СОЦІАЛЬНІ МЕРЕЖІ ЯК ЧИННИК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Огляд інтернет-ресурсів
(15.03–28.03)

2017 № 6

Соціальні мережі
як чинник інформаційної безпеки

Інформаційно-аналітичний бюлетень
Додаток до журналу «Україна: події, факти, коментарі»
Огляд інтернет-ресурсів
(15.03–28.03)
№ 6

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

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

Упорядник
І. Терещенко

Заснований у 2011 році
Виходить двічі на місяць

Київ 2017

ЗМІСТ

РОЗВИТОК І ПЕРСПЕКТИВИ СОЦІАЛЬНИХ МЕРЕЖ

20.03.2017
Instagram запустил функцию сохранения прямых трансляций

Сервис Instagram в своем официальном блоге сообщил о новой функции – сохранении прямых трансляций на устройство пользователя. Функция станет доступна сразу после обновления приложения (AIN.UA).

По словам представителей сервиса, прямые трансляции пользуются большой популярностью среди пользователей Instagram. И до недавнего времени главным минусом был тот факт, что Live нельзя было сохранить и потом снова посмотреть: он удалялся сразу после завершения стрима.

Теперь это исправили. Стрим все также будет исчезать из ленты пользователя после его завершения. Но саму запись можно будет сохранить в память устройства. В правом верхнем углу после завершения стрима появляется кнопка Save, при нажатии на которую видеозапись трансляции загружается на смартфон.

Причина запуска такой функции очевидна: ролики не становятся виральными и «живут» совсем мало. Теперь же, когда их можно загрузить на смартфон, пользователь может продолжить его жизнь: выгрузить на YouTube или Facebook. К примеру, множество блогеров на YouTube даже создают каналы своих стримов, куда после записи прямых трансляций выгружаются записи. И часто они пользуются немалой популярностью.

***

20.03.2017
Дмитрий Демченко
Чатботы в Messenger ошибаются в 70 % случаев

Facebook «прекратит активно развивать чатботы в Messenger» после того, как они не смогли удовлетворить запросы пользователей в 70 % случаях. Об этом сообщает издание The Motley Fool (AIN.UA).

Сообщается, что боты, созданные сторонними разработчиками, «имели проблемы» из-за того, что «технология для понимания человеческих запросов недостаточно хорошо разработана». Вместо того, чтобы строить масштабную экосистему чатботов, Facebook научит их разбираться «в более узконаправленных ситуациях таким образом, чтобы пользователи не были разочарованы ограничениями в автоматизации».

Изначально социальная сеть открыла доступ к чатботам компаниям, позволяя им напрямую общаться с клиентами. По состоянию на сентябрь 2016 г. в Messenger было активно 30 000 ботов. «Тем не менее, экосистема Facebook быстро наполнилась чатботами низкого качества. Такие собеседники могут

раздражать людей и портить имидж компании – поэтому социальная сеть решила переосмыслить их концепцию», – отмечает издание.

The Motley Fool подчеркивает, что в пределах компании у чатботов нет впечатляющих конкурентов. «Новостная лента не может отличить правдивые новости от ложных, а виртуальный ассистент M не набрал такой популярности, как Siri и Google Now».

Несмотря на ошибки, Facebook не перестанет инвестировать в новую технологию, полагает издание. Ожидается, что компания анонсирует свои планы по отношению к чатботам на апрельской конференции F8. «Скорее всего, там расскажут о том, как повысить качество, а не количество чатботов в Messenger. На конференции также могут представить другие ситуации, в которых можно будет использовать ботов в приложении – например, для онлайн-платежей и в играх», – прогнозирует The Motley Fool.

***

20.03.2017

«ВКонтакте» разрешит транслировать музыку в прямом эфире

В официальное приложение для прямых трансляций «VK Live» будет добавлена функция трансляции аудиозаписей. Все зрители прямого эфира смогут увидеть название трека и исполнителя, но после завершения трансляции видео будет удалено (InternetUA).

«Мы заметили тенденцию – пользователи включают фоновую музыку во время своих трансляций. Планируем в рамках эксперимента дать возможность зрителям таких эфиров видеть названия звучащих композиций и таким образом узнавать о музыкальных предпочтениях своих кумиров», – заявил представитель «ВКонтакте» Е. Красников.

Компания никак не прокомментировала законность таких трансляций с точки зрения обладателей авторских прав на музыкальные композиции. Скорее всего, именно с этим фактом связано удаление таких трансляций после завершения. Напомним, что сейчас прямые эфиры сохраняются в виде обычных видеозаписей и могут быть доступны оффлайн. Ни один из правообладателей, с которым у «ВКонтакте» заключен контракт, не получал уведомлений от компании о введении новой функциональности.

«Достаточно сложно прокомментировать решение команды соцсети. Они не обращались к нам за использованием произведений таким образом. Думаю, что именно поэтому они приняли решение не сохранять видеозаписи с музыкой», – М. Опарина, генеральный директор «Первого музыкального издательства».

***

23.03.2017

Instagram уходит в офлайн: соцсеть будет работать без Интернета

На днях стало известно о новых возможностях Instagram. Компания активно занялась разработкой офлайн-функций, предназначенных для людей, у которых возникают проблемы с подключением к Интернету (Экономические известия).

Специалисты Instagram сообщили, что сейчас идет активная стадия тестирования офлайн-функций. «Наша цель – дать возможность людям пользоваться приложением, даже если они испытывают трудности с подключением к Сети», – заявили в компании. Согласно данным Instagram число пользователей, которые ежедневно посещают соцсеть равно 400 млн. Среди такого количества людей есть те, которые не могут похвастаться быстрым трафиком или проживают в интернет-неразвитых странах, информирует news.eizvestia.com.

К сожалению, пока неизвестно, какие именно функции будут доступны пользователям в режиме офлайн. Возможно, владельцам аккаунтов разрешат делать снимки или видео без подключения к Интернету, поставить в очередь на загрузку на свою страницу, а появится контент только после подключения к Сети.

Скорее всего, подробности нововведений Instagram мы узнаем совсем скоро – 18 и 19 апреля пройдет ежегодная конференция разработчиков Facebook F8. Известно только, что на мероприятии специалисты Instagram выступят с лекцией «Building Offline Experiences for Instagram».

***

23.03.2017

Функция Facebook Live теперь доступна и на компьютерах

Facebook Live – это возможность потоковой передачи видео в реальном времени. Такая функция есть в приложении Facebook с прошлого года, а сейчас самая крупная социальная сеть в мире также запускает ее на компьютерах. Таким образом, вести прямой эфир на Facebook можно будет с помощью веб-браузера (Технофан).

Функция уже запущена, но не каждый ее видит. Согласно информации, полученной от Facebook, прямой эфир может быть запущен на компьютере с помощью кнопки Live Video, которая находится в опциях, доступных в режиме добавления поста. Затем нужно ввести описание, а также выбрать аудиторию. Потом можно начать передачу.

Facebook утверждает, что такая функция будет особенно полезна для блогов или для конференций типа Q&A. Это связано с тем, что камера в компьютере статична и не двигается. В случае мобильного приложения, когда телефон находится в руке, тяжело получить такой эффект.

***

21.03.2017

Пользователи по всему миру пожаловались на сбои программы Skype

Во многих странах мира пожаловались на некорректную работу программы для видеозвонков и передачи сообщений Skype (InternetUA).

Отзывы пользователей появились на сайте Downdetector.

Жалобы поступили из стран, которых находятся в разных уголках мира.

О сбоях заявили в США, Индии, России, Молдове, Польше, Литве, Пакистане, Норвегии, Бразилии, Греции и во многих других странах. Кроме того, проблемы в работе программы заметили и в Украине.

Отметим, что 20 марта компания заявила об обновлениях, которые, возможно, стали причиной сбоя практически во всех странах мира.

«Новые возможности. Лучшее качество связи. Улучшенние групповых вызовов и обмен сообщениями. Одно бесплатное обновление», – говорилось в Twitter Skype.

***

23.03.2017

В видеочате Google Duo появились голосовые звонки

Компания Google представила на специальном пресс-мероприятии в Бразилии обновление приложения Google Duo для Android и iOS. Напомним, Google Duo был представлен в прошлом мае, на конференции для разработчиков Google I/O 2016 (InternetUA).

По сути, это простой видеочат для звонков один-на-один и конкурент FaceTime от Apple. Тем не менее, теперь его функциональность расширяется – к видеозвонкам добавилась возможность голосовых звонков, на случай, если видео неприемлемо или соединение с сетью оставляет желать лучшего.

Новая функция появится сначала для бразильских пользователей, а в ближайшие дни начнется ее внедрение и для других регионов мира. Google Duo для iOS и Android можно бесплатно скачать в App Store и Google Play.

***

24.03.2017

Ірина Коркішко

Понад 20 мільйонів українців у Viber

Приріст аудиторії Месенджера Viber в Україні за 2017 р. становить 11 %. На сьогодні у сервісі зареєстровано понад 20 млн українців. Про це повідомляється в офіційному прес-релізі компанії (Watcher).

Таке зростання аудиторії компанія пояснює введенням багатьох корисних функцій Месенджера. Так, у листопаді минулого року у сервісі з’явилися публічні акаунти, що дали змогу компаніям спілкуватися з клієнтами у форматі особистої переписки. Також усім користувачам стали доступні опції відправки

фото та відео, що самознищуються після встановленого строку, і секретні чати, у яких відсутня можливість створення скріншотів.

***

26.03.2017

Instagram запустив двофакторну авторизацію

Розробники соціальної мережі Instagram запустили двофакторну авторизацію для всіх користувачів (Tehnot.com).

Як заявив генеральний директор Instagram К. Сістром, для включення двофакторної авторизації потрібно перейти в налаштування: нова опція з'явилася трохи вище розділу з публікаціями, яким користувач поставив лайк.

Тепер, якщо користувач спробує ввійти нового пристрою, то йому прийде SMS-повідомлення з кодом підтвердження, який треба буде ввести. При цьому резервні копії кодів можна зберігати – на випадок, якщо користувач втратить телефон. Додаток пропонує скопіювати код у додаток для нотаток або зробити скріншот. Варто відзначити, що Instagram почала вводити двофакторну аутентифікацію ще в лютому 2016 р.

Що ж стосується неприйнятного вмісту, якщо користувач поскаржиться на фото або відео, а модератор погодиться з ним, зображення стає нечітким. Щоб погодитися на перегляд, потрібно буде натиснути на картинку. При цьому розробники не уточнили, який контент буде вважатися «чутливим». За їх словами, це публікації, які не порушують правила сервісу, але все ж можуть бути проблемними (тобто – ніякої конкретики).

***

27.03.2017

В Facebook Messenger появились упоминания и реакции

С помощью двух новых функций Facebook собирается навести порядок в групповых чатах своего Мессенджера («КОММЕНТАРИИ:»).

В приложении появились упоминания и реакции, которые компания до этого тестировала во Вьетнаме, сообщает «3Dnews».

Пользователь может упомянуть члена групповой переписки, тот получит уведомление и не пропустит сообщение. Достаточно ввести @ и имя либо никнейм человека. Имя будет подчеркнуто, а пользователь сразу узнает о том, что ему хотят о чём-то сказать.

В Facebook Messenger прямиком из социальной сети пришли реакции. Теперь можно высказать своё отношение к сообщению в чате, не используя слова. На выбор предоставляются реакции «Супер», «Ха-ха», «Ух ты!», «Сочувствую», «Возмутительно», а также «Нравится» и «Не нравится». Так можно выразить согласие или несогласие либо просто намекнуть, что вы думаете о написанном.

Чтобы открыть меню реакций, нажмите на сообщение и удерживайте палец. Напротив сообщений отображаются специальные счётчики. На них можно нажимать, чтобы смотреть, кто и как отреагировал на сказанное. Реакции работают и в индивидуальных переписках.

Реакцию «Не нравится», которую символизирует палец вниз, можно воспринимать как желанный многими дизлайк. Facebook говорит, что палец вниз – это скорее отрицательный ответ. Поскольку люди часто используют Мессенджер для координации передвижений, компания хотела дать им возможность быстро голосовать за или против предлагаемых схем.

***

27.03.2017

YouTube научился подписывать звуки в видео

В YouTube появилась функция, которая автоматически подписывает в видеороликах окружающие звуки – аплодисменты, музыку и смех («КОММЕНТАРИИ:»).

Это поможет лучше понимать происходящее на экране тем, у кого имеются проблемы со слухом, сообщает «3Dnews».

Возможности системы пока ограничены тремя перечисленными категориями. YouTube использует машинное обучение, чтобы определять звуки и показывать их текстовые описания.

Компания разработала нейронную сеть и натренировала её, использовав тысячи часов видео. По словам разработчиков, сложнее всего было научить систему отличать элементы, которые звучат одновременно – например, смех и рукоплескания.

В результате описания окружающих звуков стали отображаться вместе со стандартными автоматическими субтитрами. Команда разработчиков YouTube признаёт, что подписи примитивны. Но теперь технологию будет проще усовершенствовать, потому что основа, то есть нейронная сеть, уже создана. В будущем компания хочет добавить поддержку таких звуков, как лай, стук и звон. Для этого искусственному интеллекту придётся научиться различать источники звуков: звон, например, могут издавать телефон, будильник или дверной звонок. Разработчики провели исследование, две трети участников которого сказали, что с подписями видео смотреть комфортнее.

Автоматические субтитры появились в YouTube в ноябре 2009 г. Алгоритмы компании пока далеки от идеала и их приходится дорабатывать – из-за неправильного произношения, диалектов, акцентов и фоновых шумов.

Функция очень популярна: более 15 млн роликов с автоматическими субтитрами люди смотрят каждый день, а всего таких видео в сервисе – более миллиарда.

***

27.03.2017

Google уберет SMS из Hangouts для Android с 22 мая

Компания Google уберет из своего Мессенджера Hangouts для Android поддержку SMS с 22 мая 2017 г. Как сообщил профильный ресурс AndroidPolice, извещение о таком решении Google рассылает администраторам G Suite (InternetUA).

Google предупредила, что с 27 марта пользователи начнут получать предупреждения о грядущем отключении SMS в Hangouts, предлагая подобрать для этого альтернативное приложение, как показано на иллюстрации. А с 22 мая поддержка SMS в Hangouts полностью прекратится.

***

27.03.2017

Facebook и Facebook Messenger потеряли поддержку Windows 8 и Windows Phone 8

С конца марта Facebook перестанет поддерживать своё титульное приложение и Мессенджер на Windows 8, Windows 8.1, Windows Phone 8 и Windows Phone 8.1. Facebook рекомендует желающим продолжить пользоваться этими приложениями обновить компьютеры и смартфоны или перейти на другие операционные системы (InternetUA).

Далеко не все смартфоны с Windows Phone 8 поддерживают обновление до Windows 10 Mobile. Среди устройств, которым недоступен апдейт, самая распространённая модель Windows-смартфонов – Lumia 520.

С начала марта на Windows Phone 8.1 перестало работать принадлежащее Microsoft приложение Skype. Компания объяснило это тем, что Skype переходит на новую технологию, которая не поддерживается старыми Windows-смартфонами. Если даже такие крупные компании, как Facebook и Microsoft не могут выделить ресурсы на поддержку Windows 8 и Windows Phone 8, можно ожидать, что от дальнейшего развития приложений для этих платформ в скором времени начнут отказываться и другие разработчики.

СОЦІАЛЬНІ МЕРЕЖІ ЯК ВИЯВ ФОРМУВАННЯ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА

15.03.2017

Теперь показания счетчиков можно передавать через Viber

«Киевводоканал» начал принимать показания счетчиков холодной и горячей воды через Viber (From-UA).

Об этом в Facebook сообщила пресс-служба водоканала.

Чтобы отправить данные со счетчков через Мессенджер, нужно добавить в своем Viber в контакты номер (044) 202-02-02.

***

15.03.2016

У соцмережах флешмоб з вимогою звільнити вченого, який вже 413 днів у полоні бойовиків

У соцмережах поширюється флешмоб, учасники якого вимагають звільнити з полону бойовиків на Донбасі вченого-релігієзнавця І. Козловського. Його незаконно утримують в окупованому Донецьку вже 413 днів (Західна інформаційна корпорація).

Флешмоб #freekozlovskyy ініціювала доктор філософських наук, професор, завідувач відділом філософії та історії релігії Інститут філософії ім. Г. С.Сковороди НАН України Л. Филипович.

Вона, зокрема, написала:

«Шановні друзі! У полоні, У жахливих умовах, в окупованому Донецьку вже 413 днів незаконно тримають дуже дорогу для нас людину! Всесвітньовідомого вченого – Ігоря Анатолійовича Козловського!

Ігор Анатолійович вимушений був лишатися в Донецьку на той момент, бо він доглядав за старшим сином, що є хворим з народження. Вони планували поїхати, але не встигли. Родина та друзі Ігоря Анатолійовича зверталися в міжнародні правозахисні організації, підтримку та прохання сприянню в визволенні вченого надсилали релігійні, наукові, мистецькі спільноти, але позитивного результату, поки що немає.

Прошу вас так, як би просила за власного батька! Родина, друзі, учні, громадські діячі планують флешмоб заради визволення Козловського І. А. з полону. Сфотографуйтесь, будь ласка, з хештегом #freekozlovskyy 15.03.2017 та опублікуйте фото на ваших сторінках у соціальних мережах, групах, якщо це можливо, то зверніться до ваших друзів за кордоном.

Якщо ви особисто знайомі чи засуджуєте повне порушення прав людини, що відбувається в так званій “ДНР”, напишіть коментар з цього приводу і додайте цей хештег. Ігор Анатолійович може ще багато зробити для науки, навчити та допомогти багатьом людям, але зараз він потребує нашої підтримки! Дякую! Ви, зробите добру та велику справу!»…

***

22.03.2017

Ольга Карпенко

#меняневзяли: украинский Facebook делится неудачами при устройстве на работу

Даже CEO крутого стартапа или основатель модного digital-агентства когда-то мог быть студентом, которому отказали в работе оператором колл-

центра или распространителем листовок. Сегодня в украинском Facebook раскручивается флешмоб под грустным хештегом #меняневзяли (AIN.UA).

Флешмоб перекинулся к нам из рунета, а где он зародился сказать сложно. Под этим хештегом публикуются самые разные истории. Российский писатель Б. Акунин, к примеру, вспоминает, как издательство отвергло его первый роман. Медиаменеджер Л. Бершидский (который, в частности, запускал сайт Forbes в Украине) вспоминает, как расстроился, когда его не взяли в McKinsey в 2003 г.

Среди украинцев также нашлось немало пользователей, которые не против вспомнить печальные или забавные страницы своей карьеры. Предприниматель и активист Д. Браун рассказывает, как вместе с несколькими волонтерами пытался попасть в Оппоблок, чтобы вести подрывную работу изнутри. Телеком-аналитик А. Фроленков рассказывает, как еще в детстве его не взяли в «Артек». Бывший глава украинского офиса «Яндекс» С. Петренко вспоминает о том, как мечтал стать астрофизиком. Основатель «Розетки» В. Чечеткин рассказал, как его не взяли в «Аспен».

***

25.03.2017

#Надоподписать: военные попросили Порошенко о помощи

Военные с помощью флешмоба попросили Президента Украины П. Порошенко подписать законопроект № 6172 «Об изменениях к закону о предотвращении коррупции» (Обозреватель).

Так, в сети Facebook началась акция #Надоподписать.

Отметим, что этот законопроект освобождает военных от обязательного заполнения электронной деларации о доходах.

Украинские бойцы надеются, что П. Порошенко увидит их просьбу и поскорее подпишет эти изменения в законодательство.

***

28.03.2017

У Грузії запустили «безвізовий» флешмоб на підтримку України

Громадяни Грузії, які з 28 березня можуть відвідувати країни Шенгенської зони без віз, запустили в соціальних мережах флешмоб у підтримку України (Еспресо.TV).

Учасники флешмобу публікують свої фото з хештегом #Visa_Free_For_Ukraine.

У руках вони тримають аркуш з написом: «Я не буду до кінця відчувати себе європейцем до тих пір, поки Україна не отримає безвізовий режим».

БІЗНЕС І СОЦІАЛЬНІ МЕРЕЖІ

15.03.2017

Google и Facebook возьмут под контроль 60 % рынка цифровой рекламы, – FT

По данным нового прогноза eMarketer, Google и Facebook в 2017 г. возьмут под контроль 60 % растущего рынка цифровой рекламы («БизнесЦензор»).

Об этом сообщает Коммерсант со ссылкой на Financial Times, передает БизнесЦензор.

По информации исследовательской группы, расходы на цифровую рекламу в США в текущем году возрастут на 16 %, до 83 млрд долл. Доходы Google в связи с этим увеличатся на 15 %, а Facebook – на 32 %.

Согласно данным eMarketer, Google намерена сохранить лидерство в поисковой рекламе, увеличив свою долю до 28,6 млрд долл. – 78 % американского рынка.

«Доминирование Google в поиске, особенно в мобильном поиске, во многом связано с растущей тенденцией потребителей использовать смартфоны для того, чтобы найти все: от деталей продукта до направлений», – объяснила аналитик eMarketer М. Пирт.

Facebook, в свою очередь, будет расширять свою долю благодаря приложению для обмена фотографиями Instagram, которое, как ожидается, принесет социальной сети 20 % доходов от мобильных устройств. В прошлом году этот показатель составил 15 %. В целом доля Facebook на рынке цифровой рекламы возрастет почти на 20 %. Одним из главных факторов роста интереса к Facebook, по информации аналитиков, является видеоконтент.

***

15.03.2017

На Android теперь можно переводить деньги через Gmail

Компания Google предоставила пользователям почтового сервиса Gmail новый удобный инструмент для осуществления перевода средств. Теперь прямо в своем аккаунте можно запрашивать и переводить средства с мобильного, сообщает TechCrunch. Правда, пока только в США и Британии (AIN.UA).

У Google есть специальный сервис Google Wallet, который был интегрирован с Gmail еще в 2013 г. Сейчас же компания сделала платежи более удобными – они начали полноценно работать прямо в мобайле, через приложение Gmail на Android. Все происходит по той же схеме, что и добавление в письмо файла. Только теперь вместо файла добавляется запрос на перевод денежных средств и сумма. Отправлять счета можно пользователям, у которых нет аккаунта в Gmail.

Все действия происходят прямо в приложение Gmail, переходить в сторонние сервисы пользователю нет необходимости. Подобную возможность Google запустила для конкуренции с PayPal, Venmo и Square Cash. К тому же, сегодня переводить средства можно через Snapchat, Facebook Messenger и другие Мессенджеры. Таким образом, в Google пытаются увеличить число возможностей своего пока главного сервиса для коммуникации – Gmail.

Ранее система работала исключительно с активным Google Wallet, но так и не стала популярной. Как и масса Мессенджеров и других сервисов для общения от Google, которых компания создала не мало.

***

20.03.2017

«ВКонтакте» запустила денежные переводы сообществам

Социальная сеть «ВКонтакте» запустила сервис денежных переводов в адрес сообществ, рассказали представители компании (IGate).

Чтобы отправить деньги, необходимо открыть диалог с сообществом, выбрать новый пункт «Деньги» в меню вложений, указать сумму и подтвердить перевод. Получать средства могут редакторы и администраторы группы.

Если перевод не будет востребован руководством сообщества, то через пять дней он вернется отправителю. Каких-либо «кошельков» для групп реализовано не будет, средства нужно будет получать на банковский счет, заявил представитель «ВКонтакте» Е. Красников.

«Как и в случае с денежными переводами пользователям, при отправке средств с карт Mastercard и Maestro комиссия взиматься не будет, а для карт Visa комиссия составит 1 %», – отметили в компании. У руководителей групп будет возможность посмотреть всю историю переводов.

«Сегодня мы закладываем фундамент платформы для краудфандинга на базе сообществ “ВКонтакте”. Теперь любое сообщество может профинансировать тот или иной коллективный проект при помощи своих участников. Так, инди-музыканты получат возможность собрать необходимую сумму на запись альбома, а родительский комитет 11-А класса – на выпускной», – рассказал директор по электронной коммерции «ВКонтакте» Ю. Иванов.

***

22.03.2017

Дмитрий Демченко

Дополненная реальность и сканирование мозга: над чем работает секретная группа Facebook Building 8

Издание Business Insider опубликовало материал про секретную группу Facebook Building 8. Как выяснилось, Building 8 работает над четырьмя проектами, среди которых создание устройств дополненной реальности, камер,

дронов и работа над технологией сканирование мозга. Редакция AIN.UA выбрала главное из материала и приводит его адаптированный перевод (AIN.UA).

Команда IT-ветеранов, которую Facebook начал собирать год назад, бесшумно продвигается в работе, увеличивая свой штат и количество существующих прототипов. Группа под названием Building 8 одновременно работает над четырьмя проектами, которые включают в себя разработку камер, устройств дополненной реальности и технологии сканирования мозга.

И Facebook уже думает над возможностью представить новые девайсы, чтобы подогреть к ним интерес перед полноценным запуском продаж. Building 8 не анонсировала еще ни одного устройства, но люди, приближенные к команде, говорят, что группа будет играть главную роль на мероприятии компании, которая пройдет через месяц.

Переход к разработке hardware-продуктов – рискованное и амбициозное занятие для Facebook. У компании нет опыта в этой области, но она вступает в конкуренцию с более зрелыми игроками – Apple, Google и даже Snap – на беспощадном рынке, известном низкой маржой и сложной логистикой.

И кажется, что Facebook относится к Building 8 не как к хобби. Business Insider проанализировало недавние наймы группы и список открытых вакансий, а также поговорило с людьми близкими к компаниями и узнала об амбициозных планах команды создавать и продавать миллионы устройств.

По словам источников издания, сейчас Building 8 разрабатывает камеры и устройства дополненной реальности, а недавние пополнения команды говорят о возможной работе над дронами.

В рамках другого проекта часть группы создает технологию сканирования мозга, и возглавляет ее бывший нейроученый Университета Джонса Хопкинса, который участвовал в разработке протеза, управляемого мозгом.

Еще часть группы может заниматься созданием медицинских устройств, так как работает под управлением интервенционного кардиолога из Стэнфордского университета. Building 8 также хочет начать пятый проект, но пока неизвестно, чем группа будет заниматься и кто возглавит группу.

Главой Building 8, которая наблюдает за всеми разработками, является Р. Дуган, бывшая сотрудница оборонного агентства DARPA и подразделения Google ATAP.

Структура команды похожа на ту, которая учреждена в ATAP и лаборатории X. В Building 8 глава каждого проекта считается генеральным директором небольшого масштаба. Ему дается два года на то, чтобы доказать, что концепт способен дойти до стадии поставок и продаж или сможет стать отдельной частью Facebook, как Oculus VR, WhatsApp и Instagram.

Срок одного из проектов истекает летом 2018 г. Его возглавляет Ф. Делларт, эксперт в робототехнике и компьютерном зрении. Приход Ф. Делларта может означать, что Facebook хочет создавать дроны для широкого потребления. Такие же планы есть у Snap Inc., компании-создателя Snapchat.

Перед тем как присоединиться к Facebook, Ф. Делларт был старшим ученым в стартапе Skydio, который работает над самоуправляемым дроном. За последние несколько месяцев в Building 8 пришло также ряд сотрудников из GoPro и еще один разработчик Skydio С. Макклур.

Команда Building 8 уже активно ищет пути выхода на рынок, предлагая работу новым сотрудникам в сфере розничной торговли, доставки и обслуживании клиентов. Уже открыты вакансии менеджера по розничным продажам, а также работника, который будет заключать партнерства со сторонними компаниями. Это означает, что Facebook станет использовать сторонние предприятия, чтобы продавать свои продукты.

Поставка и продажа потребительской техники миллионам людей – это новый вызов для Facebook, который до этого занимался реализацией гарнитуры Oculus VR в небольших масштабах.

Партнер инвестиционной фирмы Loup Ventures Г. Манстер считает, что деятельность Building 8 демонстрирует желание Facebook стать серьезным игроком в отрасли дополненной реальности: «Компания понимает, что должна быть частью этой новой волны, но в то же время ей стоит поспешить».

По словам Г. Манстера, для того, чтобы добиться успеха Facebook нужно будет продать около 20 млн устройств. И даже в этом случае конкуренция с большими компаниями типа Apple и быстрорастущими стартапами, как Snapchat, будет серьезной.

***

22.03.2017

У «ВКонтакте» появилось приложение «Магазин товаров»

Приложение станет дополнением к сервису «Товары» (Sostav.ua).

«ВКонтакте» выпустила приложение на базе соцсети «Магазин ВКонтакте», которое предоставляет сообществам функции онлайн-магазина. В приложении покупатели смогут просматривать каталог и заказывать товар.

Сообщается, что приложение использует данные о товарах, которые были размещены в сервисе «Товары» в сообществе. Там пользователи могли размещать информацию о своих товарах, ценах и доставке.

Для менеджеров, работающих с приемом заказов в сообществе, доступна внутренняя CRM со статусами заказов, комментариями, учетом остатка товаров, отмечают в соцсети.

***

21.03.2017

Google предоставил расширенные меры безопасности для рекламодателей

Google удаляет медийную рекламу, размещенную рядом с широким кругом контента на YouTube и других сайтах, будучи раскритикованной за то,

что ее автоматическая, программируемая реклама не может помешать брендам появляться рядом с экстремистскими и оскорбительными материалами. На прошлой неделе ряд брендов и издателей в Европе заявили, что откажутся от рекламы в сети Google после того, как их сообщения появились рядом с видео, продвигающими терроризм и антисемитизм. В ответ на критику от рекламодателей, включая британское правительство, the Guardian и гиганта Havas, Google пообещал предоставить им больший контроль над размещением рекламы в YouTube и своей сети. Директор по развитию бизнеса Ф. Шиндлер написал сегодня, что Google уже начал совершать перемены в области рекламной политики, приведения в исполнение этих политик и нового контроля для рекламодателей. «Мы приносим глубокие извинения за то, что реклама брендов появилась рядом с контентом, не соответствующим их ценностям. Мы знаем, что это неприемлемо для рекламодателей и агентств, которые доверяли нам. Поэтому мы пересматриваем рекламную политику и инструменты и публично заявили на прошлой неделе о том, что предоставим брендам больше контроля над размещением рекламы». Среди перемен и более «строгая позиция по отношению к ненавистническому, оскорбительному и негативному контенту». Предположительно, Google полностью удалит оскорбительный контент с YouTube. «Наша YouTube команда пересмотрит существующее руководство по размещению контента на платформе и не только того контента, который можно монетизировать», – указал Ф. Шиндлер (Marketing Media Review).

***

22.03.2017

Телеканалы смогут вести профессиональные прямые трансляции в Twitter

Twitter запускает API для видеотрансляций, что позволит компаниям подключать профессиональное оборудование для телетрансляций и редактирования видео, сообщает AIN.UA (Телекритика).

По информации источников издания TechCrunch, Twitter Live API будет схож с Facebook Live, запущенным в апреле 2016 г. Через API к Twitter можно будет напрямую подключать профессиональные телекамеры, доски редактирования, ПО для обработки видеопотока и передвижные телевизионные станции.

До запуска API создателям или провайдерам контента необходимо было подписать партнерское соглашение с Twitter.

***

24.03.2017

Ирина Евсюкова

Соцсеть Twitter станет платной

Сервис микроблогов Twitter планирует ввести платную подписку для пользователей, брендов и СМИ, у которых большое количество читателей, сообщается ura (podrobnosti.ua).

Планируется, что это значительно расширит функциональность соцсети. Сам сервис будет связан с приложением компании Tweetdeck, что позволяет работать сразу с несколькими учетными записями, и с множеством других функций.

О подготовке нововведения сообщили сами пользователи, которым предлагалось пройти опрос, чтобы выяснить, какой интерфейс для них будет наиболее удобным. В пресс-службе компании подтвердили, что проводят подобное исследование.

«Мы регулярно проводим исследования аудитории для сбора отзывов о работе Twitter и для лучшего информирования инвестиционных решений», – сообщила представитель компании Б. Виллабланка.

***

27.03.2017

Потери более 35 млрд долларов: крупные рекламодатели ушли с YouTube

Корпорация Alphabet (она же Google) всего за несколько дней потеряла в капитализации более 35 млрд долл. из-за того, что ряд крупных рекламодателей заявили, что временно прекращают сотрудничество с видеосервисом YouTube (Finance.Ua).

Причина такого решения – размещение рекламы в видеороликах, которые пропагандируют экстремизм. Представители Google извинились и пообещали исправить ситуацию, но инвесторам такого ответа оказалось мало.

«Мы соединяем контент и рекламу. Но поскольку мы берем контент отовсюду, порой случается, что он не соответствует рекламе. Сейчас мы активно работаем над решением этой проблемы», – заявил Э. Шмидт.

Впрочем, слова Э. Шмидта не сильно придали уверенности инвесторам Alphabet. За несколько дней стоимость акций компании просела на 4 %. Из-за этого компания потеряла в капитализации более 35 млрд долл. При этом акции продолжали показывать негативный тренд.

Временно от сотрудничества с Youtube отказались крупные британские бренды Marks & Spencer, правительство Британии, BBC, банки HSBC и Lloyds, а также американские AT&T, Verizon, Johnson & Johnson и др.

Точной суммы, которой не досчитается сервис от потери крупнейших рекламодателей, не называется. Но как сообщили в Reuters, речь о сотнях миллионов долларов только от американских рекламодателей. Всего за последний год выручка YouTube составила 14 млрд долл.

***

27.03.2017

Instagram достиг уровня в миллион рекламодателей

Социальная сеть Instagram достигла отметки в миллион рекламодателей, хотя в прошлом году их было всего 200 тыс. (Finance.Ua).

На сегодня в сервисе зарегистрировано около 8 млн бизнес-профилей, сообщила компания в своем блоге.

Для сравнения, в Facebook зарегистрировано более 4 млн рекламодателей, а в Twitter – 130 тыс.

Такие показатели роста в самой компании объясняют несколькими факторами, сообщает Techcrunch.

В частности, легкостью размещения объявлений в социальной сети, а также тем, что 80 % пользователей активно подписываются именно на бизнес-аккаунты.

***

27.03.2017

Макс Ли

К бойкоту YouTube присоединились компании PepsiCo, Walmart и Starbucks

Крупные рекламодатели – компании PepsiCo, Walmart и Starbucks присоединились к бойкотированию Google и YouTube. Причиной протеста корпораций стало размещение рекламы всемирно известных производителей рядом с видеороликами нацистского, ксенофобского и расистского содержания (HiTech-News.ru).

Скандал с транснациональной корпорацией, владеющей крупнейшей в мире поисковой системой возник ещё в феврале. О бойкотировании рекламы в YouTube заявили Marks & Spencer, McDonald’s, HSBC, Lloyds, BBC и Guardian. Эти компании и газета протестовали против того, чтобы их реклама «привязывалась» к видеозаписям, явно провоцирующим ксенофобию, ненависть и агрессию.

В середине марта история с бойкотом получила продолжение, когда представители знаменитых брендов нашли свою рекламу, транслируемую на египетском радикальном канале. Теперь к протесту присоединились компании Walmart, Starbucks и PepsiCo, опечаленные тем, что их реклама оказалась «привязана» к «пропаганде насилия и ненависти».

Транснациональная корпорации Брина и Пейджа, посчитав денежные убытки, опубликовала заявление, где признала свою ошибку. В дальнейшем руководство Google пообещало ужесточить контроль над тем, как размещается реклама.

***

26.03.2017

Facebook и Nokia займутся ускорением оптоволоконного Интернета

Объём передаваемых данных в сети Интернет увеличивается с каждым месяцем, и специалистам то и дело приходится искать новые способы доставки трафика между континентами. В настоящее время таких способов два – дорогой спутниковый Интернет и не менее дорогие трансокеанические оптоволоконные магистрали. Их число непрерывно увеличивается, но проблема заключается в сравнительно медленной прокладке и немалой стоимости. Facebook и Nokia нашли способ повышения производительности каждого отдельного канала связи, увеличивая их пропускную способность почти в 2,5 раза. При массовом внедрении технологии удастся более эффективно использовать уже проложенные оптоволоконные каналы связи (InternetUA).

Суть технологии заключается во внедрении квадратурной модуляции, которая обеспечивает существенный прирост скорости. При тестировании на коммерческом оптоволоконном канале протяженностью 3 400 мили между Нью-Йорком и Ирландией, на коммерческих линиях получилось увеличить скорость до 200 Гбит/с. В экспериментальной сети скорость возросла до 250 Гбит/с. Сообщается, что квадратурная модуляция потенциально способна приблизить скорость к максимальному пределу оптоволокна. В будущем Facebook и Nokia хотят увеличить скорость передачи данных по оптоволоконному каналу связи до невероятных 32 Тбит/с.

***

27.03.2017

Snapchat обойдет по популярности Twitter и AOL среди рекламодателей

По данным исследовательской компании Ampere Analysis, приложение будет более популярно чем Yahoo и AOL к 2020 г. Исследование предполагает, что доход сервиса составит более 3 млрд долл. в год к концу 2019 г. Прогнозы основаны на популярности сервиса среди молодежи: 51 % пользователей Snapchat видео – молодые люди до 24 лет, в отличие от Facebook и YouTube, где эта цифра составляет 23 и 17 % соответсвенно. Аналитики предполагают, что рекламодатели будут рады новым возможностям, учитывая существующую монополию Facebook и Google, которым принадлежит 58 % 141 млрд долл. глобального рекламного рынка. Ранее глава WPP М. Соррелл говорил о потенциале приложения стать «третьей силой», но многие инвесторы и аналитики до сих пор относятся с подозрением к будущему Snapchat. Акции основного капитала Snap возросли с 17 млрд до 26 млрд долл. в первые два дня торгов после выхода на IPO ранее в этом месяце, но затем остались на 19 млрд долл. У приложения сильная конкуренция со стороны Instagram, который запустил конкурента Stories в прошлом году. Ранее в этом месяце Snapchat объявил о сделке с MGM по разработке и созданию оригинального контента для платформы Discover наряду с существующими партнерами BBC, Buzzfeed, ESPN и NBC (Marketing Media Review).

***

27.03.2017

Zenith Media: Расходы на онлайн-рекламу впервые обойдут ТВ в 2017 году

Новый отчет Zenith Media прогнозирует рост расходов на рекламу в Интернете на 13 % в 2017 г. Онлайн-реклама привлечет 36,9 % всех рекламных расходов в этом году, по сравнению с 34 % в 2016 г. Самый быстрый рост в онлайн-рекламе приходится на социальные медиа – их средний рост составит 20 % к 2019 г. и достигнет £43.8 млрд. Этот рост может замедлиться из-за кризиса доверия Google. Несколько крупнейших рекламодателей, включая Havas Group UK, L'Oréal, AT&T и Verizon сняли рекламу с YouTube в ответ на опасения размещения рекламы рядом с экстремистским контентом. Тем не менее, президент Zenith уверен в росте онлайн-рекламы. Прогноз предполагает дальнейший рост рекламного рынка со скоростью 4–5 % в год до 2019 г. (Marketing Media Review).

***

27.03.2017

Ірина Коркішко

Facebook допоможе виміряти ефективність крос-медійних кампаній

Facebook у партнерстві з Nielsen допоможуть рекламодавцям виміряти ефективність крос-медійних кампаній. Компанія Nielsen Catalina Solutions представила нове рішення, що дасть змогу виміряти цю ефективність з точки зору продажів. Facebook виступив партнером по запуску. Про це пише ncsolutions.com (Watcher).

Тепер рекламодавці зможуть зрозуміти, які кампанії, що мають рекламу в Facebook та на телебаченні, впливають на ріст продажів. Також вони зможуть виміряти окупність витрат на рекламу таких кампаній.

У Nielsen Catalina Solutions зауважують, що для розуміння ефективності реклами з різних джерел, критично важливо знати внесок кожного з них в отримані результати. А також, чи є ефект від об'єднання цих медіа. У свою чергу, розуміння механізму дублювання необхідно для визначення справжнього охоплення аудиторії.

СОЦІАЛЬНІ МЕРЕЖІ І ПРОБЛЕМИ СУСПІЛЬНОЇ БЕЗПЕКИ

Інформаційно-психологічний вплив мережевого спілкування на особистість

17.03.2017
Люди, які багато користуються соцмережами, є самотніми

Можна подумати, що соціальні медіа дають змогу нам мати цілодобовий контакт з нашими близькими, але нове дослідження виявило, що насправді вони змушують нас почуватися самотніми (Закарпатські новини).

У доповіді йдеться: якщо ви проводите у соціальних мережах понад дві години, ваші шанси почути себе у соціальній ізоляції вдвічі вищі, – інформує zik.ua з посиланням на The Independent.

У дослідженні, проведеному Університетом Піттсбурга, США, вчені опитали 1,787 дорослих у віці від 19 до 32 років про їх використання 11 найпопулярніших сайтів соціальних медіа: Facebook, YouTube, Twitter, Google Plus, Instagram, Snapchat, Reddit, Tumblr, Pinterest, Vine і LinkedIn.

Вони виявили, що люди, які відвідують соціальні мережі більше 58 разів на тиждень, у три рази мають більше шансів відчути себе самотніми, ніж ті, хто заходить на сайти максимум 9 разів.

Уже давно існувала думка, що соціальні медіа сприяють зростанню Синдрому втраченої вигоди, але це дослідження показує, що проблема може бути більш серйозною.

Однак не зрозуміло, чи соціальні медіа викликають самотність, або чи вже самотні люди схильні довший час витрачати на соціальні мережі.

«Ми ще не знаємо, що з'явилося першим – використання соціальних засобів масової інформації або почуття соціальної ізоляції», – сказав співавтор дослідження Е. Міллер, професор педіатрії в Університеті Піттсбурга.

«Цілком можливо, що молоді люди, які відчували себе соціально ізольованими, звернулися до соціальних медіа. Або ймовірно, що їх ширше використання соціальних засобів масової інформації якимось чином призвело до почуття ізольованості від реального світу».

Дослідження показує, що чим більше хтось витрачає на соціальні медіа, тим менше часу у них лишається для реального життя і соціальних взаємодій, що лише призводить до загострення проблеми.

Так само, як кількість самогубств і проблем з психічним здоров'ям збільшується серед студентів і молодих людей, так і зростає роль соціальних медіа.

«Ми за своєю природою істоти соціальні, але сучасне життя має тенденцію розділяти нас замість того, щоб єднати», – сказав професор Б. Прімак зі школи медицини Університету Піттсбурга.

«Хоча може здатися, що соціальні медіа відкривають нові можливості, щоб заповнити цю соціальну порожнечу, я думаю, що це дослідження показує, що вони не можуть бути рішенням, на яке люди сподівалися», – додав він.

***

19.03.2017

Експерти розповіли, як впливають на самооцінку чужі фото в соцмережах

Виявляється, ретельно відфотошоплені світлини моделей та актрис, які ми бачимо у глянцевих журналах, не відображаються на нашій самооцінці так сильно, як фотографії друзів у соцмережах (Радіо Максимум).

Дослідники з'ясували, що жінки більш схильні порівнювати себе з подругами, аніж із жінками, яких бачать у рекламі, по телевізору тощо. І коли це відбувається у соцмережах, то порівняння не на свою користь вражає людину більше, пише The Guardian.

Проблема негативного впливу на самооцінку пересічних людей зображень худих моделей та відфотошоплених красунь у журналах існує впродовж десятиліть, але дедалі більше тривоги в спеціалістів нині викликають соцмедіа. Варто враховувати й те, що й там далеко не всі фото – правдиві.

Приблизно 70 % жінок, віком 18–35 років регулярно «покращують» власні фото, перш ніж їх запостити. Те саме робить половина чоловіків цієї вікової групи, повідомила американська організація Renfrew Center Foundation, що спеціалізується на боротьбі з розладами харчової поведінки.

Власне, деякі моделі сучасних смартфонів уже автоматично роблять своїх власників «красивішими» на фото, згладжуючи недосконалості.

Додамо, нещодавно благодійна організація Ditch the Label опублікувала відеоролик, де показано, як молоді люди брешуть та створюють «ілюзію» ідеального життя в соціальних мережах. На своїй сторінці у Facebook організація опублікувала відеоролик, де молоді люди, неправдиво формують свій образ у мережі, таким чином підносячи собі самооцінку.

Як зазначають творці в описі відео, що всі ми прибріхуємо в мережах, проте чи не зайшло це занадто далеко?

***

20.03.2017

Смертельна гра з Росії поширилась і на Польщу

Смертельна гра для підлітків «Синій кит» з Росії дійшла до Польщі. Окружна прокуратура у Щеціні розпочала слідство у справі щодо схилення

трьох дітей до самогубства, здійсненого через Інтернет (Західна інформаційна корпорація).

Три випадки самокалічення в результаті участі у цій грі зафіксовано у Західнопоморському воєводстві Польщі на північному заході країни, – повідомляє tvn24.

Поліція у Щеціні звернулася до оператора однієї з соцмереж, аби він відреагував на появу в мережі цієї гри і намагався цьому протидіяти.

Водночас генпрокуратура Польщі звернулася до міністра освіти А. Залевської з проханням відреагувати на загрозливу ситуацію.

Куратори з питань освіти в усіх воєводствах Польщі повинні будуть попередити про небезпечну гру всі школи, аби вчителі й батьки звертали увагу на поведінку дітей і вчасно виявляли можливу участь дітей у небезпечній грі.

***

21.03.2017

Перші учасниці «Синього кита» з'явилися на Сумщині

Поранення на руках виявили медики під час огляду двох учениць у Лебединській школі. Про це повідомляють у прес-службі поліції Сумської області (СпецКор).

Характерні подряпини побачив медперсонал. Про це відразу повідомили правоохоронцям. З дівчатами працівники ювенальної превенції провели розмову та відповідні перевірки. З'ясувалось, що одна з школярок і справді потрапила до такої інтернет-спільноти та отримала від «куратора» завдання видряпати собі на передпліччі лезом певне слово.

Як зазначає С. Тарасенко, дівчина завдання виконала, проте умови гри їй категорично не сподобались. Обдумавши ситуацію, в яку потрапила, вона зрозуміла, що їй це не потрібно, перервала листування, видалила з мережі свою сторінку й контент. Що ж стосується іншої учениці, то вона подряпала собі руку просто «за компанію» з однокласницею.

Наразі з обома ученицями та їх батьками вже провели відповідні бесіди. За фактом працівники поліції відкрили кримінальне провадження за ознаками «Доведення до самогубства». Тривають перевірки встановлюються всі обставини події та особа «куратора».

Працівники поліції у свою чергу радять батькам приділяти більше уваги психологічному стану дитини, перевіряти її акаунти в соціальних мережах та групи, спостерігати за поведінкою, дивитися, що малює їх «чадо». За інформацією правоохоронців, наразі на території Сумської області не зареєстровали жодного випадку самогубств дітей, пов'язаних із участю у смертельній грі.

***

23.03.2017

На Черкащині школярка видряпала циркулем на руці «Синій кит»

12-річна школярка приєдналася до гри «Синій кит». Встигла виконати кілька перших завдань. Батьки помітили дивну поведінку дитини і звернулися в поліцію. Це сталося у місті Звенигородка Звенигородського району Черкаської області (ВинницаОК).

…Дівчинка самостійно відмовилася від участі у грі. Але продовжувала слідкувати за новинами групи.

З дитиною почав працювати психолог. Вона має нестабільний психологічний стан.

Законодавчих підстав для покарання винних у поліції немає.

***

27.03.2017

На Днепропетровщине админы «Синего кита» угрожают детям расправой над родителями

Подталкивающие детей к совершению суицида администраторы «смертельных групп» «ВКонтакте» придумали новый рычаг воздействия не неокрепшую психику подростков (InternetUA).

Кураторы подростковых суицидальных групп сайта «ВКонтакте» угрожали детям убить их родителей. Об этом сообщает «Днепр Вечерний». По словам издания, начальник отдела ювенальной превенции управления превентивной деятельности ГУ ЧП в Днепропетровской области А. Голубятников рассказал, что на прошлой неделе на телефон 102 позвонили двое мальчиков, один из Днепра, другой из города Марганец.

Дети сообщили о том, что с ними связались администраторы сайтов «ВКонтакте» и угрожали убийством родителей в случае, если ребята не приступят к выполнению задач смертельной игры.

***

28.03.2017

SMS негативно влияют на способность студентов концентрировать внимание

Студенты, часто отправляющие на занятиях сообщения, испытывают трудности с концентрацией внимания и в итоге имеют плохую успеваемость, установили ученые Университета Питтсбурга, пишет The Times of India (InternetUA).

Эксперимент и опрос группы студентов показал: в среднем за 50-75 минут лекции студент прочитывал 2,6 сообщения. А отправлял 2,4 SMS во время занятий. Притом, была выявлена прямая связь между способностью длительно концентрировать внимание и самоконтролем. В итоге студент легче воспринимал материал, о чем говорили хорошие оценки.

Среди этих студентов молодые люди реже отправляли или читали SMS во время лекции. А вот неспособность себя контролировать напрямую связывалась с тем, что человек часто отвлекался на сообщения.

Студенты могут думать, будто способны одинаково концентрировать внимание во время лекции, при этом, занимаясь чем-нибудь еще вроде написания SMS. Однако многозадачность удается им не так хорошо, констатируют специалисты.

Маніпулятивні технології

15.03.2017
Шахраї за допомогою Шовковського розводили людей

Екс-воротар київського «Динамо» О. Шовковський став жертвою інтернет-афери: шахраї від імені СаШо у соцмережі Facebook розігрували квартиру в Києві (InternetUA).

У соцмережі Facebook була створена фейковая сторінка О. Шовковського, на якій з'явився пост, згідно з яким екс-динамівець подарує квартиру в Києві. Умови акції полягали в такому: усім охочим узяти участь у лохотроні необхідно лайкнути пропоновану сторінку, а також зробити репост, після чого чекати дива у вигляді квартири.

Варто відзначити, що сам футболіст категорично спростував свою причетність до цієї акції.

***

23.03.2017
На базі «фабрики тролів» з'явився найбільший у Росії медіахолдинг

Найбільшим у Росії медіахолдингом стала група видань, пов'язаних з так званою «фабрикою тролів». Про це йдеться в розслідуванні видання РБК (LB.ua).

Цей холдинг налічує нині 16 видань, два з яких присвячені переважно Україні (nahnews.org і КиевСМИ). Відвідуваність найбільшого порталу групи – Федерального агентства новин (РІА ФАН) – у лютому 2017 р. становила 11 млн осіб, а в цілому по всій групі – 36 млн осіб на місяць. Це більше від аудиторії «РИА Новости» (близько 28 млн) або «Комсомольської правди» (приблизно 33 млн осіб).

ФАН і ще кілька сайтів холдингу з'явилися в 2014 р. і спочатку працювали в будинку № 55 на вулиці Савушкіна в Санкт-Петербурзі. Саме тут базується скандально відома «фабрика тролів», працівники якої за гроші залишають коментарі на підтримку російської влади. У 2015 р. сайти медіахолдингу переїхали в інше місце.

Зараз на сайтах працюють близько 225–250 осіб, середня зарплата журналістів – близько 50–55 тис. рублів (870–950 дол.). Утримання холдингу, за різними оцінками, коштує від 3,1 млн до 4,7 млн дол. Водночас на сайтах групи майже немає реклами, тобто вони майже повністю дотуються власником.

Його імені не називають, але видання натякає, що це ресторатор Є. Пригожин, також відомий як «кухар Путіна».

Восени минулого року російський опозиціонер О. Навальний заявив, що все багатство Є. Пригожина з'явилося від того, що одного разу він у 2001 р. прислуговував В. Путіну у своєму ресторані і сподобався йому. За 15 років після цього звичайний ресторатор пройшов шлях від організації статусних обідів до сервірування церемонії інавгурації В. Путіна і багатомільярдних підрядів на харчування співробітників МНС, московських школярів і військових.

Компанії, пов'язані з Є. Пригожиним, за останні п'ять років отримали в Росії державні підряди на суму понад 200 млрд рублів (понад 3 млрд дол.).

***

23.03.2017

Несколько советов, как распознать фейк в социальных сетях

Фальшивые новостные статьи, особенно в период острого обсуждения политических новостей, стали неотъемлемым атрибутом социальных медиа. Эти сообщения, предназначенные для введения людей в заблуждение, распространяются на различных онлайн-ресурсах. Лишь много позже, если вообще когда-нибудь, читатели узнают, что истории, которыми они делились из лучших побуждений в реальности были чьей-то выдумкой (АРГУМЕНТ).

Публикации вопиюще неправдивых историй не есть чем-то характерным исключительно для цифрового века или даже прежней аналоговой эпохи – чтобы убедиться в этом, достаточно полистать подшивку старых печатных изданий. Но в современном мире всё происходит по-другому: читатель быстро пробегает глазами заголовок в Facebook, нажимает кнопку «Поделиться» – и несколько сотен его друзей делают то же самое. Скорость распространения информации возросла в разы.

Согласно исследованию BuzzFeed за последние три месяца перед выборами в США 20 наиболее искусно подготовленных и полностью выдуманных новостей на Facebook превзошли по охвату аудиторию 20 лучших реальных историй из нескольких наиболее именитых СМИ. Впрочем, не всё так плохо – аналитики уже разработали методику, позволяющую проверить достоверность информации и предотвратить публикацию статьи, которая состоит из ложных фактов. И теперь платформы социальных сетей будут вынуждены решить многие вопросы, включая уровень редакционного контроля и проверки контента для применения на своих платформах.

Facebook уже занимается разработкой способов обнаружения и удаления некоторых типов поддельных новостей. Google тоже заявила, что планирует

запретить участие сайтов с фальшивыми новостями в их сервисе продажи рекламы. Отчасти задача пресечения распространения ложных слухов и дезинформации ложится и на читателей. Ведь именно они неосмотрительно пересылают такие статьи друзьям и родным или публикуют их в социальных сетях, поддерживая популярность и доверие к новостям-фальшивкам.

Чтобы предотвратить подобные эпидемии фейков приведём краткое руководство, как распознавать ложные новости.

Читайте текст под заголовком

Одна из причин распространения фальшивых новостей заключается в том, что перед тем, как поделиться статьёй, занятые читатели не продвигаются дальше заголовка или первого абзаца. Авторы поддельных новостей иногда пользуются этим, помещая в начало рассказа правдивые данные, а далее дополняя его откровенно ложной информацией.

В иных случаях, прочтение статьи даёт возможность понять, что изложенная история действительно не имеет ничего общего с заголовком или же в ней отсутствует какое-либо подтверждения фактов.

Проверяйте источник публикации

Незнакомые сайты со множеством рекламных объявлений и заголовками из больших букв должны сразу вызвать скептицизм. Найдите этот сайт в Google и просмотрите другие статьи на таком ресурсе. Это поможет определить, заслуживает ли он доверия.

Внешний вид большинства сайтов, распространяющих фейковые новости, сразу же подтолкнёт вас к мысли, что это – пародия на серьёзный новостной ресурс. Они либо не содержат фактической информации, либо созданы с целью имитировать крупные новостные агентства. Проверьте названия URL-страниц, которые выглядят подозрительно и убедитесь, что это не сайт-обманщик, который пытается выглядеть, как надёжный источник.

Проверьте дату и время публикации

Ещё одним распространённым элементом в поддельных новостях является то, что старые статьи или репортажи о событиях могут вновь появиться на страницах СМИ и убедить людей в том, что такие события только что произошли. Проверка даты и времени публикации поможет быстро предотвратить обман.

Иногда для выяснения времени, когда реально произошло описываемое событие придётся проделать больше работы, например, если дата статьи является актуальной, но описанные события – старые. Пройдитесь по ссылкам и внимательно проанализируйте, когда это событие произошло на самом деле.

Кто автор?

Идентификация автора статьи позволит узнать много любопытного об источнике новости. Анализ других статей этого автора покажет, является ли он признанным журналистом или же имеет репутацию обманщика.

Проверьте ссылки на первоисточник

Отсутствие ссылок или источников в статье означает, что сообщение, скорее всего, ложное. Вместе с тем иногда в фейковых статьях могут

содержаться многочисленные ссылки на другие сайты – это создаёт видимость правдивой новости, однако эти другие сайты также распространяют дезинформацию. Убедитесь, что информация на других сайтах, которая подтверждается ссылками действительно поступает из надёжных источников.

Изучите цитаты и фотографии

Авторы поддельных новостей специализируются также на выдумке ложных цитат, даже приписывая их известным общественным деятелям. Скептически отнеситесь к шокирующим или подозрительным изречениям и поищите их упоминание на других сайтах.

Также, несложно сфотографировать человека на одном мероприятии и заявить, что фото сделано в другом месте. Все знают, что изображения можно ретушировать, редактировать и создавать вовсе новые образы с помощью графических редакторов. Просмотр фотографий в поиске через Google или инструментарии типа TinEye поможет изучить «историю» изображения.

Остерегайтесь эмоциональных заявлений

Людей часто привлекают те истории, которые укрепляют их мировоззрение и ощущения в отношении определённых тем. Лживые новости – не исключение, и многие из них предназначены для разжигания эмоций в читателях, делая упор на их предубеждения. Важно проверить, что новостные сюжеты основаны на фактах. Нельзя делиться ими лишь потому, что они поддерживают одну сторону дискуссии или укрепляют ваши уже существующие политические убеждения.

Ищите на нескольких сайтах

Если история выглядит подозрительно или опубликована как главная новость, посмотрите, есть ли аналогичные материалы в других СМИ. Одна-единственная статья из подозрительного источника, в которой сделано громкое заявление, должна рассматриваться с большим скептицизмом. Если нет публикации аналогичной новости в других надёжных каналах – это, вероятнее всего, фальшивка.

Сомневайтесь, прежде чем делиться ссылкой

Владельцы сайтов фальшивых новостей рассчитывают на то, что читателей привлекут их кричащие заголовки, эмоциональные статьи и они поделятся ими через социальные сети. В крайних случаях, распространение этих выдуманных рассказов может выйти из-под контроля и иметь непредсказуемые последствия для тех, кто был замешан в истории.

***

27.03.2017

Российские «тролли» нацелились на выборы во Франции и Германии

Предстоящие выборы во Франции и Германии вполне вероятно могут стать жертвами российских хакеров и «тролей» (trust.ua).

Об этом предупредил член комитета по разведке американского сената М. Уорнер в комментарии телеканалу NBC.

Что мы знаем сейчас, так это то, что Россия вмешалась в выборы в США и пытается сделать то же самое во Франции и Германии, – сказал М. Уорнер.

По его словам, РФ делает это посредством хакерских атак и проплаченных «тролей», которые заполняют информационное пространство фейковыми новостями.

Напомним, что незадолго до начала предвыборной кампании во Франции президент Ф. Олланд признал, что Россия пытается повлиять на французское общественное мнение. Фаворит предвыборной гонки Э. Макрон и вовсе обвинил российские СМИ RT и Sputnik в распространении дезинформации.

Первый тур президентских выборов во Франции назначен на 23 апреля.

Спецслужби і технології «соціального контролю»

16.03.2017
Ірина Коркішко
Німеччина хоче штрафувати соцмережі за «пости ненависті»

Німеччина створила законопроект, що передбачає штрафи для соціальних мереж, таких як Twitter і Facebook, за несвоєчасне видалення забороненого контенту. Під ним маються на увазі пости, що розпалюють ненависть, і фейкові пости. Сума штрафу може сягати 50 млн євро. Про це пише Spiegel (Watcher).

Раніше Facebook, Twitter і Youtube уже погодились притримуватись правил Євросоюзу, спрямованих на боротьбу з розпалюванням міжнаціональних, міжрелігійних та інших видів конфліктів в Інтернеті. У рамках угоди, IT-компанії зобов'язувались цілодобово реагувати на прояви ненависті в мережах і видаляти відповідні публікації.

Влада Німеччини вважає, що соціальні мережі не виконують свої обов'язки належним чином. Якщо запропонований керівництвом держави законопроект буде прийнято, то в разі відсутньої реакції на недопустимий контент у встановлені строки Twitter та Facebook понесуть матеріальну відповідальність.

***

17.03.2017
Ірина Коркішко
ЄС звинуватив Facebook, Google і Twitter у порушенні прав споживачів

Влада ЄС погрожує штрафами Facebook, Twitter та Google за порушення прав користувачів. Про це повідомляє Reuters (Watcher).

Листи з попередженнями про можливі штрафні заходи були направлені керівництву компаній ще в грудні 2016 р. Серед претензій була вимога виключити положення про те, що користувачі можуть подавати позови лише у судах Каліфорнії. Це суперечить європейському законодавству, за яким користувачі мають право подавати позови до компаній за місцем проживання. Додатково, особливі претензії викликає підхід компаній до спонсорського контенту і відсутність права користувачів розірвати угоду про користування соцмережами.

Упродовж місяця Facebook, Twitter і Google повинні змінити умови використання соціальних мереж. У протилежному випадку на них буде накладено штраф.

***

22.03.2017

Twitter заблокировал более 376 тысяч аккаунтов за «пропаганду экстремизма»

Общее количество заблокированных аккаунтов достигает 636 тыс. (Зеркало недели. Украина).

Сеть микроблогов Twitter заявила о том, что во второй половине 2016 г. она заблокировала 376 тыс. аккаунтов из-за «пропаганды терроризма». Как сообщает «Радио свобода», этот показатель возрос на 60 % по сравнению с предыдущим годом.

Последняя волна блокировки привела к тому, что общее число заблокированных аккаунтов достигло отметки в 636 тыс., начиная с августа 2015 г., когда Twitter активизировал работу по борьбе с экстремизмом.

Twitter и Facebook находились под давлением правительств многих стран мира, которые настаивали на блокировке боевиков, которые использовали платформы для привлечения новых членов экстремистских группировок и координации нападений.

***

21.03.2017

Разоблачены 10 администраторов антиукраинских групп, которыми управляли из России

За полтора месяца сотрудники СБУ разоблачили 10 администраторов антиукраинских сообществ в социальных сетях, деятельность которых координировалась российскими спецслужбами, сообщили в пресс-центре ведомства (Аналитическая служба новостей).

Отмечается, что поддерживали антиукраинские ресурсы жители Киевской, Харьковской, Днепропетровской, Черниговской, Закарпатской и Луганской областей.

«По указанию кураторов за материальное вознаграждение они преимущественно наполняли ресурсы в российских соцсетях. Администраторы выкладывали полученные из России материалы с призывами к антиконституционному устранения действующей власти, об изменении границ Украины, проведения различных протестных акций, в том числе с использованием массовых беспорядков», – рассказали в СБУ.

У администраторов сообществ провели обыски, изъяли компьютеры с доказательствами получения антиукраинских материалов от российских спецслужб.

***

22.03.2017

На Чернігівщині СБУ викрила адміністратора антиукраїнських груп у соцмережах

На Чернігівщині співробітники Служби безпеки України викрили мешканця обласного центру, який адміністрував антиукраїнські групи в російських соціальних мережах (InternetUA).

У 2016 р. непрацюючий чернігівець через соцмережі познайомився з жінкою, яка проживала на непідконтрольній Україні території в Донецькій області. Від неї він отримав пропозицію за матеріальну винагороду поширювати в мережі Інтернет матеріали, в яких дискредитувалась українська держава та Збройні сили України, популяризувалась діяльність терористичних організацій «ЛНР/ДНР», містилися заклики до антиконституційного усунення діючої влади та зміни кордонів України.

Пропагандистські «агітки», які систематично надходили від спільниці терористів через особисті повідомлення, зловмисник викладав у групи в російських соціальних мережах.

Кошти за виконану адміністратором роботу перераховувались кураторами на картку одного з родичів.

Під час обшуку за місцем проживання зловмисника правоохоронці вилучили комп’ютерну техніку з доказами здійснення антиукраїнської діяльності.

Агітатору оголошено про підозру у скоєнні злочинів, передбачених ст. 109 (дії, спрямовані на насильницьку зміну чи повалення конституційного ладу або на захоплення державної влади) та ст. 110 (посягання на територіальну цілісність і недоторканість України) Кримінального кодексу України. Триває досудове слідство.

***

22.03.2017

В Китае заблокировали соцсеть «Одноклассники»

Пользователи, находящиеся на территории Китая, сообщают, что несколько дней назад власти страны заблокировали доступ к социальной сети «Одноклассники» по адресу ok.ru. В то же время мобильное приложение соцсети по-прежнему работает, как и домен odnoklassniki.ru (InternetUA).

Так, по данным сервиса BlockedInChina, доступ к российской социальной сети ограничивается в Пекине, Шеньчжэне, провинциях Хэйлунцзян и Юньнань, а также во Внутренней Монголии. Сервис GreatFirewallOfChina подтверждает, что на данный момент ресурс ok.ru в этих регионах заблокирован. В то же время аналогичная проверка показывает, что домен odnoklassniki.ru блокировке в Китае пока что не подвергается.

Представители соцсети подтвердили факт блокировки. «Да, это так. Однако в Гонконге, где присутствует основная часть нашей аудитории в Китае, “Одноклассники” работают. Причины выясняем», – сообщили VC.ru в пресс-службе социальной сети. При этом данные о количестве пользователей в Китае в компании не раскрыли.

***

24.03.2017

В WikiLeaks рассказали, как ЦРУ взламывает «айфоны» и «макбуки»

Организация WikiLeaks опубликовала очередную порцию документов, принадлежащих Центральному разведывательному управлению США. В архиве, в частности, описываются методики, к которым прибегали спецслужбы для взлома смартфонов и ноутбуков компании Apple (U-News).

Оказалось, что разведка США на протяжении многих лет искала «дыры» в продукции i-производителя, включая iPhone и MacBook. В «киберарсенал» ЦРУ, например, входил инструмент под названием Sonic Screwdriver («Ультразвуковая отвертка»), который использовался для заражения «макбука» через порты USB или Thunderbolt.

Другие эксплойты, в целях наблюдения за владельцем компьютера, записывались непосредственно в прошивку, что делало их незаметными при помощи обычных экспертно-криминалистических техник. iOS экспертам ЦРУ было взломать сложнее: в документах идет речь только об одном «маячке», который устанавливался на iPhone перед его покупкой.

7 марта WikiLeaks выложил в свободный доступ информацию о лазейках, которыми пользовались спецслужбы США для получения доступа к «айфонам» и Android-устройствам, а также компьютерам под управлением Windows и «умным» телевизорам Samsung. В ЦРУ отказались комментировать достоверность утечки, однако эксперты признали подлинными техники взлома, которыми пользовалась разведслужба США в 2013–2016 гг.

К моменту публикации архива некоторые компании, включая производителя «айфонов», заявили, что большая часть «дыр» уже была устранена в последних версиях операционных систем.

***

27.03.2017

Британский министр пожаловалась на шифрование в Мессенджерах

Министр внутренних дел Великобритании Э. Радд выступила против шифрования в Мессенджерах, включая WhatsApp, поскольку это мешает расследованию преступлений. Об этом она рассказала в интервью BBC News (InternetUA).

Э. Радд заверила, что власти не требуют от создателей защищенных приложений открывать им полный доступ к данным пользователей. Но в случае террористических атак IT-компании обязаны раскрывать информацию о подозреваемых, особенно в случаях, когда те использовали свои мобильные телефоны для координации и планирования действий.

«Для террористов не должно существовать мест, где бы они могли укрыться. Мы должны быть уверены, что WhatsApp и десятки других похожих приложений не обеспечивают для злоумышленников места, где они могли бы общаться друг с другом», – заявила глава ведомства.

Э. Радд также подчеркнула, что руководство WhatsApp обязано сотрудничать со спецслужбами для предотвращения терактов.

***

27.03.2017

План «Большого брата»: как государство собирается следить за украинцами

За последний месяц в Украине появилось сразу несколько инициатив, позволяющих государству еще пристальнее следить за частной жизнью граждан. Чиновники пытаются установить контроль над распространением информации в Интернете и добыть у операторов связи больше данных об абонентах. В условиях войны такие меры объясняются необходимостью защищать информационное пространство страны и вычислять преступников. Как далеко может зайти «Большой брат» – в материале РБК-Украина (InternetUA).

Блок-пост в Интернете

С началом войны на Востоке Украины государство стало уделять больше внимания вопросу информбезопасности. Появилось Министерство информации, отвечающее за информационную политику. Фильмы и сериалы, которые попадают на телеэкраны, тщательно проверяются Национальным советом по вопросам телерадиовещания на предмет пропаганды российских спецслужб. Чиновники также мониторят новостные блоки украинских телеканалов и радиостанций на наличие в эфире людей и высказываний, которые могут нести угрозу информационной безопасности страны.

Если контролировать ТВ-пространство у государства получается, то Интернет по-прежнему остается тем местом, где информация распространяется бесконтрольно. Попытки закрыть сайты с контентом, нарушающим закон, обычно проваливаются и только создают проблемы законопослушным компаниям. Например, в апреле 2015 г. в поисках оборудования, на котором размещалось несколько сайтов сепаратистской направленности, СБУ изъяла сервера регистратора доменных имен NIC.UA. На работе сепаратистских сайтов это никак не сказалось, но при этом пострадали десятки тысяч клиентов регистратора, включая государственные учреждения и органы местного самоуправления.

Такие примеры не единичны и создают резонанс в обществе. Правоохранителей обвиняют в некомпетентности и нанесении ущерба легальному бизнесу. Поэтому государство ищет более легкие для себя пути «контролировать Интернет». А именно, пытается переложить функции по блокировке контента на поставщиков интернет-услуг – операторов и провайдеров.

На заседании 10 марта Кабинет Министров утвердил план мероприятий по реализации стратегии кибербезопасности Украины, согласно которому в государстве будет внедрена процедура блокировки сайтов интернет-провайдерами по решению суда. Пока что речь не идет о конкретных сроках, в апреле МВД и Нацполиция лишь должны подготовить нормативную базу для такого решения. Но провайдеры уже бьют тревогу.

Интернет Ассоциация Украины (ИнАУ), объединяющая более 130 компаний, в своем открытом заявлении назвала такие меры инструментом политической цензуры. При этом в ассоциации считают, что блокировка сайтов провайдерами не поможет бороться с распространением незаконного контента. Ведь все современные технические методы интернет-цензуры легко обходятся путем настройки стандартного программного обеспечения на компьютере (VPN, TOR, Proxy и т. д.). Те, кто ищет запрещенный контент, найдут, как получить к нему доступ – это показывает практика и Китая, и России, где интернет-пользователи массово устанавливают программы-анонимайзеры, чтобы обойти цензуру.

Вместе с тем программы для обхода цензуры меняют сетевые данные. Это значит, что при расследовании преступлений, совершенных с помощью сети, станет сложнее вычислять преступников. В ИнАУ утверждают, что единственным направлением в мире, где интернет-механизм цензуры оказался эффективным, является влияние на широкое общественное мнение и электоральные предпочтения населения за счет сужения круга распространения «нежелательной» информации. «Учитывая вышесказанное, мы склоняемся к выводу, что истинные цели внедрения интернет-цензуры в Украине – сугубо создание политической цензуры. ИнАУ желает видеть Украину в развитии сетевых технологий рядом с такими странами, как США, Япония, Германия, а не рядом с Россией, Ираном, Северной Кореей», – говорится в заявлении ассоциации.

Нежелание провайдеров блокировать контент можно объяснить и еще одной причиной – экономической. Ведь затея правительства обойдется не дешево. Как рассказывает учредитель киевской сети провайдера «Триолан» В. Сидоренко, невозможно блокировать доступ к сайтам без анализа трафика. А соответствующее оборудование, при объемах «Триолана» обойдется ему в сумму до миллиона долларов.

Кроме того, появление анализаторов трафика приведет к уменьшению скорости у абонентов. «Абонент не сразу будет попадать на ресурс, а только после того, как его трафик пройдет анализ», – объясняет В. Сидоренко.

Традиционно любое увеличение затрат провайдеров ложится на плечи абонентов в виде повышения абонплаты. Получается, что украинцы сами же заплатят за снижение скорости Интернета и «урезанный» доступ к информации.

Без суда и следствия

Государство хочет не просто контролировать распространение информации в Интернете, но и легко вычислять пользователей, которые выкладывают в сеть запрещенный контент. Согласно принятому Кабмином плану, уже этой весной МВД, Нацполиция, СБУ и Минюст должны подготовить свои предложения по имплементации в Украине конвенции кибербезопасности, которую наше государство ратифицировало еще в 2006 г. В конвенции говорится, что страны, подписавшие ее, должны принять меры по хранению и передаче компетентным органам компьютерных данных, включая данные о посещаемых пользователями сайтах. Конвенция описывает общие подходы, но каждая страна сама решает, как их имплементировать. «Мы не знаем, какие документы на выходе будут у нас», – говорит руководитель телекоммуникационной компании «ИМК» А. Федиенко. По его словам, сейчас провайдеры в Украине вообще не хранят у себя информацию о пользователях. «Сейчас оператор начинает собирать данные о пользователе только тогда, когда к нему приходит СБУ с соответствующим судебным решением. Закон обязывает операторов устанавливать специальное оборудование для этого, но не обязывает самостоятельно покупать это оборудование и постоянно собирать данные», – рассказывает А. Федиенко. По его мнению, существующая схема взаимодействия со следствием прекрасно работает.

Он предполагает, что в рамках имплементации конвенции операторов обяжут устанавливать на своей сети и за свои деньги оборудование для анализа трафика. Но, скорее всего, обяжут не всех, а только тех, кто заводит трафик в Украину, то есть, крупных операторов с собственными внешними интернет-каналами. На этом этапе может появиться коррупционная составляющая: если, например, операторов обяжут закупать оборудование у одного поставщика или платить за выдачу разрешений, сертификатов или других «бумажек». Поэтому, как считает А. Федиенко, государству стоит определиться с методикой, какие данные и как долго хранить. А оператор уже сам выберет, каким образом и на каком оборудовании это будет делаться.

Гораздо более опасной инициативой операторы и провайдеры считают законопроект № 6079 о решении проблемных вопросов антитеррористической

операции и усиления борьбы с терроризмом, который сейчас находится на рассмотрении парламента. Согласно этому законопроекту, операторы и провайдеры должны будут выдавать следователю или прокурору персональные данные абонентов всего лишь по запросу. Это данные о типе предоставленных телекоммуникационных услуг (звонки, интернет-доступ), их длительности, содержанию, маршрутах передачи информации (например, сайтах, куда заходил пользователь).

Сейчас операторы предоставляют следствию доступ к некоторым из этих данных, но только по решению следственного судьи. Например, операторы мобильной связи хранят информацию о фактах соединения за последние три года. При этом к содержанию разговоров и сообщений у них вообще доступа нет, такая информация нигде не хранится.

Как рассказали в пресс-службе оператора Vodafone Украина, выдача решения судьи обычно занимает две-три недели. Законопроект же позволяет прокурору или следователю получить такое решение постфактум. «Что будет с уже предоставленными данными, если такое решение не будет получено?», – спрашивают в компании. В случае отказа, согласно законопроекту, полученные данные не смогут использоваться как доказательство по делу. Тем не менее, весь этот механизм создает предпосылки для злоупотребления со стороны следователей и прокуроров, которые безнаказанно смогут получить всю известную оператору информацию о каждом абоненте.

В законопроекте говорится, что выдача данных по запросу возможна в исключительных случаях, связанных со спасением людей и противодействием тяжким и особо тяжким преступлениям. Впрочем, как замечают в Интернет ассоциации Украины, под это определение попадает почти все уголовное законодательство страны. «Мы только за борьбу с терроризмом. Но мы против того, чтобы была внесудебная практика», – говорит А. Федиенко.

Как считают в компании lifecell, в законопроекте необходимо прописать те исключительные случаи борьбы с терроризмом, в которых данные об абонентах будут раскрываться без решения судьи. Также необходимо ввести ответственность за доступ к информации в случае, если разрешение суда так и не будет выдано.

«Защищенный» Интернет для государства

Одновременно с попытками залезть в интернет-жизнь граждан чиновники «строят» собственную информационную крепость.

Утвержденный Кабмином план предусматривает построение защищенного от кибератак дата-центра (ЦОДа) под нужды государственных органов. Прежде всего, для сектора безопасности и обороны, финансового, энергетического и транспортного секторов.

«Конечно, дата-центры должны быть неотъемлемой частью критической инфраструктуры государства. Но в этом случае ЦОД – это последняя “проблема” во всей цепочке кибербезопасности государства», – считает руководитель компании De Novo М. Агеев.

По его словам, защита данных обеспечивается на многих уровнях. Можно построить очень надежный ЦОД, но перенести туда «кривое» приложение, которое поставит всю безопасность под угрозу. «Насколько мне известно, львиная доля информационных систем в государственных органах дырявые и ветхие», – рассказывает М. Агеев. Он считает, что кусок задачи, касающийся обеспечения работы защищенного дата-центра, можно решить силами коммерческих компаний на базе действующих дата-центров. Это дало бы огромную фору во времени и позволило бы сэкономить государственные деньги.

О характеристиках самого дата-центра, его архитектуре или задачах, которые он должен выполнять, в плане по реализации стратегии кибербезопасности ничего не говорится. Поэтому стоимость такого проекта оценить пока сложно. Но, как считает М. Агеев, счет будет идти на десятки миллионов долларов, а то и до сотни дойдет.

Помимо дата-центра, планируется также создание и развитие национальной телекоммуникационной сети, и подключение к ней государственных органов, ведомств, организаций. Это должен обеспечить лучшую защиту госведомств от прослушки, хакерских атак и других вмешательств в сеть. Но по факту государственные деньги могут осесть в карманах чиновников, как это случалось ранее.

Дело в том, что основа для государственного оператора – телекоммуникационная сеть специального назначения – уже построена компанией «Укртелеком». Еще до 2013 г. «Укртелеком» должен был передать эту сеть государству, которое, в свою очередь, должно было обеспечить в госорганах техническую возможность работы с этой сетью. Под эти нужды еще во времена президентства В. Януковича было выделено 220 млн грн. Но инфраструктура так и не была построена, а деньги «испарились». Таким образом, государство не смогло принять сеть специального назначения на свой баланс. По данному факту возбуждено уголовное дело о хищении госсредств экс-президентом, а «Укртелеком» и Государственная служба специальной связи и защиты информации до сих пор судятся за то, кто из них должен достраивать недостающую сеть доступа к телекомсети специального назначения.

Еще один пункт плана по реализации киберстратегии – это стимулирование разработки в Украине своего программного обеспечения вплоть до собственной операционной системы. Как считает руководитель компании Berezha Security и специалист по информационной безопасности В. Стыран, подобные инициативы создают предпосылки для «бессмысленного распила» государственных средств. Ведь в мире достаточно именитых компаний, продукты которых могли бы использоваться для защиты киберпространства Украины. И совсем не обязательно «изобретать велосипед».

Параллельно Кабмин собирается ввести запрет для компаний, связанных с Россией, на участие в любых мероприятиях по обеспечению кибербезопасности Украины. Запрет на использование программного обеспечения российских производителей в украинских госорганах уже

существует. Впрочем, по данным РБК-Украина, представители компаний с российскими корнями иногда участвуют в защите Украины от кибератак в качестве консультантов.

В украинской компании «Zillya! Ативирус» считают, что лучшим стимулированием разработки украинских программ станет формирование честного и открытого рынка, при котором компании будут готовы бороться в рамках четко прописанных стандартов за право продавать свой софт госорганам. «Создание программных продуктов требует серьезных вложений, ресурсов и времени. Например, в такой сфере как антивирусная защита, только по предварительным расчетам, создание антивирусного софта корпоративного уровня с нуля или на базе украинских разработок, может занять до 1,5-2 лет и будет стоить порядка 1–2 млн долл. Что несет за собой высокие риски окупаемости», – рассказывает руководитель отдела продаж и маркетинга «Zillya! Ативирус» М. Сидоренко.

Он напоминает, что государство не первый год декларирует подобные намерения, в то же время пока дальше слов дело не заходит. Вот и сейчас в Стратегии не говорится о конкретных практических шагах, достижении результатов и получении конкретного продукта на выходе. Стратегия только говорит о том, что Государственное агентство по вопросам электронного правительства и Администрация Госспецсвязи должны ко II кварталу «сформировать предложения» по господдержке разработки.

Проблема захисту даних. DDOS та вірусні атаки

15.03.2017

Протурецкие хакеры атаковали Twitter из-за конфликта с Нидерландами

Протурецкие хакеры в 15 марта атаковали сеть микроблогов Twitter, взломав аккаунты различных ведомств, организаций и компаний, и разместили надписи о «нацистской Германии» и «нацистских Нидерландах» (Finance.Ua).

Социальная сеть Twitter подтвердила информацию о хакерских атаках.

«Мы знаем о проблеме, которая сегодня утром зацепила определенное количество владельцев аккаунтов», – заявил пресс-секретарь Twitter, добавив, что источник атаки был связан со сторонним приложением, чьи данные были удалены.

Отмечается, что на страницах взломанных аккаунтов хакеры разместили записи со свастикой, хэштеги про «нацистскую Германию» и «нацистские Нидерланды» и фразы «учите турецкий» и «увидимся 16 апреля», подразумевая дату, на которую запланировано проведение в Турции референдума по расширению полномочий президента страны Реджепа Тайипа Эрдогана.

В числе прочих пострадали аккаунты Минэкономики Франции, BBC North America, Amnesty International, UNICEF USA, одного из футбольных клубов Германии и аккаунты известных людей.

По данным агентства Рейтер, сломаны также были аккаунты Европарламента, страница экс-премьер-министра Франции А. Жюппе, министерства здравоохранения Великобритании, Die Welt, Forbes и др.

***

15.03.2017

В Интернете обнаружен «Twitter для шпионов»

Не так давно портал WikiLeaks начал публикацию секретных материалов ЦРУ. Файлы предположительно были получены из малоизвестного сервиса Intellipedia, предназначенного для сотрудников американских спецслужб и являющегося своеобразной «шпионской Википедией». Мало кто знает, но помимо собственной онлайн-энциклопедии, у разведчиков есть и специализированная социальная сеть – «шпионский Twitter» под названием eChirp (Internetua).

По данным журналистов Motherboard, eChirp пользуется большой популярностью у сотрудников американских спецслужб. По состоянию на конец 2013 г. соцсеть насчитывала 60 593 пользователя с наивысшим уровнем секретности, 25 344 секретных и 15 468 незасекреченных пользователей. В eChirp было сделано 875 160 совершенно секретных, 51 632 засекреченных и 56 601 незасекреченная публикация.

Курируемый Агентством национальной безопасности США сервис очень напоминает привычный Twitter, однако зарегистрироваться в нем можно только по приглашению. По заверению АНБ, «eChirp идеально подходит для быстрого уведомления о происшествиях».

Сервис является частью Intelink – группы закрытых внутренних сетей, используемых спецслужбами США. Любой сотрудник американской разведки с доступом к Intelink может пользоваться eChirp. Соцсеть позволяет обмениваться ссылками и общаться с коллегами, разделяющими схожие интересы.

Тем не менее, практическое предназначение eChirp не совсем понятно. По словам ИБ-эксперта из Министерства обороны США М. Девоста (Matt Devost), являющегося пользователем сервиса, eChirp полезен настолько, насколько и обычные соцсети. Зачастую подписчики обмениваются ссылками, ведущими в общедоступную Сеть. «Иногда кажется глупым иметь закрытую соцсеть для доступа в обычный интернет», – отметил М. Девост.

***

16.03.2017

Пользователей WhatsApp и Telegram можно обокрасть, прислав одну картинку

В Мессенджерах WhatsApp и Telegram найдена уязвимость, которая позволяет хакеру получить доступ ко всей информации аккаунта. Для этого достаточно прислать жертве картинку, на которую она кликнет. Пользователь WhatsApp узнает о взломе, так как система распознает его как второй сеанс и вышлет предупреждение. Пользователь Telegram не узнает ничего (Internetua).

Уязвимость в WhatsApp и Telegram

В WhatsApp и Telegram обнаружена уязвимость, которая позволяет хакеру завладеть всеми данными пользователя, прислав ему безобидную с виду картинку. Уязвимость присутствует только в онлайн-версиях Мессенджеров – WhatsApp Web и Telegram Web. Благодаря полной синхронизации Мессенджеров на всех платформах, онлайн-версии содержат сообщения, отправленные пользователем из приложения.

Присланное изображение содержит вредоносный код, для его активации жертве достаточно кликнуть на изображение. Картинку хакер может создать любую, в том числе такую, у которой высоки шансы на привлечение внимания пользователя. После клика на изображении хакер получает полный доступ к локальному хранилищу. В его руки попадает вся переписка пользователя, список его контактов, а также фото, видео и другие файлы, которыми он обменивался через Мессенджер. Завладев списком контактов, злоумышленник может разослать вредоносный файл всем собеседникам жертвы от ее имени.

Уязвимость была обнаружена сотрудниками компании Check Point Software Technologies. По словам О. Вануну, главы подразделения Check Point по исследованиям и поиску уязвимостей, найденная уязвимость «подвергла риску полного захвата аккаунты миллионов пользователей». В случае с WhatsApp жертва узнает о взломе, так как Мессенджер идентифицирует атаку как сеанс на другом устройстве, и предупредит пользователя. В случае с Telegram, который позволяет вести одновременные сеансы на разных устройствах, предупреждение не поступит.

Реакция WhatsApp и Telegram

Check Point направил информацию об уязвимости в компании WhatsApp и Telegram, которые подтвердили существование проблемы и выпустили патчи для своих продуктов. Check Point уточняет, что данные были переданы 8 марта 2017 г., и обе компании отреагировали оперативно. Чтобы начать пользоваться новой версией онлайн-мессенджера, достаточно просто перезапустить браузер.

Чтобы устранить уязвимость, WhatsApp и Telegram пришлось доработать механизм проверки контента. Оба Мессенджера пользуются сквозным шифрованием, которое не позволяет кому-либо, кроме участников беседы, получать доступ к сообщениям и файлам. Однако вредоносное изображение шифруется непосредственно отправителем, что не дает Мессенджеру возможности проверить контент. То есть, уязвимость является следствием сквозного шифрования. Внесенные изменения заключаются в том, что теперь контент проверяется до шифровки.

Как это работает в WhatsApp

Механизм загрузки файлов WhatsApp поддерживает несколько определенных типов документов, таких как Office, PDF, аудиофайлы, видео и изображения. Но исследователям Check Point удалось обойти ограничения этого механизма, загрузив вредоносный HTML-документ с легитимным предварительным просмотром изображения, чтобы обмануть пользователя.

Как только жертва пытается открыть документ, веб-клиент WhatsApp запускает API FileReader HTML 5 для создания уникального URL-адреса BLOB. К адресу прикрепляется содержимое файла, отправленного злоумышленником. Далее пользователь перенаправляется по этому URL-адресу.

Веб-клиент WhatsApp хранит допустимые типы документов в клиентской переменной W[“default”].DOC_MIMES. Поскольку зашифрованная версия документа отправляется на серверы WhatsApp, для этой переменной можно добавить новый тип MIME, такой как «текст/html», чтобы обойти ограничение клиента и загрузить вредоносный HTML-документ. После добавления нового типа к клиентской переменной, клиент шифрует содержимое файла с помощью функции encryptE2Media и затем загружает его в зашифрованном виде как BLOB на сервер WhatsApp.

Изменение имени и расширения документа, а также создание поддельного предварительного просмотра путем изменения переменных клиента делает документ более безобидным в глазах жертвы. Кликнув на файле, пользователь увидит забавную кошку в объекте BLOB, которая является объектом FileReader HTML 5 по адресу web.whatsapp.com. Это означает, что злоумышленник может получить доступ к ресурсам в браузере по этому адресу.

При просмотре страницы данные локального хранилища жертвы будут отправлены хакеру, что позволит ему захватить аккаунт. Преступник создает функцию JavaScript, которая будет каждые 2 секунды проверять, появились ли в бэкэнде новые данные, и обновлять украденное им локальное хранилище.

Однако WhatsApp разрешает пользователю вести одновременно только один сеанс в Мессенджере, с какого-то одного устройства. Поэтому программа предупредит жертву, что был запущен второй сеанс, и спросит, какой из них она желает продолжить. Чтобы противодействовать этому, хакер должен дописать небольшой фрагмент кода на JavaScript, который спровоцирует зависание окна браузера у пользователя.

Как это работает в Telegram

Telegram поддерживает несколько типов документов, которые могут отправляться в веб-приложении, но только файлы изображений и видеозаписей хранятся в разделе «Файловая система» в браузере. Исследователям Check Point удалось обойти эту политику отправки файлов и загрузить вредоносный HTML-документ с типом MIME видеофайла «video/mp4». Затем они смогли отправить его жертве по зашифрованному каналу через серверы Telegram. Как только жертва откроет видео в новой вкладке браузера, начнется его воспроизведение, и данные пользователя будут отправлены хакеру.

Клиент Telegram сохраняет тип MIME в объекте t и во время процесса загрузки проверяет, соответствует ли он типу видео или изображения MIME. В случае совпадения файл будет храниться под URI-идентификатором файловой системы. Поскольку зашифрованная версия файла отправляется на серверы Telegram, можно изменить тип MIME на «video/mp4», чтобы обойти ограничение клиента и загрузить вредоносный HTML-документ в Telegram в виде видео.

После изменения типа MIME файла, клиент загружает его в зашифрованном виде на сервер Telegram. Когда пользователь захочет воспроизвести видео, файл html будет загружен в память браузера по адресу web.telegram.org. Пользователь должен открыть видео в новой вкладке, чтобы получить доступ к ресурсу в браузере с URI web.telegram.org. При просмотре видео в новой вкладке данные локального хранилища жертвы будут отправлены злоумышленнику, что позволит ему захватить аккаунт. С функцией JavaScript, которая проверяет бэкэнд, все обстоит так же, как и в случае с WhatsApp.

Поскольку Telegram позволяет пользователю вести одновременно несколько сеансов с разных устройств, жертва не узнает о взломе.

***

16.03.2017
В Google Play обезврежен крупнейший ботнет

Компания Google обнаружила в Google Play Маркете ботнет, который получил название Chamois. Он заражал смартфоны и планшеты пользователей через потенциально опасные приложения и организовывал вредоносную активность (Internetua).

Приложения с Chamois показывали пользователю навязчивую рекламу, скачивали и устанавливали другие приложения и тайно оформляли подписку на контентные услуги, рассылая SMS-сообщения. Вредоносное приложение не отображалось в списке всех установленных приложений, что затрудняло его удаление.

После обнаружения Chamois компании Google пришлось модифицировать принцип работы механизма Verify Apps, поскольку хакеры настроили ботнет таким образом, чтобы встроенный в Google Play Маркет антивирус не находил в приложениях с Chamois, ничего подозрительного. Вирус был написан профессиональными разработчиками и содержал более 100 тыс. строчек запутанного кода. По словам Google, Chamois – один из крупнейших ботнетов, выявленных в Google Play, но теперь он полностью обезврежен.

***

20.03.2017
Американец пытался убить журналиста с помощью Twitter

по материалам: BBC
автор: Анастасия Очеретнюк

Полицейские предъявили обвинение в покушении на убийство жителю штата Мэриленд Джону Рейну Ривелло, арестованному по запросу из Техаса, передает BBC (podrobnosti.ua).

Как утверждают следователи, 29-летний американец послал журналисту Newsweek К. Айхенвальду анимированную картинку, вызвав у него эпилептический припадок.

Федеральное бюро расследований США сообщило, что К. Айхенвальд страдает эпилепсией.

15 декабря 2016 г. Ривелло отправил ему в Twitter аниме, которое содержало стробоскопический эффект, то есть картинка постоянно вспыхивала и гасла. «Посылку» сопровождала подпись: «Ты заслуживаешь припадка за свою запись».

«Увидев вспыхивающую картинку, жертва немедленно испытала припадок», – говорится в сообщении.

Как отмечается, о намерении вызвать припадок Ривелло в личных сообщениях рассказывал и другим пользователям. А в принадлежащем ему аккаунте полицейские обнаружили фальшивый некролог на Айхенвальда, подписанный 16 декабря.

Ривелло искал в Интернете, как вызвать припадок у человека, страдающего эпилепсией. Теперь ему предъявлено обвинение в приставаниях в Интернете.

***

20.03.2017
Incapsula: число DDoS-атак на приложения растет

В IV квартале Incapsula отразила по своей клиентской базе 3603 DDoS-атаки сетевого уровня (на 39,4 % меньше, чем в предыдущем квартале) и 11 727 атак уровня приложений. Из текущих тенденций на DDoS-арене эксперты особо отметили появление мощных ботнетов, составленных из IoT-устройств, и преобладание одновекторных атак, обусловленное низкой стоимостью онлайн-услуг по проведению DDoS (Центр информационной безопасности).

Согласно статистике Incapsula, на атаки сетевого уровня в период с 1 октября по 31 декабря пришлось лишь 23,9 % DDoS-инцидентов. В последние два квартала их доля неуклонно снижается, но мощность растет. Так, накануне Рождества эксперты зафиксировали рекордную для своего сервиса DDoS, которая на пике показала 650 Гбит/с. Самая долгая атака сетевого уровня продолжалась 29 суток, однако 89 % таких DDoS длились не более одного часа.

Из векторов наиболее часто использовался ICMP (46,3 % сетевых атак), на долю TCP пришлось 32,5 %, на SYN flood и UDP flood – 22 и 19,4 % соответственно. Техника атак с отражением и усилением мусорного трафика,

по оценке Incapsula, стремительно теряет популярность в текущем году. В I квартале вклад DDoS с DNS-плечом в общее количество сетевых атак составил 19,4 %, в IV – лишь 9,2 %; доля NTP-атак за год сократилась таким же образом, с 13,6 до 6,9 %. Исследователи объясняют этот спад успешным латанием доступных из Интернета устройств, которые злоумышленники использовали в качестве посредников, а также появлением более привлекательного и не менее мощного орудия – IoT-ботнетов.

DDoS, использующие три вектора и более, тоже становятся редким явлением: в минувшем квартале на их долю пришлось 13,5 % сетевых атак, а вклад одновекторных возрос почти на 7 п. п., до 71 %.

Число атак уровня приложений в отчетный период оказалось рекордным для сетей Incapsula, за квартал их доля возросла на 2,9 %, а за год – почти в два раза. Самая мощная DDoS прикладного уровня на пике показала свыше 91,2 тыс. запросов в секунду, однако высокая мощность для таких атак – не главное, как справедливо отметили исследователи. В большинстве случаев, чтобы положить типовой сервер, хватит и пары сотен запросов в секунду.

Три четверти DDoS уровня приложений продолжались не более одного часа, максимальная длительность составила 47 суток. Более 58 % мишеней были атакованы повторно, 13 % – более 10 раз.

Основным источником вредоносного бот-трафика по-прежнему является Китай. В IV квартале 78,5 % DDoS-потока, направленного на сайты, опекаемые Incapsula, исходило с китайских IP-адресов. Чаще прочих ди-ддосеры атаковали мишени, прописанные в США (56,7 % атак), Великобритании (11,0 %) и Нидерландах (8,6 %).

***

21.03.2017

Начались продажи устройства для клонирования кредитных карт, лежащих в чужом кармане

Хакерская группа CC Buddies начала продажи устройства, позволяющего на расстоянии 15 см моментально «клонировать» кредитные карты, оснащенные RFID-чипами. Устройство легко спрятать под одеждой и очень трудно обнаружить. Свое изделие злоумышленники продают в открытую: сайт доступен всем желающим. Ранее для подобных «сервисов» использовался даркнет (InternetUA).

Большой апгрейд

Группа хакеров под названием CC Buddies начала открытую продажу вредоносного устройства для бесконтактного считывания и клонирования кредитных карт, оборудованных RFID-чипами. Новое устройство способно копировать 21 кредитную карту в секунду.

В 2016 г. те же злоумышленники продавали похожее устройство, но с более скромными характеристиками: их Infusion X5 позволял клонировать до 15 карт в секунду. Для успешного клонирования необходимо было, чтобы

устройство располагалось очень близко от карты – не более 8 см. Новый вариант, получивший название X6, работает с расстояния 15 см.

Близкий недружественный контакт

Для считывания карт требуется тесный контакт с потенциальной жертвой; однако в общественном транспорте в час пик, когда люди вынужденно прижимаются друг к другу, у злоумышленников, вооруженных подобными устройствами, появляется шанс на богатый улов. Шанс этот уже был неплох, когда устройства работали с расстояния 8 см, и тем более хорош он оказывается, когда рабочее расстояние возрастает вдвое.

Само устройство невелико и снабжено крепежом на руку, так что его без труда можно спрятать под длинным рукавом. Это делает его вдвойне опасным: вероятность его обнаружения стремится к нулю.

Но даже при поимке злоумышленника, доказать факт преступления будет непросто, поскольку X6 оборудовано средствами шифрования хранящихся данных.

Недешевая «игрушка»

Собранные данные карт хранятся прямо в памяти устройства, на компьютер их можно передать с помощью USB-кабеля.

Данные клонированных карт – ходовой товар на киберкриминальном рынке. С их помощью преступники делают фальшивые дебетовые карты, чем активно занимаются и сами CC Buddies.

X6 предлагается за 1,5 биткоина, что примерно соответствует 1700 долл. на нынешний момент. За дополнительные карты предлагается заплатить еще 0,1 биткоина.

Интересно, что CC Buddies развернули сайт для своего сервиса в «обычном» Интернете, а не в даркнете, как это было раньше. Несколько других групп, занимающихся сходным промыслом, продолжают работать в даркнете.

Как защититься?

«Говоря о защите от подобных устройств, стоит вспомнить теорию волн из физики. Судя по техническим описаниям предшественника этого устройства оно работает на частоте 13,5 МГц, что является короткой волной. Короткие волны характеризуются небольшой длинной волны, но при этом высокой частой колебаний, что сказывается на их проникающую способность через препятствия, – говорит Г. Лагода, технический директор компании “Монитор Безопасности”. – Однако, стоит понимать, что заявленное расстояние копирования в 15 см, скорее всего имеет место в однородной воздушной среде без препятствий (в том числе, одежда, кошелек, другие карточки и т. д.), посему наибольшая вероятность успешного копирования чужой карточки злоумышленником появляется при непосредственном контакте данного устройства с картой жертвы».

По словам Г. Лагоды, зачастую рядом с пластиковыми картами могут находиться строение излучатели – электронные пропуска и другие карты, что может создавать дополнительные помехи потенциальным злоумышленникам. В

любом случае, считает Г. Лагода, необходимо минимизировать вероятность «прямого контакта» карты с RFID-чипом с другими людьми.

Также стоит отметить, что безопасность таких карт напрямую зависит от стандартов безопасности их производителей, – отметил Г. Лагода.

***

21.03.2017

Украинцы начали получать фейковые электронные письма с предложением оплатить налоги

Письма содержат якобы ссылку на счет для оплаты налогов, однако на самом деле загружает вредоносное ПО на компьютер (InternetUA).

В течение последней недели на электронные адреса частных лиц и государственных учреждений поступают письма якобы от Государственной фискальной службы с предложением оплатить указанный счет. Об этом говорится в сообщении Киберполиции.

Злоумышленники специально подменяют адрес отправителя на адрес в зоне .gov.ua, чтобы у получателя сложилось мнение, что письмо отправлено с госучреждения. Однако ссылка на якобы счет для оплаты налогов ведет на один из взломанных сайтов, находящихся под управлением CMS (система управления контентом) Joomla и Wordpress, по которому загружается zip-архив. В архиве находится вредоносное ПО, которое может получат доступ к файловой системе компьютера и загружать вирус с предварительно взломанных серверов. Далее вирус шифрует файлы, за их расшифровку киберпреступники требуют, как правило, сумму около 300–500 долл. в криптовалюте Bitcoin. Однако суммы требуемого выкупа за разблокировку компьютера могут превышать и 1 тыс. долл.

Чтобы не стать жертвой киберпреступления в полиции советуют всегда проверять адрес отправителя (служебные заголовки письма), использовать программы для шифрования в электронном виде и цифровую подпись, а также никогда не открывать ссылки в подозрительных письмах и делать резервные копии своих файлов.

***

20.03.2017

Ірина Коркішко

Увага! Вірус в листах: no_more_ransom

Будьте уважні і обережні! Вірус no_more_ransom поширюється за допомогою електронної пошти. Лист містить вкладений заражений документ або архів. Про це повідомляє державний сайт CERT-UA (Watcher).

Вірус-шифрувальник no_more_ransom – це один з шифраторів, що вражає всі сучасні версії операційних систем Windows, включаючи Windows XP, Windows Vista, Windows 7, Windows 8, Windows 10. Автори вірусу

використовують різноманітні заголовки й зміст листів, намагаючись обманом змусити користувача відкрити вкладений до листа документ. У будь-якому разі результатом відкриття прикріпленого файла буде зараження комп'ютера вірусом no_more_ransom. Під час зараження вірус no_more_ransom може використовувати декілька різних каталогів для зберігання своїх файлів: C:\ProgramData\Windows, C:\ProgramData\Csrss та C:\Users\All Users\Csrss.

Після запуску вірус сканує всі доступні диски (включаючи мережеві) для визначення файлів, що будуть зашифровані. Після шифрування файли отримує нове ім'я та розширення .no_more_ransom, а вірус створює на всіх дисках і Робочому столі текстові документи з іменами README.txt, README1.txt, README2.txt тощо, які містять інструкцію з розшифрування файлів. Вірус no_more_ransom показує на Робочому столі попередження, намагаючись таким чином змусити жертву, не роздумуючи, вислати ID комп'ютера на адресу електронної пошти автора вірусу в спробі повернути власні файли.

Визначити, чи заражений комп'ютер вірусом no_more_ransom, легко. Якщо замість ваших персональних файлів з'явилися файли з дивними іменами та розширенням no_more_ransom, то ваш комп'ютер заражений. Крім того, ознакою зараження є наявність файлів README у ваших каталогах. Файли такого типу міститимуть інструкцію з розшифрування файлів no_more_ransom.

***

21.03.2017

Приложения из Google Play крали пароли Instagram

Специалисты ESET обнаружили на Google Play тринадцать вредоносных приложений для кражи логинов и паролей Instagram. Общее количество их загрузок превысило полтора миллиона. Приложения использовали один и тот же способ сбора учетных данных. Они предлагали раскрутку аккаунтов в Instagram – быстрый рост числа подписчиков, лайков и комментариев (Компьютерное Обозрение).

После установки приложение запрашивает у пользователя логин и пароль от Instagram. Введенные данные отправляются на удаленный сервер мошенников в виде простого текста. При этом пользователь не сможет войти в учетную запись – приложение выводит на экран сообщение о неверном пароле.

В Instagram предусмотрено оповещение пользователей о несанкционированных попытках доступа. Чтобы авторизоваться во взломанной учетной записи, не вызывая подозрений, мошенники добавили в сообщение о неверном пароле предложение пройти верификацию аккаунта. Предполагается, что пользователь подтвердит «законность» действий злоумышленников.

В ESET отследили серверы, на которые поступали украденные логины и пароли, и связали их с сайтами, продающими услуги раскрутки аккаунтов в Instagram. Взломанные учетные записи использовались для распространения спама, а также «пакетной» продажи подписчиков, лайков и комментариев.

После предупреждения ESET вредоносное ПО было удалено из Google Play. Эксперты ESET рекомендуют пострадавшим сменить пароли от Instagram, а также от других сервисов, если пароль где-либо повторялся.

***

21.03.2017

Сбой в работе «ВКонтакте»: пользователи получили доступ к скрытой информации

21 марта всем пользователям социальной сети «ВКонтакте» открылся доступ к функциям, которыми могут пользоваться только модераторы сайта (From-UA).

Об этом Информатору сообщил пользователь «ВКонтакте» Д. Волосов.

«Сегодня на несколько минут всем пользователям открылись некоторые функции, доступные только модераторам. Сейчас скрины активно удаляют из всех источников, потому что пахнет это большим скандалом», – отметил он.

Д. Волосов также успел заметить некоторые интересные особенности. Например то, что модераторам ВК платят голосами. В «админке» есть кнопка «открыть приватные фото». Кроме того, модератор может посмотреть вектор интересов, то есть получить анализ информации о вас на основе всех действий.

На фотографиях также значится загадочный коэффициент «porno_score».

Пресс-секретарь «ВКонтакте» в Украине В. Леготкин прокомментировал ситуацию.

«В результате непредвиденного сбоя на несколько минут появился доступ к некоторым служебным разделам сайта. Результаты сбоя были быстро устранены. Ни о каком доступе к личным сообщениям и речи быть не могло, поскольку у нас такого доступа также нет», – рассказал он.

В. Леготкин также добавил, что кнопка «Получить доступ к приватным фотографиям» есть далеко не у всех, а у единиц сотрудников.

«Нужна для исключительных случаев – например, для борьбы с детской порнографией. Случайно и с какими-то нерабочими целями нажать эту кнопку сотрудник не может – кнопка применяется только по обоснованным жалобам, все действия по ней записываются», – объяснил он.

На снимках также фигурировала кнопка «Сообщения». По словам пресс-секретаря «ВК», с помощью вышеобозначенной кнопки сотрудник может только подрегулировать настройки системы. Собственно, примерно для того же у самих пользователей сайта существует кнопка «Это спам».

«Доступа к личным сообщениям у сотрудников нет. Кнопка выполняет совершенно иную задачу, это быстрый шаблон для защиты от вредоносного спама», – рассказал В. Леготкин.

***

21.03.2017

Вниманию владельцев iPhone: хакеры пригрозили удалить информацию с телефонов

Хакеры, назвавшие себя «Турецкая семья преступников», угрожают удалить данные с избранных ими iPhone, если Apple не заплатит 75 тыс. долл. в биткойне или Ethereum или 100 тыс. долл. подарочных карт iTunes (From-UA).

Злоумышленники угрожают удалить несколько учетных записей iCloud и удаленно стереть информацию с некоторых iPhone 7 апреля, если Apple не заплатит запрашиваемую сумму.

Хакеры предоставили скриншоты переписки со службой безопасности Apple, а также видео, в котором они, предположительно, взламывают один из украденных аккаунтов.

***

21.03.2017

Приложение McDonald's слило в Сеть информацию о 2,2 млн пользователей

Компания Fallible, которая специализируется на сетевой безопасности, обнародовала сведения об утечке персональных данных, произошедшей через приложение McDelivery (InternetUA).

Речь идет о фирменном приложении компании McDonald's, которое работает в Индии. Через это приложение в Сеть утекли сведения о 2,2 млн жителей страны, которые воспользовались McDelivery для заказа еды. Как отмечает Fallible, приложение слило в сеть имена, адреса электронной почты, домашние адреса, номера мобильных телефонов и прочую информацию, которую могут использовать хакеры для взлома электронных кошельков и кражи средств с кредитных карт.

Представители McDonald's India уже прокомментировали эту информацию, заявив, что компания очень тщательно относится к защите данных пользователей и не собирает информацию о паролях кошельков, номерах кредитных карт и прочие банковские данные. Тем не менее, всем пользователям McDelivery порекомендовали обновить приложение.

После чего представители Fallible заявили, что они известили McDonald's о бреши в McDelivery еще 7 февраля, получив подтверждение от отдела сетевой безопасности. Однако опубликованное обновление не полностью устраняет проблему, поэтому приложение McDelivery продолжает сливать пользовательские данные в Сеть.

***

23.03.2017

В прошлом году число взломанных сайтов возросло на треть

Google рассказал об участившихся взломах сайтов (IGate).

Компания Google опубликовала отчет о состоянии интернет-безопасности за прошлый год. Согласно данным поискового гиганта, в 2016 г. число взломанных сайтов возросло на 32 % в сравнении с 2015 г. Кроме того, в ближайшее время эта тенденция вряд ли изменится.

В отчете указывается, что хакеры стали гораздо более агрессивны. При этом многие вебмастера своевременно не обновляют свои сайты и CMS-платформы, что подвергает их ресурсы риску быть взломанными.

В Google также назвали три самых распространенных типа:

Gibberish Hack. При атаке этого типа на сайте создаётся множество страниц с бессмысленным содержанием и ключевыми словами. В результате они появляются в поиске Google. При посещении этих страниц пользователи перенаправляются на нерелевантные страницы, такие как порносайты.

Japanese Keywords Hack. При атаке этого типа на сайте создаются новые страницы с текстом на японском языке. Они монетизируются за счёт использования партнёрских ссылок на магазины, продающие контрафактные товары, и показываются в поиске Google. Иногда хакеры регистрируются в Search Console как владельцы ресурса.

Cloaked Keywords Hack. При этом атаке этого типа на сайте создаётся множество страниц с бессмысленным содержанием, ссылками и изображениями. Иногда эти страницы содержат основные элементы шаблона оригинального сайта, поэтому на первый взгляд они выглядят как обычные страницы – пока пользователь не прочитает текст. В этих атаках хакеры обычно используют техники клоакинга, чтобы скрыть вредоносный контент и сделать зараженные страницы похожими на страницы оригинального сайта или страницы с ошибкой 404.

***

22.03.2017

Ольга Карпенко

«1+1 Медиа» запустила систему поиска нелегального контента: уже блокируют Facebook-группы за пиратство

В YouTube поиск и удаление контента с пиратскими элементами практикуется давно: с этим может столкнуться любой блогер, решивший использовать нелицензионную музыку или видео в своей публикации. Но блокировку аккаунтов Facebook благодаря автоматической системе распознавания пиратского контента в украинском сегменте сети можно назвать прецедентом (AIN.UA).

Группа «1+1 Медиа» разработала свою платформу Sudum, которая в реальном времени мониторит сайты на предмет нарушения авторских прав. По словам Д. Некрасова, руководителя отдела дистрибуции видеоконтента и управления правами «1+1 Медиа», эта технология умеет распознавать и блокировать нелегальный контент в социальных сетях, видеохостингах, сайтах, форумах, торрент-трекерах, платформах Google Play и App Store, в поиске

Google. С ее помощью также отправляются жалобы администрации сайтов, хостинг-провайдерам и регистраторам доменных имен.

Система работает около года. «По итогам 2016 г. мы имеем показатель эффективности зачистки – 93,5 %, при этом 100 % наших жалоб удовлетворяются крупнейшими веб-ресурсами, такими как Facebook, “ВКонтакте”, “Одноклассники”, Mail.ru, YouTube, Dailymotion, Vimeo», – говорит Д. Некрасов. Сейчас Sudum фокусируется на видео, но в планах – продукты для поиска нелегальной музыки, электронных книг, ПО и компьютерных игр.

В Facebook есть инструмент для мониторинга нарушения авторских прав Rights Manager, но он доступен не всем сообществам. Sudum для поиска такого контента использует открытое API поиска Facebook, работает платформа круглосуточно.

Недавно несколько блогеров и администраторов сообществ в украинском Facebook столкнулись с результатами ее работы. По словам известного блогера А. Барабошко, за публикацию видео его заблокировали на несколько дней. Правда, быстро вышли на связь и разобрались в ситуации:

Администраторам заблокированных страниц показывались такие уведомления:

«Решение о блокировке аккаунта и ее длительности принимается на стороне Facebook. Это может быть как временное ограничение доступа от 3 до 30 дней, так и полная блокировка аккаунта», – рассказывает Д. Некрасов.

По словам представителей компании, блокируются те пользователи, которые добавили файл непосредственно к себе в профиль или группу. Пользователя, который зашерил видео себе на страницу, система пропускает.

***

21.03.2017

Wikileaks назвал условия, при которых раскроет Apple и Google хакерские секреты ЦРУ

Основатель сайта WikiLeaks Д. Ассанж пообещал предоставить доступ к хакерским инструментам американских спецслужб Apple, Google, Microsoft и другим IT-компаниям. При этом он выдвинул ряд условий (InternetUA).

Д. Ассанж, признал, что компаниям будет сложно исправить уязвимости в своих продуктах, основываясь только на информации, почерпнутой из документов ЦРУ. Тот факт, что сами хакерские инструменты спецслужб не были опубликованы, сильно ограничивает разработчиков. Поэтому в Wikileaks приняли решение пойти производителям навстречу.

Ассанж разослал письма, в которых указал условия, при которых он поделится секретной информацией. В частности, компании должны дать гарантии, что закроют обнаруженные уязвимости в течение 90 дней. По истечении этого периода времени компании будут обязаны публично раскрыть

информацию о багах, которые эксплуатировало ЦРУ. То есть исправления должны быть разработаны и выпущены за три месяца.

«Мы приняли решение сотрудничать с ними, предоставить эксклюзивный доступ к дополнительной технической информации, которой мы обладаем, чтобы они смогли разработать исправления и выпустить их, тем самым обезопасив людей. После этого, когда мы “разоружим” эти программы, удалив критические компоненты, мы опубликуем дополнительные детали случившегося», – заявил основатель WikiLeaks.

На прошлой неделе сайт WikiLeaks опубликовал более 8 700 документов, хранившихся в изолированной внутренней сети Центра по кибербразведке, базирующегося в штаб-квартире ЦРУ в Лэнгли. В частности, представители сервиса утверждают, что хакеры ЦРУ разработали множество способов для «заражения, управления и передачи данных» со смартфонов iPhone, планшетов iPad и других аппаратов.

Также спецслужбы искали уязвимости нулевого дня, о которых могут не знать даже разработчики устройств. Известно, что на Android нашли 24 такие уязвимости, на iOS – семь.

Ранее сообщалось, что в Кремниевой долине сомневаются, стоит ли вообще сотрудничать с Д.Ассанжем. Представители ряда IT-компаний заявили, что секретный характер опубликованных документов означает, что даже простое ознакомление с ними без предварительного разрешения властей США незаконно.

***

22.03.2017

На продажу выставлены 25 млн логинов Gmail с паролями

В киберподполье на продажу выставлены более 25 млн аккаунтов Gmail и около 5 млн аккаунтов Yahoo. Все эти данные получены из крупных взломов прошлых лет, когда хакерам удавалось похитить миллионы почтовых логинов и паролей с серверов MySpace, LinkedIn, Dropbox и других компаний (InternetUA).

Оптом дешевле

В даркнете выставлены на торги миллионы логинов и паролей к почтовым ящикам Gmail и Yahoo. В качестве продавца выступает пользователь с ником SunTzu583, ранее замеченный в оптовых продажах взломанных аккаунтов Gmail и PlayStation. Сейчас он выставил на торги рекордные по размерам массивы данных, причем большую их часть составляют именно реквизиты к аккаунтам Google.

На данный момент SunTzu583 выставлены на торги несколько лотов с миллионами логинов и паролей в почтовым ящикам Gmail и Yahoo.

Первая партия размером почти 5 млн аккаунтов представлена тремя «лотами»: первые два содержат по 2262444 аккаунта и продаются за 125,48

долл. или 0,1298 биткоина, а в третий собраны сразу все 4928888 аккаунтов. Стоимость последнего лота составляет 200 долл. или 0,206 биткоина.

Согласно заверениям продавца, в этом наборе все пароли к аккаунтам расшифрованы (decrypted).

Авторы издания HackRead, проанализировав данные, предоставленные продавцом в качестве примера бесплатно, убедились, что их источниками были крупные утечки прошлых лет; в частности, из LinkedIn (когда хакерам удалось угнать 117 млн аккаунтов), Adobe (похищены 154 млн аккаунтов) и Bitcoin Security Forum (откуда утекли 5 млн паролей к Gmail). BSF как раз и является источником большей части аккаунтов, выставленных сейчас на продажу.

Продавец честно предупреждает, что далеко не все пароли сейчас сработают на Gmail. Утечки широко освещались в прессе, так что есть надежда, что значительная часть пострадавших пользователей сменили пароли.

Кроме этих 5 млн, SunTzu583 продает еще почти 22 млн аккаунтов Gmail за 450 долл. (0,4673 биткоина). Несмотря на то, что количество аккаунтов в этом наборе вчетверо выше, стоимость второго набора лишь в два с небольшим раза превосходит ценник на первом. Это связано с тем, что в нем только 75 % из предлагаемых аккаунтов доступны «из коробки» – пароли в них представлены в виде текста. Остальные пароли захэшированы.

Авторы HackRead установили, что источниками этих данных стали несколько утечек разных лет, крупнейшей из которых стал взлом Dropbox в 2012 г. Тогда были украдены данные 68 млн аккаунтов в Gmail. В общий доступ эти реквизиты попали уже только в 2016 г. Другими источниками этих аккаунтов стали утечки из Nulled.cr в 2016 г. и MPGH.net в 2015 г.

И снова Yahoo

Кроме того SunTzu583 продает 5,7 млн аккаунтов в Yahoo с расшифрованными паролями. Весь набор разделен на три части по 100 долл. каждая или доступен целиком за 250 долл.

По данным HackerRead, большая часть этих аккаунтов была украдена в разные годы из MySpace, LinkedIn и Adobe; значительная порция их уже неактивна, однако некоторые до сих пор работают.

С 2013 г. портал Yahoo несколько раз становился жертвой взломов; злоумышленникам достались данные более 1,5 млрд пользователей сервиса, что в итоге привело компанию на грань краха. Сейчас ее пытаются продать корпорации Verizon.

Что делать?

«Рекомендации всегда одни и те же: менять пароли хотя бы раз в несколько месяцев, – говорит Д. Гвоздев, генеральный директор компании “Монитор безопасности”. – Это позволит снизить вероятность тому, что ваши логины и пароли будут выставлены на продажу после очередной крупной “утечки”. Также настоятельно рекомендуется не использовать одни и те же пароли для нескольких ресурсов, чтобы не получилось так, что пароль от почты подходил к аккаунту Facebook или любой другой социальной сети».

***

23.03.2017
Как избавиться от слежки Google?

Аккаунт Google есть почти у каждого, он используется для покупки программ, ради почтового ящика и других сервисов. Но мало кто задумывается, насколько много информации собирает «корпорация добра» – истории покупок и поиска, наши личные данные, предпочтения и даже историю передвижений. Кто-то не придаёт этому значения, но есть и те, кому не нравится такая осведомлённость Google об их сугубо частной жизни. Мы не будем предлагать отказаться от аккаунта и уйти жить в лес, но расскажем в статье о том, как минимизировать количество собираемой о нас информации (InternetUA).

Под колпаком

Итак, что же именно Google о вас знает? Это выяснить проще простого: достаточно перейти на специальную страницу «Мои действия» в настройках аккаунта. Там вы увидите временную шкалу с посещёнными сайтами, поисковыми запросами, просмотренными на YouTube видео и даже запущенными Android-приложениями. За день у автора набралось более 300 подобных действий, каждое из которых было логировано и подробно описано.

Есть у Google и другой подобный сервис, но касается он геолокации. Авторизовавшись, в нём можно увидеть историю своего передвижения по всему миру. Подобные данные компания хранит сколь угодно долго, а в нашем случае самые ранние записи датируются 2013 г. К слову, отключить историю местоположений проще всего – достаточно нажать кнопку «Отключить историю» в нижней части карты.

Как, и, главное, зачем Google собирает о вас столь подробную информацию? Для большинства веб-сервисов действует аксиома: если вы не платите за услугу, то сами выступаете в качестве товара. «Продавать» пользователей можно разными способами, но в случае с Google всё весьма банально – компания получает деньги за размещение таргетированной рекламы, которая будет показана вам в зависимости от ваших предпочтений, вкусов и привычек. Причём, чем более точную информацию о вас соберёт Google, тем вероятнее такая реклама сработает, и тем больше компания сможет заработать.

Информация о вас попадает к компании разными способами. Львиная доля сведений передаётся Android-устройствами и браузером Chrome (вы ведь внимательно читали лицензионные соглашения при первом запуске смартфона и установке браузера?), но, даже если вы не пользуетесь этими продуктами, существует ещё много способов узнать о вас больше. Один из наиболее распространённых – файлы cookie, которые обычно используются для управления сессиями и авторизации на веб-ресурсах. Стоит вам хотя бы раз открыть страницу любого сервиса Google, как на вашем компьютере будет сохранён cookie-файл, с помощью которого компания сможет понять, что все ваши действия на любых сервисах компании осуществлялись именно с вашего

ПК. Это будет работать, как минимум, до очистки cookie-файлов в браузере. Не поможет избавиться от слежки и использование режима инкогнито или специального браузера: при обращении к любому сайту браузер передаёт ему информацию о своём движке, операционной системе устройства, разрешении окна и другие системные сведения. Эти сведения в совокупности составляют что-то вроде «отпечатка», который достаточно уникален для относительно точного определения одного пользователя.

Это далеко не все способы слежения за действиями пользователей: существуют и другие, более хитрые. Полностью стать анонимным в сети и скрыться от всевидящего ока Google – непростая задача, но вы вполне можете минимизировать количество слежки за собой.

Удобство или приватность?

Мир состоит не только из чёрного и белого, и сбор ваших личных данных крупными компаниями – отнюдь не зло в чистом виде. Информация о людях позволяет Google постоянно улучшать свои сервисы, причём не только в целом, для всех пользователей, но и конкретно для вас. Подробнее об этом компания рассказывается на странице «Конфиденциальность». Например, благодаря передаче данных о местоположении и скорости устройства во время навигации Google может более точно оценить загруженность дороги. Передача информации о поисковых запросах позволяет сделать поисковик умнее и предлагать более релевантные варианты для автозаполнения. А информация об активности на YouTube даёт возможность компании делать для вас более точные рекомендации.

Здесь же Google рассказывает о защите ваших данных: по заверениям компании, вся передаваемая информация надёжно шифруется и хранится в безопасности, без доступа к ней посторонних лиц. Причин не доверять этому нет, любая крупная утечка личных данных пользователей нанесла бы серьёзный удар по бизнесу корпорации.

Есть у такой осведомлённости Google о вашей жизни и третья сторона. Несмотря на принципы компании, по которым правительства и спецслужбы ни одной страны не могут получить свободный доступ к данным какого-либо пользователя, компания порой оказывается бессильна перед решениями судов и официальными запросами правоохранительных органов.

Умерить аппетит Старшего Брата

Даже если вы до конца не решили, стоит вам опасаться слежки или нет, обязательно стоит проверить свои настройки конфиденциальности. Конечно, Google ничуть не заинтересована в потере предоставляемой вами информации, а потому все галочки и кнопочки, позволяющие отключить слежку, глубоко запрятаны в самых разных меню настроек аккаунта.

Отключите историю действий. Начать стоит со страницы с недвусмысленным названием «Отслеживание действий». Здесь вы можете отключить запись действий в приложениях и истории веб-поиска, запросов на YouTube, голосового поиска, а также историю местоположений. При попытке отключения любого из перечисленных пунктов Google постарается уговорить

этого не делать – остаётся только выдержать характер и твёрдой рукой нажать кнопку «Отключить».

Настройте параметры конфиденциальности. Разобравшись с предыдущими настройками, стоит запустить мастер «Проверка настроек конфиденциальности». Пройдя последовательно несколько шагов, вы сможете выбрать, какая информация о вас будет общедоступна при поиске в Интернете, а какая – нет. Например, вы можете настроить видимость для других пользователей ваших действий на YouTube или отключить возможность поиска вашего аккаунта Google по привязанному номеру телефона.

Отключите таргетированную рекламу. Что ж, теперь самое время переходить к святая святых – рекламным настройкам Google. Перейдя по ссылке, вы увидите, на какие темы вам показывают рекламу. Список составлен автоматически на основе ваших действий в аккаунте Google, но, чтобы реклама была более релевантной, вы можете отредактировать его, удалив ненужные темы и добавив новые. Но, если вы не хотите, чтобы ваши личные данные использовались для подбора рекламы, вы можете вовсе отключить персонализацию. Реклама, разумеется, никуда не пропадёт, просто её подбор будет основываться только на вашем местоположении. Интересно, что оценки компанией Google вашего возраста и интересов точны далеко не всегда – это мы выяснили, проведя небольшой опрос. Регулярные просмотры старых советских фильмов и выступлений Л. Зыкиной на YouTube значительно увеличивают виртуальный возраст.

Прокрутив страницу в самый низ, вы найдёте кнопку «Настроить рекламу, которая видна после выхода из аккаунта». После нажатия на неё откроется страница с идентичными настройками, но относиться они будут уже к особым случаям, включая работу в режиме инкогнито, сторонние сайты и использование сервисов Google без авторизации. Да-да, Google следит за вами, даже если вы не используете сервисы компании вовсе: для этого вам достаточно посещать один из более чем двух миллионов сайтов, которые показывают рекламу Google.

И это всё?

Как вы уже могли догадаться, нет. Но всё зависит от того, какую цель преследовать. Если вы не против персонализированной рекламы и просто не хотите сообщать о себе слишком много информации, приведённая выше инструкция будет полезна. Но если вы хотите бóльшей анонимности, вам придётся завести новый аккаунт Google или вовсе от него отказаться и начать пользоваться специальными средствами защиты. Речь идёт о VPN-сервисах, анонимайзерах и специализированных браузерах вроде Tor. Один из интересных проектов предлагает компания с говорящим названием Disconnected – её одноимённое приложение для Android OS позволяет искать в Интернете информацию, не опасаясь отслеживания. Вдобавок, приложение умеет анализировать сайты на предмет встроенных модулей, которые могут использоваться для анализа ваших предпочтений. Правда, для более удобного

использования программы с любыми браузерами на смартфоне, вам придётся оплатить сервис или купить на него подписку.

В современном Интернете оставаться анонимным всё труднее: практически каждый сайт, сам или через посредников, старается собрать о вас как можно больше информации. К счастью Google вполне официально предоставляет ряд инструментов, с помощью которых вы можете регулировать количество передаваемых сведений – мы перечислили лишь некоторые из них. Ну а полная анонимность уже успела стать прерогативой людей, которые серьёзно разбираются в сетевой безопасности. Дни, когда в сети никто не знал, что вы – кот, ушли в прошлое.

***

22.03.2017

В Украине обнаружили сеть фейковых интернет-магазинов

На данный момент киберполиция принимает меры для установления всех причастных к преступной афере и обращается к обманутым гражданам сообщать на горячую линию департамента любые дополнительные факты о деятельности мошенников (InternetUA).

Департамент киберполиции в городе Киев совместно с прокуратурой раскрыли деятельность мошенников, которые путем создания фейковых интернет-магазинов завладевали денежными средствами обманутых граждан.

Об этом говорится в сообщении ведомства на официальной странице Facebook.

Так, следствие установило, что начиная с 2013 г. в стране велась деятельность следующих интернет-магазинов: konfitel.com, layaway.com.ua, docamarket.com, elman.com.ua, tradestar.com.ua, etorg.biz, zumer.com.ua, kievplasma.com.ua, kucha.com.ua, domotech.kiev.ua, tehnogarant.com.ua, которые на самом деле предлагали несуществующий товар.

Мошенники обеспечили магазинам широкую рекламу и популяризацию в сети, чтобы привлечь как можно больше граждан для своего обогащения. Для деятельности интернет-магазинов были созданы и зарегистрированы также фиктивные предприятия ТОВ «Технопарк-центр», ТОВ «ЛТД-ПРОДУКТ», ФОП «Хмеленко О. О.», ФОП «Козінцов О. С.» и другие, на которые оформлялись банковские счета и карты.

«Получив кредитные карты и контроль над счетами фиктивных предприятий, злоумышленники предпринимали действия по завладению средствами доверчивых граждан», – сообщают в киберполиции.

Для большей достоверности деятельности мошенники также создавали кол-центры магазинов, с помощью которых осуществлялась обратная связь с заказчиками товаров.

«Операторы “кол-центра” с помощью услуг интернет-телефонии, находясь по месту проживания на территории Украины, связывались и общались с заказчиками фиктивных интернет-магазинов, создавая впечатление

реального кол-центра, принимали заказы на несуществующий товар», – отмечается в сообщении.

Денежные средства, перечисленные обманутыми покупателями, мошенники обналичивали в банкоматах Киева.

По предварительным подсчетам сумма убытков составила 1 млн грн, однако в киберполиции считают, что это не окончательная сумма.

По итогам расследования организатор схемы был арестован, у него были изъяты наличные средства в размере 19 тыс. долл., 8 банковских карт, 4 ноутбука, планшет, 8 мобильных телефонов, около 50 сим-карт разных мобильных операторов, а также документы и другие вещи.

***

23.03.2017

Черкаські ІТ-фахівці фірми «eKreative» хочуть убезпечити дітей від «синіх китів»

«Ми плануємо вдосконалити унікальний для України винахід компанії – Програму батьківського контролю Kidslox, – повідомив засновник однієї із найбільших ІТ-компаній “eKreative” В. Євпак. – Це мобільний додаток, що дозволяє батькам контролювати перебування своїх дітей у мережі на мобільних телефонах і планшетах. І сьогодні ми працюємо над тим, аби дати можливість батькам не лише контролювати сайти, які відвідують їх діти, тривалість і час перебування у мережі» (ПРОЧЕРК).

«Сьогодні ми працюємо вже над такими вдосконаленням Kidslox, які дозволять батькам обмежувати дітям доступ до певного контенту, який може бути для них шкідливим. Наразі програмою Kidslox зацікавилися 6 мобільних операторів – як в Україні, так і з різних куточків світу. Ці компанії є водночас і інтернет-провайдерами – тож вони хочуть поширювати наш додаток через мережу своїх користувачів. Про все це я говоритиму на тренінгу для батьків щодо безпеки дітей в Інтернеті, що 31 березня о 17:00 відбудеться у Черкасах (територія «Вільний громадський простір» у приміщенні по вул. В’ячеслава Чорновола, 9/1)», – інформує В. Євпак.

***

24.03.2017

Ірина Коркішко

Рада прийняла закон по боротьбі з інтернет-піратством

Верховна Рада у другому читанні прийняла законопроект «Про державну підтримку кінематографії в Україні». Крім державної підтримки виробництва кіно, документ має на меті захист інтелектуальної власності і боротьбу з піратством. Про це повідомляє видання ЛІГА.net (Watcher).

Законопроект передбачає державне субсидіювання виготовлення фільмів та серіалів і закупки мобільних комплексів для демонстрації кіно у віддалених

містах і селах. У документі також йдеться про те, що власники авторських прав отримають можливість швидкого блокування нелегального відео-контенту. За відмову блокування або за необґрунтовані вимоги до блокування буде встановлена відповідальність.

***

24.03.2017

В Google пообещали подтянуть безопасность Android до уровня iOS

Главы отдела безопасности в Android заявили, что обновления, устраняющие уязвимости устройств, будут доступны не через несколько месяцев после выхода, а через несколько дней (Finance.Ua).

Обновления безопасности для устройств под управлением iOS выходят оперативно и доступны сразу на всех совместимых моделях. Чего нельзя сказать про смартфоны и планшеты на Android. Но в Google планируют решить проблему с обновлениями фирменной программной платформы. Компания пообещала сократить время, через которое апдейты станут доступны пользователям, с двух месяцев до нескольких дней, сообщает macdigger.

Почти половина пользователей Android не получает обновления безопасности вовремя, и поисковый гигант пообещал устранить эту проблему. Дело в том, что «гуглофоны» выпускают сотни различных компаний и довольно сложно сделать так, чтобы каждый пользователь мог вовремя обновлять ОС.

Как заявили А. Людвиг и М. Миллер, которые возглавляют отделение по безопасности в Android, по итогам 2016 г., около половины пользователей не смогли получить необходимые обновления вовремя. «У нас впереди еще много работы», – сказали они.

Смартфоны, которые производит Google, Pixel и Nexus, обновляются автоматически. При этом сотни других производителей, которые использует Android, выпускают их спустя недели и даже месяцы после релиза заплатки. При этом информация об уязвимости уже может появиться в открытом доступе.

***

27.03.2017

Новый троянец помогает киберпреступникам воровать вредоносное ПО у своих коллег

Эксперты Kaspersky Lab обнаружили троянскую программу, которая использует известного шифровальщика Petya для проведения целевых атак на бизнес (ITnews).

Троянец получил название PetrWrap, а его главная особенность заключается в том, что он использует оригинального зловреда без разрешения разработчиков.

Шифровальщик Petya, обнаруженный Kaspersky Lab в 2016 г., – один из наиболее заметных зловредов, распространяемых по модели «вымогатели как услуга» (Ramsomware-as-a-Service, RaaS). Авторы распространяют его через многочисленных посредников, получая часть прибыли. Для того чтобы избежать неавторизованного использования шифровальщика, разработчики вставили в его код несколько защитных механизмов, однако создателям PetrWrap удалось их обойти. При этом новый троянец использует собственные ключи шифрования вместо тех, что применяются в Petya по умолчанию, поэтому для расшифровки данных в случае уплаты выкупа PetrWrap также не требуется помощь авторов оригинального вымогателя.

Разработчики PetrWrap выбрали Petya не случайно. Это семейство вымогателей обладает почти безупречным криптографическим алгоритмом, расшифровать который чрезвычайно сложно. В предыдущих версиях программы был найден ряд ошибок, которые несколько раз позволяли экспертам расшифровывать закодированные файлы, однако с тех пор авторы закрыли почти все уязвимости. Кроме того, после заражения устройства этим вымогателем на заблокированном экране отсутствуют какие-либо упоминания зловреда, что существенно усложняет работу экспертам по кибербезопасности.

«Мы наблюдаем очень интересный процесс: киберпреступники стали нападать друг на друга. С нашей точки зрения, это признак растущей конкуренции между различными группировками. Отчасти это хорошо, ведь чем больше времени злоумышленники проводят в борьбе друг с другом, тем менее организованными и эффективными будут их атаки и они сами, – прокомментировал А. Иванов, старший антивирусный аналитик Kaspersky Lab. – В случае с PetrWrap нас беспокоит тот факт, что троянец-шифровальщик используется для целенаправленных атак. Это не первый подобный случай и, к сожалению, наверняка не последний. Мы настоятельно рекомендуем компаниям уделять максимальное внимание защите сетевой инфраструктуры от этого типа угроз, иначе последствия могут быть катастрофическими».

Для защиты организации от целенаправленных атак Kaspersky Lab рекомендует предпринять ряд мер.

• Сделайте резервную копию всех данных, которую можно будет использовать для восстановления файлов в случае атаки.

• Используйте защитное решение с технологией детектирования по поведению. Она определяет троянцев любого типа, анализируя их действия в атакованной системе. Это позволяет обнаруживать даже ранее неизвестные зловреды.

• Проведите комплексную оценку информационной безопасности сети (аудит, тестирование на проникновение, GAP-анализ), чтобы обнаружить и закрыть все лазейки, которыми могут воспользоваться злоумышленники.

• Пользуйтесь внешней экспертной оценкой: консультация авторитетных вендоров поможет предвидеть вектор будущих атак.

• Проведите тренинг по кибербезопасности для сотрудников. Особое внимание стоит уделить инженерно-техническому персоналу, его осведомленности об атаках и угрозах.

• Обеспечьте защиту как внутри периметра корпоративной сети, так и снаружи. В правильной стратегии безопасности значительные ресурсы выделяются на обнаружение атак и реагирование на них до того, как они достигнут критически важных объектов.

***

26.03.2017

Полиция предупредила пользователей iPhone о смертельно опасном розыгрыше

Правоохранительные органы предупредили владельцев iPhone об опасном розыгрыше в Интернете, который может привести к смертельным последствиям. Вирусная шутка в сети создала большую проблему для работы полиции и спасателей (InternetUA).

В социальных сетях организаторы пранка предлагают владельцам iPhone и iPad попросить голосового помощника Siri набрать номер 108, «чтобы посмеяться». И этого нельзя делать ни в коем случае.

Как выяснилось, после команды «108» голосовой помощник Apple вызывает аварийно-спасательные службы. Если такие звонки начнут поступать из множества разных точек, это займет линии экстренной связи, увеличив время отклика – а в некоторых случаях разница во времени в несколько минут может быть гранью между чьей-то жизнью и смертью, заявили в полиции.

«Скажите Siri “108” и посмотрите, что она ответит. Это уморительно».

«Все пользователи iPhone, скажите Siri “108” и закройте глаза на 5 секунд. Поблагодарите меня потом».

«Только что обнаружил способ организовать групповые звонки по FaceTime, просто скажите Siri “108”, после чего вы сможете звонить сразу двум людям».

Стражи правопорядка настоятельно рекомендует владельцам iPhone избегать команд «108», «112», «110», «999» и «000».

Во время тестирования этих номеров служба спасения установила, что набор любого из них при помощи Siri приведет к тому, что звонок будет перенаправлен в центр экстренной связи. Эту информацию обнародовал офис шерифа округа Дуглас, Вашингтон.

***

26.03.2017

Опасные смартфоны: пользователи постоянно подвергаются кибератакам

Согласно недавнему отчету исследовательского центра Pew Research Center, около 28 % пользователей смартфонов не ставят пароли на блокировку экрана, хотя эта функция является одной из базовых для соблюдения мер безопасности (InternetUA).

Кроме того, 40 % пользователей обновляют свои приложения или операционные системы на постоянной основе. Никогда не обновляют свои приложения или ОС 10 и 14 % пользователей соответственно. Однако специалисты рекомендуют это делать постоянно.

Ожидаемо, пользователи смартфонов старшего поколения менее склонны к соблюдению мер безопасности. Так, пользователи старше 65 лет намного реже ставят пароли на блокировку экрана, а также обновляют приложения и ОС (13 % против 23 %).

В результате, согласно Pew Internet, 64 % американцев становились жертвами утечки данных, включая несанкционированное снятие средств с платежных карт (41 %) и утечку персональной информации (35 %).

***

26.03.2017

Google рассказал, как прекратить распространение провокационных видео

Корпорация Google на протяжении долгого времени решительно выступает против размещения рекламных роликов вблизи видео экстримисткого содержания. В ряды представителей компании ежедневно присоединяются тысячи единомышленников (HiTech-News.ru).

Владельцы рекламных площадок пытаются бороться с этой проблемой. На протяжении долгих трех лет с проблемой пытаются справиться известные компании как Google, Facebook и Twitter. Многие уверенны, что за такое время «больного можно было вылечить».

Руководители компании Google посоветовали при регистрации пользователей обязательно требовать настоящие имена, адрес и электронную почту. Подобный метод отсеет всех ленивых, так как на заполнение всей анкеты уйдет время, а желающий оставить отзыв, либо видео три раза подумает.

Второе – профилирование интернет-гигантов. Такой метод поможет обнаружить людей со склонностями к радикализации.

И третий – внедрение искусственного интеллекта, который будет сам распознавать изображения и блокировать их. Этот метод облегчит работу людям и автоматически сможет контролировать процессы.

Но помимо вышесказанного, следует быть уверенным в чистоте своих помыслов и наконец-то начать сотрудничать с представителями правоохранительных органов.

***

27.03.2017

Хакери заблокували сайт ФДМ

Офіційний сайт Фонду державного майна не працює через DDoS-атаки, повідомляється на сторінці ФДМ у Facebook (LB.ua).

«Фонд вживає всіх необхідних заходів, щоб якомога швидше відновити роботу сайту. Уся інформація, розміщена на сайті, зберігається на серверному обладнанні Фонду», – сказано в повідомленні.

***

27.03.2017

Hancitor впервые вошел в пятерку самых популярных зловредов в февральском отчете

Check Point Software Technologies опубликовал данные ежемесячного отчета Threat Index за февраль 2017 г. Из них следует, что зловред Hancitor впервые вошел в пятерку самых активных семейств вредоносных программ (ITnews).

Загрузчик Hancitor, также известный как Chanitor, устанавливает вредоносные программы, такие как банковские трояны и вымогательское ПО. Он поднялся на 22 пункта в общем рейтинге после того, как в прошлом месяце его активность увеличилась втрое. Hancitor попадает на устройство пользователя в виде документа с поддержкой макросов в зловредных письмах с «важными» сообщениями, например, со счетами, накладными и т. д.

Самым распространенным видом вредоносного ПО стал зловред Kelihos, который используется в краже биткоинов: от него пострадали 12 % организаций. Будучи активным с 2010 г., гибкий Kelihos превратился из целенаправленной спам-компании в ботнет на прокат, доступный всем, кто готов платить. Несмотря на то, что его активность снизилась в 2011 и 2012 гг., он продолжал развиваться и достиг апогея в виде бот-сети, увеличившись более чем в три раза всего за два дня в августе 2016 г. Сегодня Kelihos продолжает расти и остается одним из самых известных распространителей спама в мире: на его счету 300 000 зараженных устройств, каждое из которых может отправлять более 200 000 сообщений в день.

Количество атак на Россию в феврале 2017 г. увеличилось, и она поднялась с 83 на 63 место в рейтинге самых атакуемых стран. Чаще всего нападения велись с использованием зловредов Cryptowall, Kelihos, Conficker, Delf, Pykspa, Kometaur, HackerDefender, Mydoom, Jeefo и Slammer. Больше всего кибератакам подвергались компании Замбии, Малави и Камбоджи. Меньше всего атак было на организации в Черногории, Барбадоса и Лихтенштейна.

В глобальном рейтинге самых распространенных вредоносных программ в феврале тройку лидеров образуют: зловред Kelihos, жертвами которого стали

12 % организаций, HackerDefender, заразивший 5 %, и Cryptowall, на счету которого 4,5 % компаний во всем мире.

Самые активные зловреды февраля 2017 г.:

1. Kelihos – Ботнет, который используется в основном для спам-рассылок и кражи биткоинов. Он работает через пиринговую связь, позволяя каждому отдельному узлу выступать в качестве командного сервера.

2. HackerDefender – Пользовательский руткит для Windows, может использоваться для сокрытия файлов, процессов и ключей системного реестра. Также его применяют в качестве бэкдора и программы для перенаправления портов, которая работает через порты, открытые существующими службами. В результате скрытый бэкдор невозможно обнаружить традиционными средствами.

3. Cryptowall – Вымогательский зловред, который начал как двойник Cryptolocker, но в конце концов превзошел его. Cryptowall стал одним из самых выдающихся вымогателей. Он известен из-за использования шифрования AES и организации связи с командным сервером через анонимайзер Tor. Зловред активно распространяется через эксплойт-киты, вредоносную рекламу и фишинговые кампании.

В рейтинге самых опасных мобильных зловредов Hiddad поднялся с третьего места на первое и стал самой активной вредоносной программой. За ним следует Hummingbad, а январский лидер, вредонос Triada, в феврале занимает третье место.

Самые активные мобильные зловреды:

1. Hiddad – Зловред для Android, который переупаковывает легитимные приложения и затем реализует их в магазинах сторонних производителей. Его главная функция – показ рекламы, однако он также может получить доступ к ключевым настройкам безопасности, встроенным в операционную систему, что позволяет злоумышленнику получить конфиденциальные данные пользователя.

2. Hummingbad – Вредоносное ПО для Android, которое, используя устойчивый к перезагрузке руткит, устанавливает мошеннические приложения и с небольшими модификациями может проявлять дополнительную вредоносную активность, включая установку программных клавиатурных шпионов, кражу учетных данных и обход зашифрованных email-контейнеров, используемых компаниями.

3. Triada – Модульный бэкдор для Android, который дает огромные привилегии скачанным зловредам, поскольку помогает им внедриться в системные процессы. Triada также был замечен в подмене URL-адресов, загруженных в браузере.

***

27.03.2017

Оставят ли хакеры Украину без света?

В зону риска хакерских атак в этом году попадут не только финансовый сектор и госструктуры, но и телеком-операторы, и даже игровые проекты (InternetUA).

Ряд успешных кибератак на госструктуры в 2016 г. заставили государство обратить внимание на проблему киберзащиты стратегических учреждений и объектов инфраструктуры.

Под модернизацию киберзащиты начали выделяться дополнительные средства. Но такие действия государства скорее похожи на латание дыр – этого явно недостаточно для отражения серьезных хакерских атак. Ожидается, что в этом году хакеры существенно расширят сферу своей деятельности – не станут ограничиваться лишь атаками на госсектор, но и активизируются в корпоративном секторе. И атаки будут на порядок серьезнее тех, что наблюдались ранее.

UBR.ua решил узнать у специалистов по кибербезопасности какие новые сюрпризы хакеры приготовили коммерческим и государственным предприятиям, а также что нужно сделать, чтобы нивелировать угрозу взлома и потери данных.

В зоне риска – стратегическая инфраструктура

Злоумышленники будут искать слабое звено и как только они его найдут – мы получим очередной громкий инцидент. Самыми уязвимыми с точки зрения кибератак являются государственные учреждения и стратегические государственные объекты: инфраструктура, энергетический сектор.

С точки зрения киберугроз этот год будет в чем-то даже решающим. Украина интересна не только «классическим» хакерам, которые занимаются кражей персональных данных, Ddos-атаками, рассылкой спама с зараженными письмами и пр., но и «государственным взломщикам».

Атаки последних волн становятся все более актуальными после начала военных действий в Украине. Нанимаются целые группы хакеров, целью которых является дестабилизация ситуации в стране.

«Постепенно уходят со сцены хакеры, которые взламывают информационные системы государств и корпораций из идейных соображений, распространяя информацию об ограничении прав, нарушении приватности и т. п.», – отметил в разговоре с UBR.ua руководитель Лаборатории компьютерной криминалистики Cyberlab С. Прокопенко.

«Государственным» хакерам ставят различные задачи в рамках стратегии той или иной страны, которые включают, в том числе кибератаки на инфраструктуру, разведывательные операции, промышленный шпионаж, влияние на социальные и политические процессы посредством информационных войн и др.

И если ранее атаки производились, в основном, на финсектор Украины (взломы Минфина и Казначейства), то в 2017 г. первостепенной целью для иностранных хакеров, по мнению экспертов, станут объекты социальной инфраструктуры.

К примеру, киберзащита тех же облэнерго оставляет желать лучшего. Около года назад хакеры вывели из строя компьютерную систему «Прикарпатьеоблэнерго», из-за чего 700 тыс. жителей Ивано-Франковской области остались без света.

По данным Госспецсвязи, кибернападениям также подвергались «Киевоблэнерго», «Черновцыоблэнерго», «Хмельницкоблэнерго» и «Харьковоблэнерго».

Примерно тогда же злоумышленники от имени «Укрэнерго» устроили массовую рассылку писем с вирусами, адресованных предприятиям электроэнергетики.

«Необходимо в срочном порядке предпринимать меры по улучшению кибербезопасности социально важных сфер жизнедеятельности украинцев, поскольку в дальнейшем атаки на госорганы и критическую инфраструктуру со стороны той же России, с целью дестабилизации ситуации в Украине, будут только усиливаться», – подчеркнул в разговоре с UBR.ua председатель набсовета компании «Октава Капитал» А. Кардаков.

Активизируются хакеры спецслужб РФ

Атаки в последнее время проводятся с целью выведения из строя серверов и сайтов госучреждений. Факт напряженных отношений между Украиной и РФ свидетельствует о том, что попытки дестабилизации госкомпаний, в первую очередь объектов критической инфраструктуры (не обязательно энергетики), будут актуальны в ближайшем будущем.

По мнению специалиста по технической поддержке проектов группы компаний «БАКОТЕК» В. Радецкого, самый массовый тип атак – это т. н. «волны рассылок», то есть нецелевой и обезличенный фишинг, направленный на различные организации.

Яркий пример – недавняя волна рассылок под видом оповещений от ПриватБанка, когда письмо содержало ссылку на «дроппер» вредоносного кода. На тот момент это был шифровальщик. Суть письма состояла в том, чтобы человек перешел по указанной ссылке для получения информации о задолженности по кредиту. Рассылки такого типа будут и дальше представлять опасность для организаций вне зависимости от отрасли, формы собственности и масштабов деятельности.

Как правило, пик массовых фишинговых рассылок приходится на начало каждого месяца, реже – середину или конец. Скорее всего, преступники рассчитывают, что люди в начале месяца более расслаблены и еще не вошли в рабочий ритм, а значит, более вероятно откроют письмо с провокационным содержанием.

«Зачастую, проникновение в систему происходит задолго до самой атаки. Активные действия хакеры обычно начинают во время выходных, праздников, летом или в конце года, когда у компании нет достаточного ресурса для выявления и отражения атаки. Удачное время для энергетического «блэк-аута» – зима. До этого же идет подготовительный этап, когда собирается информация о структуре компании или госоргана, начинается перехват рабочей почты,

подготовка вредоносных писем. Ведь чаще всего самым слабым звеном в системе киберзащиты является именно человек», – заметил в разговоре с UBR.ua R&D директор компании «ИТ-Интегратор» В. Кург.

То же самое можно сказать и о коммерческом секторе Украины. Ведь насколько бы не была крупной корпорация, как бы много денег она не выделяла на свою защиту, получить доступ к системе по-прежнему проще всего через беспечных работников, которым зачастую и рассылаются вредоносные письма.

Причем нередко на удочку злоумышленников попадаются не только рядовые сотрудники, но и топ-менеджмент компании, у которого гораздо более обширный доступ к финансовым данным корпорации.

«Выбор цели зависит от мотивов самих злоумышленников: коммерческий, финансовый интерес, дестабилизация ситуации внутри страны, просто желание заявить о себе. В этом году в зоне повышенной опасности будут находиться не только госучреждения, банковский и коммерческой сектор, но и системы массового обслуживания граждан: интернет-банкинги, телеком-операторы, транспортная инфраструктура (ж/д и авиаперевозки), а также энергокомпании. Целью также станет и коммерческий сектор», – отметил в беседе с UBR.ua А. Кардаков.

Как охотятся хакеры

Эксперты в сфере информационной безопасности утверждают, что очень важно выделять средства не только на средства киберзащиты, но и на повышение индивидуальных знаний сотрудников, проводить образовательную работу.

«Какой бы не была надежной система киберзащиты, если пользователи не следуют базовым правилам индивидуальной кибербезопасности на рабочем ПК, то в конце концов это может привести к заражению не только их компьютера, а и всей сети», – отметил технический директор антивирусной лаборатории Zillya! О. Сыч.

Один из самых простых способов дестабилизации обстановки не только отдельной компании, но и всей страны – вывод из строя серверов. Главный вызов для украинских компаний в таком случае – это способность перестроить свои стратегии и системы информационной безопасности с учетом реальных опасностей.

«Если говорить о ddos-атаках, то в группе повышенного риска – банки, хостеры, игровые проекты (серверы онлайн-игр). По нашей статистике, подобные ресурсы всегда занимают топ “жертв” ddos-атак», – заметил исполнительный директор компании DDoS-GUARD Д. Сабитов.

Цена безопасности

Сколько же стоит обеспечить хорошую защиту и отчего зависит ее цена? Все зависит от потребностей организации, и необходимого уровня защиты. Иногда это может быть покупка антивирусной программы, настроив которую, учреждение получит киберзащиту достаточного уровня. Но если этого недостаточно, то подход должен быть более комплексным.

Как отметил R&D директор «ИТ-Интегратор» В. Кург, стоимость защиты не должна превышать стоимость возможных потерь от хакерской атаки. Особое внимание нужно уделить системам раннего обнаружения угрозы, выявления аномалий в работе системы, иметь круглосуточную дежурную смену киберспециалистов.

Поэтому, очевидно, что большинству компаний и госструктур нужно перестать полагаться на одну лишь антивирусную систему.

Также компании стали больше уделять внимания резервированию файлов – созданию бэкапов для того, чтобы данные можно было восстановить в случае их удаления хакерами.

Для построения эффективной киберзащиты важно учитывать технологический и человеческий аспекты. В условиях современных кибератак главные события будут происходить скорее на рабочем компьютере нетехнического специалиста – бухгалтера или менеджера, чем системного администратора. Поэтому вопрос защиты конечных точек лежит на стыке IT и персональной ответственности каждого сотрудника.

«Учитывая тот факт, что заражение системы во многих случаях происходит именно из-за неосторожности сотрудников, некоторые компании на время работы даже ограничивают им доступ к соцсетям, Мессенджерам, личной почте. Но, как показывает практика, этого явно недостаточно. Если серьезно не заняться защитой данных, не залатать бреши с доступом к системе, то хакеры непременно воспользуются этим, ведь зачастую атака идет не по одному, а сразу по нескольким каналам», – отметил в беседе с UBR.ua А. Кардаков.

Хакерские программы и тактики постоянно совершенствуются, появляются новые модификации, вредоносному ПО разрабатываются новые функционалы. Это непрерывный процесс. Но компании, занимающиеся кибербезопасностью, также не стоят на месте.

«Борьба ведется, можно сказать, с переменным успехом. Сказать, что бороться с вредоносным ПО стало сложнее или критически невозможно, нельзя. Это вечное противостояние “меча” и “щита”. Победителем можно стать только на короткий промежуток времени», – отметил О. Сыч.

С тем, что с каждым годом сложность и изощренность кибератак только растет, согласны и другие эксперты. И чтобы от них защищаться, необходимо постоянно следить за современными угрозами, разрабатывать новые и дорабатывать существующие механизмы защиты.

***

28.03.2017

Три причины, почему антивирус больше не нужен

Вместо траты денег на дорогие и часто малополезные антивирусные пакеты (которые по-прежнему любят тормозить систему) стоит просто уделить

полчаса времени на настройку уже готовых механизмов безопасности внутри Windows, macOS или смартфона (InternetUA).

Несколько лет назад первой программой на «чистый» компьютер непременно устанавливался антивирус, а иногда и несколько. Интернет был похож на минное поле, где один случайный клик мыши мог заразить всю домашнюю сеть. Теперь концепция персональной защиты резко изменилась в лучшую сторону. Операционные системы стали заботиться о безопасности пользователей, браузеры предлагают превентивную защиту и множество расширений безопасности, магазины мобильных приложений теперь строго модерируют контент, не пропуская подозрительный продукт на рынок.

Установка обновлений ОС

Для сохранения безопасности своего ноутбука в 2017 г. нужно до смешного мало – просто поддерживать систему в актуальном состоянии. Сегодня разработчики очень серьезно относятся к вопросам безопасности. Обновления для Windows, macOS и Linux оперативно закрывают дыры в безопасности, если те были обнаружены в предыдущих версиях. От пользователя требуется только «не сопротивляться», как бы смешно это ни звучало. Автоматические обновления системы существенно снижают риск «подхватить болячку», кроме этого, они содержат идентификаторы новых вирусов и обновляют антифишинговые механизмы, уже встроенные в ОС.

«Вы точно уверены, что хотите это сделать?»

Постоянные вопросы ОС перед установкой новой программы – не способ заставить пользователя нервничать понапрасну, а действенный метод борьбы с вредоносным ПО. Если вы скачали подозрительный архив с драйверами, а ноутбук просит вас подтвердить установку китайской программы с непроизносимым названием – вы ведь не будете этого делать, правда? Конечно, в большинстве случаев так не происходит, но две секунды на клик «я точно хочу это установить» – невысокая цена за подстраховку.

Firewall и антифишинговые механизмы

Firewall по-прежнему остается одним из самых действенных способов блокировать сторонние подключения к компьютеру или передачу в Интернет персональных данных. Это своеобразный «последний рубеж», который должен пройти трафик и с одной, и с другой стороны. В него уже заложены списки подозрительных источников или пакетов, которые заставят Firewall бить тревогу и предупреждать пользователя о несанкционированном доступе к системе.

Обновления и дополнения браузера

Все популярные браузеры по умолчанию загружают и устанавливают обновления безопасности, не требуя подтверждение пользователя. Как и с файерволлом, достаточно позволить браузеру обновляться автоматически. Если вы часто используете открытые Wi-Fi сети в публичных местах – стоит задуматься об установке дополенений, пропускающих трафик через VPN, а убрать назойливую рекламу поможет uBlock (аналог adBlock после того как последний продали китайцам, и он начал показывать рекламу). Для успокоения

паранойи можно также запретить выполнение любых скриптов (NoScript) и установить в настройках браузера чекбокс «я не хочу, чтобы меня отслеживали».

Пароли и персональные данные

Не стоит держать данные о кредитных картах и пароли от своих аккаунтов в файле «пароли.txt» на рабочем столе. Для сохранения конфиденциальных данных существуют специальные программы-шифраторы и расширения для браузеров вроде LastPass или 1Password.

Безопасность смартфона

Советы по безопасности смартфонов ограничиваются всего двумя пунктами: поддержанием актуальной версии ОС (включите автоматические обновления системы, если они зачем-то выключены) и установкой приложений только из официального магазина (AppStore\Google Play). Кроме этого, не стоит кликать в браузере на предложения «ускорить систему» или «освободить место».

Антивирусные пакеты по-прежнему полезны для глубокого сканирования системы, или если за компьютером работают люди, склонные кликать на подозрительные баннера в Интернете (как правило, это дети или люди пожилого возраста). Но для сохранения безопасности сегодня достаточно просто не выключать встроенные в ОС антивирусные механизмы, не хранить пароли в незашифрованном виде и на всякий случай не обмениваться конфиденциальной информацией через открытый Wi-Fi в кафе (или использовать для этого VPN). Установка приложений с официальных сайтов и магазинов снижает до нуля риск заражения вирусным ПО, а обновления ОС и Firewall дают защиту от новых механизмов атак.

***

28.03.2017

Популярность биткоина увеличила число мошенничеств через соцсети

Согласно докладу ZeroFOX, популярность биткоин и рост цен привели к большому числу случаев мошенничества, совершаемых через социальные сети (Finance.Ua).

В документе были выявлены 3618 мошеннических URL-адреса, которые распространялись в среднем 24 раза в день, в течении всего периода наблюдения. В общей сложности, мошеннические адреса были опубликованы более 126 млн раз.

Среди обнаруженных схем, первая включает в себя передачу вредоносных URL-адресов, вторая сосредоточена на фишинге закрытых биткоин-ключей, а третья посылает обещание о невообразимо высокой доходности, после оплаты первоначального взноса.

ZeroFOX посоветовала пользователям биткоинов избегать помощи в майнинге, отмечая, что контракты на облачную добычу обычно хуже, чем выгоды от простого хранения цифровой валюты на частном кошельке.

Соціальні мережі

як чинник інформаційної безпеки

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

Упорядник **Терещенко** Ірина Юріївна

Редактор О. Федоренко

Свідоцтво про державну реєстрацію КВ № 5358 від 03.08.2001 р.

Видавець і виготовлювач
Національна бібліотека України
імені В. І. Вернадського
03039, м. Київ, Голосіївський просп., 3
Тел. (044) 524-25-48, (044) 525-61-03
E-mail: siaz2014@ukr.net
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.