СОЦІАЛЬНІ МЕРЕЖІ ЯК ЧИННИК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Огляд інтернет-ресурсів
(27.02–12.03)

2019 № 5

Соціальні мережі
як чинник інформаційної безпеки

Інформаційно-аналітичний бюлетень
Додаток до журналу «Україна: події, факти, коментарі»
Огляд інтернет-ресурсів
(27.02–12.03)
№ 5

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 2019

ЗМІСТ

Орфографія та стилістика матеріалів – авторські

РОЗВИТОК І ПЕРСПЕКТИВИ СОЦІАЛЬНИХ МЕРЕЖ

27.02.2019
Дмитрий Демченко
Telegram добавил поддержку нескольких аккаунтов в iOS-приложение

Telegram выпустил новое обновление мессенджера, в рамках которого добавил в iOS-приложение поддержку нескольких аккаунтов. Об этом сообщается в блоге компании (AIN.UA).

Раньше возможность добавить несколько аккаунтов была только на Android. Теперь пользователи iOS могут привязать к своему приложению до трех номеров. Это позволит быстро переключаться между ними без необходимости выходить из аккаунта. К тому же, пользователь будет получать уведомления со всех аккаунтов – в них будет в том числе указано, на какую учетную запись они были отправлены.

Telegram также добавил автоматический запуск видео – без звука. Пользователи теперь могут вручную установить параметры автоматических загрузок по типу чата, а также типу и размеру файла. Приложение запомнит этот выбор, если нужно будет временно изменить один из параметров.

***

27.02.2019
WhatsApp вводит ограничение для групповых чатов

Мессенджер WhatsApp вводит ограничение, согласно которому получать приглашение в групповые чаты можно будет только от пользователей, которые находятся в списке контактов. Таким образом мессенджер намерен бороться со спамом (Зеркало недели. Украина).

Отмечается, что злоумышленники используют мессенджер в корыстных целях: с помощью специального программного обеспечения они приглашают в групповые чаты всех подряд. Из-за того, что рассылка является анонимной, добавление в групповые чаты превращается в предложение запрещенных товаров и услуг. Именно с этим разработчики мессенджера и решили бороться.

Система приглашений в сообщества больше не будет существовать в прежнем виде. По умолчанию все пользователи WhatsApp смогут принимать приглашения вступить в групповой чат только от тех абонентов, кто присутствует в их списке контактов. От всех остальных предложения вступить в те или иные группы будут сразу блокироваться.

***

27.02.2019

Google запустила бесплатного «убийцу» WhatsApp для Android

Уже в первой половине 2019 года американская корпорация избавится от WhatsApp, Skype и других мессенджеров на Android, потому как пользователям гаджетов на базе данной ОС предложат альтернативный способ для общения, более простой и удобный.

Докладніше

***

28.02.2019

Facebook позволит пользователям удалять историю авторизаций на сторонних сайтах и приложениях

Финансовый директор Facebook Дэвид Венер (David Wehner) на конференции в Сан-Франциско заявил, что компания запустит функцию «Очистить историю» в 2019 году. По его мнению, новый инструмент повлияет на таргетированную рекламу в Facebook (InternetUA).

Функция позволит пользователям смотреть, на каких сайтах и приложениях они авторизовались через Фейсбук, и удалять эту информацию со своего аккаунта. По сведениям BuzzFeedNews, компания начнёт тестировать функцию весной.

Венер заявил, что после введения функции Facebook станет сложнее использовать информацию, собранную внешними сайтами, для таргетированной рекламы. По мнению The Verge, таким образом компания пытается вернуть доверие пользователей и восстановить свою репутацию после скандала с Cambridge Analytica.

Впервые о функции объявили в мае 2018 года. Тогда Марк Цукерберг сравнил функцию с удалением файлов cookie из браузера. Он сказал, что пользователи смогут удалять информацию о приложениях и сайтах, на которых они авторизовались через Фейсбук. Но если это сделать, то пользователю придётся заходить заново на каждый сайт.

***

1.03.2019

Угроза для Facebook. Число пользователей китайской соцсети превысило миллиард

Сервис TikTok, позволяющий снимать и распространять короткие видео в развлекательном стиле, почти сравнялся по темпам прироста с крупнейшей социальной сетью (InternetUA).

Количество загрузок социального приложения для распространения коротких видео TikTok превысило 1 млрд. Таким образом «приложение-выскочка» нарушило монополию западных компаний, таких как социальная сеть Facebook и мессенджер Snapchat. По данным Hootsuite, число

пользователей этих приложений в января 2019 года составляло 2,27 млрд и 287 млн соответственно. Об этом сообщила исследовательская компания Sensor Tower.

TikTok предназначен для создания и распространения коротких видеороликов, а также «живых» трансляций. Приложение предоставляет возможность снимать 15-секундные видео в различных жанрах. Например, в музыкальном, комедийном, танцевальном. Снятое видео можно «украсить» более 100 «наклейками»-эмодзи. Сервис в 2016 году запустила китайская компания ByteDance.

Только в 2018 году число установок этой мобильной программы составило 663 млн. Для сравнения, у Facebook этот же показатель достиг 711 млн, а у Instagram – всего 444 млн. Причем устанавливают приложение отнюдь не только китайские пользователи. Идея развлекательного «видео-твиттера» пришлась по душе всем жителям планеты.

***

2.03.2019

Twitter дозволить приховувати коментарі під постами

Це має зробити спілкування більш конфіденційним, тобто наблизити твітим до аналогу особистого листування. Також опція дозволить відфільтрувати записи і відповіді на них, прибравши їх зі своєї стрічки.

Докладніше

***

3.03.2019

Гра престолів. Чому Telegram вб'є Viber і що буде з іншими месенджерами

Месенджер Viber вводить плату за чат-боти. Яким чином це відіб'ється на конкуренції зі схожими додатками та який месенджер незабаром може завоювати світовий ринок?

Докладніше

***

3.03.2019

В Facebook Messenger стала доступна тёмная тема

Все пользователи Facebook знают, что несколько лет назад было запущено мобильное приложение Facebook Messenger. В какой-то мере оно является аналогом таких приложений как, например, WhatsApp, и позволяет не только общаться между собой зарегистрированным пользователям Facebook, но и находить друзей по номеру телефона (InternetUA).

Однако, несмотря на огромную популярность данной соцсети, в мессенджере до сих пор не было некоторых востребованных функций – например, возможности использовать тёмную тему, которая особенно актуальна для обладателей девайсов с AMOLED-дисплеями. Конечно, неофициально темное оформление можно было использовать и ранее, но для этого был необходим root, а ведь далеко не все пользователи готовы рисковать безопасностью своего устройства ради установки тёмной темы.

Однако в последнем обновлении разработчики Facebook Messenger добавили небольшую пасхалку: стоит отправить кому-либо из ваших контактов смайлик в виде полумесяца, как система сразу предложит включить «ночной режим», то есть перейти на то самое долгожданное темное оформление. Если этого не произошло – нужно полностью закрыть программу, убрав его из списка недавних приложений, и запустить мессенджер заново.

***

5.03.2019

В Skype будет проще выразить настроение

Команда разработчиков Skype предложила участникам собственной программы предварительного тестирования протестировать улучшенную версию «сообщений о настроении». В русскоязычной версии они почему-то именуются «новостями» (Украинский телекоммуникационный портал).

Если раньше сообщать друзьям и коллегам о своём настроении пользователям Skype нужно было вручную, набирая текст в строке состояния, теперь программа будет предлагать им набор готовых сообщений. Разумеется к тексту можно будет прикрепить и эмотикон – без картинки сегодня в сети никуда.

Текстовый вариант сообщения о настроении будет по-прежнему виден только в профиле, а вот выбранный эмотикон будет демонстрироваться рядом с именем пользователя в списке чатов и контактов.

Оценить эти изменения можно в Skype Preview для Windows версии не ниже 14.41.43.0. Разработчики уточняют: реализованы новшества по отзывам инсайдеров.

***

6.03.2019

Viber анонсировал темный режим и быстрый поиск внутри чата

Viber анонсировал запуск очередной версии, в которой доступен темный режим. В темном режиме фон чатов становится черным, в то время как буквы и элементы управления – светлыми. Новая функция позволяет экономить заряд батареи, меньше напрягать зрение и сделать свет от экрана менее ярким. Новая функция предназначена, прежде всего, для использования Viber в темноте, но она подходит для любой ситуации и любого времени суток. Темный режим уже

доступен в Viber на Android, и в скором времени также запустится на iOS (Marketing Media Review).

Среди последних обновлений также представлены групповые звонки, которые были анонсированы в рамках запуска Viber 10, но теперь становятся доступны всем пользователям в мире. Эта опция позволяет совершать конференц-звонок группам до 5 человек одновременно. При этом можно как пригласить людей присоединиться к звонку, так и позвонить участникам существующего чата. На данный момент доступны аудиозвонки, но в скором времени Viber добавит возможность совершения групповых видеозвонков.

Кроме того, в приложении появится быстрый поиск внутри чата. Поиск можно осуществлять по ключевым словам в личных диалогах, групповых чатах, сообществах и даже чат-ботах. Функция уже доступна на Android-устройствах и вскоре появится на IOS.

***

10.03.2019

Единый мессенджер Facebook создаст конкуренцию iMessage

Как известно, Facebook планирует объединить мессенджеры Messenger, WhatsApp и Instagram для улучшения конфиденциальности. В новом отчете портала Slate журналисты объяснили, как это приведет Facebook к прямой конкуренции с Apple.

Докладніше

***

11.03.2019

Twitter запустил новое экспериментальное приложение

Twitter объявил о запуске нового приложения Twttr, в рамках которого социальная сеть будет тестировать экспериментальные опции. Первая тестовая опция, доступ к которой получат пользователи Twttr – модификация интерфейса. Благодаря этой модификации разговор пользователей в соцсети становится похожим на более привычную переписку в мессенджере. При этом реплики-твиты пользователей маркируются цветом, что довольно удобно, если в разговоре участвует больше двух человек. После завершения тестирования в Twttr новый интерфейс может появиться и в основной версии соцсети (InternetUA).

Само собой, тестированием одной функции дело не ограничится. По словам представителей компании, в дальнейшем в рамках Twttr будут тестироваться и другие новшества.

Чтобы получить доступ к экспериментальному приложению, необходимо заполнить анкету и ждать приглашения. Конечно, шанс на то, что вас пригласят в рамках первой волны, очень мал. Для первого тестирования компания хочет

привлечь всего 2 тыс. пользователей, говорящих на английском и японском языках.

Впрочем, если вы очень хотите попасть в Twttr, анкету заполнить стоит. Ведь для будущих проектов разработчикам может понадобиться намного больше пользователей из разных стран.

***

11.03.2019

«ВКонтакте» выбыл: опубликован топ-15 мобильных приложений февраля

Компания Kantar TNS опубликовала свежий рейтинг популярных в Украине мобильных приложений. В феврале четверка лидеров остается неизменной. Это Viber и троица от Google – Chrome, YouTube, Gmail (InternetUA).

При этом, в сравнении с прошлым февралем охват Facebook вырос с 65 % до 80 %. Telegram показал рост с 27,5 % до 46,7 % соответственно.

Резко выросло по охвату приложение для видеочата – Google Duo. А «ВКонтакте» и Skype выбыли из топ-15. Приложения от российской соцсети не было в рейтинге уже в декабре 2018 года, а вот программа для звонков от Microsoft еще была.

СОЦІАЛЬНІ МЕРЕЖІ ЯК ВИЯВ ФОРМУВАННЯ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА

27.02.2019

#ДоброЧесніВибори. Социальная реклама призвала украинцев не продавать голоса на выборах

Общественное движение ЧЕСНО и информационная молодежная кампания «Твой голос» надеются, что месседж #ДоброЧесніВибори превратится во флешмоб и призывают всех, кто сталкиваются с попытками покупки голосов, публично заявлять об этом в социальных сетях под хэштегом #ДоброЧесніВибори.

Докладніше

***

6.03.2019

У Зе!команді похвалилися відвідуваністю сайту: рівень кампанії Обами

У команді кандидата в президенти шоумена Володимира Зеленського кажуть, що будують дуже експериментальну для української політики структуру діджиталу. Одна і та ж команда працює з усіма соціальними медіа: немає розподілу, хто конкретно відповідає за FB, Instagram і т. д.

Докладніше

***

5.03.2019

Роботодавці Кіровоградщини можуть дізнатися про нюанси зайнятості у соцмережі Facebook

У минулому році до базових центрів зайнятості Кіровоградської області (філій обласного центру зайнятості) з метою працевлаштування шукачів роботи на 34 269 вакансій звернулось 5 114 роботодавців. Серед числа працевлаштованих безробітних, 312 осіб працевлаштовані на нові робочі місця з компенсацію роботодавцям фактичних витрат у розмірі єдиного внеску на загальнообов'язкове державне соціальне страхування на випадок безробіття. Профнавчання на замовлення роботодавців пройшли 5628 безробітних (Прожектор).

«Одним із елементів співпраці з роботодавцями є проведення інформаційно-роз'яснювальної роботи з підприємцями, керівниками підприємств, працівниками кадрових та бухгалтерських служб роботодавців. Служба зайнятості Кіровоградщини йде у ногу з часом, тож ми запровадили на сторінці обласного центру зайнятості у соціальній мережі Facebook рубрику «Електронний кадровий клуб». У цій рубриці розміщується інформація про зміни в законодавстві про зайнятість населення, оглядові тематичні листи щодо висвітлення положень чинного законодавства про зайнятість населення та загальнообов'язкового державного соціального страхування на випадок безробіття, у т. ч. що стосуються професійної діяльності працівників кадрових служб, а також про ті послуги, які надає своїм клієнтам служба зайнятості Для спрощення пошуку згаданої інформації вона позначається хештегом #Електронний_кадровий_клуб»,– зазначив Богдан Стоян, заступник директора обласного центру зайнятості.

***

5.03.2019

Британська королівська сім'я почала війну з тролями у соцмережах

Модератори сторінок Британської королівської сім'ї тепер стежитимуть за коментарями на сторінках Кенсингтонського і Букінгемського палаців.

Модератори стежитимуть за сторінками Кенсингтонського і Букінгемського палаців в соцмережах і видалятимуть коментарі, які вважатимуть образливими, повідомляється на сайті Британської королівської сім'ї (Факти).

Нові правила повинні допомогти у створенні безпечного середовища на відповідних сторінках для того, аби користувачі могли проводити дискусії, ставити запитання і залишати коментарі.

Модератори видалятимуть коментарі, які є образливими, грубими, або ж містять погрози.

В останньому випадку вони навіть можуть звернутися до правоохоронних органів.

***

6.03.2019

Telegram призвал выйти на митинг против изоляции Рунета

Команда мессенджера Telegram призвала пользователей через свой канал выйти на митинг в Москве против законопроекта о «суверенном интернете».

Речь идет о митинге на проспекте Сахарова, который состоится 10 марта в 14:00. Мэрия Москвы согласовала мероприятие (InternetUA).

Руководство мессенджера считает, что власти планируют потратить миллиарды рублей и «отрезать Россию от остального мира», а затем заблокировать иностранные соцсети.

***

10.03.2019

France 24: через відомий рух у Facebook жінки можуть озвучувати свої проблеми

У міжнародний жіночий день у Парижі відбулась акція. Вона розпочалась о 15:40 на Площі Республіки і була присвячена руху за права жінок (Espreso.tv).

Чому саме такий час? За словами учасників, саме в цей час жінки починають працювати безкоштовно. Жінки у всьому світі заробляють на 26 % менше, ніж чоловіки.

За слова Саліми Бел Хадж, журналістки France 24, яка слідкує за цим рухом, з часів появи хештегу Me too у Facebook, жінки почали активніше і вільніше говорити про свої проблеми. Історії з соцмереж консолідують їх і підтримують на всіх континентах і в багатьох країнах.

«З того часу, як з’явився хештег “я теж”, жінки стали більш вільно розповідати про те, що з ними трапилось. І також в Європі, взагалі все почалось у США із цим хештегом, а потім з’явилось у Франції, і тепер стало популярним в Африці – хештег “нам не страшно”. На якомусь фестивалі у місті Буркіна-Фасо жінка, відома акторка, озповіла, що її зґвалтував продюсер. Тому все більше жінок відчувають, що можуть вільно розповідати про такі речі. І це все завдяки соцмережам. За хештегом можна знайти будь-кого. Інформація доходить до людей значно швидше», – розказала Саліма у програмі «Світ цього тижня» на французькому телеканалі France24.

БІЗНЕС І СОЦІАЛЬНІ МЕРЕЖІ

27.02.2019

Facebook тестирует отдельную папку для сообщений от компаний в Messenger

Facebook тестирует новый способ организации сообщений от бизнес-страниц в Messenger. В рамках эксперимента они собираются в одну папку с заголовком «Businesses» (InternetUA).

В Facebook сообщения о появлении новой папки прокомментировали так: «Ранее в этом месяце мы начали тестировать отдельную папку для сообщений от компаний в Messenger. Как и в случае любого другого тестирования, мы хотим убедиться, что обеспечиваем комфортный опыт взаимодействия для пользователей Messenger, предоставляя результаты для рекламодателей. Мы тестируем это нововведение на минимальном количестве пользователей Messenger и на данный момент не планируем расширять этот тест».

Предполагается, что добавление новой папки поможет отделить сообщения компаний от личных сообщений пользователей.

***

27.02.2019

Видеопосты в Instagram получают в 2 раза больше вовлечения

Исследование HubSpot и Mention проанализировало 48,065,694 постов от 306,278 пользователей и выявило, что среднестатистический пост получает 5,963 лайков, однако это число сильно искажено из-за количества лайков от влиятельных юзеров. Среднее число лайков близко к 100 и предполагает, что 50 % пользователей получают менее 100 лайков за пост. Видеопосты получают самое большое количество лайков. Среднестатистический пост в Instagram получает 100. 34 комментариев. Видеопосты в среднем получают 150 комментариев, хотя это значение искажается количеством комментариев вирусных видео. Среднее количество комментариев видео равняется 4, это значит, что более 50 % всех пользователей получают менее 4 комментариев своего видеопоста (Marketing Media Review).

В среднем, у поста в Instagram один хэштег. Большее количество хэштегов понижает средний уровень вовлечения. Лучше использовать меньше хэштегов (не более 5). Важнее всего, чтобы хэштеги были релевантными.

У 46,6 % пользователей менее 1000 фолловеров. У 33,5 % пользователей от 1000 до 10 000 фолловеров. Только у 9,8 % пользователей 10 000-50 000 фолловеров, у 2,7 % юзеров 50 000-100 000 фолловеров.

***

1.03.2019
За Facebook Workplace уже платит два миллиона пользователей

Компания Facebook представила статистику использования Workplace – ориентированной на бизнес разновидности её социальной платформы.

Докладніше

***

4.03.2019
Facebook запустит свою криптовалюту

Facebook работает над запуском собственной криптовалюты, которая будет интегрирована в Messenger, WhatsApp и Instagram (Телекритика).

В первой половине 2019 года корпорация Facebook провела переговоры с криптовалютной биржей, на которой ожидается появление собственного токена Facebook. Об этом пишет The New York Times со ссылкой на источники. Официально компания о проекте еще не рассказывала.

Stablecoin будет привязан к обычным деньгам: евро, долларам и другими национальными валютами, запасы которых находятся на банковских счетах Facebook.

Сначала криптовалюта будет интегрирована в мессенджере WhatsApp, а затем токен введут в Messenger и Instagram. Таким образом расширится ее охват до 2,7 млрд человек, которые каждый месяц пользуются одним из трех приложений. Процесс может занять больше года. С помощью валюты пользователи приложений смогут переводить средства и оплачивать покупки.

***

5.03.2019
У Києві можна оплатити проїзд через соцмережі

У столиці запустили оплату проїзду через соціальні мережі Facebook і Telegram. Оплатити можна на мобільному через спеціальний чат «Київ Пей Бот» (Gazeta.ua).

– Відкрив чат, купив квиток і готово. Є п’ять послуг щодо проїзду. Придбання цілого або половинного проїзного, поїздок, поповнення балансу електронного квитка-картки «Київ Смарт Кард», купівля QR-квитка, – каже розробник Дмитро Однокоз, 34 роки. – Чотири перші пов’язані з карткою. У боті можна лише оперувати з покупками для карти. В транспорті потрібно її фізично використовувати. А ось купівля QR-квитка – разового – не пов’язана з картою. Ви можете купити його в боті, в чат отримаєте картинку QR-коду. Його можна показувати прямо з екрана. Перевірити можна лише валідатором.

За обслуговування платіжний сервіс стягує 3 % комісії. Поїздка вартістю 8 грн подорожчає до 8,24 грн.

***

5.03.2019

Кандидати у президенти мають звітувати про політичну агітацію у соцмережах – аналітик

Кандидати у президенти мають звітувати про кожну копійку, витрачену з виборчих фондів. Та чи звітуватимуть кандидати про рекламу у соціальних мережах, поки що не зрозуміло. Про це в ексклюзивному коментарі журналісту УНН розповів аналітик Громадянської мережі «ОПОРА» Олександр Клюжев.

Докладніше

***

4.03.2019

Українські політики витрачають на рекламу в соцмережах до $4 млн на місяць

Обсяг політичної реклами в соцмережах у період активної передвиборчої кампанії в Україні може сягати $2-4 млн на місяць. Таку оцінку озвучив керуючий партнер комунікаційної групи PlusOne Максим Саваневський в матеріалі Mind «Вибори 2019: як Facebook і Google боротимуться з політичними тролями в Україні».

Докладніше

***

6.03.2019

Instagram тестирует новый рекламный формат для брендированного контента

Instagram подтвердил, что ищет новые способы, как бренды могли бы использовать контент от инфлюенсеров. С прошлого года компания тестирует новый рекламный формат для брендированного контента, который позволил бы превращать посты от лидеров мнений в рекламу. Бренды уже давно используют лидеров мнений для продвижения контента. Но они не могут использовать посты инфлюенсеров с продуктами или услугами в качестве рекламы, чтобы таргетировать пользователей за рамками органического охвата. К компании отметили, что вдохновлены фидбеком от бета-тестов рекламы и планируют использовать новый формат в 2019 году. Согласно недавнему исследованию Mediakix, самыми эффективными форматами инфлюенсер-маркетинга в Instagram являются посты и «Истории». Это же исследование обнаружило, что две трети компаний планируют увеличить бюджеты на инфлюенсер-маркетинг в 2019 году, а 89 % отметили, что Instagram является важной платформой в рамках стратегии по работе с лидерами мнений. Напомним, другое исследование также подтвердило, что инфлюенсеры приносят больше продаж брендам, чем знаменитости (Marketing Media Review).

СОЦІАЛЬНІ МЕРЕЖІ І ПРОБЛЕМИ СУСПІЛЬНОЇ БЕЗПЕКИ

Інформаційно-психологічний вплив мережевого спілкування на особистість

5.03.2019

Instagram став найпопулярнішою платформою для зловмисників, що полюють за дітьми

Про це зазначається у звіті Національного товариства Великої Британії із запобігання жорстокості по відношенню до дітей (NSPCC). Дослідження засноване на даних від правоохоронців (InternetUA).

У цій соцмережі зафіксовано найбільше випадків грумінгу – побудови емоційного зв'язку з дитиною заради отримання її довіри з метою сексуального насильства або експлуатації. Саме так визначає цей термін NSPCC.

У вищезгаданому звіті сказано, що випадки такої злочинної поведінки найчастіше викриваються поліцейськими саме у соціальних мережах. І перше місце серед платформ, де зловмисники розставляють тенета, є Instagram.

NSPCC встановив, що Instagram злочинці використовували у 32 % випадків злочинних спроб, Facebook у 23 %, а Snapchat у 14 %. Дані показують, що використання Instagram як інструменту для грумінгу спостерігалося на 200 % більше з 2017 по 2018 рік. Дані також показують, що дівчатка віком від 12 до 15 років найбільш схильні до надання зворотнього зв'язку зловмисникам.

Facebook і Instagram у коментарі виданню Mashable повідомили, що видаляють 99,2 % контенту, пов'язаного з експлуатацією або оголенням дітей, ще до того, як він буває опублікованим.

Виконавчий директор NSPCC Пітер Ванлес (Peter Wanles) заявив, що політики мають приєднатися до боротьби з грумінгом.

«Ці цифри є переконливим доказом того, що безпека дітей не може бути відповідальністю виключно соціальних мережах», – сказав Ванлес.

***

4.03.2019

Социальные сети негативно влияют на питание детей

Реклама нездоровой пищи может сильно повлиять на то, что дети хотят есть. Исследование показало, что влияние социальных сетей на рацион детей может иметь такое же воздействие – после просмотра соцсетей дети хотят есть калорийные сладкие продукты вместо здоровых аналогов (InternetUA).

Любой ребенок, имеющий мобильный телефон или учетную запись в социальной сети, вероятно, будет следить за одним или несколькими тысячами блогеров, которые регулярно публикуют информацию о том, что они делают, что им нравится и что они едят. Как правило, это молодые люди в возрасте 20 лет, которые успешны, общительны, позитивны, энергичны и «очень привлекательны» для молодежи, говорит Анна Коутс (Anna Coates), психолог в университете Ливерпуля, Великобритания. Исследование Коутс показало, что все эти привлекательные блогеры влияют на диету детей в худшую сторону.

Результаты показали, что просмотры того, популярные пользователи в социальных сетях употребляют здоровые закуски, не имело существенного значения в выборе продуктов. Но если они ели пироги, печенье или фастфуд, то это заставляет детей потреблять на 30 % калорий больше, потому что они начинают есть больше нездоровой пищи.

***

10.03.2019

Мешканці Парижа хочуть відгородитися від користувачів Instagram

Одна з паризьких вуличок стала справжнім хітом соцмереж – її фотографії публікують тисячі користувачів Instagram. Утім, жителі вулиці Кремйо (Rue Cremieux) від її популярності не в захваті. Вони закликають місцеву владу закрити доступ до вулиці для сторонніх осіб – хоча б у окремі години.

Докладніше

Маніпулятивні технології

27.02.2019

Трамп особисто схвалив спецоперацію проти російської «фабрики тролів», – ЗМІ

Президент США Дональд Трамп особисто підписав документ про операцію, яка заблокувала доступ до інтернету для російської «фабрики тролів» під час виборів в Конгрес в 2018 році (Espreso.tv).

Про це повідомляє NBC News з посиланням на джерела.

Телеканал зазначає, що це «найагресивніші» дії адміністрації Трампа для боротьби з російським втручанням у вибори.

За інформацією NBC, інтернет був відключений за кілька годин до початку голосування в Конгрес і був відсутній протягом декількох днів.

Напередодні The Washington Post з посиланням на джерела писала, що в листопаді американські військові відключили доступ до інтернету Агентству інтернет-досліджень («фабрика тролів»).

Агентство інтернет-досліджень, відоме як «фабрика тролів», внесено до списку санкцій США через втручання у вибори президента США в 2016 році. Звинувачення висунув спеціальний прокурор Роберт Мюллер, який веде розслідування «російської справи».

За даними прокурорів, агентство контролюється російським бізнесменом Євгеном Пригожиним, який має тісні зв'язки в російських військових і політичних колах.

***

1.03.2019

Єврокомісія звинуватила Google, Facebook і Twitter у невиконанні обіцянок щодо боротьби з фейками

Пошуковий сервіс Google, соціальні мережі Facebook і Twitter не виконують свої обіцянки щодо боротьби з недостовірними новинами (Espreso.tv).

Про це йдеться у заяві, яку оприлюднила Єврокомісія, передає «Радіо Свобода».

Єврокомісія звинувачує Facebook, що усупереч домовленостям, у січні компанія не надала результати розслідування щодо реклами, що вводить в оману.

Google не роз'яснив, що було зроблено для усунення дезінформації, а Twitter не надіслав результати щодо поліпшення контролю за розміщенням реклами.

У заяві Єврокомісії також йдеться про те, що компанії не продемонстрували прогресу напередодні виборів до Європарламенту.

Рік тому, восени 2018 року, Євросоюз узгодив із Facebook, Twitter і Google добровільний регламент для боротьби з недостовірними новинами.

Документ передбачає маркування політичної реклами та змушує корпорації боротися з інтернет-ботами, які поширюють недостовірну інформацію.

***

3.03.2019

Facebook подал в суд на китайские компании за продажу аккаунтов

Американские компании Facebook и Instagram подали иск в федеральный суд США на четыре фирмы и трех человек из Китая за продажу поддельных учетных записей, лайков и подписчиков. Об этом Facebook 1 марта сообщил на своем сайте (InternetUA).

«Подавая иск, мы надеемся подтвердить, что такого рода мошеннические действия недопустимы, и мы будем действовать решительно, чтобы защитить честность нашей платформы», – говорится в заявлении. Facebook настаивает на

том, что его бренд использовался нелегально, что нарушает американский закон об интеллектуальной собственности.

В пресс-релизе крупнейшей в мире социальной сети также отмечается, что мошенники из Китая использовали ложные аккаунты таких гигантов цифровой экономики как Amazon, Apple, Google, LinkedIn и Twitter.

***

10.03.2019

Російські інтернет-тролі змінили стратегію втручання у вибори через соцмережі – ЗМІ

Пов'язане з Кремлем «Агентство Інтернет-досліджень», яке ще називають «фабрикою тролів», може бути серед тих, хто намагається в новий спосіб обійти запроваджені Facebook та Twitter заходи з видалення фейкового контенту, створеного для впливу на виборців у США під час президентської кампанії у 2016 році.

Докладніше

***

12.03.2019

Украинцам предлагают заработать на аренде аккаунтов в соцсетях

Жителям Украины часто поступают предложения о сдаче в аренду своего аккаунта в популярной соцсети Facebook. Однако такой вид заработка может привести к неприятностям (facenews).

По словам аналитика-расследователя Международного волонтерского сообщества InformNapalm Кристины Добровольской, пользователям соцсети предлагают около 60 долларов в месяц за логин и пароль от Facebook-страницы.

Могут заплатить и больше, если у страницы есть история и в фотоальбоме присутствуют личные фотографии.

При этом эксперт предупреждает, что нужно быть осторожным, поскольку, хотя и говорится, что аккаунт в соцсети будет использоваться для рекламы, может быть, что от вашего имени будут разгонять какую-нибудь нехорошую информацию, в том числе и экстремистскую.

Спецслужби і технології «соціального контролю»

27.02.2019

Майя Яровая

Массовые «чистки» в Telegram: за сутки каналы лишились тысяч подписчиков. Но это коснулось не всех

В ночь на вторник, 26 февраля, мессенджер Telegram провел массовую чистку подписчиков каналов, в результате чего многие сильно просели в цифрах. Некоторые каналы потеряли до 16 000 подписчиков, впрочем есть и такие, кого зачистка не затронула вовсе.

Докладніше

***

6.03.2019

Спецслужби РФ найняли хакера для атаки на державні органи, задіяні у виборчому процесі

Співробітники Служби безпеки України у межах виконання завдань із контррозвідувального забезпечення інтересів держави у сфері інформаційної безпеки попередили спроби спецслужб РФ організувати хакерські атаки на державні установи, які задіяні в підготовці до виборчого процесу та його проведенні (InternetUA). Про це повідомляє прес-центр відомства.

«Оперативники спецслужби встановили, що куратори з Росії найняли хакера із Запоріжжя для розповсюдження шкідливого програмного забезпечення, призначеного для несанкціонованого втручання в роботу державних інформаційних ресурсів України», – йдеться у повідомленні.

Зазначається, що співробітники СБ України задокументували, що зловмисник був адміністратором закритого хакерського Інтернет форуму російського походження. Він підшукував виконавців серед активних учасників форуму, які за грошове винагородження розповсюджували шкідливе програмне забезпечення. Масове поширення здійснювалось через направлення цільових електронних повідомлень на адреси держустанов, а також уразливі ділянки Інтернет-сайтів державних органів.

За висновками фахівців такі комп'ютерні віруси застосовуються, насамперед, для блокування діяльності інформаційних ресурсів через підключення до держреєстрів України, що могло створити загрозу для роботи серверів і персональних комп'ютерів виборчих комісій.

Крім того, співробітники СБУ спільно з кіберполіцією провели обшуки за місцем проживання зловмисника, у ході яких було виявлено комп'ютерну техніку з інстальованим програмним забезпеченням для створення та модифікації комп'ютерних вірусів. Також отримано майже десять зразків шкідливого програмного забезпечення, які були підготовлені для розповсюдження серед учасників закритого хакерського форуму.

***

9.03.2019

Facebook подал в суд на двух украинских хакеров

Facebook подал в суд на двух киевских хакеров, которые с помощью вредоносных расширений браузера отфильтровывали данные профиля

пользователей соцсети и списки их друзей. Об этом сообщает The Daily Beast (InternetUA).

Андрей Горбачов и Глеб Случевский использовали онлайн-викторины для установки вредоносных расширений браузера. Они якобы использовали расширения браузера для наложения своих рекламных объявлений на новостную ленту Facebook, когда пользователи заходили через другие браузеры. Возможно, эти онлайн-анкеты использовались для обработки имен друзей в рекламной копии, имитируя форму многих подлинных рекламных объявлений Facebook.

Мужчины использовали псевдонимы, такие как «Елена Стельма», «Аманда Питт» и «Игорь Коломиец». Их схема работала с 2016 года по октябрь 2018 года.

Facebook утверждает, что данная схема была рассчитана на русскоязычных пользователей. Это нанесло компании ущерб в более 75 тыс. долларов, которые потратили для борьбы с этой схемой.

***

10.03.2019

54-річного чоловіка судитимуть за сепаратистські заклики в соцмережі

Прокуратурою Чернігівської області затверджено та скеровано до суду обвинувальний акт у кримінальному провадженні стосовно 54-річного чоловіка, якого обґрунтовано обвинувачують у посяганні на територіальну цілісність та недоторканість України (ч. 1 ст. 110 КК України) (InternetUA).

Про це повідомляє прес-служба прокуратури Чернігівської області.

Слідчими Управління Служби безпеки України у Чернігівської області під процесуальним керівництвом прокурорів зібрані докази винуватості жителя Прилуцького району у вчиненні цього кримінального правопорушення проти основ національної безпеки України.

Як з’ясувалося, чоловік, зареєструвавши власну електронну сторінку в російській соціально-орієнтованій мережі «Одноклассники», розміщував публічні заклики наступного змісту: «Донбас это Россия», «Освободить Киев, Одессу, Харьков и вместо Украины создать Новороссию», а також інші публічні заклики, спрямовані на зміну меж території та державного кордону України, на порушення порядку, встановленого Конституцією України.

Відтак, на особу очікує судовий розгляд.

Довідково: санкцією ч. 1 ст. 110 КК України передбачено покарання у виді позбавлення волі на строк від трьох до п’яти років з конфіскацією майна або без такої.

***

12.03.2019

«ВКонтакте» видаляє фото з «могилою Путіна»

Соцмережу «ВКонтакте» викрили у видаленні публікацій з фото «могили Путіна» (InternetUA).

11 березня власники відразу декількох груп у російській соцмережі почали повідомляти про зникнення постів з фото «могили Путіна». За твердженнями адміністраторів однієї із груп, соцмережа видалила пост без пояснення причин.

У коментарі прес-служба «ВКонтакте» повідомила, що фотографії видаляються, бо на них надійшло «безліч скарг» і наголосила, що ставиться з розумінням до бажання людей «рідше зустрічати публікації, які вводять їх в оману».

Фотографію з акції з надгробком Путіна в соцмережі порівняли з «неправдивими історіями про вигадану загибель відомої людини» і з фіктивними повідомленнями про надзвичайні ситуації.

«У випадках, коли користувачі розміщують публікацію просто для перевірки, але не стверджують про це як про достовірну новину – ми відхиляли скарги про введення в оману», – заявили в прес-службі «ВКонтакте».

***

12.03.2019
Владимир Кондрашов
Власти хотят ввести цензуру в Интернете по российскому сценарию

Украинские спецслужбы пытаются протянуть через Верховную Раду новый законопроект о цензуре в Интернете. Речь идет о новом законопроекте, который неожиданно «всплыл» в кулуарах парламента.

Информацию о новом законопроекте, у которого пока даже нет регистрационного номера, 12 марта опубликовала на своей странице в Facebook эксперт по стратегическим коммуникациям ОО «Информационная безопасность», бывший заместитель министра информационной политики Украины Татьяна Попова.

Докладніше

Проблема захисту даних. DDOS та вірусні атаки

27.02.2019
У СБУ заявили, що попередили масштабну кібератаку на сайт ЦВК

За інформацією правоохоронців, кібератака була спрямована на блокування доступу користувачів до інформації про підготовку до чергових виборів президента України (InternetUA).

Про це повідомляє прес-центр Служби безпеки України.

«Спеціалісти спецслужби встановили, що атаку було проведено за технологією http flood, через генерацію постійних запитів, які ускладнювали роботу інформаційної системи та блокували можливість доступу звичайних користувачів. Для проведення кібератаки зловмисники використовували розгалужену мережу сайтів на базі неоновленої версії системи WordPress, що дозволило хакерам без відома власників використати їх для генерації об'ємних запитів», – йдеться в повідомленні.

Зазначається, що фахівці СБУ здійснии низку практичних заходів, щоб припинити негативний вплив на роботу сайту Центральної виборчої комісії. Також СБУ перевіряє можливу причетність до організації кібератаки російських спецслужб та підконтрольних їм хакерських угруповань.

***

27.02.2019
Вредоносы научились использовать и отключать антивирусы

Обнаружены два вредоноса. Программа Shlayer для macOS старается отключить систему Gatekeeper, чтобы безнаказанно устанавливать новые модули. Троянец Astaroth для Windows эксплуатирует системный процесс антивируса Avast.

Докладніше

***

27.02.2019
Юри Кострубати
PowerShell становится основным инструментом для взлома

Зачем разрабатывать вредоносное ПО, если есть PowerShell? По данным IBM X-Force, получив доступ к корпоративным сетям, злоумышленники чаще всего используют не к вредоносное ПО, а скрипты для автоматизации. В 2018 году только в 43 % от всех кибератак использовались локально установленные файлы, остальные же осуществлялись непосредственно в памяти. Хакеры предпочитают пользоваться в атаках скриптами PowerShell, практически не затрагивая файловую систему атакуемого компьютера (IT Новости).

Проникнув в сеть, киберзлодею первым делом нужно получить возможность запускать вредоносные команды. Они могут заразить непосредственно ПК для дальнейшей загрузки, сохранения и выполнения вредоносного ПО. Однако, как выяснили специалисты X-Force, большинство хакеров осуществляют всю атаку с помощью команд PowerShell, начиная от похищения паролей и заканчивая майнингом криптовалюты. «В последние несколько лет злоумышленники с самыми разными уровнями навыков расширяют свои возможности с помощью PowerShell. Специалисты IBM X-Force IRIS сталкивались с случаями, когда набор вредоносных инструментов полностью состоял из одних скриптов PowerShell», – уточняется в отчете

исследователей. Выявленная специалистами тенденция является еще одним напоминанием для системных администраторов о том, что использовать для обнаружения вторжения одни лишь сигнатуры файлов недостаточно.

***

27.02.2019

Исследователи подделали электронные подписи в самых популярных PDF-ридерах

Команде ученых Рурского университета в Бохуме (Германия) удалось взломать системы электронной цифровой подписи и подделать подписи в 21 из 22 исследуемых программ для просмотра PDF-документов и пяти из семи online-сервисов для цифровой подписи PDF-документов. В числе взломанных оказались Adobe Acrobat Reader, Foxit Reader и LibreOffice, а также online-сервисы DocuSign и Evotrust (InternetUA).

Исследователи обнаружили три уязвимости в процессе цифровой подписи, используемом несколькими десктопными приложениями и online-сервисами:

Универсальная подделка подписи (Universal Signature Forgery, USF) – позволяет злоумышленнику обмануть процесс проверки подлинности подписи и заставить его отображать жертве панель, подтверждающую подлинность подписи;

Инкрементальная атака (Incremental Saving Attack, ISA) – позволяет злоумышленнику добавлять дополнительный контент в уже подписанные PDF-документы через механизм инкрементного обновления без вмешательства в уже существующую подпись;

«Заворачивание» подписи (Signature Wrapping, SWA) – уязвимость сходна с ISA, но вредоносный код также содержит дополнительную логику для обмана процесса подтверждения подлинности подписи. С ее помощью механизм валидации подписи «обертывается» вокруг добавленного злоумышленником дополнительного контента и успешно подписывает инкрементное обновление.

С октября прошлого года пятеро ученых совместно с Компьютерной группой реагирования на чрезвычайные ситуации Германии (BSI-CERT) работали над уведомлением производителей уязвимых приложений о наличии проблем в их продуктах. Команда опубликовала результаты своего исследования спустя неделю после того, как все производители выпустили соответствующие обновления безопасности.

***

28.02.2019

В App Store начали появляться клоны оригинальных приложений

Нередко авторы приложений пренебрегают требованиями, установленными Apple, и идут наперекор им, планируя извлечь из этого дополнительную выгоду. Например, занимаются клонированием приложений, что, конечно же, категорически запрещено.

Докладніше

***

28.02.2019

Як видалити особисті дані з Інтернету?

Активні користувачі соцмереж залишають на своїх сторінках безліч інформації. Наприклад, фото, відео та дописи. Яким може стати їх здивування, коли, наприклад, їхні світлини з'являються на небажаних інформаційних ресурсах. Що робити, якщо хтось використав інформацію про вас без вашого дозволу?

Докладніше

***

28.02.2019

В Україні активно розповсюджується небезпечне програмне забезпечення

В Україні активно розповсюджується шкідливе програмне забезпечення, яке використовує WinRAR exploit (#CVE-2018-20250). В архіві міститься PDF документ із законом про державне партнерство zakon.rar. Вірус завантажує powershell скрипти з їх подальшим виконанням (InternetUA).

Не всі версії winrar вразливі! Обов'язкова рекомендація оновити winrar.

***

28.02.2019

Соціальну мережу TikTok оштрафовано на 5,7 мільйона доларів за незаконне збирання інформації про дітей

Федеральна торгова комісія США прийняла рішення оштрафувати соціальну мережу TikTok на рекордні 5,7 мільйона доларів. Це найбільший у світовій історії штраф, який закон присудив стягнути з подібного роду додатку (InternetUA).

Обвинувачення вважає, що сервіс для публікації та обміну відео незаконно збирав персональну інформацію дітей без згоди їхніх батьків, пише CNN Business. TikTok збирав адреси електронної пошти, IP-адреси та дані про геолокацію. Такі дії є протиправними згідно з американським законом про захист конфіденційності дітей в інтернеті.

Облікові записи неповнолітніх користувачів TikTok були доступні будь-кому. Інші користувачі бачили фотографію профілю, його опис та ім'я.

Окрім виплати штрафу, сервіс має видалити всі відеоролики, завантажені дітьми до 13 років. Це рішення вже опубліковано на сайті Федеральної торгової комісії США.

Компанія погодилася сплатити штраф та вже підготувала оновлену версію додатка. У ній користувачі до 13 років можуть підписуватися на чужі профілі, переглядати відео та знімати свої. Втім, свої відеоролики викладати у загальний доступ вони вже не зможуть.

Наразі у TikTok зареєстровано понад 800 мільйонів користувачів. Більшість з них – діти.

***

28.02.2019

Російські хакери активізувалися для зриву виборів до Європарламенту, - ЗМІ

Російські хакери різко активізували кампанію, спрямовану на зрив виборів до Європарламенту в травні (Espreso.tv). Про це заявили три дипломати ЄС, повідомляє видання Financial Times.

«Ми знаємо, що вони вже намагаються нашкодити і, в свою чергу, ми готуємося до цього», – сказав один із дипломатів на умовах анонімності.

Експерти у сфері кібербезпеки стверджують, що протягом останніх місяців почастішали випадки прояву хакерської активності з боку проросійських груп щодо європейських держустанов, соціальних інститутів і ЗМІ.

Глава американської компанії FireEye Бен Рід, що займається кібербезпекою, зазначає про фіксацію дедалі частіших спроб атак на європейські держструктури і медіа за останні півроку. «Здебільшого ця діяльність спрямована на міністерства оборони і закордонних справ країн НАТО, а також, наприклад, на німецькі ЗМІ», – сказав він.

Як зазначається, Брюссель намагається розробити систему попередження про інформаційні атаки і боротьби з пропагандою ззовні, хоча багато дипломатів скептично сприймають таку ініціативу.

В ЄС очікують, що хакери, які працюють за вказівкою Кремля, спробують впливати на вибори до ЄП.

Представники служб безпеки США також стурбовані тим, що російські групи могли б використовувати це голосування як плацдарм для потенційних стратегій, які можуть бути розгорнуті на американських виборах наступного року, додають джерела.

«Західні демократії перебувають під загрозою втручань ззовні, і Україна є головним тестовим майданчиком таких дій. Російська Федерація випробувала багато технік і стратегії в Україні», – упевнений Девід Крамер, колишній помічник держсекретаря США.

***

2.03.2019

Хакеры высылают фейковые предложения о работе в LinkedIn

Через соцсеть для бизнеса LinkedIn киберпреступники высылают потенциальным жертвам фейковые предложения о работе и ссылки на подставные ресурсы, при переходе на которые на целевой компьютер загружаются вредоносные программы, пишет Softpedia (InternetUA).

По словам исследователей компании Proofpoint, специализирующейся на кибербезопасности, цель хакеров – внедрить на скомпрометированный компьютер бэкдор More_eggs, который позволяет атакующему удалённо развёртывать на нём другое вредоносное ПО.

Хакеры создают профили в LinkedIn и отправляют жертве небольшое сообщение с предложением вакансии. Спустя несколько дней злоумышленники уже на рабочую почту, указанную в соцсети, высылают email, в котором получателю предлагается перейти на определённый веб-сайт за дальнейшими деталями о вакансии.

URL-адреса ведут на подставные страницы, замаскированные под легитимные компании по подбору персонала. После открытия сайт начинает скачивать зловредный Word-документ с маросом, который активирует загрузку бэкдора More_eggs. Иногда URL ведут на PDF-файлы с фальшивой информацией о работе и вредоносными ссылками. Атаки могут быть более изощрёнными и использовать краткие ссылки, вредоносные вложения в письмах, защищённые паролями Word-документы и даже просто невинные email-ы без вложений или ссылок с попыткой установить контакт.

Пользователям рекомендуется игнорировать сообщения, которые ведут на подозрительные сторонние сайты или имеют потенциально опасные вложения, а также не забывать обновлять антивирусные программы.

***

3.03.2019

Киберпреступники зарабатывают в соцсетях 3,25 млрд долларов в год

Киберпреступники зарабатывают на мошеннических схемах в социальных сетях не менее 3,25 млрд долларов в год. К такому выводу пришли в компании Bromium, специализирующейся на создании технологий защиты от вредоносных угроз (InternetUA).

Мошенники используют Facebook, YouTube, Twitter и другие сервисы для распространения вирусов, «чтобы мгновенно охватить и заразить миллионы пользователей во всем мире практически без усилий».

Через соцсети распространяют программы для скрытой добычи криптовалют, вывода вредоносной рекламы, фишинговых ссылок и т. п.

«Социальные сети поддерживают киберпреступность. Они используются кибермошенниками для атак на организации и физических лиц, а также для

продажи различных незаконных товаров, услуг и знаний», – говорится в исследовании.

По оценкам экспертов, около 40 % заражений в социальных сетях происходят от вредоносной рекламы, а не менее 30 % – от плагинов и вирусных приложений.

Специалисты Bromium говорят, что социальные сети стали «глобальным центром распространения вредоносных программ», причем пятая часть всех организаций заражается через эти платформы. Согласно исследовательскому отчету, киберпреступность в социальных сетях выросла более чем на 300 % в период с 2015 по 2017 год только в США.

***

4.03.2019

Facebook тайно лоббировала смягчение закона о персональных данных

Судя по документам, которые стали известны из публикации Computer Weekly, Facebook обращалась к чиновникам по всему миру, включая бывшего канцлера Великобритании Джорджа Осборна. В обмен на поблажки в законе компания обещала больше инвестиций. Такие предложения Facebook направляла в десятки стран, включая США, Канаду, Индию, Вьетнам, Аргентину, Бразилию, Малайзию и страны ЕС.

Докладніше

***

4.03.2019

Новая волна кибератак обрушилась на PoS-терминалы

Исследователи безопасности компании Morphisec сообщили о новой вредоносной кампании, в ходе которой злоумышленники атакуют PoS-терминалы по всему миру с целью кражи данных банковских карт. Жертвами киберпреступников стали финансовые, страховые, медицинские и прочие организации в Индии, Японии, США и других странах (InternetUA).

По словам исследователей, имеющихся у них сведений недостаточно для того, чтобы с точностью определить, кто стоит за атаками. «Почерк» киберпреступников наводит на мысль о группировке FIN6, но некоторые моменты указывают на возможную связь с группировкой EmpireMonkey.

По мнению исследователей, одним из векторов атак являются файлы HTA (HTML Application), выполняющие скрипты PowerShell как часть встроенного VBScript.

Используемое злоумышленниками вредоносное ПО для похищения данных из памяти PoS-терминалов отличается от случая к случаю. В одних случаях они прибегают к инструменту FrameworkPOS, а в других – к PowerShell/WMI для загрузки ПО Cobalt Strike с расширением PowerShell

непосредственно в память. Cobalt Strike позволяет атакующим получить контроль над зараженной системой и проникать в другие системы в одной с ней сети. С его помощью злоумышленники могут похищать учетные данные жертв, выполнять код и осуществлять другие вредоносные операции.

***

5.03.2019

Facebook не хранит ваш номер телефона в секрете

Facebook регулярно попадает в скандалы, связанные с безопасностью личных данных пользователей. Новая неприятная новость связана не с утечкой данных, а с серьезной недоработкой в настройках соцсети. Оказывается, указав свой номер телефона, вы уже не можете скрыть его от чужих глаз (InternetUA).

На это обратил внимание пользователь Twitter Джереми Бердж. «Годами Facebook утверждал, что номер телефона для двухфакторной авторизации служит лишь в целях безопасности. Но теперь его можно искать, и нет ни единого способа это отключить», – пишет Бердж.

***

5.03.2019

Киберпреступники активно эксплуатируют уязвимость в маршрутизаторах Cisco

Спустя всего два дня после публикации информации об уязвимости в популярных моделях SOHO маршрутизаторов Cisco и обнародования демонстрационного эксплоита, киберпреступники начали активно атаковать уязвимые устройства.

Докладніше

***

5.03.2019

Китайские киберпреступники нацелились на Linux-серверы

Киберпреступная группировка Pacha Group, предположительно действующая из Китая, активно компрометируют Linux-серверы с целью внедрения вредоносного ПО для добычи криптовалюты. По данным экспертов Intezer, злоумышленники атакуют серверы не напрямую, а через приложения WordPress или PhpMyAdmin. Получив доступ к серверу, они внедряют вредонос Linux.GreedyAntd (Antd) (InternetUA).

Первые атаки были зафиксированы в сентябре 2018 года. По словам исследователей, исходный код вредоноса, используемого в кампании, имеет схожие черты с другой вредоносной программой – Linux.HelloBot. Предположительно, группировка Pacha Group параллельно тестируют два вида вредоносного ПО, но в своих операциях чаще использует Antd.

Вредонос представляет собой модифицированную версию майнера XMRig, использующую прокси для сокрытия настроек и адресов криптовалютных кошельков.

Antd имеет модульную структуру и может работать с несколькими управляющими серверами. Наличие широкой инфраструктуры с большим числом взаимосвязанных компонентов позволяет сохранить функциональность вредоноса в случае отключения каких-либо C&C-серверов. Кроме того, для устранения Antd с инфицированной системы потребуются значительные усилия, поскольку его поведение отличается от другого вредоносного ПО под Linux. К примеру, для сохранения присутствия на атакуемой системе вместо использования планировщика задач cronjob Antd добавляет службу Systemd, имитирующую официальный сервис mandb. Бэкдор Antd довольно сложно обнаружить, если не знать, что искать, отмечают исследователи.

***

5.03.2019

Пользователи Android TV начали видеть чужие личные фото из Google Photos

Если вы являетесь пользователем любого устройства с операционной системой Android TV, то вы давно могли привыкнуть видеть на экране телевизора в режиме ожидания фотографии из ваших альбомов в Google Photos (InternetUA).

Однако недавний баг, который был обнаружен в приложении Google Home, привел к тому, что личные фотографии из Google Photos начали отображаться у других пользователей Android TV.

Ошибка была обнаружена несколько дней назад пользователем, который сообщил о странном поведении своего телевизора, произведенного компанией Vu. Устройство работало под управлением операционной системы Android 7.0 Nougat, при этом система безопасности не обновлялась с 2017 года.

По его словам, при использовании приложения Google Home для доступа к телевизора в режиме ожидания, на экране отобразились личные фотографии из учетных записей некоторых незнакомцев. С приставкой Xiaomi Mi Box 3 подобная ошибка не проявляется. До сих пор непонятно, сколько пользователей увидели чужие фотографии из Google Photos, а также какие устройства с Android TV подвержены багу.

В качестве меры предосторожности Google отключила сервис Google Photos для Android TV, а также удаленный стриминг с помощью Google Assistant, занимаясь работой над исправлением. В Google подтвердили, что ошибка действительно скрыта в Google Home.

***

6.03.2019

Интернет без паролей стал на шаг ближе к реальности

Консорциум Всемирной паутины (W3C) и альянс FIDO приняли Web Authentication (WebAuthn) – новый стандарт, который может вытеснить пароли как средство аутентификации в онлайн-аккаунтах, сообщает Engadget (InternetUA).

Преимущества стандарта – удобство, так как он избавит от необходимости запоминать и вводить пароли и повышенная безопасность. Сайты с поддержкой API WebAuthn допускают авторизацию с помощью биометрических методов (по лицу или отпечаткам пальцев), USB-ключей или же мобильных устройств, например смартфонов или «умных» часов.

Технология связывает уникальные зашифрованные идентификационные данные с сайтами и уменьшает риск фишинга, атак с использованием кейлоггеров или других инструментов, перехватывающих вводимые пользователем данные.

Стандарт анонсировали в прошлом году. Сейчас его поддерживает большинство популярных браузеров, включая Chrome, Firefox, Edge и Safari. Также на системном уровне WebAuthn поддерживают Android, Chrome OS и Windows 10. Официальный статус, по мнению Engadget, должен ускорить принятие веб-стандарта отдельными сайтами, многие из которых не спешат отказываться от привычных паролей.

***

6.03.2019

С приближением выборов в Украине участились кибератаки на госслужащих

С приближением дня президентских выборов в Украине увеличилось количество адресных рассылок спама и фишинговых сообщений государственным служащим (InternetUA).

Об этом заявил начальник Департамента киберполиции Сергей Демедюк.

Докладніше

***

6.03.2019

Ирина Фоменко

Исследование: вредоносные URL-адреса несут самую серьезную угрозу

Согласно исследованию Mimecast по оценке риска для безопасности электронной почты, вредоносные URL-адреса в настоящее время являются распространенной проблемой – они содержатся в среднем в каждом 61 электронном письме.

Докладніше

***

7.03.2019
Ольга Карпенко
Facebook разрешит устанавливать срок хранения сообщений и других личных данных

Социальная сеть Facebook объявила о развороте в сторону защиты личных данных своих пользователей. Основатель сети Марк Цукерберг написал о том, как компания будет развивать свои сервисы с точки зрения приватности.
Докладніше

***

6.03.2019
Популярные приложения для Android оказались опасными

Популярные Android-приложения, в том числе Yelp и Duolingo, отправляют персонально идентифицируемые данные пользователей непосредственно Facebook сразу же после авторизации. Передача данных осуществляется даже в случае, если пользователь не авторизован в приложении Facebook на устройстве или вовсе не имеет активной учетной записи в соцсети (InternetUA).
Как сообщает некоммерческая организация Privacy International, помимо приложений от Yelp и Duolingo, передачей данных компании Facebook также занимаются два мусульманских приложения для молитвы, приложение для изучения Библии и приложение для поиска работы Indeed. Эти данные позволяют идентифицировать пользователей для последующего показа им таргетированной рекламы в Facebook.
Новый отчет Privacy International основывается на предыдущем исследовании, опубликованном в декабре прошлого года. Тогда специалисты организации сообщили о том, что популярные Android- и iOS-приложения без спроса отправляют Facebook данные пользователей. Отчет Privacy International возымел эффект, и две трети исследованных приложений, в том числе Spotify, Skyscanner и KAYAK, отказались от передачи данных соцсети. Тем не менее, как показало новое исследование, некоторые приложения по-прежнему обмениваются пользовательскими данными с Facebook.

***

11.03.2019
ПО для взлома банков пряталось в облаке Google

Домен облачного хранилища Google, как правило, рассматривается как заведомо надежный, чем и пользуются злоумышленники: использование этих ресурсов помогает обходить защитные инструменты в корпоративных сетях и обманывать пользователей.

Докладніше

***

12.03.2019
Стоит ли бояться вирусов для iOS

Ходят легенды, что под iOS не существует вирусов. Но почему в таком случае App Store буквально ломится от всевозможных антивирусных приложений, чьи разработчики наперебой обещают защиту ваших данных?
Докладніше

ДОДАТКИ

Додаток 1

27.02.2019
Google запустила бесплатного «убийцу» WhatsApp для Android

За всю свою более чем 20-летнюю историю компания Google успела запустить десятки успешных проектов, однако есть сферы, где ей крупно не повезло в силу ряда причин, в том числе из-за неправильных решений руководства. Тем не менее, «поисковой гигант» не собирается сдаваться и отступать под натиском своих конкурентов. Так, уже в первой половине 2019 года американская корпорация избавится от WhatsApp, Skype и других мессенджеров на Android, потому как пользователям гаджетов на базе данной ОС предложат альтернативный способ для общения, более простой и удобный (Украинский телекоммуникационный портал).

Как стало известно от официального источника, уже вскоре на базе платформы Android Messages будет запущен специальный мессенджер, который будет работать на мобильных устройствах под управлением одноименной операционной системы. Чтобы начать использовать такой сервис для общения будет достаточно просто установить SIM-карту в смартфон, после чего можно будет обмениваться сообщениями и файлами, причем совершенно бесплатно. При этом делать это окажется возможно и без подключения к интернету.

Специально для сервиса Android Messages компания Google много лет создавала технологию RCS, которая представляет из себя продвинутые SMS. Новая разработка отличается от старой тем, что с ее помощью можно отправлять тексты любого объема, а также передавать файлы на высокой скорости. Использовать такую технологию смогут клиенты таких сотовых операторов, которые ее внедрят, а среди таких уже около пяти десятков. За счет этого пользователи смогут использовать мессенджер даже при отключенном мобильном интернете.

При помощи Android Messages окажется возможно отправлять сообщения и файлы, а также, кроме того, совершать голосовые звонки и производить видеовызовы. В будущем Google обещает добавить поддержку групповых разговоров. По умолчанию данное программное обеспечение окажется установлено на смартфоны LG, Motorola, Sony, HTC, ZTE, Micromax, HMD Global (Nokia), Archos, BQ, Cherry Mobile, Condor, Fly, General Mobile, Lanix, LeEco, Lava, Kyocera, MyPhone, QMobile, Symphony и Wiko, что сделает его крайне популярным, заставив многих людей отказаться от WhatsApp и его аналогов.

Само собой, что новый сервис для общения от Google окажется полностью бесплатным, а приложение Android Messages по умолчанию окажется встроено во многие мобильные устройства на рынке, тогда как обладатели других смогут установить его из магазина Google Play. Осталось только дождаться запуска, который должен случиться в первой половине 2019 года.

(вгору)

Додаток 2

2.03.2019

Twitter дозволить приховувати коментарі під постами

Це має зробити спілкування більш конфіденційним, тобто наблизити твітим до аналогу особистого листування. Також опція дозволить відфільтрувати записи і відповіді на них, прибравши їх зі своєї стрічки (InternetUA).

Як заявляє топ-менеджер Twitter Мішель Ясмін (Michelle Yasmeen) у дописі, можливість ховати коментарі може стати новим методом користувальницької модерації та позбавить юзерів необхідності блокувати акаунти інших людей.

Користувачі не зможуть повністю прибирати відповіді під своїми постами, але стане можливим зробити їх менш помітними в обговоренні.

«Люди, які починають у Twitter цікаву розмову для нас насправді дуже цінні, тому ми хочемо уповноважити їх робити обговорення більш здоровими. Зараз користувачі вже це роблять за допомогою функцій блокування, замовчування чи звітуючи нам. Проте ці інструменти не завжди потрапляють в ціль. Блокування і замовчування лише змінює те, як бачить обговорення блокувальний, а звіти ефективні лише щодо тих постів, які порушують правила спільноти», – пояснює менеджерка продуктів компанії Мішель Ясмен Хак.

Щоб знайти нову функцію, треба натиснути на кнопку «поширити», де з’явиться опція «Приховати відповідь». Надалі користувачі не бачитимуть такі приховані коментарі у стрічці, а муситимуть для цього розгорнути усі коментарі. Також ви зможете подивитися усі приховані у минулому коментарі та, за бажання, зробити якісь із них знову видимими.

Мішель Ясмен Хак вважає, що такий підхід є балансом між інтересами автора твіту і аудиторією, пише The Verge. Крім того, дописувачі таким чином зможуть сигналізувати спільноті, що спілкування стало надто токсичним.

Поки що команда Twitter продовжує розробляти та тестувати нову функцію. Основна проблема її використання полягає в тому, що користувачі можуть «заблокувати» у своїй стрічці кого завгодно. Це може буде використано у цілях маніпуляцій та ігнорування критики деякими високопосадовцями, зазначає TechCrunch. Перегляд прихованих твітів вимагає і додаткових маніпуляцій, про які деякі користувачі можуть не знати.

(вгору)

Додаток 3

3.03.2019

Гра престолів. Чому Telegram вб'є Viber і що буде з іншими месенджерами

Месенджер Viber вводить плату за чат-боти. НВ розбиралося, як це відіб'ється на конкуренції зі схожими додатками, та який месенджер незабаром може завоювати світовий ринок (InternetUA).

Пару місяців тому, НВ писало про те, що таке чат-боти, чому вони важливі для сучасного ринку і яку роль вони відіграють у побудові бізнесу зараз. Виявилося, що як в Україні, так і в усьому світі, зростання популярності чат-ботів викликано появою та вдосконаленням різних месенджерів, а також тотальною текстовою комунікацією користувачів.

Ми, звичайно, поки не повністю перейшли у кіберпростір, але клієнтам абсолютно будь-якого сервісу вже зараз набагато зручніше спілкуватися з постачальником послуг або товарів через текст, ніж дзвонити в колл-центр та озвучувати свою проблему. Як результат – більшість сучасних компаній створюють автоматичні канали комунікації на платформах типу Facebook Messenger, Telegram, Instagram, WhatsApp, Viber і т.і.

Ці канали – власне, чат-боти – допомагають клієнту цілодобово швидко і самостійно знайти рішення його проблеми, або, принаймні, вказати напрямок цього рішення.

Що не так з Viber?

Більш популярний в пост-радянських країнах месенджер Viber також є важливою платформою для спілкування бізнесу з клієнтом. Але, як уже писало НВ, материнська компанія Viber – японська e-commerce корпорація Rakuten – вирішила зробити платними чат-боти всередині месенджера.

Rakuten придбали кіпрський сервіс онлайн-повідомлень Viber в 2014-му за $900 млн, і схоже, хочуть максимально капіталізувати своє вкладення. Повідомляється, що з першого квітня 2019-го Viber буде стягувати з операторів чат-ботів $4,5 тис. на місяць за можливість відправляти користувачам до 500 тис. повідомлень.

За те, щоб відправляти до 1 млн повідомлень на місяць потрібно буде викласти $6,5 тис. Як повідомляє видання Tech Crunch, яке одним із перших отримало інформацію про монетизацію чат-ботів у Viber, нововведення є несподіваним та може відштовхнути компанії, які використовують чат-боти Viber.

Враховуючи те, що Viber використовують більше мільярда людей по всьому світу, неоднозначне рішення дійсно може привести до масового переходу користувачів та бізнесів на інші платформи.

Чому це сталося?

Як пояснив HB CEO IT-компанії D2 Володимир Дем'яненко, одне з головних джерел доходу Viber – платні розсилки. Наприклад, в Україні вартість одного повідомлення одному користувачеві становить майже 30 копійок.

«Очевидно, що чат-боти дозволяють відправляти ці повідомлення безкоштовно, і тому Viber явно намагається компенсувати ці втрати, роблячи чат-ботів платними», – говорить Дем'яненко.

За його словами, Viber незабаром втратить свої позиції, причому, не тільки через новий платний сервіс, але і через масу накопичених проблем месенджера. Зокрема, CEO D2 впевнений, що молоде покоління абсолютно не сприймає Viber та вважає його «пенсіонерським».

«Додаток має жахливий інтерфейс і таку ж якість роботи. Viber поки є гіршим месенджером за цими параметрами. Попри оновлення дизайну, істотно мало що змінилося, – ті ж гальма і глюки, ті ж проблеми з навігацією», – заявляє Володимир Дем'яненко.

Куди підуть користувачі Viber?

Не те, щоб у них був великий вибір, але, керівник IT-компанії передбачає, що навіть якщо у смартфонах користувачів залишаться по 3-4 месенджера, у найближчому майбутньому лідерство у Viber може відібрати Telegram, як це вже сталося з рядом ринків, де Telegram, по суті, є монополістом.

З близько 180 млн чоловік активної аудиторії Telegram, більш 10 млн становлять українці. Хоч і у багатьох досі встановлені Telegram і Viber, зростання популярності Telegram спостерігається не тільки в Україні, а й в усьому світі. Месенджер пропонує зручний, швидкий та інтуїтивний сервіс обміну повідомленнями, який вже потихеньку переростає у справжню екосистему.

«Я думаю частка Viber зменшиться через платних чат-ботів, але не відразу. По суті, Telegram надає зручну, безкоштовну бот-платформу, та багато бізнесів вже активно використовують її, як сервіс для клієнтів: пошук квитків "Укрзалізниці", PatentBot, реєстрація на заходи і так далі. Якщо у Viber таких систем не буде – користувачі все менше будуть заходити туди, та все частіше повертатися в Telegram», – пояснює Дем'яненко.

Що з Facebook, Instagram і WhatsApp?

Як відомо, Facebook Messenger, який посідає третє місце за популярністю серед месенджерів в Україні, а також Instagram Direct і WhatsApp, належать Facebook. Американська соціальна мережа остаточно визначилася із політикою

монетизації через рекламу, яка не шкодить чат-ботам. Facebook дає дуже багато опцій для бізнесу і, тому, все більше цікавих чат-ботів створюється саме на цій платформі.

Але, після відходу керівників Instagram та WhatsApp, обидва дочірніх підприємства стали більше залежними від Facebook. Спочатку, засновник Facebook Марк Цукерберг обіцяв не влазити в діяльність куплених компаній, але, з часом, рекламні моделі соцмережі почали впроваджувати як в Instagram, так і в WhatsApp.

Засновник і колишній керівник колись одного з найбезпечніших месенджерів WhatsApp Брайан Ектон заявляв пару місяців тому, що разом з продажем WhatsApp, він продав приватність своїх користувачів. Одного разу, Ектон навіть закликав всіх видалити Facebook.

На тлі різних скандалів з витоками персональних даних користувачів Facebook, WhatsApp і Instagram тепер також можуть викликати побоювання у значної частини молодої аудиторії. Особливо, коли навіть по інтерфейсу цих додатків помітно, що вони стають все більше сполученими з Facebook.

Таким чином, Telegram і тут залишається на коні.

Що буде далі з Telegram?

Відносно молодий месенджер від засновників колись популярної в Україні соцмережі «ВКонтакте» братів Павла і Миколи Дурових, завоював довіру користувачів через свою чітку позицію щодо захисту їх особистої інформації.

Попри те, що російське відомство Роскомнадзор вже більше року намагається заблокувати Telegram та впроваджує різні технічні інструменти для цього, сервіс не піддається вимогам влади і не передає ключі шифрування повідомлень державним структурам.

Нападки російських політиків, зокрема, стали причиною акцій протесту в Москві, – росіяни створили спеціальний флешмоб «паперовий літачок», який символізував емблему Telegram і підтримував вільний інтернет.

Думки про те, що Telegram – це проект ФСБ, звичайно, мають певне місце в суперечках в мережі, але, в такому випадку, занадто правдоподібними виглядають мільйони доларів, які Роскомнадзор витрачає на боротьбу з непокірними Дуров. Та й сама інтернет-спільнота вже якось об’єдналося в стьобі над відчайдушними спробами застарілої державної системи заблокувати Telegram.

Крім цього, найближчими місяцями, брати Дурови готують випустити власну криптовалюту Gram, яка повинна стати повноцінною платіжною системою, пов’язаною з месенджером Telegram.

Якщо розробникам вдасться реалізувати задумане і зберегти колишній рівень безпеки системи, Telegram може стати європейською альтернативою китайському WeChat, – мессенджера, який об’єднав в собі засоби комунікації, фінансових операцій та елементи соціальної мережі.

WeChat належить китайському техногіганту Tencent і є одним з небагатьох доступних месенджерів в КНР. Через китайський FireWall –

блокування практично всіх американських соцмереж, відеохостингів, платіжних систем і т.і. – кількість щомісячних активних користувачів WeChat зросла майже до 1,1 млрд чоловік з 2011-го по 2018-й.

Згідно даним платіжної системи PayPal, у Китайський Новий рік 2016 користувачі WeChat провели більше транзакцій, ніж було у PayPal за весь 2015-й.

«У Китаї месенджер WeChat став візуальним паспортом і платіжною системою, він забезпечує зв'язок жителів Китаю з державою та багато в чому є невід'ємною частиною життя громадян», – говорить Володимир Дем'яненко.

Перефразовуючи класика, який прогнозував «одне суцільне телебачення», – цілком ймовірно, що незабаром інтернет стане одним суцільним месенджером, реалізованим через додатки типу WeChat і Telegram.

(вгору)

Додаток 4

10.03.2019

Единый мессенджер Facebook создаст конкуренцию iMessage

Как известно, Facebook планирует объединить мессенджеры Messenger, WhatsApp и Instagram для улучшения конфиденциальности. В новом отчете портала Slate журналисты объяснили, как это приведет Facebook к прямой конкуренции с Apple (InternetUA).

По мнению аналитиков, Facebook и Apple дополняют друг друга – люди покупают iPhone и используют их для просмотра Facebook и Instagram. При этом многие люди используют iPhone для общения через платформы Facebook вместо iMessage, что также облегчает переход на другие платформы, такие как Android.

«В частности, функция iMessage с отличным интерфейсом и сквозным шифрованием была преимуществом Apple, позволяющим удержать пользователей от перехода на Android-устройства. Несмотря на высокий спрос, купертиновцы никогда не планировали создать приложение iMessage для Android. В свою очередь, Google изо всех сил пыталась разработать успешный продукт для обмена сообщениями, но не смогла. Поэтому многие пользователи Android-гаджетов решили использовать Facebook Messenger и WhatsApp».

Эксперты отмечают, что сервис сообщений Apple опережает мессенджеры Facebook по количеству пользователей в США.

Стоит отметить, что сам Цукерберг назвал iMessage одним из крупнейших конкурентов Facebook. Кроме того, он также сказал, что целью объединения WhatsApp, Instagram и Messenger было создание безопасного сервиса обмена сообщениями, подобного iMessage.

В последнее время отношения между Facebook и Apple становятся все более сложными. Тим Кук неоднократно высказывался негативно о Facebook из-за проблем с конфиденциальностью у последнего. В свою очередь, Цукерберг подверг критике отношения Apple с китайским правительством.

Время покажет, может ли мессенджер Facebook стать заменой iMessage, и стоит ли доверять обещаниям Марка Цукерберга о конфиденциальности.

(вгору)

Додаток 5

27.02.2019

#ДоброЧесніВибори. Социальная реклама призвала украинцев не продавать голоса на выборах

Общественное движение ЧЕСНО и информационная молодежная кампания «Твой голос» запустили совместную социальную рекламную кампанию #ДоброЧесніВибори, направленную на то, чтобы молодежь не продавала свои голоса на выборах Президента (Marketing Media Review).

Активисты спросили детей в возрасте до 13 лет, каким должен быть Президент, уточнили пожелания украинцам перед выборами, и главным взрослым вопросом к детям был: «Что может произойти, если к власти придут те, кто покупают голоса?». Дети своими словами объяснили, что не стоит продавать голоса избирателей, а политикам не стоит покупать голоса.

Инициаторы надеются, что месседж #ДоброЧесніВибори превратится во флешмоб и призывают всех, кто сталкиваются с попытками покупки голосов, публично заявлять об этом в социальных сетях под хэштегом #ДоброЧесніВибори.

«Мы уже в четвертый раз запускаем информационную кампанию “Твой голос!” накануне выборов. Каждый раз ищем креатив, который становится ключевым в информационном пространстве. Нас поддержали около 50 публичных людей с видео обращениями в предыдущие разы, в 2019 году мы решили сделать “рупорами” нашей кампании именно детей. Ведь кто может быть более искренним, чем дети? И сегодняшние избиратели голосуют за их будущее», – рассказывает Александр Санченко, инициатор информационной кампании «Твой голос!».

В проект активно включились общественный Движение ЧЕСНО и приняли участие в создании видео. «Движение ЧЕСНО сразу согласился поддержать молодежную кампанию #ДоброЧесніВибори против подкупа избирателей, поскольку и наиболее успешной мы считаем коммуникацию по принципу “равный-равному”, когда о недопустимости продажи своего голоса говорят не взрослые уважаемые эксперты, а такие же подростки, которые хотят жить в лучшей версии Украины. – говорит менеджер по коммуникациям Движения ЧЕСНО Юлия Решитько. – Мы готовы поделиться с инициативой „Твой Голос“ всеми своими знаниями и опытом, приобретенными за семь лет работы, чтобы вместе объяснить молодым избирателям, как построен избирательный процесс, как политические мифы влияют на волеизъявление, почему важно избирать не эмоционально, а главное – почему продавать голос – это дно. Призываем всех присоединиться!»

(вгору)

Додаток 6

6.03.2019

У Зе!команді похвалилися відвідуваністю сайту: рівень кампанії Обами

У команді кандидата в президенти шоумена Володимира Зеленського кажуть, що будують дуже експериментальну для української політики структуру діджиталу (Українська правда).

Про це в інтерв'ю «Українській правді» розповів керівник діджитал-відділу штабу Зеленського Михайло Федоров.

«Всього в діджитал-команді людей, які працюють тут на фултайм, людей, певно, 10. Звичайно ж, багато команд працюють на аутсорс – по контекстній рекламі, розробники, команда з моніторингу, соціологи», – говорить Федоров.

За його словами, в цілому зараз там задіяно три десятки людей.

Федоров пояснює, що одна і та ж команда працює з усіма соціальними медіа: немає розподілу, хто конкретно відповідає за FB, Instagram і т. д.

«У нас є два копірайтера, які готують контент і для FB, і для Instagram, і для Telegram, і для Twitter. Є тімлідер, який ними керує. Ці ж люди пишуть email-розсилки», – говорить він.

«Ми будуємо дуже експериментальну структуру для нашої країни, і в принципі, для політики. У нас є наші власні медіа. Це FB, наш офіційний Instagram, наш офіційний телеграм-канал і Twitter. Ще у нас є два YouTube-каналу – Зе!президент на 210 тисяч передплатників і "Команда Зеленського" на 20 тисяч», – зазначає діджитал-стратег.

Щодо ефективності та вартості діджитал-кампанії, Федоров пояснює, що це десь 1 % загального бюджету виборчої кампанії.

«Ефект від неї дуже великий. Чи можемо його порахувати за кількістю згадок», – говорить він.

«Ми зараз на рівні з президентом за кількістю згадувань в інтернеті в цілому. Найчастіше про нас згадують навіть більше, ніж про нього. Для мене це певний KPI», – зазначає Федоров.

За його словами, ідея з «Зе» добре розходиться.

«Ще один з показників для нас – це відвідуваність. Наш сайт відвідало вже понад 2 мільйони 300 тисяч унікальних користувачів. Це приблизно рівень президентської кампанії Обами в 2008 році», – каже Федоров.

За його словами, загальна кількість передплатників на всіх Зе!ресурсах – близько 1 мільйона 200 тисяч осіб.

(вгору)

Додаток 7

1.03.2019

За Facebook Workplace уже платит два миллиона пользователей

Компания Facebook представила статистику использования Workplace – ориентированной на бизнес разновидности её социальной платформы. Если сравнивать с её основным конкурентом, Slack, насчитывающим 10 млн ежедневных активных пользователей из 85 тыс. организаций, обнародованные Facebook цифры мало впечатляют – это всего лишь 2 млн платящих подписчиков. Но компания отметила, что её сервис также предоставляется бесплатно неприбыльным организациям и учебным учреждениям. Таких подписчиков «миллионы», заявила она, не называя конкретного количества (Компьютерное Обозрение).

«Facebook для бизнеса» стартовала в октябре 2016 г., а её платная версия была введена в октябре 2017 г. Стоимость подписки на Workplace начинается с $3 в месяц на одного пользователя, для каждой из организаций со штатом более 5000 человек вопрос об оплате решается индивидуально.

У самой Facebook количество активных пользователей в месяц сейчас превышает 2 млрд, и компания всегда позиционировала Workplace как инструмент для очень больших предприятий. По её сведениям, таких корпоративных подписчиков (с числом пользователей более 10 тыс. человек) сейчас у этой платформы около полутора сотен. Среди них Walmart (крупнейший работодатель в мире), Nestle, Vodafone, GSK, Telefonica, AstraZeneca и Delta Airlines.

Хотя новая статистика не даёт нам точного количества пользователей сервиса Workplace, она демонстрирует решимость Facebook продолжать развивать этот новый источник прибыли, дополняющий поступления от рекламы в потребительской соцсети.

Компания за последних пару лет много сделала для увеличения функциональных возможностей Workplace, стремясь вывести данную платформу на уровень не только базовой Facebook, но и других служб коммуникаций, с которыми Workplace соперничает в борьбе за корпоративного пользователя. Это включает и интеграцию с множеством популярных приложений, хотя в этом отношении Workplace ещё не может равняться со Sparc, которая взаимодействует с сотнями из них.

В конце прошлого года был назначен новый глава Workplace, Карандип Ананд (Karandeep Anand). Он перешёл в Facebook три года назад из Microsoft и имеет большой опыт в сфере корпоративного ПО. Ананд контролирует вопросы технической разработки продукта, а Жюльен Кодорнью (Julien Codorniou) отвечает за продажи, связи с клиентами и развитие бизнеса Workplace.

(вгору)

Додаток 8

5.03.2019

Кандидати у президенти мають звітувати про політичну агітацію у соцмережах – аналітик

Кандидати у президенти мають звітувати про кожну копійку, витрачену з виборчих фондів. Та чи звітуватимуть кандидати про рекламу у соціальних мережах, поки що не зрозуміло. Про це в ексклюзивному коментарі журналісту УНН розповів аналітик Громадянської мережі «ОПОРА» Олександр Клюжев (УНН).

«Працівники чи розпорядники виборчих фондів кандидатів можуть укладати угоди щодо просування політичної агітації в соціальних мережах. З точки зору обсягів цієї реклами і її фінансування, ми ще зараз не можемо дізнатися, скільки її, тому що не було проміжного фінансового звіту кандидатів на пост президента України. І тому ми зараз через побічні інші ознаки і аналіз соціальних мереж намагаємося оцінити обсяги цієї реклами. Але буде цікаво подивитися на фонди кандидатів і їхню звітність щодо цього», – повідомив аналітик.

Кандидат у президенти повинен витрачати кошти на виборчу агітацію з власного виборчого фонду. Інформацію про витрачені гроші він має подавати у проміжному і загальному звітах до ЦВК.

«Будь-яка копійка, гривня, яка витрачається кандидатом на виборах, має бути з виборчого фонду. Якщо ми бачимо платну рекламу в соціальних мережах, це означає, що це виборчі витрати. І велике питання зараз: як у звітах це буде відображено і чи взагалі буде вказано?» – зазначив Клюжев.

До слова, у Законі України «Про вибори Президента України», зокрема, у статті 43 «Порядок формування виборчого фонду та використання його коштів», зазначено, що виборчий фонд кандидат на пост Президента України формує за рахунок власних коштів, за кошти партії, яка висунула кандидата, а також добровільних внесків осіб, які, відповідно до Закону України «Про політичні партії в Україні», мають право здійснювати внески на підтримку партій. А контроль за надходженням, обліком і використанням коштів виборчих фондів здійснює Центральна виборча комісія та установа банку, в якій відкрито рахунок виборчого фонду.

Як повідомляв УНН, в Україні запрацювала інформаційно-аналітична система «Вибори-2019», яка дозволяє перевірити онлайн інформацію щодо порушень на виборах, їхню кількість, географічне розташування, тип та процесуальний статус кожного правопорушення.

(вгору)

Додаток 9

4.03.2019

Українські політики витрачають на рекламу в соцмережах до $4 млн на місяць

Минулої весни партії витратили на всю рекламу близько 43 млн грн, у період активних передвиборчих кампаній цифри будуть в десятки разів вищими.

Обсяг політичної реклами в соцмережах у період активної передвиборчої кампанії в Україні може сягати $2-4 млн на місяць. Таку оцінку озвучив керуючий партнер комунікаційної групи PlusOne Максим Саваневський в матеріалі Mind «Вибори 2019: як Facebook і Google боротимуться з політичними тролями в Україні» (mind).

Співзасновниця та CEO агенції BASE Agency Ксенія Омельченко погоджується з такою оцінкою. Вона нагадує, що минулої весни партії витратили на всю рекламу, зокрема в соцмережах, на телебаченні, радіо та онлайн, близько 43 млн грн. А бюджети тільки на політичний digital, за її оцінками, обчислювалися сотнями тисяч доларів. У період активних передвиборчих кампаній цифри будуть у десятки разів вищими.

За словами Саваневського, деякі кампанії, особливо направлені проти конкурентів, можна називати маніпулятивними. Наприклад, це може бути розміщення новини на якомусь маловідомому сайті, а потім розганяння її рекламними інструментами в соцмережах. При цьому новина не обов'язково повинна бути неправдивою. Маніпулювати можна шляхом правильного підбору фактів, їх гіперболізації.

«Є лідери думок, які за гроші просувають вигідні деяким політичним силам наративи», – розказує Саваневський.

Але значно частіше користувачі соцмереж стикаються з маніпуляціями, зав'язаними на людській психології та ефекті «інформаційної бульбашки». Коли хтось є прибічником певної думки, він послуговується будь-якими аргументами, або довести свою правоту і «глухий» до інших аргументів. Разом із тим він знаходиться в «інформаційній бульбашці» – тобто алгоритми пошуку подають йому здебільшого ту інформацію, яку він хоче бачити. А отже, це лише посилює відчуття власної правоти, і часто люди починають щиро вірити в неправдиві факти, які вони наводять як аргументи.

Боротися з цим, на думку Саваневського, можна хіба що за допомогою розвитку критичного мислення, розширення кругозору, читання книжок.

«Це може допомогти, але не гарантувати, що ви не станете жертвою маніпуляції або ж самі не станете маніпулятором», – пояснює він.

(вгору)

Додаток 10

10.03.2019

Мешканці Парижа хочуть відгородитися від користувачів Instagram

Одна з паризьких вуличок стала справжнім хітом соцмереж – її фотографії публікують тисячі користувачів Instagram (InternetUA).

Утім, жителі вулиці Кремйо (Rue Cremieux) від її популярності не в захваті. Вони закликають місцеву владу закрити доступ до вулиці для сторонніх осіб – хоча б у окремі години, пише BBC.

Один із жителів навіть створив окремий акаунт в Instagram, щоб документувати всю небажану активність під вікнами свого будинку.

Ця ситуація – хороша ілюстрація того, що бажання одних людей зробити ідеальне фото, може стати серйозною проблемою для інших, каже тревел-блогерка Кріс Мортон.

Жителі вулиці просять паризьку владу встановити ворота, які можна буде закривати, коли потік людей є найбільшим – ввечері, на вихідних, а також на світанку і на заході сонця – вважається, що саме в ці години освітлення для фото є найбільш вдалим, що привертає увагу багатьох «інстаграмерів».

«Ми сидимо вдома, їмо, а надворі бачимо купу людей, які роблять фото; реперів, які по дві години знімають кліпи прямо у нас під вікнами; студентів, які влаштовують випускні вечірки і можуть кричати цілу годину. Чесно кажучи, все це дуже втомлює», – розповів один з жителів вулиці Кремйо радіостанції France.info.

Блогерка Кріс Мортон розповіла BBC News, що подорожуючи світом, ставала свідком багатьох ситуацій, коли користувачі Instagram вели себе недопустимо.

«Якось я стояла і разом зі своїм хлопцем просто спостерігала за тим, як всі навколо фотографуються в одних і тих самих позах. Ми чекали кілька хвилин, поки якась жінка змушувала свого партнера робити десятки фотографій – вони блокували шлях для всіх інших. Зрештою я не витримала і просто пішла прямо на них».

Втім, каже пані Мортон звинувачувати у подібних речах треба конкретних людей – самі по собі мобільні додатки ні в чому не винні.

«Робити фото для Instagram – це не проблема. Якщо ці знімки надихають інших людей подорожувати – це чудова річ. Але проникати на приватну власність, захоплювати вдалі локації і заважати усім іншим, аби встигнути зробити 100 фотографій, – це не нормально».

(вгору)

Додаток 11

10.03.2019

Російські інтернет-тролі змінили стратегію втручання у вибори через соцмережі – ЗМІ

Пов’язане з Кремлем «Агентство Інтернет-досліджень», яке ще називають «фабрикою тролів», може бути серед тих, хто намагається в новий спосіб обійти запроваджені Facebook та Twitter заходи з видалення фейкового контенту, створеного для впливу на виборців у США під час президентській кампанії у 2016 році (ДетекторМ).

Про це з посиланням на експертів з кібербезпеки пише Bloomberg. передає «Українська правда».

«Замість того, щоб створювати контент самостійно, ми бачимо, що вони поширюють контент. Таким чином, він не обов’язково фейковий, і це дає їм можливість ховатися за когось іншого», – сказав директор з аналітичного аналізу в FireEye Inc. Джон Хультквіст.

За словами старшого дослідника загроз в Symantec Corp. Кендіда Вуеста, інші хакери зламують комп'ютери і використовують їх для створення великої кількості облікових записів в соціальних мережах, які виглядають, як справжні, а також правдоподібних фоловерів і «лайків» для них.

За словами експертів, поширення створеного іншими контенту, який розколює суспільство, не є новою технікою, проте російські тролі почали в значній мірі використовувати її саме напередодні наступних президентських виборів в США у 2020 році.

Вуест повідомив, що він помітив скорочення кількості випадків створення нового контенту за допомогою фейкових облікових записів з 2017 по 2018 рік і перехід до створення масових фоловерів, яких можна було б використовувати наступного року для поширення певних повідомлень.

Директор Федерального бюро розслідувань Крістофер Рей днями заявив, що соціальні мережі залишаються основним засобом іноземного впливу на вибори в США.

«Що практично не слабшає і тільки посилюється в ході виборчих циклів – це кампанія зі зловмисного іноземного впливу, особливо з використанням соціальних мереж. Це триває, і ми готуємося до того, що це продовжиться і буде рости до 2020 року», – сказав він.

Глава політики кібербезпеки в Facebook Натаніель Глейхер, у свою чергу, зазначив, що контроль цих спроб є «неймовірно складним балансом». Він пояснив, що компаніям потрібно знайти способи створити труднощі для зловмисників, які намагаються впливати на дискусію, без одночасного ускладнення публічного обговорення для користувачів.

Нагадаємо, світового розголосу набула оприлюднена 6 січня 2017 року доповідь американських спецслужб, у якій ідеться про втручання Росії в президентські вибори у США за допомогою хакерів і ЗМІ. У відкритій частині звіту йдеться про те, що наказ почати кампанію довкола виборів віддав Володимир Путін. Це було покликано збільшити шанси на перемогу Дональда Трампа, дискредитуючи його суперницю Гілларі Клінтон. Мета такої кампанії – підірвати довіру американців до виборчого процесу та зменшити шанси Клінтон на перемогу. Водночас, як зазначено у звіті, втручання Росії не поширювалося безпосередньо на підрахунок голосів.

Під час своєї першої прес-конференції 11 січня 2017 обраний президент США Дональд Трамп визнав втручання Росії у процес виборів шляхом хакерського зламу серверів американських установ, але заявив, що це могли робити й інші країни.

Окрім кібернападів, Росія впливала на кампанію й засобами пропаганди – частина звіту присвячена аналізу діяльності Russia Today і «тролів» в інтернеті. Звіт містить цитати із заяв головної редакторки RT і Sputnik Маргарити Симоньян, які свідчать про зв'язки цих ЗМІ з урядом Росії (сама Симоньян розкритикувала цю доповідь).

Міністерство юстиції США висунуло обвинувачення 13 росіянам і трьом російським компаніям у справі про втручання у вибори американського

президента у 2016 році. В обвинуваченні йдеться, що співробітники «Агентства інтернет-розслідувань» самі визначили своєю метою підрив довіри до політичної системи Сполучених Штатів. За цими даними, росіяни контактували зі співробітниками кампанії Трампа та його штабу, однак ті не здогадувалися, що мають справу з громадянами Росії, а не з американськими активістами, за яких видавали себе «тролі».

(вгору)

Додаток 12

27.02.2019

Майя Яровая

Массовые «чистки» в Telegram: за сутки каналы лишились тысяч подписчиков. Но это коснулось не всех

В ночь на вторник, 26 февраля, мессенджер Telegram провел массовую чистку подписчиков каналов, в результате чего многие сильно просели в цифрах. Некоторые каналы потеряли до 16 000 подписчиков, впрочем есть и такие, кого зачистка не затронула вовсе (AIN.UA).

Инцидент активно обсуждают в большом комьюнити админов Telegram-каналов. Предполагается, что мессенджер решил избавиться от ботов и неактивных аккаунтов, но официальной информации от представителей Telegram на этот счет пока не поступало. Примечательно, что каналы с украинской аудиторией чистка не затронула.

Одним из первых ситуацию прокомментировал основатель Zaichenko Team Максим Зайченко, который ведет Telegram-канал с предложениями по работе. По его мнению, таким образом Telegram начал бороться с накрученными подписчиками. «Это удар по ботоводам, которые кричат “Приведем вам энное количество целевых подписчиков на канал и в ваш бизнес”. К сожалению, на украинском рынке таких “экспертов” много, как правило они называют себя создателями более 100 каналов и так далее», – отмечает Зайченко в посте на Medium.

По его наблюдениям, у каналов с только украинской аудиторией подписчики остались на месте. А те, у кого было много подписчиков из других стран СНГ, лишились от 1000 до 8000 подписчиков.

«Возможно, это аккаунты, которые уже давно не юзают Telegram, и их просто деактивировали. Возможно, это боты, которые как-то привязаны к мобильным номерам стран СНГ. Потому что там больше всего идет отписка», – акцентировал Максим.

Канал самого Зайченко от чистки не пострадал. А вот канал Digitalizator Эда Кузьмина, основателя консалтинговой компании DIGITTERRA, за ночь лишился более 1000 подписчиков.

«Чтобы это ни было: зачистка ботов (у меня ботов нет), удаление “мертвых”/неактивных аккаунтов или баг Telegram, вывод должен быть один: нужно “раскладывать яйца в разные корзины”, то есть, если вы используете

Telegram-канал в маркетинговых целях, то важен комплексный подход– на один канал полагаться просто опасно. У вас должна постоянно и системно работать несколько ключевых каналов продвижения – от SMM, таргета, контекста до Online PR, мессенджеров, SEO и т.д.”, – комментирует Кузьмин.

У некоторых потери намного серьезнее, чем у Digitalizator. Например, популярный украинский канал «Магия утра» за ночь лишился 12 000 подписчиков. На это обратил внимание украинский медиапредприниматель, основатель ряда популярных Telegram-каналов Артур Оруджалиев.

«В украинском Телеграме есть секта – “Магия Утра”. “Магия Утра, это – абсолютно уникальное комьюнити людей, которые просыпаются до 6 утра. Создатель канала – предприниматель Андрей Пивоваров, которого вдохновила книга “Магия Утра” Хэла Элрода”. На днях Телеграм начал удалять ботов из каналов. И сразу стало понятно кто чего стоит. “Абсолютно уникальное комьюнити” только за один день поредело на 12500 “человек”», – отмечает Оруджалиев.

Андрей Пивоваров пока не ответил на запрос AIN.UA. Каналы самого Артура: «Мне это интересно» (5000+ подписчиков), «Афиша Киева» (43 000+) и «Афиша скидок» (20 000+) – не пострадали. «Пропало 0 [подписчиков], так как нет ботов. Всегда есть отписки – это естественный процесс. Но это единицы, максимум десятки», – пояснил он.

(вгору)

Додаток 13

12.03.2019
Владимир Кондрашов
Власти хотят ввести цензуру в Интернете по российскому сценарию

Украинские спецслужбы пытаются протянуть через Верховную Раду новый законопроект о цензуре в Интернете. Речь идет о новом законопроекте, который неожиданно «всплыл» в кулуарах парламента (InternetUA).

Информацию о новом законопроекте, у которого пока даже нет регистрационного номера, 12 марта опубликовала на своей странице в Facebook эксперт по стратегическим коммуникациям ОО «Информационная безопасность», бывший заместитель министра информационной политики Украины Татьяна Попова.

– Я держу перед собой сравнительную таблицу проекта Закона Украины «О внесении изменений в некоторые законодательные акты Украины относительно обеспечения информационной безопасности Украины». Передали его мне анонимные источники, и это тот законопроект, который, по слухам, хотят вынести одновременно с законопроектом о языке и «обменять», условно говоря, голоса одного законопроекта на голоса для другого. У законопроекта нет еще номера, но по слухам, он его очень быстро получит и быстро будет выставлен на голосование, если в Раде сложится «благоприятная атмосфера».

Надеюсь, после сегодняшней публикации этого не произойдет, – написала Попова.

В комментарии нашему изданию Татьяна Попова отметила, что текст данного законопроекта уже должен быть в депутатов профильных парламентских комитетов – по вопросам информатизации и связи и по вопросам свободы слова. Тем не менее, уверена Попова, зная активную позицию этих комитетов по вопросу противодействия цензуре, авторы законопроекта попытаются обойти данные комитеты. Например, с помощью Комитета ВР по вопросам национальной безопасности и обороны, где подобные решения принимаются «по щелчку пальцев».

Новым безымянным законопроектом, среди прочего, предлагается создание «Единого реестра исполнения судебных решений и применения санкций в сфере телекоммуникаций» (украинского аналога реестра запрещенных сайтов от Роскомнадзора), которым почему-то будет заниматься Министерство Юстиции Украины.

Кроме того, законопроектом предполагается обязать операторов и провайдеров телекоммуникаций за собственный счет закупать и устанавливать «технические средства, которые соответствуют техническим требованиям, определенным ГСССЗИ Украины по согласованию с СБУ, необходимые для ограничения доступа к информационным ресурсам».

– Это, во-первых, отразится на стоимости доступа к сети Интернет, ведь такое оборудование – дорогостоящее. Кроме того, нет гарантии, что данное оборудование будет только ограничивать доступ к каким-то ресурсам. Вполне вероятно, что таким образом будет мониториться весь трафик абонентов провайдера, – отмечает Попова.

Также в законопроекте предусмотрены изменения в Уголовный кодекс, которые регулируют «применение судом мер по ограничению доступа к определенному информационному ресурсу [...] и удаления из него информации, которая распространяется через этот ресурс (сервис), и непосредственно угрожает интересам национальной безопасности, территориальной целостности, общественному порядку, может привести к беспорядкам или преступлений, грозит здоровью населения, разглашает информацию, полученную конфиденциально…»

– То есть станут абсолютно невозможны не только будущие «Майданы», а, вероятно, и оппозиционные акции вообще. Что тут еще интересно: теперь все источники, которые конфиденциально предоставляют информацию, например, «Схемы» или ресурс «Наші гроші», будут нарушать тем самым этот закон. «Схемы» и «Наші гроші», скорее всего, будут заблокированы, а возможно, даже Facebook и Youtube, если они не удалят сообщение от «Наші гроші» и «Схем», если у них была «информация, полученная конфиденциально», – считает Попова.

Также изменения предлагаются и ст. 145 и 148-2 КУоАП, предусматривая дополнительное наложение штрафа на должностных лиц предприятий до 600 необлагаемых минимумов доходов граждан. А при повторном нарушении в

течение года – до 900 необлагаемых минимумов. То есть, кроме штрафа на предприятие будет еще штраф на должностных лиц. А значит, все операторы будут вынуждены сотрудничать, чтобы избежать штрафов предприятия и личных.

Изменения в п. 10 ст. 131 УПК дают возможность заблокировать сайт просто сразу после возбуждения дела.

– То есть, не понравились, например, господину Пашинскому материалы в «Новом времени» – их можно будет просто заблокировать сразу после возбуждения дела. И то же будет касаться всех других сайтов, – объясняет Попова.

Кроме того, в ст. 213-1 УПК предлагается добавить пункты о том, что с предварительным предупреждением медиа-ресурс может быть заблокирован сроком до 2-х месяцев. Предупреждение выдается по электронной почте, на адрес, указанный владельцем ресурса. Если же собственник не обнародовал своих контактных данных на соответствующем сервисе – это блокирование доступа возможно даже без его ведома. И даже если ответственное лицо будет отсутствовать на судебном заседании – это также не будет препятствовать рассмотрению ходатайства.

– В свою очередь, суд вправе слушать любого свидетеля, исследовать любой материал. То есть любая общественная карманная организация или любой гражданин сможет пожаловаться на любой канал, например, на «1 + 1» и господина Дубинского – и это будет означать, что можно будет, по словам этого свидетеля, заблокировать сайт, – говорит Татьяна Попова. – Также новый п. 5 ст. 213-5 УПК дает возможность повторных обращений любого лица даже в случае отказа судьей или судом в применении временного ограничения доступа к ресурсу. То есть они могут так мучить одного и того же судью несколько раз своими ходатайствами, пока различными методами не заставят его сделать нужные вещи. Интересный п. 4 ст. 213-6 УПК с уточнением, что ограничение доступа к ресурсам, размещенным за пределами Украины, будет обеспечиваться СБУ.

Пока неизвестно, кто именно стоит за данным документом. Эксперт отмечает, что следы его могут весть в СБУ или Государственную службу специальной связи и защиты информации (последние, напомним, на днях выдали неоднозначный приказ «Об утверждении общих требований к техническим средствам для блокировки доступа к определенному (идентифицированному) ресурсу (сервису) в телекоммуникационных сетях»)

– Точно не могу сказать, кто его автор. Отмечу, что законопроект сделан намного качественней, чем тот же скандально известный 6688. Судя по тому, что защищают в сети его комментаторы из СБУ, я склоняюсь к версии об их авторстве документа, – отмечает Попова. – При этом документ намного хуже скандального 6688.

(вгору)

Додаток 14

27.02.2019

Вредоносы научились использовать и отключать антивирусы

Обнаружены два вредоноса. Программа Shlayer для macOS старается отключить систему Gatekeeper, чтобы безнаказанно устанавливать новые модули. Троянец Astaroth для Windows эксплуатирует системный процесс антивируса Avast (InternetUA).

Отключаем или используем

Эксперты по безопасности выявили сразу два новых вредоноса, так или иначе атакующих или эксплуатирующих антивирусные программы на разных платформах.

В частности, новый вариант многоступенчатой программы Shlayer атакующей macOS, научился отключать защитную систему Gatekeeper, чтобы запускать неподписанный код.

Второй вредонос – это PC-троянец Astaroth, который способен использовать процессы антивируса Avast и продукты бразильской компании GASTecnologia для кражи данных и установки новых вредоносных модулей.

Некоторые подробности

Первый вариант Shlayer был выявлен еще год назад. Как и многие другие вредоносы под macOS, он выдавал себя за обновления AdobeFlash. То же самое делает и новая версия, с той лишь разницей, что если первый вариант распространялся через торренты, то новый – через взломанные домены или клоны легитимных сайтов, выводящих пользователям всплывающие окна с предложением скачать обновление. Также были отмечены случаи, когда ссылки на Shlayer попадались в рекламе, размещенной на легитимных сайтах.

Shlayer атакует все версии macOS, включая последнюю – 10.14.3 Mojave. На компьютеры жертв он попадает в виде файла .DMG, .PKG, .ISO или .ZIP, часть из которых снабжена подписью разработчика Apple, чтобы придать им большую легитимность.

Новая версия Shlayer также использует вредоносные shell-скрипты для скачивания дополнительных компонентов.

Как пишут исследователи группы CarbonBlack, при монтировании образа DMGи запуске мнимого инсталлятора из скрытой папки в смонтированном разделе запускается скрипт .command, который декодирует и дешифрует второй скрипт, содержащий, в свою очередь, другой закодированный скрипт, который позднее также будет запущен.

Последний скрипт из этой «гирлянды» представляет собой финальный этап первой стадии заражения; он собирает данные о версии macOS, установленной на целевой машине, включая уникальный идентификатор платформы, генерирует сессию GUID (используя uuidgen), создает специальную URL-ссылку, используя информацию, сгенерированную на предыдущих двух этапах, и скачивает вредоносный компонент для второй стадии заражения.

Затем он пытается скачать .ZIP-файл, используя curl, создает папку в /tmp и деархивирует в нее скачанное, используя пароли, вшитые в скрипт. Скачанный файл преобразуется в исполняемый и запускается, а окно скрипта закрывается с помощью команды killallTerminal.

После этого вредонос пытается повысить привилегии в sudo, используя /usr/libexec/security_authtrampoline. (Эту методику еще в 2017 г. описал эксперт Патрик Уордл (PatrickWardle).)

После этого Shlayer пытается отключить Gatekeeper, чтобы, с точки зрения операционной системы, все скачанные и запущенные модули выглядели как легитимные.

На случай, если это не получится, некоторые компоненты второй стадии снабжены действующими подписями разработчика Apple.

На данный момент Shlayer распространяет исключительно нежелательную рекламу, но в любой момент он также может начать распространять и более опасные компоненты.

Троянский конь Иштар

Astaroth – троянец, который атакует бразильских и европейских пользователей. Как и прошлые версии, новая эксплуатирует «легитимные системные процессы Windows для осуществления вредоносных операций и скрытной доставки вредоносных модулей», – так гласит описание, приводимое экспертами CybereasonNocturnus. Однако теперь троянец способен использовать в своих целях также «известные [защитные] инструменты и даже анивирусное ПО для расширения собственной функциональности».

Известно, что, как и более ранние версии Astaroth, нынешняя были способна использовать средства, называемые Living-off-the-landBinaries (или LOLbins), такие как интерфейс командной строки WindowsManagementInstrumentationConsole (WMIC) для скрытного скачивания и установки вредоносных модулей. Теперь же он также использует утилиту WindowsBITSAdmin – для скачивания из дополнительных источников (точнее, с командных серверов) новых модулей, которые спрятаны либо в изображениях, либо в файлах без расширений. Все это снабжено весьма эффективной обфускацией (запутыванием).

Что же касается антивирусов, то вредонос способен производить инъекцию вредоносного модуля в процесс aswrundll.exe антивируса Avast. Этот процесс используется и для сбора сведений о зараженной машине, и для подгрузки дополнительных модулей.

Аналогичным образом Astaroth может эксплуатировать процесс unins000.exe, запускаемый антивирусом GASTecnologia для поиска и сбора персональных данных о пользователе системы, если на ней нет антивируса Avast.

Троянец функционирует как кейлоггер, перехватывает вызовы операционной системы и собирает информацию из буфера обмена. Кроме того, он пытается собирать любые логины и пароли пользователей.

Со своей стороны, разработчики Avast так прокомментировали информацию о новом троянце. «Авторы эксплуатируют доверенный двоичный код для запуска вредоноса; в данном случае они использовали процесс Avast, вероятно, по причине большого размера нашей пользовательской базы в Бразилии... Важно понимать, что речь не идет ни об инъекции, ни о повышении привилегий. После установки, двоичные файлы Avast снабжены механизмом самозащиты, предотвращающим инъекции. В нашем случае, злоумышленники используют файл Avast для запуска двоичного кода таким же образом, как это может делать любая DLL, использующая встроенную в Windows программу rundll32.exe.»

Разработчики Avast также отметили, что уже снабдили свой антивирус средствами защиты от Astaroth и прорабатывают изменения в антивирус, которые позволят блокировать попытку использовать процесс подобными троянцами.

«Использование LOLbins, т. н. living-off-the-landbinaries – это действительно не инъекция кода, строго говоря. Троянец Astaroth злоупотребляет особенностью операционной системы, а не слабыми местами конкретных программ, так что ответственности Avast тут действительно никакой нет, – считает Олег Галушкин, директор по информационной безопасности компании SECConsultServices. – Намерение снабдить антивирус защитой от действия подобных вредоносов можно только приветствовать».

(вгору)

Додаток 15

28.02.2019

В App Store начали появляться клоны оригинальных приложений

Высокая степень безопасности App Store не возникла из ниоткуда. Она является результатом тщательно выверенных действий модераторов, проверяющих публикуемое в каталоге ПО, а также строгих правил, которым обязаны следовать все разработчики. Но нередко авторы приложений пренебрегают требованиями, установленными Apple, и идут наперекор им, планируя извлечь из этого дополнительную выгоду. Например, занимаются клонированием приложений, что, конечно же, категорически запрещено (InternetUA).

Как сообщил TechCrunch, App Store постепенно начали захватывать приложения-клоны, которые практически в точности дублируют функциональность исходных программ, их интерфейс, имея только лишь отличающееся название. Но примечательнее всего то, что авторами клонов являются разработчики исходных приложений.

Тем не менее, этот факт, казалось бы, не вызвал ни малейшего интереса ни у рядовых модераторов, но и у их руководства, которые, вероятно, предпочли закрыть на него глаза.

Приложения-клоны

На момент выхода публикации TechCrunch насчитал как минимум четыре приложения, у которых есть так называемые авторизованные клоны. Все они были выпущены создателями оригинальных программ. При этом некоторые из них имеют по два и более клонов:

-TextMe – TextMe Up, FreeTone
-Texting/Calling Phone Burner – Texting Shield – Phone Number – Business Line Phone Number – Burner Phone Number SMS/Calls – Smiley Private Texting SMS
-Phoner 2nd Phone Number Text – Text Burner – Texting Anonymous – Second Line – 2nd Phone Number
-Dingtone – Telos

Как понять, что перед вами приложение-клон

Некоторые разработчики подходят к вопросу клонирования более основательно и меняют не только название приложения, но и вносят некоторые изменения в его интерфейс, чтобы их было сложнее отличить. Пара Dingtone – Telos – как раз из таких. Тем не менее, понять, что это одно и то же приложение можно путем авторизации с использованием одного и того же аккаунта.

Зачем это разработчикам

Зачем разработчики все это делают, спросите? Ответ прост. Создавая несколько клонов одного и того же приложения, они могут использовать разные названия, разные описания и теги, которые пользователи ищут чаще всего. От этого зависит охват аудитории, который способна обеспечить программа, увеличивая тем самым общее количество загрузок. Несет ли это какой-то вред для рядового потребителя? Нет, если не считать того, что тем самым разработчики засоряют App Store, провоцируя и других быть менее честными по отношению к нам с вами.

(вгору)

Додаток 16

28.02.2019
Як видалити особисті дані з Інтернету?

Активні користувачі соцмереж залишають на своїх сторінках безліч інформації. Наприклад, фото, відео та дописи. Яким може стати їх здивування, коли, наприклад, їхні світлини з’являються на небажаних інформаційних ресурсах (InternetUA).

Що робити, якщо хтось використав інформацію про вас без вашого дозволу? Поширена ситуація: фото з вашої сторінки у Фейсбуку опублікували на інформаційному сайті без вашого дозволу. Але щоб його видалити, не потрібно звертатися до послуг хакерів. Це можна здійснити у законний спосіб.

Спосіб 1: звернутися до власника сайту

Потрібно розуміти, що видаляється тільки той контент, який розміщений неправомірно або який порушує будь-який з міжнародних законів і норм. Наприклад, Google реагує на повідомлення у рамках закону США «Про авторське право в цифрову епоху», який має назву DMCA. Перш за все,

експерти радять звернутися через форму скарги напряму до власника сайту, реєстратора доменного імені або хостинг-провайдера, тобто компаній, які надають доступ в Інтернет та реєструють адреси сторінок. Проте, відповідь на скаргу залежатиме від юрисдикції сайту, наголошує експерт з інформаційної безпеки Микита Книш.

«Досить часто власники сайту відмовляють у видаленні контенту, який використовувався без відома його автора, посилаючись на локальні закони країни. Наприклад, закон DMCA не діє в ряді арабських країн. Тому власники сайтів, які регулярно порушують правову політику, розміщують сайти у реєстраторів в ісламських державах, які не реагують на подібні скарги», – говорить експерт з інформаційної безпеки Микита Книш.

Книш наголошує, зазвичай великі та впливові сайти одразу реагують на скарги, тому що переживають за свою репутацію. Бо їх можуть виключити з пошукової видачі, що може призвести до відтоку відвідувачів, і як наслідок фінансових втрат.

Спосіб 2: прибрати сайт з пошукової видачі

Якщо вашу особисту інформацію розмістили на дошках оголошень або на сайтах, які не мають форму зворотного зв'язку – експерти радять прибрати цей сайт по ключовому запиту у пошуковиках. Наприклад, у Google. Для цього потрібно заповнити відповідну форму.

«Ви повинні бути власником цього контенту, власником авторського права на цей контент або мати документи, що підтверджують особу. Якщо, наприклад, опубліковано техпаспорт на машину з вашим ім'ям, це є підставою для видалення цих даних з результатів пошукової видачі», – пояснює Микита Книш.

Спосіб 3: звернутися до суду

Якщо не вдалося видали інформацію через форми скарг, потрібно звертатися до суду. Якщо суддя зобов'язав видалити якийсь контент, провайдер обов'язково це виконає.

З появою соціальних мереж люди отримали можливість спілкуватися з великою кількістю людей без кордонів. Проте, не варто заради лайків виставляти на показ усю інформацію про себе. Пам'ятайте, все, що потрапляє в мережу, залишається там назавжди.

(вгору)

Додаток 17

4.03.2019

Facebook тайно лоббировала смягчение закона о персональных данных

Судя по документам, которые стали известны из публикации Computer Weekly, Facebook обращалась к чиновникам по всему миру, включая бывшего канцлера Великобритании Джорджа Осборна. В обмен на поблажки в законе компания обещала больше инвестиций. Такие предложения Facebook

направляла в десятки стран, включая США, Канаду, Индию, Вьетнам, Аргентину, Бразилию, Малайзию и страны ЕС (InternetUA).

Facebook лоббировала свои интересы среди политиков по всей Европе, чтобы смягчить «чрезмерно ограничительный» закон о персональных данных. Среди документов также обнаружили заявление бывшего ирландского премьер-министра Энда Кенни, который отметил, что его страна «может оказывать значительное влияние на ЕС», продвигая интересы Facebook, хотя формально должна была оставаться нейтральной.

Кроме того, компания использовала феминистические мемуары Шерил Сэндберг, операционного директора компании, чтобы «сблизиться» с женщинами-комиссарами ЕС.

Документы, которые появились в СМИ, взяты из судебного дела против Facebook, возбужденного разработчиком приложения Six4Three в Калифорнии. Судя по ним, Сэндберг считает европейское законодательство о защите данных пользователей «критической угрозой» для компании. В записке, составленной после Давосского экономического саммита в 2013 году, Сэндберг говорит о «нелегкой борьбе», с которой столкнулась компания в Европе.

Также документы включают в себя подробности о «прекрасных отношениях» компании с Эндой Кенни. Ирландия играет ключевую роль в регулировании деятельности технологических компаний в Европе, поскольку ее комиссар по защите данных действует от имени всех 28 государств.

В его меморандуме отмечается «признательность» за решение Facebook разместить свою штаб-квартиру в Дублине и указывается, что новое законодательство о защите данных представляет собой «угрозу для рабочих мест, инноваций и экономического роста в Европе». Далее в нем говорится, что Ирландия готова взять на себя председательство в ЕС и поэтому имеет «возможность влиять на решения Европейской директивы по данным».

Представитель Facebook заявил, что документы все еще недоступны для общественности, поэтому они не могут прокомментировать их. «Как и другие документы, которые опубликовали в обход суда, они рассказывают одну сторону истории и не учитывают важный в этом случае контекст».

(вгору)

Додаток 18

5.03.2019

Киберпреступники активно эксплуатируют уязвимость в маршрутизаторах Cisco

Спустя всего два дня после публикации информации об уязвимости в популярных моделях SOHO маршрутизаторов Cisco и обнародования демонстрационного эксплоита, киберпреступники начали активно атаковать уязвимые устройства (InternetUA).

Речь идет об уязвимости CVE-2019-1663, позволяющей в любом браузере выполнить произвольный код через web-интерфейс уязвимого устройства.

Проблема затрагивает Cisco RV110W Wireless-N VPN Firewall, Cisco RV130W Wireless-N Multifunction VPN Router и Cisco RV215W Wireless-N VPN Router.

По данным компании Rapid7, в настоящее время в Сети доступны более 12 тыс. уязвимых устройств, большинство из них расположены в США, Канаде, Индии, Польше, Аргентине и Румынии. Согласно информации специалистов из Bad Packets, активное сканирование на предмет уязвимых устройств началось 1 марта нынешнего года. В ходе атак злоумышленники используют PoC-код, опубликованный экспертами компании Pen Test Partners 28 февраля.

Компания Cisco уже выпустила патч, устраняющий уязвимость. Пользователям рекомендуется как можно скорее установить обновление. В случае если устройства уже скомпрометированы, потребуется перепрошивка маршрутизаторов.

Новые атаки лишний раз доказывают, что публикация PoC-кодов только играет на руку злоумышленникам. Ранее похожая ситуация сложилась вокруг сайтов на базе CMS Drupal – спустя три дня после выпуска патча для уязвимости CVE-2019-6340 в ядре Drupal злоумышленники активно начали внедрять криптомайнер CoinIMP на уязвимые сайты, используя доступный на различных ресурсах PoC-код.

(вгору)

Додаток 19

6.03.2019

С приближением выборов в Украине участились кибератаки на госслужащих

С приближением дня президентских выборов в Украине увеличилось количество адресных рассылок спама и фишинговых сообщений государственным служащим (InternetUA).

Об этом заявил начальник Департамента киберполиции Сергей Демедюк, передает «Интерфакс-Украина».

«Я могу констатировать, что с начала избирательной кампании мы начали фиксировать очень большое количество таких кибер-инцидентов, которые связаны с рассылкой государственным служащим, работникам, которые имеют отношение, в том числе, и к избирательному процессу. Очень большое количество фишинговых сообщений, спам-рассылок. Это означает, что преступники пытаются получить доступ к компьютеру того или другого чиновника», – сказал Демедюк.

По его словам, такое вмешательство учащается с каждым днем приближения выборов. Хакеры атакуют украинские министерства и ведомства, в том числе Министерство иностранных дел, органы, которые обслуживают и являются партнерами Центральной избирательной комиссии, а также местные администрации.

Начальник Департамента киберполиции также рассказал, что на закрытых форумах появляются заказы о возможности получить доступ, «как они считают,

к Реестру избирателей, которые позволят преступникам, а также агрессору нивелировать процесс выборов». По словам Демедюка, анализ обнаруженных фактов свидетельствует о том, что большинство подобных заказов идут из Российской Федерации.

«Но это происходит также из Украины, из других стран Европейского Союза и стран за его пределами», – рассказал начальник Департамента киберполиции.

По его словам, также наблюдается массовый выброс дезинформации, как в соцсетях, так и в «непроверенных электронных изданиях, которые вырастают просто как грибы». Демедюк утверждает, что киберполиция тесно работает с Instagram и Facebook, пытается эту информацию выявлять и либо блокировать в соответствии с правилами сети, либо не давать доступ к такой информации гражданам.

Демедюк также отметил, что киберполиция тесно взаимодействует со Службой безопасности Украины.

«Когда информация касается их подотчетности, она немедленно передается в СБУ, и мы вместе работаем», – сказал чиновник.

Он объяснил, что под попытками вмешательства в работу ЦИК понимается не только вмешательство в работу сайта Центризбиркома, но также в работу страниц членов ЦИК и других работников комиссии в социальных сетях.

«Мы видим, что активизируются огромные трафики и заинтересованность», – сказал начальник департамента.

Он также сообщил об обнаружении ложных Интернет-сайтов Центральной избирательной комиссии.

«Когда идут массовые DDOS-атаки, когда начинается создание фейковых страниц ЦИК, это тоже способ фишинга – только здесь уже получение данных или создание определенной аудитории… Мы таких две заблокировали фактически», – отметил Сергей Демедюк.

(вгору)

Додаток 20

6.03.2019

Ирина Фоменко

Исследование: вредоносные URL-адреса несут самую серьезную угрозу

Согласно исследованию Mimecast по оценке риска для безопасности электронной почты, вредоносные URL-адреса в настоящее время являются распространенной проблемой – они содержатся в среднем в каждом 61 электронном письме (InternetUA).

Так, количество вредоносных URL-адресов в электронных письмах увеличилось более чем на 125 % по сравнению с результатами прошлого квартала. Почти половина (45 %) из 1025 респондентов исследования

сообщили, что объем атак с опасными вложениями значительно возрос за последний год.

Кроме того, 5 миллионов спам-писем, 26 713 вложений вредоносных программ, 53 753 атак нарушителей под видом законных пользователей, 23 872 опасных файлов из почти 232 миллионов проверенных электронных писем были пропущены поставщиками решений по обеспечению безопасности и доставлены в почтовые ящики. Это подвергло риску людей и организации.

«Электронная почта и Интернет являются естественным дополнением, когда дело доходит до проникновения в организацию. Электронная почта предоставляет правдоподобный контент и легко кликабельные URL-адреса, которые могут привести непреднамеренных жертв к вредоносным веб-сайтам. URL-адреса в email буквально являются точкой пересечения электронной почты и Интернета. Организациям нужна прозрачность по обоим каналам, чтобы обеспечить защиту», – заявил стратег по кибербезопасности Mimecast Мэтью Гардинер. – «Киберпреступники постоянно ищут новые способы, как избежать обнаружения, часто обращаясь к более простым методам, таким как социальная инженерия, для получения информации о человеке или фото с Интернета, чтобы узаконить свои попытки выдать себя за другого с целью “выудить” данные от ничего не подозревающих пользователей».

Количество случаев с нарушителями, выдающими себя за законных пользователей, продолжает расти: 41 % респондентов сообщили об этом типе мошенничества со стороны продавцов или деловых партнеров, которые просят деньги, конфиденциальную информацию или учетные данные. Еще 38 % заявили о мошенничестве с имитацией известных интернет-брендов.

Между тем, по-прежнему существует проблема, связанная с отсутствием эффективной подготовки по вопросам кибербезопасности, особенно когда речь идет о непреднамеренном открытии фишинговых писем сотрудниками.

По словам главного технического консультанта Mimecast Гарретта О’Хары, обучение, основанное на соблюдении требований, просто не работает. В прошлом году Mimecast приобрел платформу Ataata, разработанную американским военным, правоохранительным и разведывательным сообществом, которая помогает предприятиям бороться с нарушениями, вызванными погрешностями сотрудников. Компания утверждает, что 95 % случаев являются результатом человеческих ошибок.

«Что действительно интересно: вы можете подключить ее к шлюзу, а затем выполнять такие действия, как “защита” от реальных атак, и использовать ее в качестве способа измерения поведения для конечных пользователей», – прокомментировал О’Хара.

(вгору)

Додаток 21

7.03.2019
Ольга Карпенко

Facebook разрешит устанавливать срок хранения сообщений и других личных данных

Социальная сеть Facebook объявила о развороте в сторону защиты личных данных своих пользователей. Основатель сети Марк Цукерберг написал о том, как компания будет развивать свои сервисы с точки зрения приватности. Одно из ключевых изменений: сеть даст пользователям возможность устанавливать сроки хранения для приватного контента (подобно тому, как сейчас она делает с историями, они хранятся 24 часа). Например, можно будет выставить срок для сообщения, от нескольких секунд до месяца (AIN.UA).

Вот его ключевые тезисы:

– «Мы создали что-то вроде цифровой городской площади, а пользователям нужно что-то более приватное, вроде гостиной».

– «Понимаю, почему многие люди не верят, что Facebook сможет или захочет строить платформу, основанную на приватности, поскольку, если честно, у нас сейчас не самая лучшая репутация в построении сервисов, защищающих приватность. И мы исторически фокусировались больше на инструментах для открытости и шеринга. Но мы также и демонстрировали, что можем развиваться и делать то, что нужно самим пользователям».

– «Пользователи должны получить простые и закрытые сервисы, где только они контролируют, кто с ними общаются, и при этом быть уверенными, что никто чужой не получит доступ к их информации».

– Частная переписка пользователей должна быть безопасной, в частности – зашифрованной end-to-end-шифрованием. Никто, включая сам Facebook, не может иметь доступ к ней.

– Пользователи не должны волноваться о том, что их старые сообщения «ударят» по ним позднее. Поэтому сеть планирует дать пользователям возможность устанавливать срок хранения сообщений и другой приватной информации.

– Facebook не будет хранить данные пользователей на территориях стран, где нарушаются права человека.

По словам Цукерберга, за следующие несколько лет компания перестроит свои сервисы, включая Messenger и WhatsApp, так, чтобы они соответствовали этим принципам. Компания также собирается полностью внедрить в свои сервисы end-to-end-шифрование.

(вгору)

Додаток 22

11.03.2019
ПО для взлома банков пряталось в облаке Google

Домен облачного хранилища Google, как правило, рассматривается как заведомо надежный, чем и пользуются злоумышленники: использование этих

ресурсов помогает обходить защитные инструменты в корпоративных сетях и обманывать пользователей (InternetUA).

Облако под подозрением

Банковские и финансовые учреждения в США и Великобритании стали объектом фишинговой кампании, в ходе которой основные вредоносные программные элементы хранятся и раздаются через Google Cloud Storage.

Атака начинается с массовой рассылки сообщений, содержащих ссылки на сжатые файлы с расширениями .zip или .gz. Внутри архивов содержится вредоносный код.

Хостинг вредоносов на storage.googleapis.com позволяет злоумышленникам обходить защитные инструменты: огромное количество компаний используют этот домен для своих нужд, так что он рассматривается как заведомо надежный, и коммерческие защитные инструменты обычно игнорируют его.

«Это пример растущей популярности “репутационного перехвата” – атаки, при которой злоумышленники прячутся за хорошо известными, популярными хостинг-сервисами, чтобы избегать обнаружения», – говорится в анализе фирмы Menlo Labs, выявившей проблему.

Злоумышленники не случайно выбирают такой способ распространения угрозы. Многие защитные продукты легко распознают вредоносные вложения в почту, однако переход по ссылкам на веб-ресурсы злоумышленников будут блокировать только в том случае, если домены уже находятся в черном списке. Домен storage.googleapis.com, естественно, не будет рассматриваться как вредоносный.

Houdiniu QRat – старые знакомые

Эксперты Menlo Labs проанализировали вредоносное содержимое рассылаемых в рамках кампании архивов. Часть этих файлов представляла собой скрипты VBS, подвергнутые тщательной обфускации (запутыванию кода). Аналитикам удалось выяснить, что эти скрипты скачивали вредоносы семейства Houdini/jRAT и QRat.

Houdini представляет собой типичного компьютерного червя, который появился в 2013 г. и с тех пор активно используется и столь же активно совершенствуется. В течение 2019 г. было отмечено три всплеска распространения вредоноса через ресурсы Pastebin.

В свою очередь, jRAT и QRat – это средства удаленного управления зараженными компьютерами.

«RAT – один из инструментов, наиболее активно используемых злоумышленниками для закрепления в инфраструктуре атакуемой организации, – отмечает Михаил Зайцев, эксперт по информационной безопасности компании SEC Consult Services. – При атаках на финансовые организации злоумышленники заинтересованы в длительном сохранении присутствия и возможности доступа к ключевым узлам корпоративных сетей. Средства удаленного администрирования в этом плане для них – незаменимая вещь».

(вгору)

Додаток 23

12.03.2019
Стоит ли бояться вирусов для iOS

Ходят легенды, что под iOS не существует вирусов. Якобы из-за тщательного подхода Apple к обеспечению безопасности своей операционной системы она оказывается практически полностью защищена от вредоносных программ вроде червей и троянцев. Но почему в таком случае App Store буквально ломится от всевозможных антивирусных приложений, чьи разработчики наперебой обещают защиту ваших данных? Пришло время разобраться и, наконец, поставить точку в этом вопросе (Украинский телекоммуникационный портал).

Точнее, чем исследователи в области информационной безопасности, на этот вопрос не ответит никто, решили журналисты Business Insider и обратились за комментариями к ним.

Вирусы для iOS

По словам Амита Серпера, руководителя отдела исследований в компании Cybereason, риск заражения iOS-устройства вирусом настолько мал, что им вообще можно пренебречь. Все дело в обеспечиваемых самой операционной системой уровнях защиты, препятствующих самопроизвольному проникновению вредоносного программного обеспечения, называемого вирусом, на устройство. Впрочем, это не означает, что пользователи iOS не подвержены никаким угрозам.

В мире существует несколько (их точное число неизвестно) программ с признаками вирусов, которые проникают на устройства жертв по чьему-то указанию. Их немного, но они есть, и в большинстве случаев они являются продуктом спецслужб тех или иных стран. «В том, что государства ищут способы взламывать мобильные устройства, нет ничего удивительного. Вспомните дело Сан-Бернардино, когда Apple отказалась создавать бэкдор, спровоцировав целый скандал», — сказал Роджерс.

Вероятность схлопотать заражение правительственным вирусом крайне мала, объяснил исследователь. Как правило, они направлены на конкретных лиц, которые признаны режимом, к примеру, изменниками родины. Поэтому риск оказаться зараженным программами вроде Pegasus, разработанных по приказу властей ближневосточных стран, практически нулевой. Но и это не значит, что можно расслабиться.

Приложения-мошенники

Поскольку Apple всячески пресекает возможность установки ПО из сторонних источников, чаще всего злоумышленники используют App Store для распространения мошеннических программ. Большинство из них направлены на списание денежных средств теми или иными способами. Например, некоторые оформляют на пользователя еженедельную подписку, в результате

чего с его банковской карты списываются небольшие суммы, чтобы он ничего не заподозрил.

Но иногда попадаются и более продвинутые мошенники, чьи приложения предлагают отсканировать палец якобы для поиска архивных данных о пользователе и его родственниках, подставляя в этот момент окно подтверждения транзакции на ту или иную сумму.

Вывод: существуют ли вирусы под iOS? Да, существуют, но их настолько мало, что о них можно забыть. Куда важнее следить, не воруют ли деньги приложения, которые вы считаете легитимными. Для этого необходимо проверить список оформленных подписок. Это можно сделать в App Store, в разделе личного профиля.

(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.