не известно. Однако, по данным Всемирного банка, доступ к интернету имеют менее 10% из 8 млн жителей страны.

Приостановка работы соцсети «позволит собрать информацию, чтобы идентифицировать, отфильтровать и удалить пользователей Facebook, скрывающихся за фейковыми учетными записями, выгружающих порнографические изображения, размещающих ложную и вводящую в заблуждение информацию», – заявил министр связи Папуа - Новой Гвинеи Сэм Бэзил.

Кроме того, власти намерены изучить, как с Facebook взаимодействуют другие государства.

***

30.05.2018

Чекисты в России хотят лишить юзеров анонимности – якобы ради борьбы с «группами смерти»

Представитель Следственного комитета РФ Сергей Коротких предложил отменить анонимность в рунете и принудить юзеров ходить в интернет исключительно через портал госуслуг. По его мнению, это поможет уменьшить число подростковых самовыпилов и нападений на школы.

Докладніше

***

30.05.2018

СБУ затримала одеситку за розповсюдження сепаратистських матеріалів

Співробітники Служби безпеки України під процесуальним керівництвом прокуратури викрили мешканку Одеси, яка через російські соцмережі розповсюджувала антиукраїнські матеріали (InternetUA).

Правоохоронці встановили, що жінка регулярно розміщувала на персональних сторінках матеріали із закликами до зміни державного кордону і конституційного ладу України та популяризацією терористичних організації

«ДНР/ЛНР». Інформацію агітатор отримувала з російських пропагандистських Інтернет видань та сайтів бойовиків з тимчасово окупованих територій.

Під час обшуку за місцем проживання зловмисниці співробітники спецслужби вилучили кілька мобільних гаджетів та комп'ютерну техніку із доказами розміщення сепаратистських матеріалів.

Слідчими Управління СБУ в Одеській області відкрито кримінальне провадження за ч. 1 ст. 110 Кримінального кодексу України. Затриманій оголошено про підозру в скоєні злочину.

Триває досудове слідство.

***

24.05.2018

Facebook устанавливает жесткие правила размещения политической рекламы

Перед публикацией политических объявлений пользователи Facebook в США должны будут предоставить последние цифры номера социального страхования и фотографию удостоверения, выданного правительством (U-News).

Новые правила ввели из-за попыток пророссийских троллей повлиять на президентские выборы в США в 2016-м.

Социальная сеть теперь требует от всех желающих опубликовать объявления, связанные с политическими кампаниями, гражданскими правами, иммиграцией, оружием, экономикой и другими вопросами, доказать, что они на самом деле находятся в США.

Кроме номера социального страхования и удостоверения пользователям, желающим публиковать рекламу, необходимо будет предоставить почтовый адрес США. После того, как Facebook проверит полученную информацию, компания отправит код на указанный адрес, который позволит публиковать рекламу. После проверки информация будет удалена.

Соцсеть отмечает, что в опубликованных объявлениях будут указаны источники их финансирования. Вся подобная реклама будет храниться в особом архиве.

***

24.05.2018

Twitter считает пишущих на кириллице болгар русскими ботами

В 2017 году Твиттер объявил о начале активной борьбы с ботами. Из-за активных действий, начавшихся в мае 2018 года, множество пользователей из Болгарии оказались заблокированными. Скорее всего, дело в кириллице, сообщает The Verge (IGate).

Очевидно, русские боты настолько сильно беспокоили руководство социальной сети, что борьбу за чистоту информационного пространства начали

именно с них. Для того, чтобы меры работали наиболее эффективно, по всей видимости, алгоритмы Твитера были настроены на блокировку любых сообщений, написанных на кириллице.

Сильнее всех пострадал болгарский сегмент сервиса микрособщений.

Пользователи, случайно попавшие под санкции, могут довольно быстро восстановить свои учетные записи. Но твиты от них продолжают скрываться, а другим участникам беседы не приходят уведомления о новых сообщениях от них. На жалобы служба поддержки отвечает, что аккаунт не заблокирован, и все в порядке.

После того, как подобные случаи участились, представители социальной сети все-таки признали проблему и выпустили заявление, что работают над решением сложившейся ситуации, не забывая бороться с злонамеренным распространением спама и автоматизированных аккаунтов.

***

1.06.2018

В Уганді ввели податок на користування соцмережами

В Уганді прийняли закон про податок на користування соціальними мережами. Документ набуде чинності в липні наступного фінансового року (ZIK). Про це повідомляє «PaySpace».

Відповідно до закону, за використання таких соціальних мереж, як Facebook, Twitter, і месенджер WhatsApp користувач повинен буде платити 200 шилінгів ($ 0,05) в день. У Міністерстві фінансів розповіли, що плату стягуватимуть через мобільних операторів. Користування соцмережами буде реєструватися через сім-карти.

Відповідне рішення прийняв президент Уганди Йовері Мусевені, тому що, на його думку, через соцмережі поширюються чутки. Міністр фінансів Девід Бахаті повідомив, що в країні підвищуються податки, щоб оплатити зростаючий держборг.

Закон про податок на користування соцмережами викликав критику з боку правозахисників. Один з представників місцевої правозахисної організації і адвокат Ніколас Опьйо назвав податок «новим інструментом удушення свободи самовираження, яка не піддавалася контролю з боку держави».

***

31.05.2018

В ОАЕ правозахисника засудили до 10 років в'язниці за пости в соцмережах // Монархи з високою самооцінкою не терплять публічної критики

В Об'єднаних Арабських Еміратах відомого активіста і правозахисника Ахмеда Мансура засудили до 10 років позбавлення волі. Він критикував владу

в своїх публікаціях у соціальних мережах. Про це повідомляє Reuters з посиланням на Associated Press (mind).

Мансура було затримано в березні 2017 року. Суд визнав його винним у тому, що той ображав статус і престиж ОАЕ, а також керівництво еміратів. Активіста також засудили до штрафу в розмірі $272 000.

Абсолютистський монархічний режим ОАЕ не терпить публічної критики, зазначає видання. Разом з Мансуром ще кількох продемократичних активістів засудили за образу лідерів країни.

Правозахисні організації вимагають звільнення активіста, називаючи його арешт порушенням свободи волевиявлення і переконань.

Ахмед Мансур є членом правозахисної організації Human Rights Watch по Близькому Сходу, Північній Африці та країнах Перської затоки.

***

4.06.2018
Ирина Фоменко
За Белым домом шпионят через телефон

В прошлом году Министерство внутренней безопасности США запустило экспериментальный проект в Вашингтоне: была развернута сеть датчиков для обнаружения телефонов, через которые ведется слежка. Оказалось, что International Mobile Subscriber Identity (IMSI) использовали вблизи «таких стратегических объектов, как Белый дом».

Докладніше

***

5.06.2018
Минюст Греции заподозрил Facebook в поддержке нацизма

Министр юстиции Греции Ставрос Контонис подозревает Facebook в поддержке нацизма. Поводом для подобных мыслей стало то, что несколько дней назад в соцсети была удалена статья греческого журналиста Никоса Бойопулоса о массовом убийстве мирных граждан в деревне Канданос (о. Крит) во время немецкой оккупации.

Докладніше

Проблема захисту даних. DDOS та вірусні атаки

24.05.2018
Facebook запросил у пользователей интимные снимки

Социальная сеть Facebook тестирует алгоритм, который защитит жертв порномести. Об этом сообщается на официальной странице, посвященной безопасности сервиса (InternetUA).

Новый упреждающий инструмент разработан для тех, кто опасается распространения своих интимных фотографий. Пользователь может связаться с любым из партнеров Facebook (в этот список входят государственные организации нескольких стран) и получить одноразовую электронную форму для загрузки этих файлов. Они позволят специальным сотрудникам создавать уникальные цифровые отпечатки, по которым можно будет отслеживать их будущие загрузки. Эта практика может быть распространена на сервис Messenger и соцсеть Instagram.

По действующим правилам, Facebook практикует блокировку подобных изображений по жалобам жертв. Сотрудники соцсети утверждают, что в основном объектами травли становятся женщины, которые постоянно сталкиваются с жестокостью и несправедливым отношением в интернете.

***

24.05.2018

Cisco сообщила о готовящейся кибератаке на украинские предприятия

Компании Cisco в официальном блоге сообщила, что располагает информацией, которая указывает, что группа хакеров, аффилированная или поддерживаемая напрямую государством, готовит масштабную атаку на государственные и частные структуры (Компьютерное Обозрение).

Исследователи Talos, подразделения Cisco, отмечают, что для атаки будет использован вирус VPNFilter и на протяжении последних двух недель идет массовое им заражение роутеров с наибольшей активностью именно в Украине. Предполагается, что данное ПО было разработано той же группой, что и вирус Petya.

VPNFilter может перехватывать весь трафик, идущий через роутер и кроме того полностью контролировать само устройство, включая его полную блокировку.

Сообщается, о том, что уже зафиксировано более 500 тыс. заражений роутеров. VPNFilter заражает устройства Linksys, MikroTik, Netgear и TP-Link, а также сетевые накопители Qnap.

В интервью Reuters сотрудник Cisco Крейг Уильямс, заявил, что основная кибератака против Украины, вероятнее всего, запланированы на День конституции, 28 июня. Также эксперты компании заявили, что за хакерами обнаруженной волны активностей стоит российское правительство.

***

28.05.2018

Хакеры украли криптовалют на $1,2 млрд менее чем за полтора года

С начала 2017 года киберпреступники похитили криптовалют на сумму, эквивалентную порядка $1,2 млрд, сообщается в отчёте антифишинговой

рабочей группы (Anti-Phishing Working Group, APWG). В исследование были включены как зарегистрированные, так и незарегистрированные кражи. «Кроме оборота наркотиков и отмывания денег с помощью криптовалют мы видим ещё одну проблему – воровство токенов», – заявил в интервью Reuters генеральный директор компании CipherTrace и председатель APWG Дэйв Джеванс (Dave Jevans) (InternetUA).

По оценкам Джеванса, из украденных $1,2 млрд возвращены были лишь около 20 %. При этом эксперт считает, что в будущем ситуация не только не улучшится, но даже осложнится. В этом он винит постановление Европейской комиссии о защите данных (GDPR), которое вступает в силу 25 мая 2018 года. «GDPR негативно отразится на безопасности в Интернете и непреднамеренно сыграет на руку киберпреступникам. Ограничивая доступ к важной информации, новый закон значительно затруднит расследование киберпреступлений – кражи криптовалют, фишинга, вымогательства, распространения вредоносных программ, взломов», – уверен Джеванс.

Дело в том, что GDPR запрещает компаниям публиковать информацию, с помощью которой можно было бы идентифицировать пользователей Интернета. Согласно постановлению, использование протокола WHOIS является незаконным, так как он позволяет установить имя, адрес электронной почты и номер телефона того, на чьё имя зарегистрирован тот или иной домен во Всемирной паутине. Но именно WHOIS был одним из важнейших инструментов правоохранительных органов в борьбе с преступлениями в киберпространстве.

***

25.05.2018
Ирина Фоменко
Facebook следит за пользователями через свое приложение

Facebook использовал свое приложение для сбора информации о пользователях и их друзьях, в том числе о тех, кто не подписан на социальную сеть, читая их текстовые сообщения, отслеживая местоположения и получая фотографии.

Докладніше

***

25.05.2018

Зафиксированы новые атаки, похожие на деятельность группировки Cobalt

В Positive Technologies обнаружили вредоносную активность, характерную для группировки, ранее атаковавшей более 250 компаний по всему миру.

Докладніше

***

28.05.2018

Найден способ остановить новейший опасный вирус

Сотрудники ФБР посоветовали владельцам маршрутизаторов потребительского класса и сетевых накопителей как можно скорее перезагрузить свои девайсы. Об этом сообщает Ars Technica (InternetUA).

По мнению американских правоохранительных органов, такие действия временно помогут противостоять вредоносным программам российского производства, заразившим сотни тысяч устройств.

Кроме того, ФБР предложили пользователям, чьи маршрутизаторы оказались в зоне риска, рассмотреть возможность отключения параметров удаленного управления на устройствах, а также защитить роутеры надежным паролем и шифрованием при включении. «Прошивку сетевых устройств следует обновить до последней версии», – заключили сотрудники министерства.

В бюро предупредили, что несмотря на меры предосторожности, устройства останутся уязвимы для повторной атаки хакеров. Однако эти действия увеличат шансы для выявления источника инфекции и ее нейтрализации.

***

30.05.2018

Xenotime нацелилась на системы безопасности предприятий США

На хакерскую группу, стоявшую за прошлогодней атакой вредоносного ПО Triton на критическую индустриальную инфраструктуру на Ближнем Востоке, эксперты возлагают ответственность за подготовку новой волны кибератак, ориентированных уже на системы аварийного управления (Incident Control System, ICS) в США.

Докладніше

***

30.05.2018

В платформе IBM QRadar обнаружены опасные уязвимости

Исследователь безопасности Педро Рибейро (Pedro Ribeiro) обнаружил в платформе IBM QRadar 3 опасные уязвимости, которые при совместной эксплуатации позволяют удаленному неаутентифицированному злоумышленнику выполнять произвольные команды с привилегиями суперпользователя (InternetUA).

IBM QRadar представляет собой продукт для обеспечения и управления корпоративной безопасностью, предназначенный для оказания помощи

аналитикам в выявлении сложных угроз в сети и устранении последствий инцидентов.

Уязвимостям присвоен общий идентификатор CVE-2018-1418. По словам специалистов, в QRadar есть встроенное приложение для проведения анализа файлов. Приложение отключено в версии Community Edition, однако его код полностью не удален, и часть его все еще работает.

Приложение имеет два компонента: сервлет Java и основной PHP-компонент. В первом компоненте присутствует уязвимость, которая может быть использована для обхода аутентификации, а во втором - проблема, позволяющая выполнять произвольные команды. Помимо этого, Рибейро обнаружил третью уязвимость, которая может быть проэксплуатирована для повышения привилегий.

По данным IBM, уязвимости затрагивают версии QRadar SIEM 7.3.0 - 7.3.1 Patch 2 и QRadar SIEM 7.2.0 - 7.2.8 Patch 11. Соответствующие исправления включены в версии 7.3.1 Patch 3 и 7.2.8 Patch 12.

***

29.05.2018
Дмитрий Сизов
UKR.NET повысил уровень безопасности Почты

25 мая Европа перешла на новые правила обработки персональных данных, установленные Общим регламентом о защите данных (Регламент ЕС 2016/679 или GDPR – General Data Protection Regulation). Производитель самой популярной украинской электронной почты @UKR.NET, которой пользуются более 40 % пользователей e-mail сервисов в Украине, также ввел повышенные стандарты защиты персональных данных.

Докладніше

***

31.05.2018
Ирина Фоменко
ФБР рекомендует: перезагрузите роутер, чтобы вас не взломали российские хакеры

Хакеры могут воспользоваться интернет-шлюзом для кражи пользовательских данных. Недавно ФБР настоятельно рекомендовало перезагрузить все домашние и офисные маршрутизаторы в связи с обнаружением Cisco Talon group хакерской российской программы VPNFilter, заразившей не менее 500 000 сетевых устройств.

Докладніше

***

31.05.2018

Михаил Сапитон

Обновление Google Chrome позволит авторизоваться на сайтах без паролей

Google выпустила стабильную версию Chrome 67 для Windows, Mac и Linux. Помимо исправления 34 багов, связанных с безопасностью, компания добавила в браузер несколько важных функций (AIN.UA).

Отныне Chrome поддерживает спецификацию WebAuthn, которая позволяет авторизироваться на сайтах при помощи биометрической информации (отпечатка пальца, скана лица) или USB-ключа. Новый метод включен по умолчанию, однако его работа зависит в том числе от разработчиков сайтов, которые должны настроить поддержку WebAuthn на серверной стороне.

Также новая версия позволяет экспортировать все пароли в формате .csv. Это пригодится, если вы хотите перенести их в другой менеджер паролей.

В Chrome 67 появилась поддержка Generic Sensor API – фреймворка, позволяющего браузеру получать информацию с сенсоров устройства, вроде акселлерометра или гироскопа. Инновация ориентирована на мобильные устройства, а также игры в виртуальной и дополненной реальности. Помимо этого, для помощи разработчикам, создающим VR и AR контент, появился WebXR Device API. Google обещает, что этот фреймворк позволит унифицировать разработку под разные шлемы.

Chrome 67 расширяет применение технологии изоляции сайтов. Она не позволяет вкладкам получать данные от других открытых страниц. Функция нацелена на решение проблем с уязвимостью Spectre. Отмечается, что изоляция на 10-11% повышает нагрузку на оперативную память.

***

1.06.2018

Twitter массово блокирует аккаунты пользователей, которым на момент регистрации не было 13 лет

Разработчики Twitter начали блокировать пользователей, чей возраст не соответствовал правилам пользования сервисом на момент регистрации учетной записи.

Докладніше

***

1.06.2018

Facebook до сих пор не знает, какие именно данные получила Cambridge Analytica

Макс Яначек

Главная операционная директор компании Facebook Шерил Сандберг (Sheryl Sandberg) заявила, что в 2016 году они не заметили злоупотреблений с данным миллионов пользователей, потому что сосредоточились на противодействии спаму и фишинговым атакам.

Докладніше

***

1.06.2018

Chrome и Firefox сливали данные о пользователях Facebook

С 2016-го года в Google Chrome и Mozilla Firefox существовала уязвимость, которая позволяла сайтам получать информацию о Facebook-профилях посетителей.

Докладніше

***

4.06.2018

Facebook уличили в «сливе» данных пользователей производителям смартфонов

Компания Facebook предоставляет доступ к личным данным пользователей крупнейшим производителям смартфонов и иных электронных устройств. Об этом пишет The New York Times (InternetUA).

По данным издания, соцсеть в течение последних десяти лет заключила множество соглашений с крупными производителями электронных устройств, которые позволяют компаниям получить доступ к данным пользователей Facebook.

Как отмечается, эти соглашения ставят под сомнение соблюдение компанией Марка Цукерберга правил защиты данных пользователей.

При этом, по мнению экспертов, производители смартфонов получили доступ к данным не только пользователей Facebook, но и их друзей.

***

4.06.2018

Сеть ZenCash лишилась свыше $550 тыс. в результате хакерской атаки

Третьего июня блокчейн ZenCash стал жертвой «атаки 51 %», в результате которой злоумышленникам удалось похитить более $550 тыс. в эквиваленте криптовалюты ZEN (InternetUA).

Согласно сообщению команды ZenCash, атакующие осуществили повторное расходование двух транзакций на 13 тыс. ZEN и 6,6 тыс. ZEN.

Средства были выведены на адрес zneDDN3aNebJUnAJ9DoQFys7ZuCKBNRQ115. Злоумышленникам удалось реорганизовать 38 блоков, длительность атаки составила менее четырех часов.

Команда ZenCash приняла меры по обеспечению безопасности средств пользователей и в настоящее время проводит расследование инцидента.

***

4.06.2018

Уровень распространения эксплойта EternalBlue превысил показатели 2017 г

Выявления EternalBlue в течение 2017-2018 гг. в соответствии с Eset Live Grid (Компьютерное Обозрение).

Год назад программа-вымогатель WannaCryptor.D (также известная как WannaCry и WCrypt) вызвала одни из самых разрушительных последствий в цифровом мире. И хотя сама угроза уже не представляет большой опасности, эксплойт EternalBlue, который вызвал волну распространения, по-прежнему угрожает системам без надлежащей защиты и примененных исправлений. По данным телеметрии Eset, его распространенность в течение последних нескольких месяцев растет, а недавно уровень выявления угрозы превзошел самые высокие показатели 2017 г.

EternalBlue использует уязвимость (в Microsoft Security Bulletin MS17-010) реализации протокола Server Message Block (SMB) в устаревшей версии Microsoft. В результате атаки киберпреступники сканируют Интернет на наличие открытых портов SMB, а обнаружив их, запускают код эксплойта. При наличии уязвимости злоумышленники запускают выбранный под жертву компонент. Именно с помощью этого механизма год назад через сеть распространялась угроза WannaCryptor.D.

В течение следующих месяцев после пика распространения WannaCryptor количество попыток использовать эксплойт EternalBlue уменьшилась до сотни в день. Однако с сентября прошлого года использование угрозы начало медленно расти, достигнув новых высоких показателей в середине апреля.

***

4.06.2018

«Умные» часы могут быть использованы для слежения за их владельцем

Эксперты «Лаборатории Касперского» выяснили, какие возможности открывает анализ сигнала носимых устройств для потенциальных злоумышленников.

Докладніше

***

5.06.2018

Злоумышленники используют Google Play для распространения вредоносного кода

В мае специалисты «Доктор Веб» выявили в каталоге Google Play троянца Android.Click.248.origin, которого злоумышленники распространяли под видом таких известных программ как Skype и «Алиса».

Докладніше

***

5.06.2018

Группировка Andariel Group нашла в ActiveX дыру нулевого дня

Эксперты обнаружили новую кампанию по кибершпионажу с использованием как минимум девяти брешей в платформе ActiveX, в числе которых уязвимость нулевого дня. Предположительно за атаками стоит группировка Andariel – одна из дочерних организаций Lazarus.

Докладніше

***

5.06.2018

Взломан израильский генеалогический сайт с данными ДНК его пользователей

Израильская компания MyHeritage сообщила, что хакеры похитили данные учетных записей 92 миллионов пользователей. Скомпрометированы данные пользователей, которые зарегистрировались на сайте до 16 октября 2017 года (InternetUA).

Популярный генеалогический ресурс недавно стал предоставлять своим пользователям новую услугу: с помощью простого теста ДНК они могли больше узнать о своих корнях, а также найти родственников. Для того, чтобы сделать тест надо было сделать соскоб со слизистой оболочки щеки ватной палочкой, и уже через 3-4 недели можно было получить детальный отчет о своем происхождении и о том, в какой части света жили предки. Если на сайте имелись данные его дальних родственников, пользователь получал об этом уведомление.

В январе 2017 года израильские СМИ сообщали, что на веб-сайте MyHeritage хранятся 35 миллионов генеалогических деревьев.

Четвертого июня, главному специалисту компании по компьютерной безопасности стало известно о том, что на стороннем сервере был обнаружен файл под именем myheritage, содержащий адреса электронной почты пользователей и хэшированные пароли. В компании отмечают, что для получения доступа к учетным записям пользователей этой информации недостаточно.

Вместе с тем, в MyHeritage заверяют клиентов, что никакие другие их данные не были скомпрометированы. Данные о кредитных картах обрабатываются сторонними сервисами, такими как PayPal, а данные о ДНК – хранятся в системе, на связанной с адресами электронной почты.

***

5.06.2018

Хакеры через Минздрав пытались атаковать дипмиссию страны НАТО

СБУ предотвратила атаку на дипломатическое ведомство одной из стран Альянса: злоумышленники воспользовались данными взломанного ресурса Минздрава (InternetUA).

Специалисты Службы безопасности Украины блокировали кибератаку на дипломатическое ведомство неназванной страны-члена Североатлантического альянса, которая стала возможной из-за халатности чиновников одного из предприятий Минздрава. Об этом инциденте сообщил пресс-центр СБУ.

В ходе расследования выяснилось, что были нарушены правила защиты информации и эксплуатации автоматизированных систем на одном из ГП Минздрава. Это привело к тому, что хакеры получили доступ к информационно-телекоммуникационным системам учреждения.

Более того, в дальнейшем злоумышленники попытались использовать полученные данные для взлома ресурсов иностранного представительства.

После проверки руководство Минздрава решило уволить гендиректора госпредприятия: ему сообщили о подозрении в совершении преступления по ст. 363 УК (нарушение правил эксплуатации АЭВМ).

ДОДАТКИ

Додаток 1

24.05.2018

Каждую минуту в Viber регистрируются 2 тысячи новых пользователей

Представители одного из самых популярных в Украине мессенджеров Viber поделились результатами использования своего сервиса. В частности, по их данным пользователи проводят в мессенджере на 69 % времени больше по сравнению с 2017 годом. Они совершают более 7 млн действий в минуту, включая 2 тысячи новых регистраций, 7 тысяч лайков и 1,5 млн отправлений фото (IGate).

Одним из самых популярных направлений сотрудничества бизнеса и Viber стали чат-боты: более 75 % аудитории ведут общение с ними в мессенджерах. При этом 80 % аудитории считают, что боты развивают потребительский сервис, а 3 из 4 пользователей переписываются с ботами тех брендов, которые они знают.

По словам представителей Viber, сервис работает над постоянным расширением функционала и возможностей для брендов: так, на платформе мессенджера уже можно брать кредиты (Приват), следить за состоянием счета, а также получать кредитные/дебетовые карточки (ПУМБ). Кроме того, благодаря партнерству с Avias клиенты АЗС могут в Viber получить топливную карту сети или же проверить баланс, отсканировав QR-код.

Возможности коммуникации с аудиторией, в том числе с использованием чат-ботов, расширились благодаря еще одному нововведению в Viber. В феврале 2018 года мессенджер ввел новый формат – сообщества. Первым воспользовалось новыми возможностями шоу «Голос Страны», канал которого в период с марта по май успел набрать более 100 000 участников.

«Мы постоянно работаем над расширением возможностей мессенджера, чтобы нашим пользователям не приходилось переключаться с одного приложения на другое во время общения с близкими. Увеличение количества времени, проведенного в приложении, – это отличное доказательство, что наши усилия не напрасны и пользователи высоко ценят функционал, удобство и надежность мессенджера, – прокомментировала директор по коммуникациям Viber в СНГ Яна Рожкова.

(вгору)

Додаток 2

5.06.2018
В Viber появились новые функции

Мессенджер Viber объявил о появлении новых дополнений для чатов: «Яркие сообщения», «Избранное» и «Местоположение». Функции станут доступны постепенно для всех пользователей в разных странах в мобильном приложении Viber для iPhone и Android (InternetUA).

«Яркие сообщения» выделят главные реплики в чате, добавив к ним яркий фон. На момент запуска доступно более 20 тем, но в будущем Viber будет представлять новые, как глобально, так и на отдельных рынках.

«Избранное» – полезное дополнение для чатов, которое позволяет сохранять любимые и часто используемые GIF-изображения, ссылки и видео в одном месте. При длительном нажатии на любой GIF, ссылку или видео с YouTube в чате, пользователь получит возможность добавить его в «Избранное». После этого можно легко получить доступ к избранному контенту в разных чатах Viber и в один клик отправлять сохраненный контент собеседникам.

«Местоположение» – это новый инструмент для обмена данными с актуальной информацией о находящихся поблизости местах, позволяющий мгновенно отправлять их в чат. Обновленные сообщения с местоположением включают кнопку «Открыть», с помощью которой пользователи смогут выбрать подходящее приложение для навигации. Для обеспечения максимальной безопасности данных, функция доступна только пользователям, которые предоставляют Viber доступ к данным о своем местоположении, таким образом, приложение получает данные только в случае, если пользователь открывает дополнение для отправки местоположения своим друзьям.

Дополнения для чатов впервые появились в Viber в декабре 2016 года. Они позволяют не покидать чат для того, чтобы мгновенно находить и отправлять GIF, видео на YouTube, музыку из Spotify, рестораны на Yelp и другую информацию. По данным мессенджера, дополнения – одна из самых быстро растущих опций. За прошедший год пользователи Viber применяли различные дополнения более 4,5 млрд раз.

(вгору)

Додаток 3

26.05.2018

Активист надеется отсудить у Google и Facebook до $8,8 млрд

С 25 мая в Евросоюзе вступил в силу новый регламент защиты персональных данных, известный как General Data Protection Regulation (GDPR). В первый же день работы закона австрийский юрист и борец за защиту данных Макс Шремс подал жалобы против Google, Facebook, Instagram и WhatsApp от имени некоммерческой организации None of Your Business («Не ваше дело») (IGate).

Шремс утверждает, что крупные компании принудительно добиваются согласия пользователей на принятие новых условий под угрозой ограничения доступа к своим сервисам, что противоречит требованиям GDPR.

В разговоре с CNBC юрист заявил, что Facebook уже заблокировала учётные записи нескольких пользователей, которые не согласились с новыми условиями.

«У пользователей был выбор либо удалить учётную запись, либо нажать кнопку “согласен” – это не похоже на свободу выбора, это больше напоминает выборы в Северной Корее», – подчеркнул Шремс.

По новым правилам интернет-компании, которые расположены в Европе или работают с пользователями из стран Евросоюза, обязаны получить согласие каждого пользователя на обработку его данных. У пользователей при этом должна быть возможность не согласиться с новыми условиями без ущерба себе. Они также могут в любой момент запросить у компании информацию о том, какие именно данные она собирает о нём и в каких целях используют.

В случае нарушения норм GDPR компаниям грозит штраф в размере до 4 % от годовой выручки либо €20 млн ($23,4 млн) – в зависимости от того, какая сумма больше.

NOYB подала четыре жалобы в разных европейских странах. По расчётам Шремса, при назначении максимального штрафа общая сумма наказания для Google и Facebook, которой принадлежат Instagram и WhatsApp, может составить €7,6 млрд ($8,8 млрд).

Директор Facebook по защите персональных данных Эрин Иган сообщила CNBC, что компания готовилась к вступлению в силу GDPR в течение последних 18 месяцев, чтобы убедиться, что все сервисы отвечают новым требованиям. По её словам, компания сделала свою политику более понятной и облегчила поиск параметров конфиденциальности для пользователей.

Иган напомнила, что в начале мая Facebook добавила функцию, которая позволяет пользователям удалять историю своих действий вне Facebook или вовсе запретить сбор таких сведений.

Представитель Google также сообщил, что за последние 18 месяцев компания обновила политики всех своих сервисов, чтобы предоставить пользователям более прозрачный контроль за их данными.

В первый день действия GDPR некоторые сайты перестали работать, так как не изменили свои политики к 25 мая. Для жителей Европы оказались недоступны сайты многих американских СМИ, включая Los Angeles Times, New York Daily News, Chicago Tribune и Mashable, а также сервисы, связанные с криптовалютами.

В 2015 году Шремс уже выиграл один судебный спор против Facebook. Тогда Европейский суд встал на его сторону и признал незаконным соглашение между Евросоюзом и США, которое позволяло компаниям передавать персональные данные европейских пользователей в США.

(вгору)

Додаток 4

6.06.2018

Дмитрий Демченко

В сети появился сайт, где можно «наказать» депутата, пожертвовав деньги на Facebook-рекламу его проступков

«Центр противодействия коррупции» запустил сайт «Серпом по рейтингу». Здесь можно «наказать» депутата-мажоритарщика, пожертвовав деньги на рассказ о его коррупционных схемах среди избирателей (AIN.UA).

Принцип действия сайта заключается в следующем. Пользователю нужно выбрать депутата, который был замечен в коррупционных скандалах, и пожертвовать любую сумму. Эти деньги пойдут на оплату таргетированной рекламы в Facebook среди пользователей соцсети его региона. Цель – рассказать потенциальным избирателям о проступке конкретного депутата.

Создатели проекта отмечают, что оптимальная сумма для одной такой мини-кампании – 1300 гривен. «За эти деньги можно показать “зашквар” депутата примерно 20 тысячам избирателей его округа. При том, что в среднем мажоритарщик побеждал на выборах с разницей в несколько тысяч голосов», – говорится в описании проекта.

Мы показываем только самые очевидные коррупционные зашквары депутатов: представление законопроекта, который узаконивает их коррупционное имущество, взятие ими на поруки задержанных топ-коррупционеров, отказ от голосования за лишение иммунитета фигурантов расследований НАБУ и тому подобное.

Чтобы показать, что такой механизм может повлиять на будущие голосования, создатели проекта приводят несколько примеров. Например, Юрий Соловей, победитель 89 округа Ивано-Франковской области, выиграл на выборах с отрывом примерно в 6 тысяч голосов. Охват таргетированной рекламы в Facebook на пользователей региона составляет от 12 000 до 18 000 людей. Таким образом они смогут узнать, что Соловей брал на поруки директора «Львовского бронетанкового завода» Романа Тымкива, который, в свою очередь, обвинялся в растрате госбюджета.

На сайте есть уже четыре депутата, на «рекламу» которых пользователи собрали больше 500 грн: Дмитрий Голубов (собрали 1242 грн), Сергей Березенко (1106 грн), Олесь Довгий (506 грн) и Владимир Кацуба (506 грн). Всего же в базе есть 14 «зашкваров».

(вгору)

Додаток 5

30.05.2018
Услуги ПУМБ теперь можно заказать через Viber

Первый Украинский Международный Банк (ПУМБ) с апреля запустил для своих розничных клиентов канал коммуникации в мессенджере Viber (ITnews).

Онлайн-банкинг ПУМБ в Viber предоставляет клиентам в формате 24/7 актуальную информацию о движении средств, сумме минимального платежа по карте и сумме до полного погашения, размере последнего зачисленного и следующего платежа по кредиту. Также через Viber можно оформить кредитную, дебетную карты и подать заявку на оформление кредита.

«Предоставление продуктов и услуг через Viber – это первый шаг ПУМБ по внедрению social commerce. Банк активно развивает новые функционалы в социальных сетях и мессенджерах, тем самым предоставляя клиентам традиционно качественный сервис в удобном формате. Ежемесячно в колл-центр ПУМБ поступает порядка 44 тысяч звонков – с целью уточнения суммы досрочного погашения кредита, обязательного платежа и последнего поступления. Теперь все эти клиенты смогут в любое удобное время оперативно получить необходимую информацию, приложив для этого минимум

усилий. В планах банка масштабировать услуги и на другие мессенджеры», – прокомментировал Себастиан Рубай, заместитель председателя правления ПУМБ.

Перечень услуг ПУМБ в Viber представлен удобным и простым в навигации меню на трех языках – украинском, русском и английском. Меню содержит шесть основных разделов:

– карточные продукты
– кредитные продукты
– информация о движении средств
– курсы валют
– пополнить мобильный
– изменить язык.

Использование онлайн-банкинга ПУМБ в Viber позволит качественно снизить нагрузку на колл-центр. Ежемесячно центр обслуживания клиентов ПУМБ получает около 7 тысяч звонков по вопросу уточнения суммы последнего поступившего платежа по кредиту, около 20 тысяч звонков касательно уточнения суммы досрочного погашения кредита, около 2 тысячи звонков с целью узнать сумму обязательного платежа по кредиту. Теперь эту информацию клиенты смогут получить в течении нескольких минут, выбрав соответствующий раздел в меню.

Чтобы начать работу в онлайн-банкинге ПУМБ в Viber, необходимо сначала зайти в паблик-аккаунт ПУМБ (находится в открытом доступе во вкладке «Публичные аккаунты»), и перейти в чат. После этого пользователю будет предложено меню, в котором в несколько кликов можно выбрать вышеописанные продукты и услуги. Подключение к Онлайн-банкингу ПУМБ в Viber абсолютно бесплатно и позволит клиентам банка получать услуги 24/7 в любой точке мира.

(вгору)

Додаток 6

6.06.2018

Эксперты заподозрили Google и Facebook в недобросовестной конкуренции из-за запрета рекламы криптовалют

В марте этого года холдинг Alphabet, владеющий компанией Google, объявил, что в июне интернет-поисковик введет запрет на рекламу криптовалют и иных спекулятивных финансовых инструментов, включая бинарные опционы и финансовые пари. Аналогичные запреты также ввели сервис микроблогов Twitter и соцсеть Facebook (InternetUA).

Как пишет газета Independent, решение Google и Facebook вызвало вопросы у ряда экспертов по криптовалютам, которые заподозрили компании в нечестной конкуренции. Так, недавно Google и Facebook проявили интерес к сфере криптовалют и лежащей в их основе технологии блокчейн. Это

заставляет предположить, что запрет на рекламу криптовалют был мотивирован не только борьбой с мошенниками.

«Я подозреваю, что запрет был введен в связи с потенциальными планами компаний выпустить собственные криптовалюты в ближайшем будущем», – заявил исполнительный директор британской инвестиционной компании Blackmore Group Филлип Нунн.

В свою очередь, Гарет Мална, адвокат по финансам из юридической компании Burges Salmon, полагает, что запрет на рекламу криптовалют противоречит самой сути крупнейшего в мире интернет-поисковика.

«Решение Google выступить в роли квази-регулятора может обернуться серьезными проблемами, учитывая коммерческую власть компании. Самой Google может казаться, что речь идет о защите потребителей, но это потенциально выходит за пределы роли привратника у двери, ведущей к информации», – сказал Мална.

Как напоминает The Independent, в мае Google предложила работу основателю криптовалюты Etherium Виталику Бутерину. Сам программист написал об этом в своем микроблоге, однако затем удалил свой пост, отмечает РБК.

Представитель Google отказался комментировать возможную выгоду компании от запрета рекламы криптовалют. При этом в марте в Google признавали, что изучают потенциальные возможности использования технологии блокчейн, но пока речь не идет о конкретных планах ее внедрения.

Facebook недавно также дала понять, что проявляет интерес к сфере криптовалют. Так, Дэвид Маркус, возглавлявший Facebook Messenger, недавно объявил, что будет руководить исследовательской группой, которая займется изучением блокчейна.

(вгору)

Додаток 7

4.06.2018
Ирина Фоменко
Как доверять новостям в сети после «фейковой смерти» Бабченко

Можно доверять смерти. «Альтернативные факты» и «фейковые новости», отсутствие «объективности» как «иной формы субъективности», утверждения об относительности истины… Все не имеет значения перед бесспорным, неопровержимом факте смерти, пишет The Guardian (InternetUA).

Так было до 30 мая, когда журналист Аркадий Бабченко, официально объявленный погибшим 29 мая, оказался на самом деле жив, а его убийство было спецоперацией.

Бабченко, бежавший из России за Украину, утверждал, что фейковая смерть была необходимостью: СБУ узнала о российской спецоперации по убийству журналиста, а единственный способ поймать организаторов – сымитировать его. Никто не сомневается, что Бабченко все еще в опасности.

Слишком рано выяснять, были ли действия СБУ эффективными. Однако какова цена этой операции? Подняло это или наоборот, снизило авторитет украинских чиновников? Можно ли считать теперь информацию о других убитых журналистах «фейковой»?

На прошлой неделе британская ежедневная газета Evening Standard предложила компаниям написать заказной материал: грань между рекламой и репортажем никто бы не заметил. В свою очередь, Evening Standard отрицает это. Между тем, английский телевизионный эксперт (который комментировал королевскую свадьбу для американского ТВ) оказался жителем Нью-Йорка.

Раньше считалось, что наличие большого количества телеканалов поспособствует обсуждению и взаимопониманию. В США, в частности, это привело к тому, что зрители Fox и CNN теперь живут в абсолютно противоположных мирах.

Интернет, который должен был избавить нас от гегемонии телевидения, оказался еще лучшим средством манипулирования: с огромным количеством фейковых аккаунтов, принадлежащих Кремлю или Bell Pottinger, и ботами, привлекающими внимание к «трендовым темам».

На просторах Интернета, например, на 4Chan или Discord, можно встретить цифровых активистов, распространяющих руководства КГБ и Центра правительственной связи по манипулированию информацией – своего рода инструкции по «формированию реальности». Кто-угодно, а не только СБУ, может играть роль медиа Макиавелли. И в каком-то смысле мы все стали мини-пиарщиками. Каждый раз, когда мы загружаем фото на Facebook, ставим «лайки» и делаем репосты, мы становимся цифровым источником влияния. Впрочем, чувство самоутверждения, которое нам дает социальная сеть, заставляет больше рассказывать о себе – потом эти данные Facebook продает другим компаниям.

Однако должно же быть что-то, на что можно положиться? Самые надежные люди спасают жизни: медики, спасатели, солдаты. Критик Путина и украинских властей, журналист и один из ведущих украинских лидеров ЛГБТ Максим Эристави положительно оценил спецоперацию с Бабченко: это первый случай, когда службы безопасности оказались на стороне журналистов.

Но даже вера в тех, кто рискует жизнью ради других, пошатнулась. «Белые каски» стали мишенью дезинформации: с фото девушки, которую спасают три разных человека, можно сделать вывод, что она – актриса. На самом деле это не так: пострадавших передают от одного спасателя к другому в любой операции. Живя в мире, где всем можно манипулировать, люди действительно начинаются сомневаться.

В течение нескольких минут после известий о смерти Бабченко, обычно соперничающие команды следственных журналистов начали расследование, зная, что властям никогда не следует доверять. Были собраны средства для поддержки семьи Бабченко. Другие журналисты-расследователи вылетели из Москвы.

Более сильный жест – это самопожертвование. В России украинский кинорежиссер Олег Сенцов объявил голодовку, чтобы привлечь внимание к 64 украинским политзаключенным в РФ. Мы все можем строить доверительные отношения, помогая спасти жизни.

(вгору)

Додаток 8

24.05.2018

США намагаються знешкодити російських хакерів, які планують кібератаку проти України

Американська влада повідомила, що вона буде намагатися взяти під контроль сотні тисяч маршрутизаторів і пристроїв, уражених хакерами, які планували кібератаку проти України (Espreso.tv).

Про це повідомляє видання Reuters.

Зазначається, що федеральний суддя Пенсільванії дозволив ФБР взяти контроль над доменом в інтернеті, який використовується російською хакерською групою Sofacy для управління зараженими пристроями.

Розпорядження судді дозволяє представникам ФБР направляти сигнал пристроїв для зв'язку з підконтрольним ФБР сервером. Цей сервер буде використовуватися для виявлення місця розташування ураженого хакерами обладнання, інформацію про що будуть передавати владі різних країн світу. Останні завдяки цьому зможуть видаляти шкідливе програмне забезпечення з гаджетів.

«Ця операція є першим кроком зі знищення бот-мережі, яка надає представникам Sofacy безліч можливостей, які можуть використовуватися для різних шкідливих цілей, включаючи збір розвідувальних даних, крадіжку цінної інформації та руйнівні кібератаки», – наголосив помічник генпрокурора з питань нацбезпеки Джон Демерс.

Така заява американської влади з'явилася після того, як компанія Cisco Systems (транснаціональна корпорація США, яка є найбільшим у світі виробником мережевого обладнання) 23 травня опублікувала звіт про хакерську кампанію, що має бути націлена на пристрої від Linksys, MikroTik, Netgear Inc (NTGR.O), TP-Link і QNAP.

Тоді у Cisco заявили, що найбільша кількість заражень від веб-віруса VPNFilter сталася в Україні, що наштовхнуло на думку, що Росія планувала атаку проти країни.

Компанія Cisco поділилася технічними деталями з урядами США та України, а також з конкурентами, які продають програмне забезпечення, обладнання та послуги для забезпечення безпеки.

У СБУ на це відповіли, що Росія вже продемонструвала підготовку до великомасштабної кібератаки перед фіналом футбольного матчу Ліги чемпіонів, який відбудеться в суботу в Києві.

(вгору)

Додаток 9

24.05.2018
Ирина Фоменко
Amazon и Google втихаря сотрудничают с полицией и военными

Группы защиты гражданских прав возмущены тем, что Amazon предоставляет технологии распознавания лиц правоохранительным органам США. Об этом сообщает The Fortune (InternetUA).

Американский союз защиты гражданских свобод (ACLU) и 40 других групп 22 мвая потребовали, чтобы Amazon запретил правительству использовать инструмент Rekognition, который, по словам компании, может определить «все лица на групповых фотографиях и в общественных местах». Среди клиентов Amazon – город Орландо и округ Вашингтон в штате Орегон, создавший базу данных из 300 000 изображений для Rekognition.

«С Rekognition правительство теперь может создать систему для автоматизации идентификации и отслеживания всех людей», – убеждены в ACLU. – «Благодаря этой технологии у полиции появится возможность определить протестующих. Иммиграционная и таможенная полиция США будет постоянно следить за иммигрантами. Как и в случае других технологий наблюдения, эти системы, несомненно, будут непропорционально ориентированы на группы меньшинств».

В свою очередь, Amazon защищает свои технологии. «Наше качество жизни значительно ухудшится, если мы объявим вне закона новую технологию только потому, что некоторые люди могут злоупотреблять ею. Представьте, если бы клиенты не могли купить компьютер, потому что его можно использовать в незаконных целях», – сообщают в компании.

Новая ситуация напоминает сделку Google «Project Maven» с Пентагоном. Так, Google должен предоставлять военным США технологию «искусственного интеллекта» для анализа видеороликов с дронов. Сотрудники опасаются, что технология может навредить людям, поэтому некоторые подали в отставку в знак протеста.

Не похоже, что в прошлом общественность не возмущалась связями Big Tech с властями США. Откровения Эдварда Сноудена о таких программах, как Prism, благодаря которым крупные онлайн-платформы предоставляют данные о клиентах разведывательным службам, спровоцировали серьезный скандал.

Поставка технологий военным не должна быть расценена как изначально плохое явление – действительно, Google, IBM, Amazon и Microsoft стремятся продавать облачные сервисы Пентагону, но никто не заставляет эти компании предоставлять технологии распознавания лиц тем, кто может использовать их для нарушения прав граждан.

Стоит отметить, что некоторые предприятия руководствуются этическими соображениями в вопросах продажи своих передовых

инструментов. Microsoft, например, сообщил Wired в начале этого месяца об отказе от нескольких контрактов, из-за которых все могли бы узнать, как компания создает собственные системы искусственного интеллекта.

Нынешняя ситуация в США отличается от китайской, где такие компании, как Alibaba, помогают правительству создать систему «социального кредита», предусматривающую массовый надзор. Однако отношения между крупными техническими фирмами и властями Америки по-прежнему довольно тесные.

(вгору)

Додаток 10

30.05.2018

Чекисты в России хотят лишить юзеров анонимности – якобы ради борьбы с «группами смерти»

Представитель Следственного комитета РФ Сергей Коротких предложил отменить анонимность в рунете и принудить юзеров ходить в интернет исключительно через портал госуслуг. По его мнению, это поможет уменьшить число подростковых самовыпилов и нападений на школы. Также он считает, что для СМИ нужно ввести жёсткие ограничения на публикации по этим темам (InternetUA).

Это предложение прозвучало 29 мая в его докладе на дискуссионной площадке «Право ребёнка на безопасность».

В своём креативе пан Коротких рассказывал о резком росте количества самоубийств среди подростков в первой половине 2017 года. Он связал это с так называемыми «группами смерти» в соцсетях: мол, с 2016 по первую половину 2017 года количество жертв самовыпила, которые в них состояли, выросло с 20 до 287 человек. Однако уже во второй половине 2017 года самоубийств среди подростков стало меньше – в качестве основной причины сэр криминалист назвал аресты нескольких администраторов таких групп.

Коротких выдал «гениальное» предложение по решению проблемы – «упразднить анонимность в российском сегменте интернета». Регистрация в соцсетях, по его словам Большого Брата, должна быть возможна только с использованием данных, по которым можно установить личность юзера. Более того, в идеале он будет вообще регаться через портал госуслуг.

Также, по словам чекиста, интернет-провайдеры и соцсети не заинтересованы в блокировке «нежелательной для детей информации», и поэтому необходимо заставить их это делать насильно. Накануне глава Следственного комитета Александр Бастрыкин в качестве примера придушенного интернета привёл Турцию, где, по его словам, «вместо Yandex, Google есть своя информационная система работы для детей».

Хитрая уловка товарищей чекистов у власти – прикрываясь заботой о детях, ввести драконовские законы и наложить лапу на святое – анонимность в интернете. Которой как бы и так остальнось не много из-за того, что

государства планомерно внедряют ограничения, якобы призванные обезопасить пользователей (последний пример – принятие 25-го мая GDPR), а по факт – связать им руки.

Сначала упыри принимают закон Димы Яковлева, который лишает тысяч детей в России возможности быть усыновленными гражданами США, теперь они «проявляют заботу» о двух сотнях самовыпилившихся детях, между делом нагибая миллионы граждан и завинчивая гайки свободы еще плотнее. Впрочем, это Росссия, детка, так что ничего нового. Главное чтоб у нас такой же феерии не происходило.

(вгору)

Додаток 11

4.06.2018
Ирина Фоменко
За Белым домом шпионят через телефон

В прошлом году Министерство внутренней безопасности США запустило экспериментальный проект в Вашингтоне: была развернута сеть датчиков для обнаружения телефонов, через которые ведется слежка. Оказалось, что International Mobile Subscriber Identity (IMSI) использовали вблизи «таких стратегических объектов, как Белый дом». Об этом сообщает The Verge (InternetUA).

Сенатор Рон Виден из штата Орегон, член Комиссии по разведке, получил письмо от выполняющего обязанности заместителя министра по вопросам национальной защиты и управления программами (NPPD) Кристофера К. Кребса. В нем Кребс отметил, что цель экспериментального проекта – «лучше понять потенциальную активность ловца IMSI» в регионе. И, хоть NPPD отслеживала активность вблизи Белого дома, организация не проверяла или не связывала эту деятельность с какими-либо «конкретными субъектами или устройствами». По его словам, контрразведка США и сотрудники правоохранительных органов «определили, что некоторые обнаруженные сигналы получены от законных вышек сотовой связи». Впрочем, некоторые из них могли быть и не от американских властей.

Как утверждает Кребс, Министерство внутренней безопасности США «получило сообщения от третьих сторон о несанкционированном использовании технологии IMSI, а также об использовании злоумышленниками уязвимости системы Signal System Seven (SS7) для отслеживания коммуникации американских граждан».

Ловец IMSI – это устройство, маскирующее себя под базовую станцию сотовой телефонной сети, которое может перехватывать сообщения. Ловец IMSI использовали Служба маршалов США, Департамент полиции Нью-Йорка, Иммиграционная и таможенная полиция США и даже Налоговое управление США. Комитеты Конгресса призвали Конгресс принять законодательство, регулирующее использование IMSI.

The Washington Post отмечает, что исследование Министерства внутренней безопасности подтверждает предположения других исследователей: иностранные разведывательные службы использовали эту технологию для сбора информации о должностных лицах США. Сенатор Виден заявил, что целью шпионажа может быть президент Дональд Трамп, другие высокопоставленные чиновники и американские граждане. Виден призвал Федеральную комиссию по связи и Исполнительный офис президента США предпринять меры по обеспечению безопасности.

Кроме того, Виден критикует «телефонные привычки» Трампа, заявляя, что он подает плохой пример. В прошлом году оказалось, что президент использовал незащищенный Samsung, в то время как недавний отчет Politico показал, что у Трампа было всего два iPhone – один для совершения звонков, другой для Twitter. Президент отказывался менять телефон для Twitter ежемесячно, потому это «слишком неудобно». Около 5 месяцев эксперты не могли проверить устройства на безопасность.

(вгору)

Додаток 12

5.06.2018

Минюст Греции заподозрил Facebook в поддержке нацизма

Министр юстиции Греции Ставрос Контонис подозревает Facebook в поддержке нацизма. Поводом для подобных мыслей стало то, что несколько дней назад в соцсети была удалена статья греческого журналиста Никоса Бойопулоса о массовом убийстве мирных граждан в деревне Канданос (о. Крит) во время немецкой оккупации, сообщает Keep Talking Greece (InternetUA).

Как отмечается, Контонис поднял соответствующий вопрос вчера на заседании Совета министров ЕС по вопросам юстиции и внутренних дел. В частности, он рассказал коллегам, что 2 июня Facebook удалил статью и заблокировал на сутки страницу журналиста Никоса Бойопулоса, который написал о массовом убийстве нацистами мирных граждан в деревне Канданос на Крите в 40-х годах, а также о том, что сейчас в стране идеи национал-социализма возрождает ультраправая партия «Золотая заря».

«Блокировка статьи греческого журналиста Facebook представляет собой серьезное нарушение свободы информационного процесса, это превентивная цензура», – подчеркнул он.

Министр юстиции Греции считает введение цензуры со стороны Facebook неприемлемым средством заглушить как историческую память о зверствах нацистов в Канданосе, так и стремлением скрыть неонацистскую идеологию членов «Золотой зари».

Партия «Золотая заря» зарегистрирована в Греции 1 ноября 1993 года, характеризует себя как «Народное националистическое движение» и резко выступает против нелегальной иммиграции. Ранее, публикации в партийном журнале включали похвальные статьи о Третьем Рейхе.

Європейський комиссар Джулиан Кинг согласился с мнением Контониса и призвал расследовать этот «очень серьезный инцидент» с Facebook. В то же время министры юстиции других государств-членов ЕС также поддержали коллегу из Греции.

(вгору)

Додаток 13

25.05.2018
Ирина Фоменко
Facebook следит за пользователями через свое приложение

Facebook использовал свое приложение для сбора информации о пользователях и их друзьях, в том числе о тех, кто не подписан на социальную сеть, читая их текстовые сообщения, отслеживая местоположения и получая фотографии. Об этом сообщает The Guardian (InternetUA).

Претензии по поводу массового наблюдения являются частью иска против Facebook, возбужденного Six4Three. Компания была упомянута в документах, поданных в вышестоящий суд в Сан-Матео в рамках судебного дела, которое продолжается уже более двух лет.

По словам пресс-секретаря Facebook, обвинения Six4Three безосновательны, и компания будет защищаться. Среди документов, поданных в суд на прошлой неделе, конфиденциальные письма и сообщения между руководителями Facebook.

Как заявили в Facebook, дело должно быть отклонено, поскольку закон Калифорнии обеспечивает свободу слова. В свою очередь, Six4Three отстаивает свою позицию.

Обвинения о наблюдении появились в январском иске. В нем утверждается, что Facebook использовал ряд методов, некоторые из которых адаптированы под разные телефоны, для сбора информации в коммерческих целях.

«Facebook продолжал изучать и реализовывать способы отслеживания местоположения пользователей, читал сообщения, контролировал использование конкурирующих приложений, а также отслеживал и контролировал звонки», – говорится в документе суда.

Но все подробности о схеме массового наблюдения были отредактированы по запросу Facebook в последних документах Six4Three. Facebook утверждает, что это конфиденциальные деловые вопросы. Чтобы не допустить обнародования документов, компания должна подать иск в суд до следующего вторника.

Разработчик подает в суд на Facebook за свое приложение Pikinis. Так, Facebook завлекала разработчиков и инвесторов на платформу, преднамеренно вводя их в заблуждение относительно элементов управления данными и настроек конфиденциальности. Таким образом компания следила за пользователями без их согласия.

На телефонах Android компания смогла собирать метаданные и контент из текстовых сообщений. На iPhone Facebook мог получить доступ к большинству фотографий, в том числе к тем, которые не были загружены в социальную сеть.

Facebook дистанционно активировал Bluetooth для точного определения местоположения пользователя без их согласия. Кроме того, срок действия настроек конфиденциальности был довольно коротким.

«Six4Three уже пятый раз меняет и добавляет новые обвинения в иск, а все его претензии касаются одного пункта: редакционного решения Facebook прекратить публикацию определенного пользовательского контента через свою платформу сторонним разработчикам приложений», – прокомментировали в компании.

В одной из заявок в суд 2013 и 2014 утверждается: «Facebook частично раскрыл информацию относительно настроек конфиденциальности, но не сообщил, что после определенного периода времени настройки становятся недействительны».

Согласно иску, о возможности компании читать текстовые сообщения на телефонах Android пользователям сообщили как о способе облегчения ведения журнала, но Facebook использовал ее для сбора других данных.

Кроме того, Facebook собирал информацию тех людей, у которых даже не было аккаунта в социальной сети. Поскольку они не являлись пользователями Facebook, у них не было возможности получить соглашение на сбор данных.

«Facebook публично сообщил о чтении сообщений для лучшей аутентификации пользователей, но компания не указала тип получаемых данных, сроках и причинах для доступа к информации этих пользователей Android», – говорится в иске. – «Facebook использовал данные для предоставления определенных продуктов и имеет несправедливое конкурентное преимущество перед другими социальными приложениями на Facebook Platform».

Недавно Facebook признал, что компания собирала данные о вызовах и текстовых сообщениях пользователей, но только с предварительного согласия. Сеть не смогла увидеть текстовые сообщения владельцев iPhone, но получала доступ к фотографиям. Как утверждает обвинитель, если у пользователя есть приложение Facebook, установленное на iPhone, Facebook анализирует фото, сохраненные на телефоне.

(вгору)

Додаток 14

25.05.2018

Зафиксированы новые атаки, похожие на деятельность группировки Cobalt

В Positive Technologies обнаружили вредоносную активность, характерную для группировки, ранее атаковавшей более 250 компаний

по всему миру. В середине мая специалисты компании зафиксировали вредоносную рассылку фишинговых писем в организациях кредитно-финансового сектора. По ряду признаков можно предположить, что атака организована группой Cobalt или кем-то из ее бывших участников – предполагаемый лидер группировки был арестован в Европе в марте этого года (Компьютерное Обозрение).

Первое расследование по Cobalt Positive Technologies провела в 2016 г.: тогда за одну ночь группировка совершила крупную кражу из шести банкоматов одного восточноевропейского банка. В 2017 г. к списку обычных для группы Cobalt целей, находящихся в странах СНГ, Восточной Европы и Юго-Восточной Азии, добавились компании, расположенные в Северной Америке, Западной Европе и даже в Южной Америке. Деятельность около 75% компаний, включенных группой в список для рассылки фишинговых писем, связана с финансами. По данным Positive Technologies, только в первой половине 2017 г. Cobalt разослала фишинговые письма с зараженными файлами более чем 3 тысячам получателей из 250 компаний в 13 странах мира.

«На первом этапе атаки группировка Cobalt активно использует методы социальной инженерии для доставки вредоносных файлов, что и неудивительно: согласно нашей статистике, по ссылкам в фишинговых письмах переходят почти 30% получателей, – рассказывает Алексей Новиков, руководитель экспертного центра безопасности Positive Technologies. – Для противодействия атакам со стороны подобных группировок мы рекомендуем в первую очередь организовать проведение регулярных работ по повышению осведомленности сотрудников компании в вопросах ИБ. Необходимо также наладить процесс своевременной установки обновлений безопасности, в том числе и для прикладного ПО, использовать современные средства защиты и проводить мероприятия по расследованию инцидентов».

Cobalt не рассчитывает на одну только невнимательность пользователей или недостатки спам-фильтров на почтовых серверах. Для повышения эффективности своих атак они используют взлом публичных сайтов со слабой защитой для загрузки на них вредоносных файлов, поддельные письма от имени финансовых регуляторов и контрагентов, рассылки не только на корпоративные почтовые адреса, но и на личные адреса сотрудников. Целью рассылки фишинговых писем являются, как правило, компрометация узлов, связанных с управлением банкоматами, и заражение АТМ вредоносным ПО для манипуляций с диспенсером. На финальном этапе подставные лица забирают из банкоматов деньги.

Технические особенности фишинговой рассылки, зафиксированной в мае этого года, повторяют различные атаки группы Cobalt. Похожая структура домена для рассылки писем применялась во время атак этой группы на банки России и Восточной Европы. Структура скачанного по ссылкам вредоносного документа схожа с документами, сгенерированными с помощью эксплойт-кита Threadkit, который Cobalt использовала с февраля 2018 г. В ходе новой атаки эксплуатировалась привычная схема доставки загрузчика, предназначенного

для скачивания бэкдора, и аналогичный метод расшифровки. Кроме того, бэкдор имеет все те же функции: разведка, запуск программ, загрузка новых модулей, самообновление, самоудаление, поиск антивирусов в системе, шифрование трафика. В данном случае специалисты не зафиксировали использования инструментария Cobalt Strike, из-за которого группа и получила свое название, но техника и тактика очень напоминают атаки, которые проводились ранее.

(вгору)

Додаток 15

30.05.2018

Xenotime нацелилась на системы безопасности предприятий США

На хакерскую группу, стоявшую за прошлогодней атакой вредоносного ПО Triton на критическую индустриальную инфраструктуру на Ближнем Востоке, эксперты возлагают ответственность за подготовку новой волны кибератак, ориентированных уже на системы аварийного управления (Incident Control System, ICS) в США (Компьютерное Обозрение).

Эту группу, получившую название Xenotime, исследователи информационной безопасности из фирмы Dragos характеризуют как «наиболее опасную из широкоизвестных». Она использует вариант вредоносного ПО Triton (Trisis), который нацеливает на разнообразное оборудование, контролирующее безопасность производственных процессов, включая системы, разработанные Schneider Electric SE для нефтегазовой отрасли, но не ограничиваясь ими.

Характерная особенность планируемых атак это их точная нацеленность, а также задача: не только нарушать работу систем, но и вызывать физические повреждения. «Прицел на систему безопасности демонстрирует, что нанесение значительного ущерба и человеческие жертвы были намеренными или допустимыми последствиями атаки», – объяснили исследователи.

Системы аварийного контроля помогают инженерам сохранять управление производственными процессами и отключать их в случае аварии. «Dragos с умеренной уверенностью оценивает, что Xenotime намерена обеспечить себе необходимый доступ и способность вызвать потенциальное нарушающее работу или даже разрушающее происшествие», – утверждают исследователи.

Орен Аспир (Oren Aspir), CTO Cyberbit, указывает на параллели с приписываемой русским хакерам атакой на ответственную инфраструктуру США, о которой US-CERT сообщала в этом году.

«Обе атаки начались с социальной инженерии, чтобы убедить сотрудников открывать фишинговые письма или посещать инфицированные (watering hole) веб-сайты, – объяснил Аспир. – Затем атакующие получали административный доступ к ИТ-сетям, через которых они определяли точки

соприкосновения информационных (ИТ) и операционных (ОТ) технологий для проникновения в ICS».

Аспир рекомендует начать с решений для ОТ, обеспечивающих видимость и выявление аномалий. Их можно установить за пару дней, и это позволит легко обнаруживать атаки Triton.

(вгору)

Додаток 16

29.05.2018
Дмитрий Сизов
UKR.NET повысил уровень безопасности Почты

25 мая Европа перешла на новые правила обработки персональных данных, установленные Общим регламентом о защите данных (Регламент ЕС 2016/679 или GDPR – General Data Protection Regulation). Производитель самой популярной украинской электронной почты @UKR.NET, которой пользуются более 40 % пользователей e-mail сервисов в Украине, также ввел повышенные стандарты защиты персональных данных (InternetUA).

В Общих настройках обновленной версии почты @UKR.NET появился отдельный раздел «Настройки безопасности», что позволяет быть информированным о событиях, связанных с безопасностью аккаунта. В нем собрано шесть подразделений: Открытые сессии, Журнал безопасности, Смена пароля, Контакты для восстановления, Личные данные и Удаление аккаунта.

Открытые сессии

С помощью подраздела «Открытые сессии» можно убедиться, что к почтовому ящику нет постороннего доступа, просмотрев устройства, которые сейчас подключены к вашей почте, и подробности открытых сессий. А именно:

•подробная информация про дату и время создания сессии, а также – об устройстве, с которого произошел вход в почту;

•тип устройства, на котором зафиксировано текущую активность пользователя и другие детали: операционная система устройства и его версия (например, Windows 10);

•браузер (например, Chrome 64);

•IP-адрес, с которого используется аккаунт;

Это актуально, когда, например, вы проверяли почту и оставили ее открытой на компьютере друзей или забыли выйти из личного ящика на рабочем компьютере. Вам не придется возвращаться или беспокоить кого-то с просьбой выйти из вашего почтового ящика. Можно закрыть такие сессии самостоятельно, нажав на крестик напротив соответствующего сеанса в списке открытых сессий и подтвердив действие паролем.

В этом подразделе также доступна детальная информация про неактивные сеансы и сессии с пользовательской активностью.

Скажем, вам необходимо было срочно распечатать билет со своей почты и вы воспользовались публичным компьютером (ваш вход в ящик – текущая

сессия). На поезд вы успели, а вот выйти из своего ящика на этом устройстве – нет (такая сессия будет отражена как неактивная). И теперь следующий пользователь компьютера может случайно получить доступ к вашей почте. Если он начнет, например, просматривать ваши письма, сеанс будет обозначено как «Сессия с активностью пользователя». Но не беспокойтесь – вы можете закрыть такие сессии самостоятельно, нажав на крестик напротив соответствующего сеанса в списке открытых сессий и подтвердив действие паролем.

Журнал безопасности

Просмотреть действия, связанные с безопасностью почтового ящика, можно в подразделе «Журнал безопасности». Он фиксирует все попытки входов в ящик, изменения контактов для восстановления, доступ внешних программ, изменение настроек пересылки писем на другие адреса, подтверждение удаления аккаунта, неудачные попытки изменения настроек безопасности и тому подобное. Всего Журнал фиксирует более полусотни событий, связанных с безопасностью.

Список событий по умолчанию отображается в развернутом виде. Возле каждого события показана детальная информация о сессии (сессиях), в рамках которой было зафиксировано действие:

•дата и время события;

•информация об устройстве: название, браузер и его версия, операционная система и ее версия;

•IP-адрес и флаг страны, за которой она закреплена.

Контакты для восстановления

В разделе «Контакты для восстановления» можно добавить мобильные телефоны и резервные e-mail-ы для восстановления доступа, а также обновить их в случае изменения. Контактные данные для восстановления позволяют быстро вернуть доступ к ящику, если, например, пользователь не помнит пароль от него. Кроме того, на эти контакты будут приходить оповещения о событиях, связанных с безопасностью аккаунта.

Чтобы обезопасить себя, можно указать основные и резервные e-mail-ы, а также номера мобильных телефонов. Например, номер доверенного лица на случай, если ваш мобильный телефон будет недоступен.

Кроме того, в Настройках безопасности можно сменить пароль, воспользовавшись рекомендациями относительно его надежности. @UKR.NET советует не использовать пароли, которыми пользовались на других сайтах и сервисах, ведь, «взломав» их, посторонние могут получить доступ и к ящику. Также – пароль желательно менять по крайней мере раз в год.

Подраздел «Личные данные» содержит информацию, которую пользователь указывал при регистрации почтового ящика @UKR.NET: имя, фамилия, дата рождения и пол. Они нужны для восстановления доступа к аккаунту по письменному заявлению, если восстановить пароль в онлайне по каким-то причинам не удается (например, не были указаны контакты для

восстановления). Поэтому эти данные должны совпадать с данными паспорта или ID.

Настройки безопасности имеют дополнительную степень защиты: ни одна смена невозможна без подтверждения правильным паролем. Таким образом, даже если другие лица получили доступ к ящику, они не смогут ни закрыть любую другую сессию, ни сменить пароль или добавить свой контакт для восстановления, ни удалить аккаунт. О неудачных попытках изменить настройки безопасности с другого устройства, на котором, например, не была нажата кнопка «Выход», когда проверяли почту с другого компьютера, пользователь сможет узнать из соответствующих записей в Журнале безопасности.

Раздел «Настройки безопасности» доступен в новом интерфейсе почты @UKR.NET в Общих настройках. Подробнее о новые функции в обзоре.

(вгору)

Додаток 17

31.05.2018

Ирина Фоменко

ФБР рекомендует: перезагрузите роутер, чтобы вас не взломали российские хакеры

Хакеры могут воспользоваться интернет-шлюзом для кражи пользовательских данных. Недавно ФБР настоятельно рекомендовало перезагрузить все домашние и офисные маршрутизаторы в связи с обнаружением Cisco Talon group хакерской российской программы VPNFilter, заразившей не менее 500 000 сетевых устройств (InternetUA).

Что за угроза?

Угроза может быть довольно серьезной, поскольку весь трафик идет через маршрутизатор. «VPNFilter способен вывести офисные и домашние роутеры из строя. Вредоносная программа может также собирать информацию, проходящую через маршрутизаторы», – предупреждают в ФБР.

Роутеры обычно являются легкой целью для хакеров, так как они подключены непосредственно к Интернету и редко защищены антивирусами, а большинство пользователей не устанавливают обновления прошивки маршрутизатора. Согласно заявлению ФБР, обнаружить взлом сложно, потому что VPNFilter шифрует сетевой трафик.

По данным Cisco, последние взломы были зафиксированы в Украине. Министерство юстиции США считает, что VPNFilter связан со шпионской российской организацией Sofacy Group.

Какие маршрутизаторы под угрозой?

ФБР рекомендует владельцам роутеров перезагрузить свои устройства. Кроме того, по словам представителей Cisco Talon group, «действия по обеспечению безопасности должны быть предприняты для всех устройств SOHO или NAS».

Symantec выпустил следующий список маршрутизаторов и устройств NAS, которые, как известно, восприимчивы к VPNFilter. Некоторые из них – довольно популярные модели.

- Linksys E1200
- Linksys E2500
- Linksys WRVS4400N
- Mikrotik RouterOS Cloud Core Routers: версии 1016, 1036, и 1072
- Netgear DGN2200
- Netgear R6400
- Netgear R7000
- Netgear R8000
- Netgear WNR1000
- Netgear WNR2000
- QNAP TS251
- QNAP TS439 Pro
- Другие QNAP NAS устройства, использующие ПО QTS
- TP-Link R600VPN

Как перезагрузить роутер?

Перезагрузка маршрутизатора устраняет то, что Cisco называет элементами «Этап 2» и «Этап 3» VPNFilter – разрушительную частью вредоносного ПО.

Перезапустить роутер очень просто: нужно отключить его от питания на 30 секунд и снова подключить.

Что еще нужно предпринять в мерах безопасности?

ФБР и некоторые производители устройств рекомендуют отказаться от функций удаленного управления маршрутизатором, которые в большинстве случаев отключены по умолчанию. Также можно изменить учетные данные для входа в аккаунт, создав новый уникальный пароль, который не используется для других веб-сайтов или служб.

Несмотря на то, что антивирус ПК обычно не защищает маршрутизаторы, Symantec заявляет, что его программное обеспечение может обнаруживать VPNFilter. Использование антивируса может обезопасить пользователя от взлома.

Нужен ли полный заводской сброс?

«Этап 1» VPNFilter может сохраняться даже при перезагрузке, что позволяет вредоносному ПО впоследствии получить доступ к данным. Министерство юстиции «арестовало» домен, который программа использовала для установки поздних этапов VPNFilter на зараженных компьютерах. Однако, как сообщают в ФБР, это не является гарантией устранения угрозы.

Единственный способ полностью удалить вредоносное ПО – выполнить заводскую перезагрузку маршрутизатора и обновить его до последней версии прошивки, которая будет защищать от известных уязвимостей.

Точная процедура сброса маршрутизатора может варьироваться, хотя обычно достаточно на обратной стороне роутера нажать на соответствующую

кнопку, а затем подключить его к ПК для завершения настройки. Linksys, MikroTik, Netgear, QNAP и TP-Link опубликовали инструкции по восстановлению заводских настроек маршрутизаторов.

(вгору)

Додаток 18

1.06.2018

Twitter массово блокирует аккаунты пользователей, которым на момент регистрации не было 13 лет

Разработчики Twitter начали блокировать пользователей, чей возраст не соответствовал правилам пользования сервисом на момент регистрации учетной записи (ITUA.info).

Поскольку сервис микроблогов Twitter был запущен в 2006 году, многим из таких пользователей сейчас гораздо больше 18 лет, пишет Guardian.

На такой шаг администрация Twitter пошла в попытке выполнить требования «Общего регламента по защите данных» (GDPR – General Data Protection Regulation), который вступил в силу с 25 мая 2018 на территории Евросоюза.

«Я получил сообщение о том, что мой аккаунт был заблокирован, и для обработки моих данных потребуется родительская согласие, или мой аккаунт будет удален», – сказал Guardian один пользователь, которому 20 лет. Он завел аккаунт в 2009 году, указав день рождения, а потом поставил поддельный возраст, как только компания представила возможность добавить эту информацию. Затем он обновил ее до своего фактического дня рождения.

Twitter пока не комментирует официально эту ситуацию. При этом источники в компании подтвердили, что решение о блокировании было принято. Поскольку в соцсети нет инструментов для разделения контента, созданного пользователем в возрасте до 13 лет и контента, созданного тем же человеком, которому уже исполнилось 13 разработчики решили, что единственным способом соблюдения нового закона будет блокирование некоторых пользователей.

Однако, Twitter, пожалуй, работает над более адекватным решением, а некоторые пострадавшие сообщили о возможности восстановления доступа к своим аккаунтам, после предоставления документов, подтверждающих их нынешний возраст.

(вгору)

Додаток 19

1.06.2018

Facebook до сих пор не знает, какие именно данные получила Cambridge Analytica

Макс Яначек

Главная операционная директор компании Facebook Шерил Сандберг (Sheryl Sandberg) заявила, что в 2016 году они не заметили злоупотреблений с данным миллионов пользователей, потому что сосредоточились на противодействии спаму и фишинговым атакам (Bad Android).

Об этом она сказала на конференции Code 30 мая, сообщает Tech Crunch.

Напомним, в марте британские и американские СМИ опубликовали расследование, согласно которым британская компания по политическому консалтингу Cambridge Analityca незаконно получила данные миллионов профилей пользователей Facebook. Сначала речь шла о данные 50 миллионов юзеров, однако позже Facebook сообщила, что на самом деле их было до 87 миллионов. Эти данные могли использоваться в политических целях. С Cambridge Analityca сотрудничал в том числе и штаб кандидата в президенты США Дональда Трампа.

«Если вы вернетесь в 2016 год и подумаете, что тогда беспокоило людей по наций, государств и безопасности выборов, то это в основном спам и фишинговые атаки», – отметила госпожа Сандберг, напомнив о поражении электронных почт Sony. Главная операционная директор подчеркнула, что Facebook тогда сумела избежать проблем, которые предстали перед другими компаниями.

Шерил Сандберг также подчеркнула, что работая над предупреждением этих угроз, Facebook не заметила, как возникла другая, еще большая. Однако по ее словам, сейчас компания уже полностью ее осознала и сможет лучше ей противодействовать во время будущих выборов.

Со сцены госпожа Сандберг также заявила, что Facebook не только поздно обнаружила несанкционированный доступ Cambridge Analytica к данным ее пользователей, но и до сих пор точно не знает, какие именно данные попали в распоряжение британской компании по политическому консалтингу.

Главная операционная директор сообщила, что Facebook проводил собственное расследование относительно этого, когда правительство Британии заявил, что начинает свое. За это компания приостановить свой внутренний аудит.

«У них не было никаких данных, которые мы не могли бы идентифицировать как наши. На сегодняшний день мы до сих пор не знаем, какие данные должна Cambridge Analytica», – отметила Шерил Сандберг.

(вгору)

Додаток 20

1.06.2018

Chrome и Firefox сливали данные о пользователях Facebook

С 2016-го года в Google Chrome и Mozilla Firefox существовала уязвимость, которая позволяла сайтам получать информацию о Facebook-профилях посетителей (InternetUA).

Проблема просуществовала более года, ее исправили в обновлениях: Chrome 63 (вышел в прошлом году) и Firefox 60 (вышел две недели назад).

Причиной появления уязвимости стала новая функция, которая появилась в языке CSS в 2016 году. Она называется mix-blend-mode и вводит смешивание разных цветов. Она же позволяла сайтам получать информацию из Facebook.

Использовались iframe-элементы (так встраивают кнопки лайка или логина) и необычный способ обработки данных. Объектом «слива» были лишь пиксели – баг не позволял выгружать целые картинки или посты.

Сайты анализировали то, что «видели» на iframe-элементе, помещая сверху дополнительные слои-обработчики, поскольку получить доступ к его содержимому не могли.

Изъятые пиксели можно обработать при помощи системы оптического распознавания. Таким образом они узнавали имена пользователей или изображения их профилей.

Хотя со стороны процесс выглядит довольно сложно, на выполнение всех операций компьютер мог потратить не более 20 секунд, отмечает издание Slashgear.

При этом, обычно в браузерах действует политика безопасности, что не позволяет доменам обмениваться информацией, которую они хостят – однако в данном случае правила были нарушены.

Браузер Safari не подвергался уязвимости, а в Internet Explorer и Edge просто не было поддержки mix-blend-mode.

Однако, как опасаются исследователи, которые обнаружили проблему, с осложнением веб-технологий и увеличением возможностей HTML и CSS появится все больше способов получать доступ к чужим данным.

(вгору)

Додаток 21

4.06.2018

«Умные» часы могут быть использованы для слежения за их владельцем

Эксперты «Лаборатории Касперского» выяснили, какие возможности открывает анализ сигнала носимых устройств для потенциальных злоумышленников. Например, получив доступ к умным часам, киберпреступники могут собрать сигналы встроенных в них сенсоров, изучить их и впоследствии получить набор уникальных данных о владельце. Они позволяют сформировать поведенческий профиль человека и зафиксировать моменты ввода критически важных данных: определить, когда он приходит на работу, вводит пароль доступа от корпоративного компьютера, разблокирует телефон. Сопоставив данные о перемещении пользователя с координатами, можно также определить моменты посещения банка и ввода ПИН-кода на клавиатуре банкомата (Компьютерное Обозрение).

В повседневной жизни многие регулярно пользуются умными часами и фитнес-трекерами. В большинство этих гаджетов встроены датчики ускорения (акселерометры), вращения (гироскопы) и даже магнитного поля (магнитометры). Записывая сигналы с этих сенсоров, злоумышленники могут получить доступ к личной информации пользователя. Вот почему важно уделять внимание, казалось бы, менее очевидным потенциальным источникам киберугроз – IoT-устройствам.

Вероятный сценарий использования носимых устройств злоумышленниками связан с загрузкой на умные часы приложения (например, фитнес-трекера), которое может отправлять на серверы киберпреступников пакеты данных. Для более точного профилирования жертвы достаточно всего один раз отправить геопозицию владельца IoT-устройства или запросить разрешение на получение адреса его электронной почты, после чего уникальные сведения о поведении пользователя и его конфиденциальная информация потенциально становится лёгкой добычей. При этом стоит отметить, что приложения, допускающие передачу данных акселерометров и гироскопов третьим лицам, на данный момент считаются легитимными с точки зрения магазинов приложений.

«Лаборатория Касперского» рекомендует владельцам смарт-часов обращать внимание на следующие признаки того, что их данные могут находиться под угрозой, и соблюдать определенные правила безопасности:

- если приложение отправляет запрос на получение данных об аккаунте пользователя (разрешение GET_ACCOUNTS в Android), это может означать, что злоумышленник пытается сопоставить «цифровой отпечаток» с его владельцем;
- если приложение дополнительно запрашивает разрешение на отправку геолокационных данных – это повод насторожиться, не стоит выдавать фитнес-трекерам, загружаемым на умные часы, лишних разрешений, а также не рекомендуется указывать корпоративные электронные адреса при регистрации;
- если исправное носимое устройство держит заряд вместо суток всего несколько часов, не исключено, что сигналы встроенных в него сенсоров передаются на серверы киберпреступников.

(вгору)

Додаток 22

5.06.2018

Злоумышленники используют Google Play для распространения вредоносного кода

В мае специалисты «Доктор Веб» выявили в каталоге Google Play троянца Android.Click.248.origin, которого злоумышленники распространяли под видом таких известных программ как Skype и «Алиса» (голосовой помощник

от компании «Яндекс», в действительности недоступный в виде отдельного приложения). Троянец загружал мошеннические веб-сайты, где пользователей подписывали на платные услуги (Компьютерное Обозрение).

Также в каталоге Google Play был обнаружен троянец Android.FakeApp, распространяющийся под видом популярных приложений. По команде вирусописателей Android.FakeApp переходил по заданным ими ссылкам и загружал веб-сайты, накручивая счетчик их посещений.

Кроме того, в мае в официальном каталоге ПО для ОС Android были обнаружены очередные представители троянцев семейства Android.HiddenAds, такие как Android.HiddenAds.267.origin и Android.HiddenAds.277.origin. Эти вредоносные программы распространялись под видом безобидных и известных приложений. Главная функция троянцев – показ рекламы.

В минувшем месяце специалисты по информационной безопасности обнаружили несколько новых Android-троянцев, которых злоумышленники использовали для кибершпионажа. Один из них распространялся через Google Play и получил имя Android.Spy.456.origin. Вредоносная программа похищала фотографии, SMS-сообщения, а также контакты из телефонной книги зараженных мобильных устройств и загружала их на удаленный сервер киберпреступников. Другой мобильный троянец-шпион, выявленный в мае, был добавлен в вирусную базу Dr.Web как Android.Spy.457.origin. Он крал изображения и видеоролики, хранящиеся в памяти Android-смартфонов и планшетов, похищал SMS, отслеживал координаты мобильных устройств, а также мог прослушивать окружение и записывать телефонные разговоры.

В конце месяца специалисты компании «Доктор Веб» обнаружили новую версию коммерческой программы-шпиона Onespy, получившую имя Program.Onespy.3.origin. Это приложение способно перехватывать SMS-сообщения и телефонные звонки, отслеживать местоположение зараженного устройства, прослушивать окружение, красть фотографии, видео, документы и другие файлы, следить за перепиской в популярных программах для общения, таких как Skype, Viber, WhatsApp, Line, Facebook и других, а также выполнять прочие опасные действия.

Несмотря на усилия корпорации Google, злоумышленникам по-прежнему удается распространять Android-троянцев через каталог Google Play. Кроме того, вредоносные и потенциально опасные программы для мобильных устройств подстерегают пользователей и вне официального каталога приложений. Для защиты смартфонов и планшетов их владельцам рекомендуется использовать проверенные временем антивирусные продукты для Android.

(вгору)

Додаток 23

5.06.2018

Группировка Andariel Group нашла в ActiveX дыру нулевого дня

Эксперты обнаружили новую кампанию по кибершпионажу с использованием как минимум девяти брешей в платформе ActiveX, в числе которых уязвимость нулевого дня. Предположительно за атаками стоит группировка Andariel – одна из дочерних организаций Lazarus. Целью преступников является хищение данных крупных южнокорейских предприятий (Центр информационной безопасности).

Как сообщают исследователи безопасности, атаки начались еще в прошлом месяце. По примеру родительской группировки участники Andariel заражают легитимные сайты трояном, который затем передается посетителям. Злоумышленникам остается только ждать компрометации одного из устройств интересующих их организаций.

Киберпреступников из Lazarus, предположительно связанных с руководством Северной Кореи, уже не впервые ловят на эксплуатации уязвимостей в ActiveX. Как сообщает представитель южнокорейского агентства интернет-безопасности (KISA), на этот раз в качестве одной из лазеек использовалась уязвимость нулевого дня.

Технические детали нападений пока не раскрыты, однако эксперт, пожелавший остаться неизвестным, сообщил, что эта же брешь в защите сделала возможной атаку на Samsung SDS Acube – распространенный в Южной Корее инструмент для совместной работы.

Andariel связали с Lazarus южнокорейские исследователи из компании AhnLab, причем это далеко не единственная дочерняя организация киберсиндиката, на счету которого – целый ряд нашумевших инцидентов. Считается, что именно эта APT-группировка стояла за массовой утечкой данных компании Sony Pictures в 2014 году, а «коллеги» Andariel из Bluenoroff совершили нападения на финансовые организации, казино и коммерческие структуры, оперирующие криптовалютой.

Министерство внутренней безопасности США ассоциирует с деятельностью Lazarus группировку Hidden Cobra, которая проводила масштабные DDoS-атаки против американских СМИ, промышленного и финансового сектора. Около месяца назад Тайландский центр быстрого реагирования на компьютерные преступления ThaiCERT захватил один из командных серверов Hidden Cobra, совместно с международными экспертами вскрыв масштабную вредоносную кампанию GhostSecret.

(вгору)

Соціальні мережі

як чинник інформаційної безпеки

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

Упорядник **Терещенко** Ірина Юріївна

Свідоцтво про державну реєстрацію КВ № 5358 від 03.08.2001 р.

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