СОЦІАЛЬНІ МЕРЕЖІ ЯК ЧИННИК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Огляд інтернет-ресурсів
(17.01–31.01)

2017 № 2

Соціальні мережі
як чинник інформаційної безпеки

Інформаційно-аналітичний бюлетень
Додаток до журналу «Україна: події, факти, коментарі»
Огляд інтернет-ресурсів
(17.01–31.01)
№ 2

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

© Національна бібліотека України
імені В. І. Вернадського, 2017

Київ 2017

ЗМІСТ

РОЗВИТОК І ПЕРСПЕКТИВИ СОЦІАЛЬНИХ МЕРЕЖ

***

17.01.2017

Зафиксировано рекордное количество посетителей «ВКонтакте» в Украине

Количество пользователей социальной сети «ВКонтаке» в Украине достигло отметки 15 млн за сутки (STYLER).

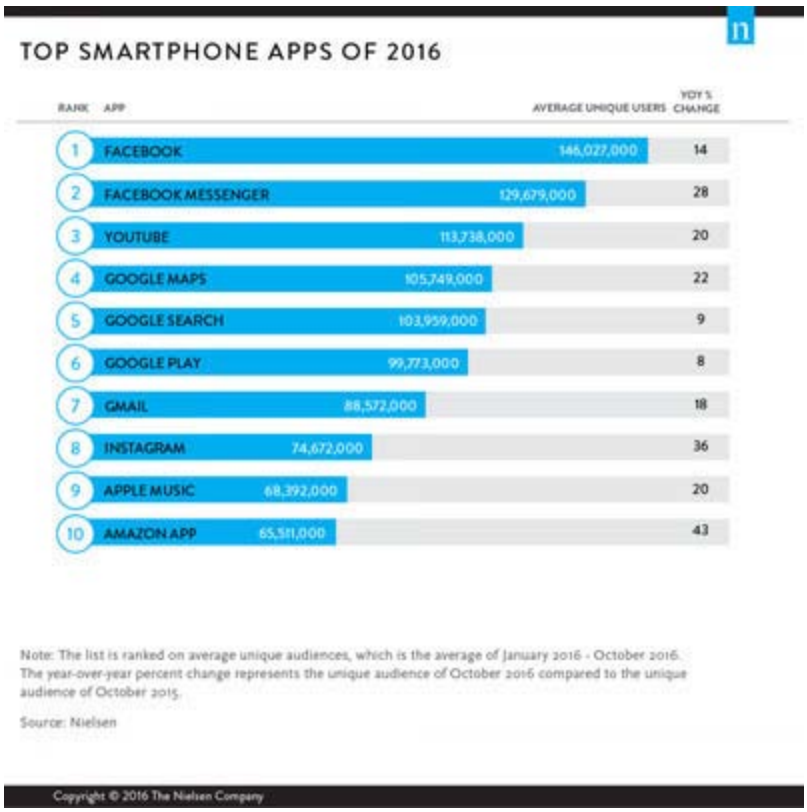
О новом рекорде сообщил пресс-секретарь «ВКонтакте» В. Леготкин, ссылаясь на данные Liveinternet за декабрь 2016 и январь 2017 г. «Отдельные масс-медиа целый год пугали заголовками, будто “ВКонтакте” теряет популярность в Украине. Однако за последний год мы выросли еще на один миллион, а в январе уверенно повышаем рекордную отметку», – сказал он. По данным В. Леготкина, в январе 2014 г. среднесуточное количество уникальных посетителей ВКонтакте с Украины было на уровне 12 млн. С каждым годом эта цифра регулярно увеличивалась на один миллион. Он также отметил, что весь предыдущий год стал очень важным и насыщенным для «ВКонтакте». «Мы полностью перешли на новый дизайн в настольной версии сайта, представили умную ленту новостей, что учитывает интересы человека, добавили возможность отправки голосовых сообщений, запустили тестирование стриминговой платформы для игровых трансляций, а также представили экспериментальный фотоприложение Vinci, использует возможности нейронных сетей, и мобильное приложение для прямых трансляций VK Live, который скоро появится на Android и уже доступен для устройств на iOS», – рассказал он. Украинская команда «ВКонтакте» в 2016 г. поддержала социальную инициативу по популяризации чтения книг на украинском языке #bookchallenge_ua и экологическую акцию let’s do it, Ukraine!. Совместно с Всемирным фондом природы WWF организовала прямой эфир в честь Часа Земли, представила перевод сайта на русинском языке и галицким говором, в качестве ментора приняла участие в масштабном украинском хакатони Media Hack Weekend. В октябре 2016 г. «ВКонтакте» исполнилось десять лет.

***

17.01.2017

Стало известно о том, какие приложения оказались наиболее популярными в 2016 г.

Facebook занял первое место. Его средние показатели – 146 млн уникальных пользователей в месяц и 14-процентный рост в сравнении с прошлым годом (ITnews).



Далее идет YouTube у которого 113 млн уникальных пользователей в месяц.

Но что еще интереснее, благодаря своим сервисам, Google заняла больше всего позиций в первой десятке. Так, помимо отмеченного видеохостинга, здесь еще Google Maps, Google Search, Google Play и Gmail.

Любопытный рост в прошлом году за Amazon. В период праздничных продаж ряд электронных площадок побил множество рекордов и в упомянутой копании рост 37 %. В Nielsen отмечают, что пользователи больше всего товаров заказывали именно посредством мобильного приложения.

***

18.01.2017

Павел Дуров подтвердил планы добавить аудиозвонки в Telegram

Telegram обзаведется новой важной функцией (IGate).

Основатель и генеральный директор популярного мессенджера Telegram П. Дуров на своей странице в Twitter рассказал, что в будущем компания намерена добавить функцию аудиозвонков в сервис.

Комментируя предложение одного из пользователей, добавить в Telegram возможность совершать звонки, а также менять тему внутри сервиса П. Дуров согласился, ответив, что сделают это. Какой-либо точной информации о планах компании и предполагаемых сроках реализации функций П. Дуров не предоставил.

Отметим, что поддержка пользовательских тем уже появилась в десктопной версии мессенджера.

О запуске аудиозвноков в Telegram ходят слухи еще с весны 2015 г. Тогда представители компании упоминали о тестировании технологией зашифрованных звонков, однако позже заявляли, что эта функция не является приоритетом для команды разработчиков.

На сегодняшний день, возможность совершения звонков является стандартным атрибутом мессенджеров. Она реализована в WhatsApp, Facebook Messenger, Viber, Hangouts и других популярных сервисах.

***

18.01.2017

Соцсеть LinkedIn намерена вернуться в Россию

Мосгорсуд признал законным блокировку LinkedIn в России по просьбе Роскомнадзора за нарушение закона «О персональных данных» (Экономические известия).

Вице-президент и один из основателей социальной сети LinkedIn А. Блю рассказал в интервью «РИА Новости» о планах компании вернуться в Россию, информирует eizvestia.com.

«Для нас очень важно тесно работать с российским правительством, чтобы быть уверенными в том, что мы реагируем на озабоченности обеих сторон. И мы рассчитываем делать это», – заявил он.

А. Блю уточнил, что не может точно сказать, когда соцсеть вернется в страну, добавив, что не хочет говорить «о специфике переговоров».

7 января 2017 г. Google и Apple удалили LinkedIn из магазина приложений по требованию российских властей.

***

19.01.2017

Как Facebook будет бороться с фейковыми новостями в Германии

Проверкой сомнительных новостей в немецкоязычной версии Facebook будет заниматься исследовательский центр Correctiv. DW выяснила, что это за компания и как будет проходить проверка (Deutsche Welle).

После обрушившихся на Facebook громких обвинений в распространении во время президентских выборов в США фейковых новостей компания начала думать о том, как бороться с появляющейся в соцсети фальшивой информацией. В Германии проверять информацию из соцсети на достоверность будет берлинская исследовательская компания Correctiv, которая называет себя «первым некоммерческим исследовательским центром в немецкоговорящей среде».

Накануне выборов в бундестаг, которые состоятся осенью, эту превентивную меру многие приветствуют. После скандала, разразившегося в

связи с распространением сфальсифицированных новостей во время избирательной кампании в Америке, немцы опасаются, что дезинформация может повлиять на исход парламентских выборов в их стране.

Компания Correctiv будет проверять фейковые новости для Facebook в Германии

Как объяснил в интервью второму каналу немецкого телевидения (ZDF) глава Correctiv Д. Шравен (David Schraven), 25 экспертов из его команды будут проверять сомнительные новости на достоверность. Денег за свою работу Correctiv получать не будет: с момента основания компания финансируется за счет пожертвований и грантов от различных фондов. На первое время так и будет продолжаться, хотя на странице Correctiv в Facebook Д. Шравен отмечает, что «будет сложно тратить пожертвованные деньги на оздоровление Facebook».

Как Correctiv будет проверять фейки

В ближайшем будущем руководство соцсети планирует как можно скорее разоблачать появляющиеся на ее станицах ложные публикации – неважно, на какую тему – и предупреждать об этом пользователей. Чтобы обуздать наплыв фейков, в США Facebook уже работает с целой сетью независимых организаций. Теперь и в Германии Correctiv будет проводить оценку достоверности сомнительных публикаций. Однако для начала Facebook предстоит улучшить технические настройки.

В отличие от американских юзеров, у пользователей немецкоязычной версии соцсети пока нет возможности сообщать Facebook о сфальсифицированной информации. Они могут лишь пометить предположительно фейковые новости как спам, не конкретизируя при этом, что речь идет именно о ложных сведениях.

Однако уже в ближайшее время и в немецкоязычной версии Facebook будет добавлен пункт «Речь идет о фальшивой новости». Как только публикация наберет «соответствующее количество отметок», ее начнут проверять в редакции Correctiv, объясняет Д. Шравен. Если окажется, что пост, на который пожаловались пользователи, действительно содержит фальшивую информацию, он будет отмечен предупреждающим знаком и по возможности сопровожден ссылкой на верные факты. Удалять такие посты не будут.

В случае с некоторыми постами – например, если речь идет о неверных цитатах – в Correctiv рассчитывают, что на исправление и соответствующую маркировку не потребуется много времени. В более сложных случаях, когда вокруг правдивого фактического ядра неожиданно возникают «дикие выдумки», работа редакторов будет выглядеть совсем иначе, подчеркнул Д. Шравен.

Важную роль в разоблачениях фейков будут играть и пользователи, поскольку именно они стимулируют весь процесс проверки подлинности информации. Если в редакцию Correctiv не поступит достаточное количество жалоб на пост в Facebook, проверка осуществляться не будет. Д. Шравен не

исключает, что его компании придется увеличить количество сотрудников, но это станет окончательно понятно только после завершения тестовой фазы.

На данный момент у Correctiv не настолько большой штат, чтобы редакторы могли проверять каждую ссылку. Технические и организационные моменты тоже нужно прояснить, отметил глава компании в интервью газете Süddeutsche Zeitung. Необходимо подумать и о финансировании на долгосрочную перспективу, чтобы создать для проекта прочную основу, рассуждает он и добавляет, что Facebook, возможно, впоследствии все же придется выделять деньги.

При этом сам Д. Шравен не уверен, окажется ли идея проверять на достоверность новости из Facebook эффективной в борьбе с фейковыми сведениями, которые благодаря своему быстрому распространению уже приобрели огромные масштабы. «Мы убеждены, что одной этой инициативы недостаточно, чтобы стабильно справляться с фальшивыми новостями. Нужно найти много различных способов. Но мы рады, что Facebook по крайней предпринимает эти шаги», – написал он на странице в соцсети.

Facebook принимает меры, но снимает с себя ответственность

Facebook также планирует препятствовать использованию постов для «зарабатывания денег». Об этом в середине декабря объявил в своем блоге вице-президент компании А. Моссери. Это решение было принято после того, как во время президентской кампании в США некоторые пользователи, прикинувшись новостными СМИ, зарабатывали, распространяя в соцсети фальшивую информацию.

Между тем немецкие политики считают, что Facebook опоздал с предложенными мерами по борьбе с ложной информацией. Так, министр юстиции ФРГ Х. Маас (Heiko Maas) уже давно требовал принять жесткие меры в отношении соцсети и призвать ее к ответственности. В субботу, 14 января, правящая коалиция договорилась ужесточить меры против публикации в социальных сетях комментариев, разжигающих ненависть, и поддельных новостей. Глава фракции ХДС/ХСС в бундестаге Ф. Каудер (Volker Kauder) потребовал, чтобы Facebook и Twitter создали отделы претензий, которые работали бы 24 часа в сутки и реагировали бы на жалобы пользователей.

Руководство соцсети, похоже, наконец-то прислушалось к критике немецких властей. Американская компания заявила, что помимо Correctiv планирует найти и других партнеров в Германии для борьбы с фейковыми новостями. Однако тем самым соцсеть снимает с себя ответственность, по крайней мере редакционную. А значит, посыл ее руководства, по всей видимости, таков: вранье постят другие – и исправлять его тоже другим.

***

17.01.2017

В Twitter запустили возможность 360-градусной трансляции из Periscope

Западные СМИ сообщают о том, что в Twitter появилась возможность 360-градусной трансляции видео (ITnews).

Как отмечается, на данный момент эта функция доступна лишь «избранным пользователям», и как быстро «доберется» до остальных, пока не прогнозируется.

Зато смотреть такой контент могут все и уже сейчас.

Стоит также добавить, что прямые трансляции контента такого плана помечаются специальным значком одновременно и в Periscope и в Twitter. Изменять угол наклона можно двумя способами – двигая телефон в разные стороны, либо водя пальцем по экрану.

***

17.01.2017

BuzzSumo назвала самый вовлекающий тип постов в Facebook

Потребители лучше взаимодействуют с очень короткими постами в Facebook, отмечает новое исследование BuzzSumo. Компания проанализировала данные 800 млн постов в сети, размещенные в 2016 г. Исследователи учитывали количество шеров, лайков и комментариев для каждого поста и общее вовлечение. Посты с менее чем 50 знаками получили самое большое общее вовлечение (общее количество шеров, лайков и комментариев). Взаимодействие сильно падало для постов, чья длина превышала 50 знаков. Размещение постов в «низкие» периоды – поздно ночью и в непиковые дни, такие как воскресенье, приводило к большему вовлечению. Посты с вопросами генерировали больше лайков в Facebook. Видео получали больше шеров, чем другие типы постов (Marketing Media Review).

***

24.01.2017

Twitter сохранит доступ к архиву 6-секундных роликов Vine

Несмотря на остановку Vine, эта служба обмена короткими циклическими роликами не канет в Лету со всем накопленным пользователями за четыре года видеоматериалом. Twitter объявила об открытии архива Vine по прежнему адресу, где доступны категории, рейтинги и списки для удобства ориентирования в миллионах архивных записей. С помощью поиска можно найти конкретного пользователя (InternetUA).

К сожалению, теперь отсутствует простой способ встраивания видео, остаётся только возможность поставить ссылку на архивную страницу Vine. Между тем, старые ссылки для встраивания по-прежнему работают на связанных страницах. Число отметок, перепубликаций и просмотров тоже замерли во времени.

Любители коротких роликов, как выяснилось, могут по-прежнему их записывать с помощью нового мобильного приложения Vine Camera,

унаследовавшего значительную часть функций из полноценного окружения Vine, за исключением социальных возможностей и инструментов Vine Soundboard, Snap-To-Beat, Featured Track для наложения звуковых дорожек. Эти записи можно размещать прямо в Twitter, причём они будут воспроизводиться циклически.

Предполагается, что архив не будет закрываться, но ничего не бывает вечным, тем более в Интернете. А тем, кто не желает продлевать жизнь своему собранию видеозарисовок Vine, следует просто удалить учётную запись.

***

24.01.2017

Для Windows-версии Viber вышло крупное обновление

Популярный мессенджер Viber в прошлом регулярно получал обновления для Windows 10 и Windows 10 Mobile, но на днях разработчики выпустили крупнейший апдейт с того момента, как приложение стало универсальным. Одним из самых заметных нововведений в последней версии для Windows 10 стал переработанный пользовательский интерфейс. Особенно изменения заметны в разделе обмена информацией, который был полностью обновлён (InternetUA).

Изменения в новой версии Viber для Windows 10:

– обновлённый пользовательский интерфейс раздела Share с новыми возможностями и улучшенной функцией обмена фотографиями;

– нажатие кнопки Share в окне чата предлагает на выбор шесть вариантов действий: отправить фото и видео, сделать фото и видео, отправить файл, отправить контакт, отправить местоположение, нажать и говорить;

– при нажатии на иконку Share автоматически открывается меню для выбора фотографий;

– появилась возможность прикрепить одну или несколько фотографий и отправить их одновременно (на PC можно прикрепить и отправить только один снимок);

– полностью переработанное меню Share.

Обновление пока что доступно небольшому числу пользователей. Таким образом компания планирует собрать статистику и определить стабильность работы приложения перед масштабным релизом.

***

26.01.2017

Facebook тестирует функцию исчезающих публикаций

В Facebook появилась новая функция самоуничтожающихся постов, что сделано по аналогии Instagram и Snapchat. Об этом сообщает информационное издание Business Insider (Grifonsoft).

В сети Facebook начали работать самоуничтожающиеся посты, которые исчезают спустя 24 часа после публикации. Эта функция доступна в разделе Facebook Stories, который сейчас проходит режим тестирования на территории Ирландии. Разработчики сообщают, что в скором времени новинка окажется доступна для всех желающих мира. Раздел Facebook Stories работает по аналогии с «Историями» в сети Instagram, располагается над лентой новостей и доступен только в мобильной версии. Главной особенностью является то, что пользователи могут отправить любое количество своих фото, видео и других файлов, которые будут автоматически ликвидированы спустя 24 часа.

Представители Facebook сообщают, что проект Stories был создан в виду того, что люди стали отправлять гораздо больше контента и разработчики разнообразили этот процесс с помощью дополнительной функции.

***

30.01.2017

Пользование соцсетями в мире возросло на 21 %: Hootsuite

Крупнейшая в мире SMM-платформа Hootsuite в партнерстве с SMM-агентством We Are Social выпустила отчет Digital in 2017, в котором проанализировала основные тенденции развития социальных медиа и digital-тренды, сообщает Cossa (Телекритика).

Один из ключевых выводов исследования заключается в том, что за последний год глобальное проникновение Интернета возросло на 10 % достигнув 3,8 млрд пользователей всемирной сети, или 50 % населения Земли.

Кроме того, согласно исследованию, глобальное потребление социальных медиа в прошлом году возросло на 21 %, достигнув 2,8 млрд пользователей.

***

31.01.2017

Twitter заменит «Моменты» более полноценным разделом Explore

Более года назад сервис микроблогов Twitter запустил «Моменты» – функцию, позволяющую пользователям следить за наиболее важными новостями, появляющимися в сервисе. Теперь компания объявила о замене этого раздела новой вкладкой под названием Explore («Исследование») (InternetUA).

Тем не менее, от «Моментов» Twitter не избавляется целиком и полностью. На самом деле, компания собирается интегрировать старую функцию в новую вкладку. Explore, по словам разработчиков, предоставляет пользователям быстрый доступ к новейшим тенденциям, моментам и поиску.

«До сегодняшнего дня вам нужно было переходить в различные места, чтобы найти каждый из этих опытов, – написала компания в своём блоге. – В рамках наших постоянных усилий упростить просмотр того, что сейчас происходит, мы собрали всё это в одном месте. Очень скоро вы сможете найти

тренды, моменты, поиск и лучшие прямые трансляции во вкладке Explore. Весь последний год мы рассматривали различные способы, позволяющие пользователям находить и использовать тренды, моменты и поиск. В процессе исследования люди рассказали нам, что новая вкладка Explore помогала им легко находить новости, события, тенденции и то, что сейчас популярно».

Twitter тестирует раздел Explore уже некоторое время, но скоро он станет доступен всем пользователям iOS. Также, вероятно, в ближайшие месяцы компания предоставит доступ к новой вкладке пользователям Android и Windows 10. До этого момента в официальных приложениях Twitter можно будет продолжать использовать вкладку «Моменты».

***

30.01.2017

Базиленко Анна

Facebook додав функцію авторизації за допомогою електронного ключа

У Facebook з'явилася можливість авторизації за допомогою електронного ключа, йдеться в офіційному блозі компанії. Втім, нова функція поки доступна лише для окремих браузерів, зокрема останньої версій Chrome, і недоступна для мобільного додатку Facebook. Виняток становлять лише Android-пристрої з функцією NFC і встановленим Google Authenticator (Watcher).

Замість того, щоб вводити SMS-код для підтвердження входу, тепер користувачі зможуть скористатися USB-накопичувачем, зареєстрованим як електронний ключ. У компанії переконані, що використання стандартної двофакторної аутентифікації не гарантує повну безпеку даних.

Для того, щоб активувати нову функцію, потрібно додати ключ у налаштуваннях облікового запису (Налаштування – Безпека – Підтвердження входу).

Подібні ключі вже продаються в різних компаніях, включаючи Yubico.

***

30.01.2017

В WhatsApp появится функция отслеживания местоположения и редактирование отправленных сообщений

Скоро мессенджер WhatsApp получит функцию живого обмена информацией о местоположении. Об этом свидетельствуют утечки информации от инсайдеров компании. Предполагаемая функция позволит передавать собеседнику координаты конкретного места, в котором находится автор сообщения (InternetUA).

По данным инсайдера, WhatsApp будет поддерживать живой обмен геолокационными данными. Эта функция вошла в перечень изменений тестовой сборки приложения. Такую возможность получат владельцы

устройств на iOS и Android. Касается это версий 2.17.3.28 и 2.16.399 соответственно.

По умолчанию функция будет отключена, но пользователь сможет ее активировать при желании. Включить отслеживание можно на 1, 2, 5 минут или на неопределенный срок (до выключения). Это удобно, так как пользователь сможет узнать, к примеру, насколько далеко находятся участники группы от места, где договорились встретиться. Каждый из участников группы может запретить другим следить за его местоположением – это также настраивается в мессенджере.

WhatsApp – самый популярный в мире мессенджер, потому неудивительно, что реакция пользователей на это нововведение была крайне бурной. Одни заявили, что давно ждут чего-то подобного, ведь теперь встречи с друзьями и партнерами по бизнесу станет проще планировать. Другие же сомневаются, не было ли введено это дополнение под прессингом со стороны спецслужб. Представители WhatsApp воздерживаются от комментариев по поводу нововведения.

Другое новшество в WhatsApp касается возможности отзыва и редактирования уже отправленных сообщений. Обе функции будут применимы к сообщениям, которые адресат еще не прочитал. Редактирование позволяет изменить текст отправленного сообщения; адресат увидит обновленный вариант и не сможет посмотреть историю изменений.

Еще одно нововведение приложения касается предупреждения о разрядке смартфона. Если во время разговора аккумулятор разрядится слишком сильно, мессенджер отправит соответствующее уведомление.

О сроках введения новых функций в WhatsApp, источники не сообщают.

***

30.01.2017

Эмодзи увеличивают вовлечение в Instagram на 17 %

Новое исследование Quintly подтвердило позитивное влияние эмодзи на вовлечение пользователей с постами в Instagram. Исследование проанализировало 22 000 профилей и 6,2 млн постов. Уровень взаимодействия постов с эмодзи составлял 2,07 по сравнению с 1,77 для постов без смайликов. Исследование также отметило, что чаще всего пользователи использовали эмодзи камеры, за ним следовал сигнал «OK» и розовые сердца (Marketing Media Review).

СОЦІАЛЬНІ МЕРЕЖІ ЯК ВИЯВ ФОРМУВАННЯ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА

***

17.01.2017

Трамп просит прийти на свою инаугурацию через Facebook

Издание «Independent» сообщает, что Д. Трамп 17 января стал приглашать «всех желающих» посетить свою инаугурацию с помощью социальной сети Facebook. По оценкам его службы безопасности на торжественное мероприятие придут около 900 000 человек, в то время как на инаугурации Б. Обамы последний раз было более 1,8 млн американцев, – передает replyua.net (replyua).

Американские СМИ высмеивают этот «пиар ход» Д. Трампа – еще никто из американских президентов не просил прийти на свою инаугурацию, тем более, при помощи рекламы на Facebook. Согласно последним социальным опросам, проведенным ABC News и Washington Post, Д. Трамп имеет поддержку лишь 40 % американцев, что на 21 % меньше, чем имел Б. Обама. В рекламе Д. Трамп заявляет: «Инаугурация – это важнейший момент в истории нашей страны. Я хочу, чтобы вы были со мной в этот день. Приходите, будет интересно». По словам специалистов, это реклама направлена на аудиторию совершеннолетних граждан США старше 27 лет.

Как сообщалось ранее, свой бойкот инаугурации Д. Трампа уже объявили 26 конгрессменов, а также десятки голливудских звезд и представителей американского шоу-бизнеса, в том числе Мадонна и С. Йоханссон. Многие американские звезды отказали Д. Трампу и в выступлении на концерте в честь инаугурации.

***

17.01.2017

Трамп продолжит вести свой личный аккаунт в Twitter на посту президента США

Избранный президент США Д. Трамп заявил о намерениях и дальше вести свой личный аккаунт в социальной сети Twitter, сообщает The Times (InternetUA).

«Я думаю, что сохраню @RealDonaldTrump», – отметил он, отвечая на вопрос журналиста, под каким именем он продолжит писать в Twitter.

Трамп подчеркнул, что в настоящее время число его подписчиков, включая Twitter и Facebook, составляет 46 млн человек.

«Пресса так нечестно пишет обо мне, что я высказываю свое мнение в Twitter», – добавил миллиардер.

По его словам, существует «пара человек», которые помогают ему вести микроблог.

«Я просто что-то диктую, и они набирают текст», – уточнил республиканец.

***

18.01.2017

Трамп: если бы пресса была честной – я бы не пользовался Twitter

Избранный президент США Д. Трамп объяснил, что пользуется социальной сетью Twitter только для собственной защиты от нечестной прессы. Об этом Д. Трамп во время интервью сообщил телеканалу Fox News, передает УНН (Версии).

«Мне не нравится писать твиты. Есть другие вещи, которые я могу делать. Однако я сталкиваюсь с очень нечестными СМИ. Это мой единственный способ им противостоять. Когда люди представляют меня в ложном свете, у меня по крайней мере есть способ сказать, что это заявление не соответствует действительности. Если бы пресса была честной, хотя она таковой не является, я бы совсем не пользовался Twitter», – сказал он.

***

18.01.2017

«Батьківщина» закликає долучитись до флешмобу «United Ukraine»

Депутати «Батьківщини» долучились до міжнародного флешмобу «United Ukraine» до Дня Соборності України.

Як повідомив 18 січня під час брифінгу в парламенті член фракції І. Крулько, мета заходу – привернути увагу світу до ситуації на Донбасі, анексованого Криму, до потреби припинення агресії та гібридної війни, яку РФ здійснює в Україні.

Депутати «Батьківщини» також закликали всіх українців і друзів нашої країни з усього світу приєднатися до акції та продемонструвати свою позицію та прагнення до відновлення територіальної цілісності України та контролю нею своїх державних кордонів.

За словами парламентаря, цей флешмоб проводиться вже третій рік поспіль і він об’єднує українців усього світу.

Серед тих, хто доєднався до флешмобу, – європарламентарі, конгресмени США, дипломати, депутати Канади та інших світових парламентів, представники найбільш впливових неурядових організації, лідери найбільших українських церков і конфесій.

За даними координатора акції, заступника голови «Батьківщина молода» О. Захарченка, за сім днів до акції долучилось понад 3 тис. учасників із 25 країн світу. Серед них – губернатор штату Огайо Дж. Кейсік, конгресвумен М. Каптур, депутати європарламенту тощо. До того ж акцію благословив Л. Гузар.

***

18.01.2017

Мешканці Дніпра міряються у соцмережах рахунками за тепло

У Дніпрі мешканці міста жваво обговорюють у соцмережах рахунки за теплопостачання. Про це Depo.Дніпро стало відомо з постів у Facebook (Depo.ua).

«Прийшов рахунок за тепло в грудні за двушку (58 квадратів) – 1500 грн (за лічильником). А скільки ж тоді без лічильника? Ще потрібно заплатити за світло, воду, газ, квартплату», – повідомляє автор посту.

У коментарях городяни пишуть, що на «Червоному Камені» за квартиру у 80 кв. м заплатили 1200 грн, а за квартиру 65 кв. м – 1600 грн, і здивовані такою різницею.

В інших районах різниця теж велика – 650 грн за 45 кв. м і майже така сама площа в елітному домі з котельнею на даху – 1580 грн.

У деяких мешканців Дніпра, у яких стоїть лічильник у квартирі, обігрівання площі у 112 кв. м обійшлося у 504 грн.

На «Лівобережному» за опалення у нежитловому будинку 38,6 кв. м власнику довелося викласти 2900 грн.

Хоча в лівобережній частині міста є й ті, хто за квартиру площею 35 кв. м виклав лише 272 грн.

***

18.01.2017

Хмельницький обласний художній музей долучився до міжнародного флешмобу музейних селфі

Фото з Моною Лізою, Шекспіром та «Дівчиною з перлинною сережкою». 18 січня – флешмоб музейних селфі. Україна бере в ньому участь уже третій рік поспіль. Долучились й подільські мистецькі заклади (Хмельницька ОДТРК «Поділля-центр»).

Хмельницький обласний художній музей у міжнародній акції участь бере вже вдруге. Його співробітники зізнаються: у такий спосіб популяризують свій заклад.

М. Фролова – завідувач науково-експозиційного відділу Хмельницького обласного художнього музею:

– Вирішили долучитися з метою популяризації українського мистецтва. Нам є що представити. І є чим пишатися. Тому думаю, що кожному відвідувачу буде цікаво сфотографуватися на фоні улюбленого експонату. До того ж сьогодні, у день акції, вхід до музею є вільним.

Підтримують таку акцію й відвідувачі музею.

Аби приєднатися до флешмобу потрібно прийти до музею, обрати експонат, який сподобався, та зробити селфі на його фоні. Після цього

завантажити світлину до соціальної мережі з відповідним хештегом: #MuseumSelfie та #ХОХМ. Саме там представники художнього музею будуть відслідковувати ваші світлини. У музеї функціонує п’ять виставкових зал. І у будь-якій з них можна зробити селфі з експонатом. Проте є лише одне обмеження – фотографуватися без спалаху, бо це шкодить експонатам. До того ж, за селфі у музеї можна отримати подарунок.

М. Фролова:

– Буде обрана найцікавіша світлина. І автору презентуємо невеличний музейний подарунок.

Крім Хмельницького обласного художнього музею участь у флеш-мобі беруть ще два подільські заклади: обласний краєзнавчий музей та Кам’янець-Подільський державний історичний музей-заповідник.

***

19.01.2017

Штутман ініціював флешмоб #MadeInUkraine

Голова наглядових рад ПрАТ «Гідросила ГРУП» та ПрАТ «Ельворті ГРУП» П. Штутман ініціював флешмоб #MadeInUkraine, яким закликає підтримати українське виробництво. Про це він написав на своїй сторінці у Facebook (Кіровоградська правда).

«Україна і українці варті більшого! Розвиток промисловості – найефективніший, якщо не єдиний шлях до добробуту народу і величі держави. Підтримай флешмоб #MadeInUkraine!», – написав П. Штутман.

Шоб долучитися до флешмобу, необхідно зфотографуватися з якимось товаром українського виробництва та опублікувати фото на своїй сторінці у Facebook з хештегом #MadeInUkraine.

***

23.01.2017

У соціальних мережах запустили новий флешмоб на підтримку учасників АТО

Українці масово віджимаються. У соціальних мережах запустили новий флешмоб на підтримку учасників АТО, які повертаються з війни з посттравматичним синдромом (Новини Закарпаття).

Дедалі більше набирає обертів флешмоб #22PushupChallenge. Аби підтримати воїнів, які повертаються з АТО та нерідко зазнають психологічних травм, українці віджимаються 22 рази.

Ця цифра фігурує неспроста. Акція надійшла до України із США, де, за підрахунком департаменту в справах ветеранів, протягом 2014 р. 22 ветерани щоденно вчиняли самогубство.

***

18.01.2017

Карина Лукьяненко

«Культурный фронт Николаевщины» поучаствовал во флешмобе инициированный губернатором Савченко

Николаевский колледж культуры и искусств принял участие во флешмобе #22PushupChallenge, который был инициирован на Николаевщине губернатором А. Савченко (Новости N).

Видео с флешмоба у себя на странице выложил директор колледжа культуры и искусств С. Мыцик, который назвал учебное заведение «Культурным фронтом Николаевщины».

Отжимались студенты и преподаватели во главе с ректором прямо перед колледжем и в один голос считали количество отжиманий, а именно 22 раза.

***

30.01.2017

Львовский мусор появился в Twitter

Львовские остряки создали аккаунт «львовскому мусору», об этом пишет сайт Львів Сьогодні со сылкой на inform-ua (НОВИНИ МІСТА ЛЕВА).

На странице размещены сообщения о невывозе кучи мусора с культурной столицы, фото мусора, свалок, из которых вываливаются отходы.

На основе экологической проблемы, люди создали такой аккаунт, чтобы хоть немного абстрагироваться от катастрофы.

Поскольку туризм и ИТ являются приоритетами во Львове, сейчас городской совет рассматривает два пути: мусорный туризм и диджитализация мусора – пишут в Twitter.

Пользователи также шутят, что во Львове решили создать мусорную полицию, которая будет следить за сортировкой отходов.

БІЗНЕС І СОЦІАЛЬНІ МЕРЕЖІ

***

18.01.2017

Facebook запускает стартап-инкубатор в Париже

Facebook планирует открыть в париже весной 2017 г. свой первый стартап-инкубатор, получивший название Startup garage, заявила исполнительный директор Facebook Ш. Сэндберг (ReklaMaster.com).

Facebook откроет свой инкубатор в кампусе Station F, который должен начать работу в апреле 2017 г. на месте бывшей железнодорожной станции. Помещение площадью 34 тыс. кв. м рассчитано на три тысячи рабочих мест.

Ш. Сэндберг заявила, что компания намерена организовать для участников программы 80 рабочих мест и каждые полгода работать с 10-15 стартапами. Facebook планирует проводить с участниками инкубатора семинары и практические занятия на тему дизайна, пользовательского опыта, маркетинга, техподдержки и т. д.

Компания уже принимает заявки на участие в инкубаторе через страницу проекта в социальной сети. В Facebook заверили, что не намерены претендовать на доли в проектах участников программы и на их интеллектуальную собственность.

В Facebook планируют вложить в программу «миллионы евро в течение нескольких лет». Помимо соцсети с проектом Station F будут сотрудничать французские и международные венчурные фирмы, организаторы бизнес-инкубаторов и высокотехнологичные компании.

«Мы рады поддержать новое поколение французских стартапов с огромным потенциалом для роста экономики и создания рабочих мест», – заявила Ш. Сэндберг.

Комментируя сотрудничество с Facebook, глава Station F Р. Варза (Roxanne Varza) назвала соцсеть «вдохновляющим примером для предпринимателей со всего мира», а бизнес компании – «отличной моделью для тысячи молодых стартапов».

Инвестором Station F выступает французский техномиллиардер К. Ниль. Вложения в проект составляют 250 млн евро. Помимо основного пространства для бизнес-инкубаторов план проекта предусматривает создание конференц-залов, кафе, бара и кухонной зоны. Стартапы смогут воспользоваться услугами кампуса за 195 евро в месяц.

Организаторы Station F также намерены перестроить два соседних здания, организовав в них корпуса для проживания 600 человек, пишет VentureBeat.

***

18.01.2017

Мартин Соррелл: Snapchat становится третьей силой после Google и Facebook

Клиенты WPP потратили 90 млн долл. на Snapchat в прошлом году, по словам главы сети. Прогноз холдинга составлял 30 млн долл. В сентябре eMarketer спрогнозировал, что Snapchat, которая недавно объединила продукты под зонтиком родительской компании Snap Inc, сгенерировала 366,69 млн долл. рекламных доходов за 2016 г., а к 2017 г. эта цифра приблизится к 1 млрд долл. По словам главы WPP, расходы брендов на Snapchat все еще малы по сравнению с 5 млрд и 1,7 млрд долл., потраченными на Google и Facebook.

Однако он считает, что Snapchat может представлять риск для Facebook, и даже называет его «угрожающей альтернативой». «Это большая возможность для них, – отметил М. Соррелл CNBC. – Мы знаем, что владельцы Facebook несколько раз пытались купить Snapchat и выпустили продукты, аналогичные продуктам приложения. Я думаю, в Facebook обеспокоены потенциальной оппозицией». По данным eMarketer, 95 % доходов Snap получает из США, но к 2018 г. четверть его доходов будет приходить из других регионов. Компания недавно инвестировала в другие страны, включая и Великобританию, где открыла офис (Marketing Media Review).

***

18.01.2017

Контент-план для Facebook на 2017: топ-советы от эксперта по маркетингу

М. Смит, эксперт по маркетингу в Facebook, спикер и автор, поделилась контент-планом для социальной сети на 2017 г. Среди ключевых рекомендаций (Marketing Media Review):

– создавайте видео и фотоконтент, которым пользователи захотят делиться;

– усиливайте охват некоторых постов платным промо;

– используйте следующий метод для усиления поста: вначале позвольте нарасти органическому охвату в течение 24 часов, затем поддержите пост платно. Подождите еще 24 часа для роста охвата и затем добавьте немного денег для увеличения промо поста;

– используйте кнопки призыва к действию и ссылки;

– используйте сервис видеостриминга Facebook Live;

– тестируйте раздачу призов со своей аудиторией;

– размещайте посты пять раз в неделю, экспериментируйте с постами в нерабочее время;

– увеличьте количество видеопостов;

– используйте ретаргетинг вовлеченной аудитории, исходя из просмотров видео, взаимодействия со страницей, аналогичной аудитории;

– фокусируйтесь на образовании и, где возможно, развлечении вашей аудитории.

***

23.01.2017

YouTube будет использовать данные аккаунта Google для таргетинга

Клиенты YouTube смогут использовать демографические данные и информацию о поисковом поведении авторизированных пользователей Google. Кроме того, компания расширила возможности использования таргетинга Customer Match на YouTube. Так, рекламодателям предоставлена возможность

нацелить показ рекламы на тех пользователей, которые подписались на рассылку об акциях на их ресурсах. Более того, если пользователь отключит показ рекламы от конкретного рекламодателя в поиске Google, то она автоматически заблокируется для него и на YouTube (Marketing Media Review).

***

24.01.2017

WOG запускает бота в Telegram и Facebook Messenger

Компания WOG выпустила бота для пользователей мессенджеров Telegram и Facebook Messenger (ITnews).

Сейчас основные функции виртуального помощника WOG BOT – это: поиск ближайшего АЗК, информирование о ценах на топливо, а также содействие в работе с картой PRIDE и системой лояльности. А еще с помощью бота пользователи могут приобрести топливо или кофе заранее, что сэкономит их время на кассе.

Сейчас бот представлен в бета-версии и в большей мере являет собой справочник, помогающий клиентам WOG быстро сориентироваться в часто задаваемых вопросах. Глава диджитал отдела WOG Д. Демидов говорит: «Появление WOG BOT – оптимизация коммуникации между клиентом и WOG. По многим позициям пользователю уже нет необходимости звонить на горячую линию или писать в службу поддержки – бот решает часть задач».

«Когда появится расширенная версия WOG BOT и будут ли у него новые функции – зависит от пользователей, от их реакции – комментариев и запросов в компании охотно ждут», – поясняет Д. Демидов. Тем не менее в ближайшее время компания планирует выпустить WOG BOT еще и для пользователей Viber и Skype.

Чтобы установить помощника WOG BOT, пользователю необходимо в выбранном мессенджере в строке поиска ввести @wogpridebot. Далее будет предложен выбор языка и меню задач.

WOG стала первой среди топливных компаний, кто запустил виртуального помощника. Компания не боится экспериментировать с инновациями и продолжает активно предлагать клиентам интересные, полезные и удобные ИТ-решения.

***

26.01.2017

«ПриватБанк» представил бота для оформления рассрочки через Facebook

Клиенты «ПриватБанка» могут оформлять рассрочку через Facebook с помощью бота @payparts. Об этом сообщает представитель пресс-службы «ПриватБанка» И. Музычук на своей странице в Facebook (Минфин).

С помощью бота пользователи соцсети могут оформить желаемую сумму в кредит, а также найти товары, на которые действует программа беспроцентной рассрочки «Оплата частями».

«Рассрочку на оплату любых покупок теперь можно оформить за минуту без бумаг и необходимости посещать отделение банка», – заявил руководитель бизнеса по работе с торговыми предприятиями «ПриватБанка» Е. Васильцов.

Новый сервис доступен всем владельцам платежных карт «ПриватБанка». Для использования бота необходимо перейти по следующей ссылке или набрать в поиске @payparts.

Бот также позволяет клиентам банка узнать доступный лимит использования сервисов рассрочки «Оплата частями» и «Мгновенная рассрочка», получать новости о выгодных предложениях торговых сетей.

Чтобы получить желаемую сумму в кредит, необходимо указать свой финансовый номер телефона, подтвердить через СМС-пароль, далее ввести сумму и последние 4 цифры номера карты, на которую будут зачисляться деньги.

***

26.01.2017

В мессенджере от Facebook заработала реклама

Социальная сеть Facebook запустила на просторах мобильного приложения Messenger возможность размещения рекламы. Пока эта функция доступна в тестовом режиме, информирует онлайн-портал Techcrunch (Grifonsoft).

Согласно данным от источников, первыми рекламу в мессенджере от Facebook смогут протестировать жители Австралии, а также Таиланда. Объявления, размещенные на просторах приложения, моментально отражаются на экране в виде ссылки, сопровождаемой картинкой. Кликнув на адрес пользователи Facebook получат возможность увидеть подробную информацию о предложении, при этом разработчик уверяет, что реклама не будет «выпрыгивать» во время обмена сообщениями до тех пор, пока человек сам не кликнет на объявление.

***

26.01.2017

Вице-президент Xiaomi возглавит разработку технологии виртуальной реальности в Facebook

Вице-президент Xiaomi возглавит разработку технологии виртуальной реальности в Facebook. Информациию подтвердил не только сам Х. Барра, но и основатель и глава соцсети М. Цукерберг (Хроника.инфо).

Вице-президент по международному развитию китайской Xiaomi Х. Барра перешел на пост руководителям VR-подразделения Facebook. Он будет

отвечать за все VR-проекты Facebook, включая разработку шлема виртуальной реальности Oculus. По словам М. Цукерберга, Х. Барра разделяет его уверенность в том, что виртуальная и дополненная реальность станет одной из крупнейших отраслей в будущем.

Во время работы в Xiaomi Х. Барра помог компании выпустить ее собственную VR-гарнитуру Mi VR. «Работа над VR была моей мечтой еще тогда, когда это было научной фантастикой», – сказал Х. Барра.

***

30.01.2017

Топ-10 избитых маркетологами слов в CV и профилях, по версии LinkedIn

Социальная сеть для профессионалов решила помочь специалистам в сфере маркетинга внести необходимые изменения в профили, чтобы не звучать шаблонно. Компания просмотрела профили 31 000 британских маркетологов и выявила слова, наиболее часто используемые в отрасли. Среди них: стратегический, креативный, специализированный, лидерство, страстный, опытный, сфокусированный, увлеченный, эксперт, достижения. С. Блейкмен, директор глобальных аккаунтов в OMD, отметил: «Если я читаю профиль, где присутствует более рациональный выбор позитивных профессиональных прилагательных (к примеру, квалифицированный, скрупулезный и оптимистичный), я склонен сделать вывод, что о кандидатах стоит говорить» (Marketing Media Review).

СОЦІАЛЬНІ МЕРЕЖІ І ПРОБЛЕМИ СУСПІЛЬНОЇ БЕЗПЕКИ

Інформаційно-психологічний вплив мережевого спілкування на особистість

***

18.01.2017

Американку уволили из школы за троллинг учащихся

Работницу SMM-службы окружного департамента образования штата Мэриленд К. Нэш (Katie Nash) уволили за троллинг учащихся в Twitter. Об этом сообщает The New York Post (InternetUA).

Как утверждается в материале издания, 5 января один из учеников обратился к администрации местной школы через Twitter и попросил закрыть

учебное заведение на завтрашний день. В своем обращении школьник допустил ошибку и написал слово завтра (tomorrow) с двумя буквами «а» (tammarow). На это обратила внимание 33-летняя К. Нэш, которая решила подшутить над неграмотностью ребенка от лица школы и задала ироничный вопрос: «Но как вы тогда узнаете, как пишется слово “завтра”?».

Ее ответ собрал более тысячи ретвитов и лайков. К. Нэш даже обзавелась собственным хэштегом #KatiefromFCPS и принялась «исправлять» посты учащихся.

После нескольких подобных инцидентов, администрация попросила работницу SMM-службы перестать троллить детей в Twitter. Но это не оказало никакого влияния на К. Нэш, и она продолжила общаться с учащимися с профиля школы. В итоге женщина получила письмо, в котором сообщалось, что ее контракт аннулирован.

Сама К. Нэш призналась, что действительно игнорировала настойчивые рекомендации администрации учебного заведения. «Любой специалист SMM ищет способы повышения вовлеченности аудитории. Я считаю, что беседа о том, как мы взаимодействуем с учащимися, была бы совершенно уместна. Я бы только приветствовала это», – отметила она.

***

22.01.2017

Ученые изучат мемы и смайлики для создания психологических портретов

Британские социологи решили изучить некоторые феномены современного Интернета – смайлики, так называемые эмодзи, мемы и иные средства невербальной коммуникации в сети, чтобы научиться выявлять определенные черты характера авторов сообщений. По словам ученых, смайлы могут работать так же, как и, например, жесты в реальном разговоре (InternetUA).

«Характерные особенности того, как мы жестикулируем в реальном мире, часто связаны с особенностями нашего характера, и смайлы, как мы считаем, работают схожим образом, о чем говорят различия в том, как и почему мы их используем», – пояснили авторы исследований.

Первые смайлы, как сегодня считают историки, появились более 30 лет назад. Сегодня смайлами, эмодзи и мемами осознанно пользуется примерно 90 % пользователей сети, многие употребляет их, не понимая, о чем идет речь.

Плюсом для ученых является то, что в Интернете все разговоры и диалоги записываются. Благодаря этому социологи и психологи, при содействии владельцев соцсетей и поисковых систем, могут получить доступ к практически огромному массиву данных о поведении людей, не подозревающих, что за ними наблюдают.

***

23.01.2017

Ученые выяснили, что Facebook для человеческого мозга сродни кокаину

Норвежские ученые пришли к выводу, что Facebook оказывает на мозг человека влияние сродни тому, что и употребление кокаина. Как выяснили журналисты «Фразы», в ходе исследования у добровольцев при постоянном просмотре ленты новостей нарушались функции нервной системы (UKR-TODAY.com).

Как сообщает Head Insider, в исследовании медиков из Бергенского университета приняло участие 20 добровольцев. Научные сотрудники фиксировали реакцию студентов на визуальные раздражители, которые связаны с активностью в соцсети Facebook.

Оказалось, что постоянный просмотр новостной ленты оказывает наркотическое воздействие на нервную систему человека. Исследователи утверждают, что респонденты показывали высокую скорость реакции на появляющиеся образы в социальной сети, имели склонность к развитию зависимости от этого интернет-ресурса.

Изображения из новостной ленты вызывали активизацию миндалевидного и полосатого тела. Любопытно, что такое же воздействие на человеческий организм оказывает кокаин. Ученые объяснили, что зависимых людей отличают высокая возбудимость на объекты. В данном случае, такую реакцию вызывала активность в соцсети.

Также у добровольцев нарушалась функции нервной системы. Медики считают, что результаты их исследований станут основой для формирования методики лечения от подобной зависимости от соцсетей.

***

26.01.2017

Исчезновение на 24 часа: новый опасный флешмоб среди подростков

В Украине набирает обороты новый челлендж среди подростков «Исчезновение на 24 часа». Главная суть этого действа – подросток должен уйти из дома, никого не предупредив, а вернуться домой может только через сутки (From-UA. Новости Украины).

Об этом сообщает днепрянка Т. Лупова на своей странице в Facebook.

– Оказывается, флешмоб «Исчезновение на 24 часа» не такая уж и шутка. Инициативные группы, которые занимались поиском пропавшей девочки в Днепре, предупреждают, что «Исчезновение на 24 часа» набирает популярность среди подростков. Это экстремальное развлечение распространяется через соцсети. Суть заключается в том, что подросток должен уйти из дома и не объявляться в течение суток.

Первые случаи пропажи детей были зарегистрированы в Киевской области. Там, с разницей в три дня, «исчезли» двое мальчиков. Через сутки

после случившегося и одного, и второго нашли. Ничего криминального с ними не произошло.

Проследить, где скрывается несовершеннолетний практически невозможно, а также очень сложно выяснить, действительно ли подросток пропал, либо так играется. Специалисты настоятельно советуют родителям поговорить с подрастающими детьми и объяснить всю опасность такой забавы. Другого способа борьбы с модным экстремальным развлечением несовершеннолетних пока не придумали, – предупреждают правоохранители, – пишет обеспокоенная днепрянка.

Маніпулятивні технології

***

24.01.2017
У Twitter виявили багатотисячні мережі ботів

Британські дослідники виявили, що у соціальній мережі Twitter існують величезні мережі фейкових акаунтів. Про це повідомляє BBC.

Найбільша така мережа нараховує 350 тис. профілів, проте дослідники припускають, що можуть існувати й більші мережі.

Їх виявили випадково – науковці кажуть, що хотіли лиш порахувати, скільки насправді людей користуються Twitter.

Боти у Twitter – це акаунти, керовані віддалено, у яких налаштоване автоматичне публікування повідомлень та інша активність. Деякі такі профілі використовують, щоб «накручувати» кількість підписників-фоловерів, надсилати спам іншим користувачам чи штучно підсилювати інтерес до деяких тем.

«Важко оцінити, скільки точно акаунтів у Twitter-боти», – каже студент магістратури Університетського коледжу Лондона Х. Ечеверрія, який і виявив мережі фейків.

Для дослідження він вирішив проаналізувати діяльність 1 % користувачів Twitter, аби краще зрозуміти, як люди користуються цією соцмережею. Проте його розрахунки місцями дали дивні результати, і придивившись детальніше, він виявив багато пов’язаних між собою профілів і припустив, що одна людина чи група людей може керувати ними всіма.

Ці акаунти не діяли як звичайні Twitter-боти, тому не потрапляли у об’єктив інших дослідників, проте було очевидно, що за ними стоять аж ніяк не живі люди.

Наприклад, акаунти із 350-тисячної мережі виділилися як фейкові й пов’язані між собою за рядом підозрілих ознак.

По-перше, твіти в усіх них надсилалися із місць, де ніхто не живе, по-друге, усі вони були надіслані із Windows-телефонів, і по-третє, за контентом твіти майже повністю складалися з цитат із «Зоряних воєн».

Важко встановити, хто стоїть за цими мережами фейків, хоч є свідчення, що невеликий відсоток цих акаунтів продається чи береться в оренду, оскільки вони не приєднують користувачів Twitter за межами цих бот-мереж.

У Twitter, у свою чергу, заявили, що соцмережа має доволі чітку політику щодо автоматизації профілів: користувачам заборонено використовувати додаткові програми, що автоматично фоловлять чи анфоловлять інші акаунти, надсилають повідомлення чи відповідають на дописи.

«Водночас, як ми маємо системи за засоби для виявлення спаму у Twitter, ми також покладаємося на користувачів у тому, що вони повідомлятимуть нам про спам», – заявили у Twitter.

***

19.01.2017
Facebook заблокував відео Russia Today

Facebook тимчасово заблокував російському пропагандистському телеканалу RT публікувати на його англомовній сторінці повідомлення, які містять посилання, відео та картинки.

Про це повідомляється на сайті телеканалу (ESPRESO.TV).

«Заборона з'явилася після трансляції прес-конференції президента США Б. Обами. Припускається, що Facebook помилково визначив, що у RT відсутні права на трансляцію», – йдеться в повідомленні.

Обмеження діятиме до 10:25 за московським часом 21 січня. Таким чином, воно поширюється на час інавгурації президента США Д. Трампа, яка завершитися 20 січня.

***

20.01.2017
Ирина Евсюкова
В Германии молодежь вербуют в ИГИЛ с помощью соцсетей

Террористическая группировка «Исламское государств» вербует недовольных жизнью молодых людей в Германии по средствам социальных сетей и мессенджеров, используя для этого специальных «охотников за головами», заявил глава Федерального ведомства по охране конституции Х.-Г. Маасен (podrobnosti.ua).

Отдельным их жертвам едва исполнилось 13-14 лет, передает DW.

Такие хедхантеры, по словам главы ведоства, «общаются с молодежью и привлекают ее исламистской идеологией».

Х.-Г. Маассен провел исторические параллели между деятельностью пропагандистов ИГ и агитацией коммунистов или национал-социалистов под

предводительством А. Гитлера. Около 20 % из 900 завербованных ИГ в Германии лиц, которые отправились воевать за исламистов в Сирию и Ирак, – женщины, отметил глава спецслужбы.

Глава контрразведки также отверг критику в адрес спецслужб относительно берлинского террориста А. Амри. По словам Х.-Г. Маасена, ведомства безопасности были хорошо знакомы с А. Амри и следили за ним, но не смогли взять под стражу.

Он также отметил, что в Европе сейчас радикализируется немало «порядочных граждан» – через общение в закрытых сообществах в Интернете взгляды людей со схожими убеждениями взаимно усиливаются в сторону готовности к насилию.

Х.-Г. Маасен добавил, что правоохранители следят за деятельностью 548 исламистов, которые составляют потенциальную угрозу, однако по закону они не могут арестовать их до совершения преступления.

***

24.01.2017

СБУ розібралась з поширенням у мережі відео «руського міра» з Кропивницького

Силові структури попередили про поширення відео, знятого біля джерела Св. Даниїла на Водохреще, яке дискредитує кропивничан. Про це повідомляє Златопіль з посиланням на Depo.Кропивницький (InternetUA).

Розсилка в соцмережах «Прощанія славянки» від жителів Кропивницького, які святкують Водохреща біля джерела Св. Даниїла, виявилась фейковою. Зловмисники представили все так, ніби кропивничани діляться «ностальгійною мелодією» одне з одним.

СБУ вже встановила джерело розсилки.

«Любов виявилася штучною, а проросійські флешмоби – фейковими. Ми встановили і організаторів цих антиукраїнських акцій, і слухняних виконавців. З цими особами вже проведено профілактичні бесіди. Ми – не проти різних пісень, але знаємо точно – і у Кропивницькому, і по всій Україні, сьогодні люди замовляють іншу музику», – повідомила речник СБУ.

***

23.01.2017

Фейки помогут качественной журналистике усилить свои позиции: Reuters Institute Бизнес

Reuters Institute выпустил новое исследование с перечнем трендов и прогнозов развития журналистики, медиа и технологий в текущем году, сообщает MMR (Телекритика).

Аналитики прогнозируют, что, президентство Д. Трампа и выборы во Франции и Германии укажут на усиливающееся влияние новых каналов

коммуникации, в то время как традиционные медиа продолжат терять влияние и деньги. Кроме того, в мире назреют дебаты о роли и масштабах технологических платформ и регуляции их активностей.

Фейковые новости стали главной темой в последнее время, и большинство медиаменеджеров считают, что они благоприятны для бизнеса. По данным опроса Reuters Institute, в котором приняли участие 145 руководителей изданий, редакторов и digital-лидеров в 24 странах, 24 % считают, что их позиция будет «усилена» желанием потребителей получать точные и заслуживающие доверия новости. Большинство же респондентов видят в росте количества фейковых новостей «шанс для выхода на первый план качественной журналистики».

17 % опрошенных считают, что фейковые новости ослабят позицию новостных медиа, 8 % высказались за то, что они никак не повлияют на положение вещей, а 5 % затруднились с ответом.

Также в отчете прогнозируется «взрыв» числа фактчекинговых сервисов, тем более, что Facebook и Google уже инвестируют в них. А в BBC собрали новую команду для проверки новостей, которые расшариваются в сетях.

Кроме того, 56 % опрошенных отметили, что Facebook Messenger станет важной частью их инициатив в этом году, 53 % высказались о том же в отношении WhatsApp, а 49% проголосовали за Snapchat.

***

24.01.2017

Політики платять за те, щоб Google пам’ятав про них тільки хороше

Почати життя з чистого аркуша тепер можливо. Ця опція нині дуже популярна серед політиків, які наймають спеціальні фірми, що замітають їхні сліди в Інтернеті. Послуги, щоправда, не з дешевих – від 5 тис. дол. на місяць, але політтехнологи впевнені: вони дуже ефективні (Інтернет-видання «Паралелі»).

«Зараз з’явилося дуже багато фірм, що надають послуги з чищення інформації про політиків в Інтернеті в цілому, і в соцмережах зокрема, – розповідає доцент кафедри реклами та зв’язків з громадськістю КНУ М. Калина. – Існують і так звані чорні тролі. Вони публікують негатив, а після цього приступають до роботи білі тролі, які перебивають негатив позитивними відгуками і новинами. При цьому в штабах на випадок форс-мажорів працюють цілі спецгрупи із зачистки негативної інформації».

«Як правило, до нас звертаються перед призначенням на нову посаду. В основному просять прибрати згадки в Інтернеті про корупційні скандали, якщо були такі публікації. І друге за популярністю прохання – видалити згадки про небажаних друзів, з якими не хочуть, щоб їх пов’язували», – розповів нам керівник агентства з управління онлайн-репутацією SERM Г. Маленко.

Технологія така: у топи виводять сторінки новинних сайтів з позитивною інформацією про політика або чиновника, а негатив ховають подалі. Гортаєш

пошуковик з прізвищем кандидата – і здається, що він просто ідеал. Google пам'ятає все. Але ми робимо так, що небажана інформація в пошукових системах шукається в рази гірше. Наприклад, в «Яндексі» і Google весь негатив йде на третю сторінку і далі, а перші дві заповнені виключно позитивною інформацією про нашого клієнта. Ця робота триває не менше трьох місяців, коштує – від 5 тис. дол. на місяць», – уточнив Г. Маленко.

Неофіційно експерти кажуть, що взагалі прибрати з деяких сайтів негативну інформацію про замовника коштує від 1 тис. дол. до кількох десятків тисяч доларів. Мовляв, усе залежить від постаті замовника: великий політик, бізнесмен – буде платити дорожче.

За словами Г. Маленка, в інформаційному полі негативна інформація про людину підхоплюється за хвилини і поширюється з величезною швидкістю. «Тоді працюємо оперативно, з'ясовуємо, чи не підключилися чи до роботи тролі і репутаційні терористи, які спеціалізуються на усуненні "замовлених" кимось політиків, і швидко перебиваємо чорний піар позитивом», – зазначив Г. Маленко.

***

24.01.2017

ЄС виділяє додатково 800 тис. євро на боротьбу з пропагандою в Європі

Євросоюз виділяє додаткові 800 тис. євро оперативній робочій групі зі стратегічних комунікацій East StratCom Task Force для протидії спробам Росії вплинути шляхом дезінформації і пропаганди на вибори в Європі. Про це повідомляє The Guardian (LB.ua).

За даними видання, ЄС активізує свої зусилля в протидії кампанії гібридної війни на хвилі перемоги Д. Трампа, оскільки є побоювання, що президент РФ В. Путін спробує вплинути на вибори по всій Європі.

Як наголошують, протягом найближчих місяців відбудуться вибори в Німеччині, у Франції та Нідерландах, тому ЄС і прийняв рішення про надання додаткових коштів у розмірі близько 800 тис. євро. Гроші будуть витрачені протягом найближчих шести місяців і йдуть із поточного бюджету Служби зовнішньої дії ЄС.

«Члени Європарламенту визнають, що є побоювання, що очевидний вплив Росії на недавні вибори в США тільки заохотить здійснювати такі кампанії на континенті», – зазначає видання.

Зарубіжні спецслужби і технології «соціального контролю»

***

17.01.2017

У Росії хочуть відслідковувати кількість згадок в Інтернеті про своїх чиновників // За відмову обіцяють карати розірванням службового контракту

Міністерство праці Росії готує інструкцію для чиновників, яким доведеться звітувати про діяльність в Інтернеті («Главком»).

Про це повідомляє радіо «Ехо Москви» з посиланням на газету «Комерсант».

Такий обов'язок з'явилася у державних і муніципальних службовців з цього року. До 1 квітня чиновники повинні заповнити форму про адреси сайтів або сторінок, на яких розміщувалася пов'язана з ними інформація. Відмова надати ці дані буде загрожувати розірванням службового контракту.

Ті, хто хочуть вступити на службу, повинні повідомити про свої дії в Інтернеті за останні три роки.

***

24.01.2017

У Росії готуються взяти під контроль онлайн-месенджери

Роскомнагляд і МВС Росії розробили законопроект про ідентифікацію користувачів текстових повідомлень на мобільних пристроях (Економічна правда).

Законопроект пропонує включити до закону «Про зв'язок» поняття «інформаційно-комунікаційні сервіси обміну миттєвими повідомленнями» і організатори поширення даних в Інтернеті повинні будуть надавати програмне забезпечення, що дає можливість ідентифікувати користувача.

Передбачається, що документ буде внесений до Держдуми разом з проектом, що передбачає регулювання сім-карт.

Відповідно до нового законопроекту, основною умовою роботи месенджерів в РФ повинна бути ідентифікація користувачів, для чого організатори зобов'язані укласти договори з операторами зв'язку. Крім того, месенджери на вимогу влади повинні обмежувати масову електронну розсилку, а також передачу повідомлень, які містять інформацію, що поширюється з порушенням законодавства.

Раніше президент Медиакоммуникационного союзу П. Степанов говорив, що мова йде про повідомлення, на отримання яких користувач месенджера не давав згоди і в яких містяться у першу чергу екстремістські заклики або реклама. Якщо ці вимоги не будуть виконуватися, влада буде домагатися блокування організаторів.

***

25.01.2017

У РФ заарештували топ-менеджера «Лабораторії Касперського»

Один з топ-менеджерів «Лабораторії Касперського», керівник відділу з розслідування кіберзлочинів Р. Стоянов був затриманий в кінці грудня минулого року у справі про державну зраду (Економічна правда).

Про це пише «Комерсант» з посиланням на джерело, близьке до Федеральної служби безпеки (ФСБ).

Зазначається, що до 2006 р. Р. Стоянов працював в управлінні спеціальних технічних заходів столичного ГУВС (так зване управління «К»).

Видання пише, що зараз Р. Стоянов перебуває в слідчому ізоляторі «Лефортово».

Як повідомив співрозмовник, його арешт може бути пов'язаний з розслідуванням справи щодо одного із заступників голови центру інформаційної безпеки ФСБ С. Михайлова.

Як пише видання, він підозрюється в порушенні ст. 275 Кримінального кодексу («Державна зрада»).

На думку слідства, С. Михайлов отримав гроші від однієї з іноземних компаній за посередництва співробітника російської фірми у сфері інформаційної безпеки.

На думку співрозмовників газети, справу стосовно С. Михайлова може відбитися на всьому ринку кібербезпеки і електронної комерції, так як саме Михайлов «по суті курирував весь інтернет-бізнес у Росії», – зазначає видання.

***

23.01.2017

Китай ужесточил контроль над VPN-сервисами

Правительство КНР намерено усилить контроль за деятельностью VPN-сервисов, позволяющих пользователям получить доступ к интернет-контенту в обход цензуры «Золотого щита», передает издание South China Morning Post со ссылкой на сообщение Министерства промышленности и информационных технологий Китая (InternetUA).

Согласно сообщению ведомства, в стране запущена программа по «очистке» китайского сегмента Сети, направленная на интернет-провайдеров, операторов дата-центров, а также сети доставки и распространения контента (Content Delivery Network, CDN). По новым правилам, начиная с 22 января 2017 г., все провайдеры, предоставляющие услуги виртуальных частных сетей, должны получать государственную лицензию. Кампания «по очистке» продлится до 31 марта 2018 г.

Как поясняют в Министерстве, китайский рынок доступа к услугам интернет-коммуникаций «демонстрирует признаки неупорядоченного развития и нуждается в срочном регулировании и управлении».

По данным общественной организации GreatFire, отслеживающей факты блокировки интернет-ресурсов на территории КНР, в стране запрещен доступ к 135 из 1000 мировых сайтов-лидеров по посещаемости, в том числе Facebook, Twitter и YouTube.

***

30.01.2017

Белый дом обсуждает возможность запрашивать аккаунты в соцсетях у въезжающих в США

В Белом доме обсуждается возможность запрашивать информацию о сайтах, которые посещают въезжающие в США лица, а также ссылки на их страницы в социальных сетях. Об этом сообщает CNN со ссылкой на источники в администрации президента США (InternetUA).

По их данным, об этом говорил советник Д. Трампа С. Миллер. Он также упоминал возможность требовать у иностранных гостей контакты их мобильных телефонов. Отмечается, что если они откажутся предоставить эту информацию, то им могут отказать во въезде в США.

Тем не менее, отмечают источники телеканала, обсуждения этого вопроса ведутся на предварительном этапе.

Проблема захисту даних. DDOS та вірусні атаки

***

17.01.2017

Кіберполіція порадила, як уникнути «сюрпризів» у соцмережах

Віртуальні контакти, а також використання інтернет-ресурсів, так само як і будь-які інші соціальні зв'язки і правовідносини в суспільстві, мають певний позитивний і негативний бік (Сумські Дебати).

Інтенсивний розвито інтернет-комунікацій, які значно спростили життя звичайним користувачам, сприяли не тільки задоволенню їх культурно-естетичних і побутових потреб, але і виникненню нових видів кібер-загроз. Мова йде про сітьові шахрайства, кіберхуліганства, про поширення негативного контенту. Домагання, грубі та цинічні висловлювання, шантаж та ін.

Тому дуже важливо вже сьогодні розповісти інтернет-користувачам, по-перше, про існування забороненого контенту, по-друге, про правила поведінки, що оберігають від небезпек, які таїть у собі віртуальне середовище, і, по-третє, про існування законодавчих приписів, що встановлюють заборону на протиправну поведінку в глобальній мережі.

Існують основні види віртуальних загроз, яких слід остерігатися:

– заборонений контент: порнографія, пропаганда екстремізму, алкоголю та наркотиків, нецензурні тексти;

– порушення безпеки: комп’ютерні віруси, троянські програми, спам (небажана пошта: листи щастя, пропаганда), онлайн-шахрайства (робота, інтернет-магазини, аукціони, телефонні афери тощо);

– незаконні контакти: погрози, сексуальні домагання, шантаж тощо.

Поліція наводить прості правила для інтернет-користувачів, які допоможуть звести до мінімуму віртуальні ризики.

Не слід розміщувати в Інтернеті персональну інформацію (номер мобільного телефону, домашню адресу та особисті фотографії (на яких ви, ваша сім’я або друзі)).

Не додавайте незнайомих (або малознайомих) людей у власному аккаунті соцмереж, а також до контакт листа в профілях ICQ, Skype, Viber та в ін. Пам’ятайте, що віртуальні знайомі можуть бути не тими, за кого себе видають.

Небажано відповідати на спам, до якого відносяться листи щастя, пропаганда, DoS і DDoS-атаки, масова розсилка від імені іншої особи (для того щоб викликати до неї негативне ставлення), масова розсилка листів, що містять комп’ютерні віруси (для їх початкового поширення). Приміром, розсилка листів щастя, яку начебто сплачує якийсь інтернет-провайдер, проводиться з метою збору e-mail адрес (вашого і ваших знайомих).

***

17.01.2017

Пользователям Facebook угрожает новая мошенническая кампания

По сети Facebook распространяется новая мошенническая кампания, направленная на сбор учетных данных пользователей. По данным ресурса Hackread, в рамках кампании злоумышленники рассылают сообщения с темой «You are in this Video?» («Вы на этом видео?») и просьбой перейти по указанной ссылке. Темы сообщений могут варьироваться (InternetUA).

Аттакующие эксплуатируют естественное желание пользователей перейти по ссылке в сообщении, якобы отправленном другом. Попавшиеся на удочку пользователи становятся жертвами фишинговой атаки, направленной на хищение учетных данных.

В вышеуказанной вредоносной кампании мошенники используют два сценария. В рамках первого, при переходе по ссылке жертва оказывается на поддельной странице авторизации, требующей ввода логина и пароля. В рамках второго сценария переход по ссылке ведет на сайты, инфицированные вредоносным ПО. Жертву просят скачать кодек, плагин, обновление или другое ПО для того, чтобы просмотреть видео. Однако на самом деле загружаемые программы являются ни чем иным как вредоносным ПО.

***

18.01.2017

Не стоит верить бесплатному Интернету от WhatsApp

Эксперты сообщают о массовом обмане пользователей WhatsApp, которым предлагается бесплатный интернет (iLenta.com).

Злоумышленники рассылают пользователям WhatsApp сообщения, в которых предлагают воспользоваться «революционной технологией», предоставляющей бесплатный Интернет.

Предлагаемый ими сервис не является открытой точкой Wi-Fi, а для подключения к нему, якобы, необходимо разослать это сообщение тринадцати друзьям.

После чего пользователям WhatsApp предлагается установить несколько приложений, которые и будут воровать личные данные и номера банковских карт.

***

19.01.2017

Уязвимость в Facebook позволяет узнать скрытые номера телефонов

Бельгийский исследователь Инти Де Кекелайре (Inti De Ceukelaire) утверждает, что выявил новый метод, позволяющий получить доступ к скрытым мобильным номерам пользователей Facebook, сообщает издание Computerworld (InternetUA).

Как заявил эксперт, он может легко идентифицировать номера телефонов известных лиц, в том числе политиков и знаменитостей, путем анализа номеров, связанных с профилем пользователя в Facebook. Стоит отметить, что эти номера относятся к конфиденциальной информации, которая не должна быть видима окружающим. Согласно изданию, при помощи обнаруженного метода Де Кекелайре удалось получить номер министра внутренних дел Бельгии Ж. Жамбона (Jan Jambon).

Эксперт уже дважды предупреждал о проблеме команду безопасности Facebook, однако, по мнению представителей компании, это не уязвимость, а функция. При этом Facebook сослалась на документацию, поясняющую как контролировать поиск пользователя по номеру мобильного телефона или адресу электронной почты. Тем не менее, исследователь утверждает, что эта ситуация – серьезная угроза конфиденциальности, поскольку речь идет о номерах, неразрешенных для просмотра широкой публики.

Проблема далеко не нова. О ней стало известно еще в 2012 г. С тех пор Facebook модифицировала настройки конфиденциальности, но, по всей видимости, не до конца устранила уязвимость. Де Кекелайре не предоставил подробности о том, как именно работает обнаруженный им метод, однако пообещал обнародовать информацию, если Facebook не исправит ситуацию.

***

18.01.2017

Уязвимость в Facebook Messenger позволяет похищать голосовые сообщения

Пользователи Facebook Messenger, предпочитающие аудиосообщения текстовым, рискуют стать жертвами атаки «человек посередине». Как сообщает издание The Hacker News, египетский исследователь Мохамед А. Басет (Mohamed A. Baset) обнаружил в мессенджере уязвимость, позволяющую похищать с сервера Facebook пересылаемые аудиофайлы и прослушивать голосовые сообщения пользователей (InternetUA).

При каждой записи голосовое сообщение сначала загружается на сервер CDN (https:// z-1-cdn.fbsbx.com/...), а уже оттуда по протоколу HTTPS передается как отправителю, так и получателю. Находящийся в той же сети злоумышленник может с помощью инструмента SSL Strip осуществить атаку «человек посередине» и получить абсолютные ссылки (в том числе встроенный в URL секретный токен для аутентификации) на все аудиофайлы, которыми обмениваются отправитель и получатель. Затем атакующий может изменить HTTPS на HTTP и загрузить файлы без аутентификации.

Атака возможна, поскольку сервер CDN не использует HSTS – механизм, активирующий форсированное защищенное соединение через протокол HTTPS. Кроме того, компания не позаботилась об обеспечении надлежащего процесса аутентификации. Пересылаемые между двумя пользователями файлы должны быть доступны только им двоим, даже если у кого-то третьего есть абсолютная ссылка на данные файлы с секретным токеном.

Исследователь уведомил Facebook об уязвимости, однако компания не спешит исправлять ее. Согласно полученному экспертом ответу, в настоящее время Facebook занимается развертыванием HSTS на своих поддоменах facebook.com.

***

17.01.2017

Facebook две недели пытался удалить вирусное видео самоубийства девочки

Facebook на протяжении двух недель не мог остановить распространение по соцсети ролика с самоубийством 12-летней Кейтилин Николь Дэвис (Katelyn Nicole Davis), транслировавшей свой суицид через платформу потокового видео Live.Me. Об этом пишет The Next Web (InternetUA).

Дэвис совершила суицид в конце декабря. Непосредственно перед самоубийством в онлайн-трансляции он заявила, что безуспешно боролась с депрессией, которая усугубилась, когда она подверглась сексуальному насилию со стороны одного из членов семьи. Последние 10 минут в прямом эфире транслировалось ее безжизненное тело. За онлайном одновременно следили тысячи людей из разных частей планеты.

Пугающий ролик просочился на YouTube и в социальные сети. Видеохостинг по требованию полиции оперативно удалил противоправный

контент. Facebook тоже заблокировал ролик, но разные версии записи расползлись по пабликам и частным страницам.

Видя, что запись продолжает распространяться по соцсети, пользователи начали обращаться в администрацию ресурса. Когда в Facebook написал новозеландский психотерапевт К. Макдональд (Kyle MacDonald), ему ответили, что видео не нарушает стандарты сообщества, писала The Guardian. Тогда же к соцсети обратилась окружная полиция округа Полк в Джорджии, заявив, что на них обрушился шквал звонков и писем от бдительных пользователей.

***

18.01.2017

Шахраї від імені футболістів просять грошей в соцмережах

Зловмисники замаскувалися під Циганкова, Зінченка та Борячука (InternetUA).

Півзахисник київського «Динамо» В. Циганков у своєму Instagram попросив уболівальників бути пильними – шахраї в соцмережах просять допомогти з грошима.

Виявляється, грошей просять не тільки від імені Циганкова. Подібні повідомлення надходять від гравця ПСВ О. Зінченка і футболіста «Шахтаря» А. Борячука.

У всіх одна історія: товариш застряг на трасі з маленькою дитиною. І просять 400 грн на бензин, нібито потім повернуть.

***

19.01.2017

«Доктор Веб» обнаружила троянец, который самостоятельно скачивает программы

Среди множества Android-троянцев широкое распространение получили вредоносные программы, которые незаметно загружают ПО на мобильные устройства (ITnews).

С их помощью злоумышленники получают вознаграждение за каждое успешное скачивание или установку того или иного приложения. Один из таких троянцев, которого обнаружили вирусные аналитики компании «Доктор Веб», внедряется в активный процесс программы Play Маркет и незаметно накручивает счетчик установок в каталоге Google Play.

Android.Skyfin.1.origin предположительно попадает на мобильные устройства благодаря некоторым троянцам семейства Android.DownLoader (например, Android.DownLoader.252.origin и Android.DownLoader.255.origin), которые после заражения смартфонов и планшетов пытаются получить root-доступ и скрытно устанавливают вредоносные программы в системный каталог. Код этих троянцев содержит характерные для Android.Skyfin.1.origin строки, поэтому с большой долей вероятности можно говорить о том, что

распространением Android.Skyfin.1.origin занимаются именно указанные вредоносные приложения.

При запуске Android.Skyfin.1.origin внедряет в процесс программы Play Маркет вспомогательный троянский модуль, получивший имя Android.Skyfin.2.origin. Он крадет уникальный идентификатор мобильного устройства и учетной записи его владельца, которые используются при работе с сервисами компании Google, различные внутренние коды авторизации для подключения к каталогу Google Play и другие конфиденциальные данные. Затем модуль передает эти сведения основному компоненту троянца Android.Skyfin.1.origin, после чего тот вместе с технической информацией об устройстве отправляет их на управляющий сервер.

Используя собранные данные, Android.Skyfin.1.origin подключается к каталогу Google Play и имитирует работу приложения Play Маркет. Троянец может выполнять следующие запросы:

/search – поиск в каталоге для симуляции последовательности действий пользователя;

/purchase – запрос на покупку программ;

/commitPurchase – подтверждение покупки;

/acceptTos – подтверждение согласия с условиями лицензионного соглашения;

/delivery – запрос ссылки для скачивания apk-файла из каталога;

/addReview /deleteReview /rateReview – добавление, удаление и оценка отзывов;

/log – подтверждение скачивания программы, которое используется для накручивания счетчика установок.

После скачивания заданного злоумышленниками приложения Android.Skyfin.1.origin не устанавливает его, а лишь сохраняет на карту памяти, поэтому пользователь не видит новые программы, возникшие из ниоткуда. В результате троянец увеличивает свои шансы остаться незамеченным и может продолжать накручивать счетчик установок, искусственно повышая популярность приложений в Google Play.

Вирусные аналитики компании «Доктор Веб» выявили несколько модификаций Android.Skyfin.1.origin. Одна из них умеет скачивать из каталога Google Play единственное приложение – com.op.blinkingcamera. Троянец имитирует нажатие на баннер Google AdMob с рекламой этой программы, загружает ее apk-файл и автоматически увеличивает число загрузок, подтверждая «установку» на сервере Google. Другая модификация Android.Skyfin.1.origin более универсальна. Она может скачивать любые приложения из каталога – для этого троянец получает от злоумышленников список программ для загрузки.

***

19.01.2017

«Доктор Веб» исследовал червя, заражающего архивы и удаляющего других троянцев

Вирусные аналитики компании «Доктор Веб» исследовали одного из троянцев, который инфицирует RAR-архивы, удаляет другие опасные приложения и использует для своего распространения систему удаленного доступа VNC. (ITnews).

Червь, названный BackDoor.Ragebot.45, получает команды с использованием протокола для обмена текстовыми сообщениями IRC (Internet Relay Chat). Для этого он подключается к чат-каналу, по которому злоумышленники отдают троянцу управляющие директивы.

Заразив компьютер под управлением Windows, BackDoor.Ragebot.45 запускает на нем FTP-сервер, посредством которого скачивает на атакуемый ПК свою копию. Затем он сканирует доступные подсети в поисках узлов с открытым портом 5900, используемым для организации соединения при помощи системы удаленного доступа к рабочему столу Virtual Network Computing (VNC). Обнаружив такую машину, BackDoor.Ragebot.45 пытается получить к ней несанкционированный доступ путем перебора паролей по словарю.

Если взлом удался, червь устанавливает с удаленным компьютером VNC-соединение и отправляет сигналы нажатия клавиш, с помощью которых запускает интерпретатор команд CMD и выполняет в нем код для загрузки по протоколу FTP собственной копии. Так червь распространяется автоматически.

Еще одна функция BackDoor.Ragebot.45 – поиск и заражение RAR-архивов на съемных носителях. Обнаружив RAR-архив, червь помещает в него свою копию с именем setup.exe, installer.exe, self-installer.exe или self-extractor.exe. Для успешного заражения компьютера пользователь должен сам запустить извлеченный из архива исполняемый файл.

Кроме того, троянец копирует себя в папку ICQ-клиента, а также ряда программ, предназначенных для установки P2P-соединений. Получив от злоумышленников соответствующую команду, BackDoor.Ragebot.45 ищет в системе других троянцев, при обнаружении которых завершает их процессы и удаляет исполняемые файлы. Троянец располагает специальными «белыми списками», содержащими имена файлов (в основном системных файлов Windows), которые он игнорирует, позволяя им работать на инфицированной машине.

Образцы одной из старых версий BackDoor.Ragebot.45 некоторое время назад попали в свободный доступ. Можно предположить, что благодаря этому вредоносная программа будет активно распространяться и в дальнейшем.

***

19.01.2017

Кількість кібератак на мережі НАТО зросла більш ніж удвічі, – Столтенберг

У 2016 р. щомісяця на мережі НАТО проводилося в середньому 500 хакерських атак, що на 60 % більше, ніж роком раніше (Західна інформаційна корпорація).

Про це в інтерв'ю газеті Die Welt заявив генсек альянсу Й. Столтенберг, пише DW.

Він вказав, що в середньому за місяць у 2016 р. налічувалося 500 небезпечних кібератак на натовські установи, які вимагали рішучих заходів з боку експертів. При цьому більшість цих атак здійснювалися не приватними особами, а фінансувалися державними інстанціями різних країн.

Кібератаки представляють дуже велику потенційну небезпеку, оскільки можуть порушити, наприклад, енергопостачання або медичне обслуговування або завдати шкоди іншим важливим інфраструктурам.

«Крім того, вони можуть нашкодити обороноздатності НАТО і вплинути на роботу наших збройних сил, – сказав Й. Столтенберг, пояснивши, що будь-яка військова діяльність базується сьогодні на передачі даних. – Якщо цей процес (передачі даних. – Ред.) порушується, то може бути завдано великої шкоди».

Тому, заявив генеральний секретар НАТО, в разі широкомасштабних кібернападів може бути задіяна ст. 5 статуту альянсу, що припускає допомогу всіх його членів постраждалій країні.

Є. Столтенберг висловив також стурбованість можливою маніпуляцією даними в ході виборчих кампаній.

«У НАТО надходять повідомлення від різних урядів країн-членів, які побоюються, що хакери будуть намагатися втрутитися в національну передвиборну боротьбу. У такому випадку кіберзлочинці будуть підривати демократію», – повідомив Й. Столтенберг.

За словами глави Північноатлантичного альянсу, з недавнього часу НАТО пропонує всім своїм членам допомогу кризових команд, які пояснюють, як можна поліпшити захист своїх мереж.

***

20.01.2017

У Путіна скаржаться на щоденні сотні тисяч кібератак з-за кордону

За словами Д. Пєскова, у Росії є дані про можливу причетність деяких іноземних спецслужб до атак на російські системи («Главком»).

Щодня на російські електронні системи здійснюються сотні тисяч кібератак з-за кордону. Про це заявив прес-секретар президента РФ Д. Пєсков.

В інтерв'ю програмі Бі-бі-сі HARDtalk він знову категорично відкинув звинувачення в причетності Росії до злому електронної пошти штабу Х. Клінтон під час передвиборної кампанії в США.

За словами Д. Пєскова, Росія піддається величезній кількості кібератак щодня – деякі з них здійснюються з США, деякі – з Німеччини і Великобританії.

«Невже ви думаєте, що це з великою часткою ймовірності означає, що ці атаки на наші електронні системи підтримуються урядами в Вашингтоні, у Лондоні чи Берліні? Ви, швидше за все, скажете “ні”. Про це не може бути й мови», – сказав Д. Пєсков.

Водночас прес-секретар В. Путіна також додав, що у Росії є дані про можливу причетність деяких іноземних спецслужб до атак на російські системи.

***

22.01.2017

Число атак банковских троянцев на пользователей Android возрастет

Антивирусная компания «Доктор Веб» прогнозирует увеличение количества атак банковских троянцев на пользователей Android-смартфонов и планшетов. Дело в том, что на одном из хакерских форумов выложен исходный код одного из таких вредоносных приложений вместе с инструкциями по его использованию (InternetUA).

«Доктор Веб» обнаружил троянца Android.BankBot.149.origin, созданного на основе предоставленной киберпреступниками информации. Этот вирус, который распространяется под видом безобидных программ, после установки на мобильном устройстве жертвы запрашивает доступ к функциям администратора, чтобы усложнить свое удаление. Затем программа убирает свой значок с главного экрана, но остается в системе.

Android.BankBot.149.origin крадет у пользователей конфиденциальную информацию, отслеживая запуск приложений «банк-клиент» и ПО для работы с платежными системами, а также пытается похитить информацию о банковской карте владельца зараженного мобильного устройства, контролируя запуск популярных приложений, таких как Facebook, Viber, YouTube и WhatsApp.

Все украденные Android.BankBot.149.origin данные загружаются на управляющий сервер и доступны в панели администрирования. С ее помощью киберпреступники не только получают интересующую их информацию, но и управляют вредоносным приложением.

***

22.01.2017

Создатели Meitu опровергают информацию о слежке за пользователями

Ранее сеть заполонили фотографии, обработанные с помощью приложения Meitu. С его помощью можно делать людей на снимке чрезмерно милыми – в аниме-стиле. Программа существует уже несколько лет, но лишь

недавно она стала доступна за пределами Китая. Внимательные пользователи заметили, что приложение собирает слишком много личных данных, которые, казалось бы, никак не связаны с обработкой фотографий. На фоне этого сразу же появились теории о слежке за людьми со стороны китайских разработчиков. Создатели сервиса Meitu незамедлительно отреагировали на эти слухи и выступили с официальным заявлением (InternetUA).

В своём заявлении разработчики опровергли слухи о слежке за пользователями и передаче их данных третьим лицам. По словам создателей сервиса, все данные, что они собирают, необходимы для оптимизации работы приложения и лучшего понимания того, как пользователи взаимодействуют со встроенной рекламой. Также они рассказали, что сервисы отслеживания статистики App Store и Google Play попросту заблокированы в Китае, поэтому они используют другие сервисы, расположенные за пределами страны. Они отмечают, что все данные передаются ими в Китай с применением многослойного шифрования, а их сервера оснащены передовым брандмауэром и IPS/IDS-защитой для блокировки внешних атак.

В дополнение к своему заявлению разработчики Meitu рассказали, для чего они используют разные пользовательские данные:

– MAC-адрес и IMEI – оба параметра используются для создания уникального идентификатора для каждого пользователя, чтобы собирать статистику;

– IP-адрес локальной сети – необходим для предотвращения бизнес-мошенничества;

– код страны SIM-карты – используется для приблизительного определения местонахождения пользователя, чтобы иметь представление о статистике по регионам;

– GPS и местоположение по мобильным сетям – используются для определения стран и регионов, чтобы можно было показывать «правильную» рекламу;

– мобильный оператор – стандартный параметр для аналитики;

– запуск приложения при включении устройства – так как сервисы Google, в том числе GCM, не работают в Китае, то разработчики используют сторонний сервис Getui, чтобы пользователи получали уведомления.

***

21.01.2017

Эксперты по безопасности попросили The Guardian исправить статью об уязвимостях WhatsApp

Британское издание The Guardian 13 января выпустило статью, в которой Т. Белтер, исследователь Калифорнийского университета в Беркли, указал на явный пробел в безопасности мессенджера WhatsApp: несмотря на шифрование, хакеры могут получить доступ к переписке. Ряд экспертов по

безопасности направили в редакцию заявление с требованием опубликовать опровержение (AIN.UA).

Что случилось?

В апреле 2016 г. пользователи WhatsApp могли заметить информационное сообщение: мессенджер ввел сквозное шифрование. Благодаря этому сообщения шифровались на устройствах и получить к ним доступ в ходе передачи информации стало невозможным. Об этом, по крайней, рассказывали в WhatsApp.

По утверждением Т. Белтера, это оказалось не совсем правдой. В ходе его исследования удалось выяснить, что приложение может самостоятельно менять ключи шифрования. Зачастую это происходит, когда человек меняет устройство, но в случае с WhatsApp такое возможно даже при редкой активации приложения. Как результат, отметил Т. Белтер, злоумышленники или спецслужбы могут получить доступ к сообщениям пользователя. Причем для последних добыть данные может даже сам WhatsApp.

В WhatsApp сообщили, что о наличии особенности со сменой ключа шифрования знают, но никаких действий предпринимать не собираются.

WhatsApp никого не обманывал

Несколько дней спустя ряд экспертов по безопасности (из компаний Tor, Mozilla, Open Crypto Audit Project и даже Signal) во главе с профессором З. Туфекчи из университета Северной Каролины обратились в The Guardian с просьбой исправить текст или удалить его вовсе. «Ваша статья идентична словам “вакцины убивают людей”, – говорится в письме. – Подобное нельзя писать, не пообщавшись предварительно с большим числом экспертов».

В дискуссию также включились разработчики протокола одного из наиболее защищенных мессенджеров Signal. Напомним, ранее именно они помогали WhatsApp вводить шифрование. По их словам, принадлежащий Facebook мессенджер не нарушает никаких правил и работает исправно. «Приложение уведомляет пользователя о смене ключа. К тому же, после замены ключа хакеры смогут прочитать только те сообщения, которые не были доставлены, а не получить доступ ко всей переписке пользователя», – говорится в сообщении Signal. Другое дело, отмечают в The Guardian, что эту функцию необходимо включать отдельно, о чем многие пользователи забывают.

Также в своем заявлении эксперты отметили, что статья The Guardian имеет негативный эффект не столько для мессенджера, сколько для обычных пользователей. «Из-за постоянного потока информации о якобы найденных уязвимостях, люди просто устают от таких новостей и в будущем уже не будут обращать на них внимание – это так называемый эффект “усталости от предостережений”, – говорится в сообщении. – Если на одного человека бросят огромные ресурсы для перехвата его сообщений, то это не значит, что сервис опасен для миллиарда человек. А ведь именно он сегодня является одним из самых безопасных для общения».

В The Guardian отметили, что не станут удалять заметку о проблемах WhatsApp, но дадут возможность использовать всем свою площадку для развития дискуссии.

***

23.01.2017

В США из-за хакерских взломов расследуют деятельность Yahoo!

Федеральная Комиссия по ценным бумагам и биржам США инициировала расследование деятельности компании Yahoo! в связи с масштабными случаями хакерских взломов ее систем. Это привело к краже личных данных миллионов пользователей, сообщила газета The Wall Street Journal (HiTech-News.ru).

Американские власти планируют проверить, насколько своевременно Yahoo! оповестила своих инвесторов об обнаружении утечек информации. По правилам Федеральной комиссии США, компании обязаны сразу обнародовать клиентам факты выявленных уязвимостей системы кибербезопасности. Источники издания отмечают, что следствие находится пока на самой начальной стадии.

***

23.01.2017

Число хакерских атак в США возросло в 2016 г. на 40 %

В 2016 г. США пострадали от рекордно большого количества кибератак – свыше 1 тыс. случаев. Об этом сообщает RNS (InternetUA).

По сравнению с прошлым годом, в 2016 г. число взломов и утечек на территории Соединенных Штатов Америки возросло на 40 %. Рост атак происходит несмотря на увеличение затрат на обеспечение информбезопасности – в 2016 г. на специальное оборудование было потрачено 73,7 млрд долл.

***

23.01.2017

Хакеры разместили в Twitter NYT сообщение о «ракетном ударе» России по США

В одном из аккаунтов The New York Times в социальной сети Twitter появилось сообщение о том, что Москва приняла решение о ракетном ударе по Соединенным Штатам Америки. Впоследствии выяснилось, что страничка подверглась хакерской атаке, сообщает The Hill (Osp-Ua.Info).

«Срочная новость. Из заявления В. Путина следует, что Россия нанесет ракетный удар по Соединенным Штатам Америки», – говорилось в сообщении, опубликованном в микроблоге New York Times Video в воскресенье утром.

Однако вскоре издание заявило о взломе аккаунта: «Мы удалили несколько твитов, опубликованных без нашего разрешения этим утром. Мы проводим расследование».

По данным The Hill, страничка NYT могла попасть в руки хакеров из команды OurMine, чья деятельность неоднократно привлекала к себе внимание прессы. Так, через Twitter группировка распространяла слухи о смерти Елизаветы II и певицы Бритни Спирс. Также, по данным СМИ, OurMine причастна к взлому страничек Marvel, Netflix и Sony Music Global.

***

24.01.2017

Не хакеры: стало известно, кто чаще всего взламывает страницы соцсетей

Канадские научные сотрудники из Университета Британской Колумбии выяснили, что аккаунт пользователя в социальных сетях чаще всего пытаются взломать его друзья. Это делает каждый четвертый из списка знакомых (InternetUA).

Ученые в своем исследовании опросили 1308 человека, результаты которого показали, что 24 % были настолько заинтересованы личной жизнью своих друзей, что предпринимали попытки взлома страницы в соцсетях с целью узнать подробности. Заполучив доступ к странице, они читали переписку и скрытые записи.

Были зафиксированы случаи, когда поводом для взлома становились месть и ревность.

Исследователи отметили, что часть опрошенных признались, что заводили страницы несуществующих людей, чтобы оставлять комментарии под записями других.

***

24.01.2017

Как хакеры взламывают страницы «ВКонтакте»?

«ВКонтакте» – одна из самых продвинутых соцсетей в плане защищённости, но её пользователей всё равно очень часто в взламывают. Как хакерам это удаётся, если страница защищена паролем и привязана к номеру телефона (InternetUA)?

Пароль

Пароль – самое слабое место любой учётной записи. Если злоумышленник знает ваш логин, email-адрес или номер телефона, ему остаётся только подобрать пароль. Сделать это можно разными способами: перебрать брутфорсом популярные пароли, подсмотреть, перехватить через открытую точку Wi-Fi. Если вы используете один и тот же пароль на всех сайтах, вы сильно упрощаете задачу злодею: если он взломает вашу почту и увидит в

открытом виде пароль, который вы используете на других сайтах, он догадается, что он подходит к вашей странице в соцсети. Некоторые хакеры сначала ломают именно почту, а потом всё остальное.

Пароли также перехватываются с помощью кейлогеров на компьютерах в общественных местах. Если вы заходите в аккаунт с чужого компьютера, подумайте, доверяете ли вы его владельцу и нет ли вероятности, что на ПК установлена программа, перехватывающая все вводимые символы.

Вирусы и расширения

Уводить логины и пароли могут вирусы и расширения для браузеров, запрашивающие доступ к «ВКонтакте». Кроме того, сбором этих данных могут заниматься приложения, «паразитирующи» на «ВКонтакте» (например, аудиоплееры), а также программы, расширяющие возможности соцсети или сайты, позволяющие зарабатывать на лайках, репостах, комментариях и добавлениях в друзья. Если вы пользуетесь чем-то подобным, почаще меняйте пароль – возможно, он давно уже слит и продан потенциальным мошенникам.

Взлом смартфона

Пароль можно сбросить по SMS, поэтому не оставляйте свой смартфон без присмотра и блокируйте устройство так, чтобы никто не смог прочитать на нём входящие сообщения. Если вы отдыхаете с компанией и уснули, а ваш смартфон защищён только сканером отпечатков пальцев, заблокируйте его так, чтобы для входа дополнительно потребовался пароль. Так его не смогут взломать, даже если подставят к сканеру ваш палец, пока вы спите.

Перехват SMS

У SMS есть уязвимость, которую никто не может устранить. Эта уязвимость позволяет настроить перехват SMS-сообщений и взломать аккаунт «восстановлением» пароля. В Интернете полно объявлений о взломе страниц «ВКонтакте» и других аккаунтов, привязанных к номеру телефона, – хакеры пользуются именно этой уязвимостью.

Как защититься от взлома?

Прежде всего придумайте сложный пароль, используйте его только для этой соцсети и регулярно меняйте его на новый. Зайдите в настройки безопасности «ВКонтакте» и как минимум установите оповещения о входе в аккаунт. Также можно настроить двухфакторную аутентификацию, при которой каждый вход будет подтверждаться кодом, пришедшим по SMS. Но помните, что защитить свой аккаунт от взлома на 100 % у вас всё равно не получится, поэтому не держите в нём ничего, что могло бы вас скомпрометировать.

***

23.01.2017

В Twitter обнаружен гигантский ботнет «Звездные войны»

Сеть насчитывает около 350 тыс. аккаунтов, ее создатель неизвестен (Зеркало недели. Украина).

Ученые обнаружили в сети микроблогов Twitter гигантскую сеть из ботов, в которую входят 350 тыс. фейковых аккаунтов. При этом, кто создал ботнет и с какой целью на данный момент неизвестно. Об открытии ученых сообщается в статье, опубликованной на сайте arXiv.

Ботнеты могут быть использованы злоумышленников для проведения разнообразных махинаций в сети: от рассылки спама до скрытого влияния на политические процессы и общественное мнение. Поэтому создатели сети из ботов стараются сделать их как можно более обширными и скрытыми.

Теперь же исследователи обнаружили ботнет, в которых входит почти 350 тыс. аккаунтов. Находка была сделана почти случайно: ученые заметили, что в сообщениях некоторых англоязычных аккаунтов содержатся странные геотеги, которые указывали на пустыню или океан.

Исследовав эти аккаунты, ученые установили, что большинство из них были активны в июне – июле 2013 г. При этом авторы всех из них оставляли несколько цитат из «Звездных войн» и «замолкали». Кроме того, все сообщения были отправлены с Windows-смартфонов, а у всех аккаунтов было только по нескольку фолловеров.

Геотеги же проставлялись случайным образом, поэтому они оказались в абсурдных местах. Проведя поиск по схожей активности в тот же период ученые обнаружили, что в сеть ботов входит по меньшей мере 350 тыс. аккаунтов. Кто их создал и с какой целью на данный момент неизвестно.

***

24.01.2017

Редкий троян для Mac OS три года терроризировал медицинские компании

Антивирусный вендор Malwarebytes выявил редкий зловред, атакующий компьютеры Apple Mac. Вредоносное ПО, получившее название Fruitfly у Apple и Quitmitchin у Malwarebytes, по-видимому, использовалось на протяжении нескольких лет для таргетированных атак и кибершпионажа. Мишенями чаще всего становились компании, занимавшиеся биомедицинскими исследованиями (InternetUA).

Фруктовый паразит

Компания Malwarebytes объявила о поимке зловреда, атакующего компьютеры Apple Mac. Эксперты назвали его Fruitfly («плодовая мушка»).

Специалисты считают, что это довольно редкий пример вредоносного ПО, успешно заражающего Mac. Они отмечают, что подавляющее число зловредов пишутся под Windows – просто в силу того, что компьютеры под этой операционной системой намного более распространены, нежели ПК Apple.

Fruitfly был выявлен по чистой случайности: некий системный администратор обнаружил странный трафик, исходящий с ПК под операционной системой Mac OS X.

Оказалось, что трафик генерировало вредоносное ПО. Как написал аналитик Malwarebytes, эксперт по безопасности Mac OS Т. Рид (Thomas Reed), ничего похожего он прежде не видел.

Вредонос, состоящий из двух файлов, поначалу показался эксперту довольно незамысловатым, однако на поверку оказался весьма занятным явлением.

Антикварные компоненты

Fruitfly регулярно делает скриншоты и пытается получить доступ к веб-камере, причем для этого используются функци, которые Т. Рид назвал «антикварными»: они применялись еще до выхода Mac OS X (первый релиз которой датирован 2001 г.).

Также зловред использует открытую библиотеку libjpeg, которая в последний раз обновлялась в 1998 г.

Java, perl и команды Shell

Зловред также содержит код Java, с помощью которого злоумышленники могут удаленно управлять компьютером, в том числе менять местоположения курсора мыши, имитировать клики, а также нажатия клавиш на клавиатуре. Это рудиментарный, но вполне действенный способ удаленного управления, считают эксперты.

Помимо этого, Fruitfly может скачивать со своего командного сервера дополнительные модули для сканирования сетевого окружения и установления соединения с устройствами в локальной сети.

Примечательно, что в зловреде присутствуют команды оболочки shell для Linux. Как выяснилось, зловред успешно запускается под Linux, не работает только код, написанный специально под Mac.

Он здесь не первый день

Исследователь предполагает, что Fruitfly может циркулировать по Сети уже несколько лет. Ему и его коллегам удалось найти в библиотеке VirusTotal исполняемый код под Windows, который устанавливает соединения с тем же C&C-сервером, что и Fruitfly и также использует библиотеку libjpeg. Сэмплы этого зловреда попали в VirusTotal в 2013 г. Лишь несколько антивирусных движков способны выявить его присутствие, и то под самыми общими обозначениями.

По словам Рида, в тексте perl-скрипта, используемом для сканирования сетевого окружения, обнаружились комментарии, указывающие на изменения, которые были внесены специально для версии Mac OS X 10.10 Yosemite, вышедшей в 2014 г.

Присутствие «антикварного» кода, по мнению Т. Рида, может означать, что зловред действительно имеет весьма почтенный возраст. Но куда более вероятно, считает автор исследования, что создатели Fruitfly не слишком хорошо разбираются в Mac OS X и использовали очень старую документацию. Либо же они использовали старые функции, чтобы избежать противодействия со стороны систем безопасности Mac OS X, чьи средства поведенческого анализа скорее среагируют на более новый код.

«Что забавно, несмотря на возраст и сложность зловреда, он использует все тот же незамысловатый метод обеспечения постоянного присутствия в системе, что и другие зловреды под Mac: скрытый файл и агент запуска. Таким образом, его легко обнаружить, если появляется повод для пристального изучения заражённой машины (например, подозрительный трафик). Его также легко выявить и устранить», – пишет Т. Рид.

По его мнению, единственная причина, по которой зловред оставался незамеченным до сих пор, это его редкое использование. Fruitfly применялся только в узконаправленных атаках.

Ну, а его функции ясно указывают на «шпионскую» природу зловреда.

«Кимитчин»

Fruitfly – это название, которое зловреду присвоила компания Apple. Malwarebytes дала другое наименование – OSX.Backdoor.Quimitchin. «Кимитчинами» назывались шпионы, которых ацтеки тайно засылали во вражеские племена. «Учитывая возраст некоторых элементов зловреда, мы решили, что такое название – в самый раз», – заметил Т. Рид.

Apple выпустила соответствующее обновление для Mac OS X, которое устанавливается автоматически.

Интересно, что никто так и не знает, каким именно образом этот зловред заражает компьютеры.

Эффект репутации

«Несмотря на то, что у Mac OS X репутация достаточно безопасной операционной системы, вредоносное ПО существует и для нее. Уверенность некоторых пользователей устройств Apple в собственной безопасности зачастую работает на злоумышленников, так как они не ожидают атак и теряют бдительность, – говорит Д. Гвоздев, генеральный директор компании «Монитор Безопасности». – Но программного обеспечения, полностью лишенного ошибок и уязвимостей, попросту не существует. В свою очередь, кибершпионские кампании обычно организуют серьезные профессионалы, которые как раз очень хорошо знают уязвимые места систем, которые собираются атаковать. Как часто бывает в таких случаях, нельзя сказать однозначно, действительно ли Fruitfly-Quimitchin является разработкой серьезных профессионалов. Возможно это и не так, поскольку профессионалы могли бы заметать следы и получше. Но как бы там ни было, этот зловред оставался незамеченным на протяжении длительного срока и выдал себя по чистой случайности».

***

23.01.2017

Хакеры взломали Twitter BBC и сообщили, что Трамп ранен в руку

Хакеры 21 января, взломали Twitter-аккаунт подразделения британской корпорации BBC в Нортгемптоне (BBC Northampton) и сообщили о ранении Президента США Д. Трампа во время церемонии инаугурации (Електронні Вісті).

В сообщении утверждалось, что «Президент Трамп получил огнестрельное ранение в руку».

Вскоре после публикации пост был удален, однако целый ряд пользователей успел его ретвитнуть.

Позднее в Twitter корпорации появилось сообщение о ложном характере размещенной информации: «Приносим свои извинения всем, кто увидел необычный твит на нашем аккаунте этим утром. По всей видимости, нас взломали. Сейчас мы устанавливаем, каким образом».

Представитель медиакомпании уточнил, что принимаются меры, чтобы избежать повторения подобной ситуации.

***

26.01.2017

Хакеры атаковали систему планирования учений Минобороны Швеции

В Министерстве обороны Швеции подтвердили факт массированной кибератаки на компьютерную систему, которая привела к отключению системы планирования военных учений, сообщает «Европейская правда» со ссылкой на Dagens Nyheter (Аналитическая служба новостей).

В оборонном ведомстве Швеции сообщили, что пока неизвестно, кто стоит за хакерской атакой. Детали нападения, в том числе время и возможный ущерб, в Минобороны Швеции отказались комментировать.

По информации источников издания, кибератака была направлена на компьютерную систему Caxcis, что отвечает за планирование учений. В результате инцидента систему планирования учений пришлось отключить.

Издание отмечает, что кибератака произошла тогда, когда вооруженные силы страны проводят подготовку и планирование крупных военных учений «Аврора -17», которые должны состояться в сентябре при участии более 19 000 военных шведской армии, а также Дании, Эстонии, Финляндии, Франции, Норвегии, Германии и США.

***

31.01.2017

«ВКонтакте» запретила банкам собирать информацию о пользователях

Руководители российской социальной сети под названием «ВКонтакте» обратились в суд с заявлением прекратить сотрудникам банков собирать в личных целях информацию о пользователях. Администрация решила судиться с представителями бренда Double Data (Grifonsoft.ru).

Как утверждают представители администрации «ВКонтакте», сотрудники Национального бюро кредитных историй и компании Data могут использовать информацию пользователей, находящуюся в открытом доступе, для своих

коммерческих целей. По мнению руководителей социальной сети, работники организации по полученным данным определяют уровень платежеспособности человека, а также на основе анализа информации могут передавать результаты в различные банковские структуры.

Чтобы получить запрет на получение информации о пользователях, сотрудниками сервиса Double Data, представители администрации «ВКонтакте» решили обратиться в суд. Сами ответчики сообщают, что претензии руководителей соцсети основываются на их же решении монетизировать данные зарегистрированных людей. Отмечается, что специалисты проводили исследование, в результате которого выяснилось, что соцсетями пользуются 60 % россиян и большинство предпочитает общаться в «ВКонтакте».

***

30.01.2017

Дмитрий Черевков

WhatsApp ответит в суде за передачу конфиденциальных данных Facebook

В Германии союз защиты прав потребителей начал судебную тяжбу с компанией WhatsApp. По мнению истца, компания нарушила конфиденциальность пользователей, передавая их телефонные номера в Facebook (HiTech-News.ru).

Федеральный союз потребителей осенью прошлого года уже предупреждал руководство WhatsApp о недопустимости передачи личных данных третьей стороне. Истцы уверенны в том, что дело может разрешиться мирно только после полной ликвидации социальным ресурсом всей имеющейся информации о клиентах.

Популярным приложением WhatsApp сейчас пользуется более миллиарда человек. По мнению экспертов, из-за этой бесплатности системы сотовые операторы несут убытки в десятки миллиардов долларов ежегодно.

***

31.01.2017

В браузере Chrome появилась неотключаемая защита от пиратства

Разработчики из Google лишили пользователей браузера Chrome возможности отключить DRM-защиту, которая не дает смотреть или копировать аудио и видео, защищенное авторскими правами (InternetUA).

Запускать всегда

Разработчики Google внесли изменения в браузер Chrome, начиная с версии 57, которые удалят из него возможность пользовательского управления рядом плагинов, в том числе отвечающими за DRM (digitalrightsmanagement – управление цифровыми авторскими правами). Это программные средства,

которые ограничивают либо затрудняют просмотр и копирование аудио- и видеофайлов, защищенных копирайтом.

Как пишет обозреватель Ghacks, немецкий журналист М. Бринкманн (Martin Brinkmann), в Chrome 56 или более ранних версиях браузера пользователи могут загрузить страницу chrome://plugins, позволяющую включать или отключать плагины, а также активировать режим «запускать всегда». Кроме действий, на этой странице браузера можно посмотреть версию плагина и место его расположения на локальном диске.

Функция полезна тем, что через нее можно отключить плагины, которые невозможно сделать неактивными через опцию настроек. Допустим, Flash или PDF Viewer можно отключить через настройки. Widevine, плагин поддержки EME API, который предназначен для работы с техническими средствами защиты авторских средств – DRM и позволяет правообладателю запретить копирование аудио-видеоконтента через HTML5, можно отключить только через chrome://plugins.

Это относится и к другим плагинам, которые могут появиться в Chrome в будущем. Таким образом, пользователи Chrome 57, а также браузера с открытым исходным кодом Chromium, такой возможности лишены.

Лечение удалением

Бринкманн отмечает, что удаление возможности управления плагинами по сути продолжает тенденцию: уже в Chrome 56 плагины автоматически переподключались при очередной загрузке устройства. Таким образом, в последующих версиях браузера плагины по умолчанию будут активными. По мнению М. Бринкманна, таким образом разработчики Google демонстрируют, что ряд плагинов, вроде Widevine или NaCL (технология для создания защищенных плагинов для браузера), рассматриваются как неотъемлемая часть Chrome. При этом Flash или PDF Viewer таковыми не признаются.

Единственным решением проблемы, по словам журналиста, является физическое удаление папки с плагином с жесткого диска – C:\Program Files (x86)\Google\Chrome\Application\[Chrome Version]\WidevineCdm\. Однако папка появится снова при очередном обновлении браузера.

«Google лишил пользователя контроля за плагинами, и это достойно критики, поскольку ничего дружественного по отношению к пользователю здесь нет. Будем надеяться, что другие разработчики браузеров не последуют этому примеру», – резюмирует автор материала.

***

30.01.2017

Хакеры взломали аккаунты CNN в Facebook

Хакерская группировка OurMine взломала аккаунты американского телеканала CNN в Facebook, сообщает Mashable (Соцпортал).

Речь идет о профилях CNN International и CNN Politics.

«Привет, это OurMine. Мы просто тестируем вашу защиту, пожалуйста, свяжитесь с нами для дальнейшей информации», – портал приводит пример текста сообщения, опубликованного хакерами на обеих страницах.

Как видно из скриншотов, сделанных Mashable, хакеры также оставили на странице CNN Politics свой логотип.

Как отмечает портал, спустя примерно 30 минут сотрудники CNN восстановили доступ к аккаунтам и удалили сообщения хакеров.

Соціальні мережі

як чинник інформаційної безпеки

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

Упорядник Терещенко Ірина

Редактор О. Федоренко

Свідоцтво про державну реєстрацію КВ № 5358 від 03.08.2001 р.

Видавець і виготовлювач
Національна бібліотека України
імені В. І. Вернадського
03039, м. Київ, просп. 40-річчя Жовтня, 3
Тел. (044) 524-25-48, (044) 525-61-03
E-mail: siaz2014@ukr.net
www.nbuv.gov.ua/siaz.html

Свідоцтво про внесення суб'єкта видавничої справи
до Державного реєстру видавців виготівників
і розповсюджувачів видавничої продукції
ДК № 1390 від 11.06.2003 р.