СОЦІАЛЬНІ МЕРЕЖІ ЯК ЧИННИК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Огляд інтернет-ресурсів
(26.04–16.05)

2017 № 9

Соціальні мережі
як чинник інформаційної безпеки

Інформаційно-аналітичний бюлетень
Додаток до журналу «Україна: події, факти, коментарі»
Огляд інтернет-ресурсів
(26.04–16.05)
№ 9

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

Орфографія та стилістика матеріалів – авторські

РОЗВИТОК І ПЕРСПЕКТИВИ СОЦІАЛЬНИХ МЕРЕЖ

26.04.2017
iOS-версия WhatsApp приносит новую полезную функцию

Создатели популярного мессенджера WhatsApp неустанно трудятся над улучшением работы сервиса. К примеру, не так давно в бета-версии для Windows Phone и Windows 10 Mobile появилась функция автоматического уведомления контактов и групп о смене номера. При этом в настройках пользователь может выбрать, кому именно придёт уведомление. Ещё одну новую возможность теперь могут опробовать владельцы iPhone. Версия WhatsApp 2.17.20 для устройств под управлением iOS может привлечь внимание пользователей, нуждающихся в более комфортной работе сервиса, или же отпугнуть тех, кто обеспокоен вопросом безопасности личных данных (InternetUA).

Разработчики WhatsApp расширили возможности Siri. Ранее посредством виртуальной помощницы можно было только надиктовывать и отправлять сообщения. Теперь в случае, если у пользователя нет возможности взять в руки смартфон, к примеру, он находится за рулём, то можно попросить Siri прочесть последние сообщения. Функция доступна для владельцев устройств под управлением iOS 10.3 и выше.

Помимо расширения возможностей Siri, обновление приносит с собой ряд небольших визуальных изменений. Они коснулись вкладок звонков, контактов и групп. Кроме того, пользователи теперь могут одновременно выбирать несколько статусов на экране «Мои статусы» для того, чтобы переслать или удалить их.

***

26.04.2017
В 2017 году жители Украины отправили с помощью Viber в 1,5 раза больше сообщений

Количество сообщений, которые украинские пользователи мессенджера отправили собеседникам с января по апрель, увеличилось на 58 % по сравнению с аналогичным периодом в 2016 году. (ITnews).

Кроме того, пользователи Viber в Украине в 2017 году чаще общались с помощью аудиовызовов Viber. За первые три месяца 2017 года жители страны использовали приложение, чтобы позвонить собеседнику почти 500 млн раз, что практически втрое превышает прошлогодние показатели. При этом средняя продолжительность разговоров перевалила за отметку 6 минут. Более 89 % из всех устройств, с которых пользователи заходили в Viber в первые месяцы 2017 года, – это мобильные телефоны, и лишь 11 % – планшеты и компьютеры.

Наибольшее количество активных пользователей Viber в Украине было зафиксировано в Киеве. Также в тройку «самых активных» городов по общению в Viber вошли Днепр и Одесса.

***

26.04.2017

Ежемесячная аудитория Instagram достигла рекордных 700 млн пользователей

Количество ежемесячно активных пользователей сети Instagram достигло отметки в 700 млн человек, что является историческим максимумом для платформы. (Grifonsoft).

В сообщении компании уточняется, что в течение последних четырех месяцев, фактически с начала 2017 года, аудитория Instagram пополнилась 100 млн пользователей. Данный скачок считается наиболее стремительным за всю историю существования платформы. Впрочем, всего два года назад ежемесячная аудитория соцсети достигала только 300 млн граждан, когда сейчас насчитывается 700 млн активных пользователей.

***

26.04.2017

Сервис YouTube Kids заработал на смарт-телевизорах

В 2015 году компания Google представила специальную версию сервиса YouTube, предназначенную исключительно для детей. В отличие от стандартной версии YouTube, где представлен самый разнообразный контент, в YouTube Kids можно найти видеоролики, предназначенные только для юных пользователей. Кроме этого, YouTube Kids имеет переработанный интерфейс с большими иконками, а поисковая система распознаёт и отклоняет поисковые запросы, содержащие нежелательные для детей слова. До недавних пор YouTube Kids был доступен в качестве мобильного приложения для смартфонов и планшетов, но теперь сервис заработал и на смарт-телевизорах (InternetUA).

С момента запуска приложение YouTube Kids достигло невероятной популярности с 30 миллиардами просмотров и более чем 8 миллионами зрителей еженедельно.

Приложение YouTube Kids для телевизоров уже доступно для загрузки в 26 странах мира.

***

27.04.2017

Днепропетровщина сидит в российских соцсетях, – исследование

Большинство интернет-пользователей Днепропетровской области пользуются российскими социальными сетями – «ВКонтакте» и «Одноклассники» (События Днепра)..

Об этом говорится в исследовании компании GfK Ukraine.

Так, согласно результатам исследования, 43% респондентов в Днепропетровской области пользуются соцсетью «ВКонтакте», 38 % – «Одноклассниками». Имеют аккаунты в Facebook 23 % опрошенных, в Instagram – 9 %, в Twitter – 6 %.

В Днепре картина несколько отличается: в областном центре сетью «ВКонтакте» пользуются 44 %, «Одноклассниками» – 39 %, Facebook – 29 %, Instagram – 11 %, Twitter – 9 %.

Во втором по величине городе области Кривом Роге приверженцев «ВКонтакте» насчитали 38 %, «Одноклассников» – 28 %, Facebook – 15 %, Instagram – 11 %, Twitter – 5 %.

***

2.05.2017

Компания Facebook тайно изучала эмоциональный статус пользователей

Компания Facebook осуществляла мониторинг эмоций своих пользователей, а впоследствии передала полученную информацию рекламодателю. Австралийский новостной сайт сообщает о получении внутренней исследовательской документации социальной сети Facebook, в которой говорится, что публикуемая пользователями информация классифицирует их на подгруппы, в соответствии с выражаемыми в постах чувствами: «нервные», «тревожные», «находящиеся под стрессом» и т. д. Рекламодатели могут воспользоваться данной информацией для того, чтобы «атаковать подростков в момент, когда они потенциально более уязвимы». Этот факт Facebook отрицает (The Экономист).

Социальная сеть утверждает, что рекламодатели не могут использовать платформу Facebook для того, чтобы направлять свои усилия на аудиторию в соответствии с эмоциональным статусом людей, однако не отрицает, что факт передачи полученной в ходе исследований информации все же имел место.

Этот случай является не первым, когда компанию Facebook критикуют за проведение мониторинга эмоционального статуса пользователей социальной сети.

***

28.04.2017

Facebook запустив Messenger Lite у 150 країнах

Компанія Facebook запустила полегшену версію Messenger у 150 країнах світу. Зараз Messenger Lite є в Німеччині, Японії, Італії, Марокко, Нідерландах, Перу та Україні, у тому числі (Корреспондент.net).

Видання TechCrunch зазначає, що з анонсованих 150 країн мессерджер став доступний поки в 132. Однак, ймовірно, він з'явиться в Google Play найближчим часом і для інших.

Messenger Lite доступний для смартфонів, які мають невеликий обсяг пам'яті, малопродуктивний процесор, а також низьку швидкість підключення.

Додаток забезпечує відправку фото, посилань і стікерів. Однак за низкою критеріїв він дещо менш функціональний, ніж оригінальна версія.

***

3.05.2017

Илья Кабачинский

Facebook наймет 3000 модераторов для мониторинга контента и прямых трансляций

В середине апреля в США человек в прямом эфире на Facebook убил мужчину и сообщил, что до этого сделал еще 15 убийств. Только после сотен жалоб трансляцию закрыли. Событие сразу породило дискуссию: должна ли соцсеть прекращать проводить прямые трансляции, ведь подобное случается уже не первый раз – до этого в прямых трансляциях на Facebook убивали, насиловали и издевались. В компании о закрытии функции говорить не хотят и предлагают менее радикальный способ решения проблемы (AIN.UA).

Основатель компании Марк Цукерберг заявил, что Facebook возьмет на работу более 3000 человек по всему миру, пишет Engadget. Департамент, который в целом будет состоять из 7500 сотрудников, займется модерацией контента в социальной сети, в том числе и прямыми трансляциями.

«Эта команда возьмет на себя миллионы тех репортов, которые поступают к нам каждую неделю. Цель – пресечь появление в Facebook вещей, которые там запрещены, вроде издевательства и ругани», – отметил Цукерберг.

Основатель соцсети заметил, что сейчас основной показатель работы команды – скорость: чем быстрее удастся выявить нежелательный контент, тем быстрее его можно будет убрать. Поэтому Facebook получит упрощенную систему жалоб. Также компания предпринимает действия против суицидов: за счет искусственного интеллекта соцсеть может обозначить потенциальных жертв. За счет этого сотрудникам социальной сети не так давно даже удалось предотвратить одно из них.

***

3.05.2017

В WhatsApp можно будет закреплять избранные чаты

Современные мессенджеры позволяют перенести любое общение в онлайн-пространство, будь то беседа с родственниками, друзьями или коллегами по работе. Иногда в одном мобильном приложении скапливается несколько десятков активных чатов и поиск наиболее важных из них отбирает много времени. Функция закрепления выбранного чата вверху списка решает эту проблему и не является новой для многих сервисов быстрых сообщений. К примеру, в Telegram число прикрепленных бесед может достигать 5, а в Viber – больше 10. Однако разработчики WhatsApp только сейчас приступили к тестированию этой функции в закрытой бета-версии клиента (IGate).

Закрепить в начале списка можно будет как индивидуальные, так и групповые чаты, но не больше трех одномоментно. Возможно, в финальной версии их число будет увеличено. При закреплении чатов остальные беседы, даже при наличии непрочитанных сообщений, будут располагаться под ними.

***

3.05.2017
Facebook запустил новые игры в Messenger

Компания Facebook расширила ассортимент игр, доступных прямо в мессенджере Facebook Messenger. Теперь всего в Messenger доступно порядка 50 игр. Кроме того, начинается внедрение игровых возможностей, позволяющих реализовывать более насыщенный геймплей (IToboz.com).

Среди новых геймерских возможностей – пошаговые игры, таблицы результатв и турниры. Чтобы начать игру в переписке, надо просто нажать на знак плюса рядом с текстовым полем и перейти к опции «Игры», после чего выбрать подходящую по настроению игру. Например, можно сыграть в ностальгические Snake, PacMan или Space Invaders, вариации карточных Blackjack до Gin Rummy и Solitaire, а также судоку, боулинг, приготовить гамбургер в Cooking Mama или стать Бэтменом в Bat Climb. Новые игры будут распространяться в международном масштабе в следующие недели для iOS и Android.

***

4.05.2017
Facebook разрешила «реагировать» на комментарии

Команда социальной сети Facebook без особого шума запустила новую полезную возможность для своих пользователей. Теперь можно ставить не только «лайки» к комментариям, но и использовать «реакции» для их оценки (IToboz.com).

Facebook также запустила реакции в фирменном мессенджере Messenger чуть больше месяца назад.

***

5.05.2017

Facebook популярний серед чверті населення Землі

У першому кварталі 2017 року прибутки компанії Facebook суттєво зросли завдяки новим юзерам. За результатами нового дослідження, кількість користувачів соцмережі сягає майже двох мільярдів (Інформаційна агенція «Вголос»).

Щомісяця Facebook користуються 1,94 млрд людей, з них приблизно 1,3 млрд людей – щодня, повідомили в компанії, передає BBC.

Доходи Facebook у першому кварталі поточного року сягнули 3 млрд доларів, на 76 % більше у порівнянні з аналогічним періодом минулого року.

Проте в компанії зауважили, що зростання доходів від реклами уповільнилось.

В останні тижні компанію також постійно критикували за історії, пов'язані із мовою ненависті, жорстокого поводження з дітьми та демонстративним нанесенням собі шкоди в соціальній мережі.

Третього травня голова Facebook Марк Цукерберг повідомив, що взяв на роботу додатково 3 тис. людей, які будуть модерувати контент на сайті.

Зараз соцмережею щомісяця користується чверть населення земної кулі. Причому нові юзери – переважно не з Європи та Північної Америки.

Після оголошення результатів дослідження пан Цукерберг зауважив, що такий масштаб дозволяє збільшувати роль Facebook і розвиватися в напрямку телебачення, охорони здоров'я та політики.

***

9.05.2017

Facebook тестирует возможность подписки на новости по теме

Facebook тестирует возможность подписываться не на определенные страницы, а на страницы по темам. Например, пользователь может подписаться на топики «театр», «фильмы ужасов» или «фотографии» (REALIST.ONLINE).

Подписавшись на ту или иную тему, пользователь будет иметь возможность читать различные страницы, которые пишут об этом, независимо от того, подписался ли человек на конкретную страницу или нет.

Это поможет разнообразить пользователям список источников своей новостной ленты.

Ранее основатель Facebook Марк Цукерберг обращал внимание на то, что в соцсети стараются не только дать альтернативную точку зрения для того или иного пользователя, но предоставить ему «широкую и полную картину» на то или иное событие.

***

9.05.2017

Пользователи «ВКонтакте» не смогли разобраться с новой функцией

Пользователи социальной сети «ВКонтакте» не смогли разобраться с новой функцией. Примерно неделю назад портал создал специального бота с названием «Лис», который должен был привлечь юзеров к разделу «истории» (GFS).

Новый раздел дает возможность опубликовать фотографию или короткое видео, которое будет находиться в ленте новостей сутки. После этого оно самостоятельно удалится. После введения данной функции администрация отметила низкий спрос на нее. В связи с этим, было решено начать вирусную рекламную кампанию, в рамках которой и был выпущен бот.

На странице Лиса имелось сообщение, согласно которому каждый пользователь, который запостит определенное количество историй, получит набор стикеров в подарок. В итоге раздел начал набирать большую популярность. Несмотря на то, что он имеет относительно простой интерфейс, многие пользователи запутались в нем, о чем написали в службу поддержки социальной сети.

Некоторые пользователи неправильно поняли послание бота, начав постить свои истории из жизни в текстовом виде. После этого они обратились к администрации, потребовав свои законные паки стикеров. Представители ресурса разъяснили ситуацию, после чего сделали соответствующее сообщение, которое появилось в ленте у всех юзеров.

***

9.05.2017

Фотографии в Instagram теперь можно публиковать через мобильную версию сайта

Разработчики популярного сервиса Instagram обновили мобильную версию своего сайта. Теперь пользователи могут загружать фотографии не только с помощью мобильного приложения, но и через веб-версию сервиса. К сожалению, загрузка видео, фильтры, создание «Историй» и сообщения в этом случае недоступны (IToboz.com).

Сообщается, что в первую очередь обновление нацелено на пользователей из развивающихся стран, которые могут испытывать проблемы с быстрым доступом в Интернет или не обладать устройством с достаточным количеством встроенной памяти.

***

11.05.2017

Лаборатория искусственного интеллекта Facebook анонсировала новый метод машинного обучения

Пока что технология существует только как исследовательский проект – она еще не стала частью продукта Facebook. Но инженеры компании Майкл

Аули и Дэвид Гренджье уверены, что скоро это произойдет. Социальная сеть уже использует ИИ для автоматического перевода статусов на другие языки, но переход от прототипа к приложению всегда требует много работы (Finance.Ua).

По мнению Кристофера Маннинга, профессора Стэнфордского университета, специалиста по машинному переводу и рецензента работы, это «впечатляющее достижение», в особенности потому, что может обучать переводческие модели быстрее, чем существующие системы. И Facebook понемногу распространяет эту технологию на свою социальную сеть, покрывающую 1,8 млрд человек.

За последние пару лет в области технологий перевода произошло больше нового, чем за предыдущие десять. Свои разработки создают Google, Microsoft, Baidu. Но подход Facebook слегка отличается от большинства крупных игроков. Она использует так называемую сверточную нейронную сеть, которая может анализировать множество различных элементов за раз, чтобы потом организовать их в логической иерархии, сообщает Wired.

В результате Facebook может тренировать свою систему, расходуя значительно меньше вычислительных мощностей. То есть, продвигать свою технологию гораздо быстрее.

Сверточная нейронная сеть уже доказала свою эффективность при распознании объектов на фотографиях. Другие команды тоже применяли ее как базовую технологию для машинного перевода, например, DeepMind. Но, как считает Маннинг, система, разработанная Facebook, наиболее продвинутая на сегодня.

***

11.05.2017

Facebook буде знижувати в стрічці новин посилання на сайти з неякісним контентом

Соціальна мережа Facebook оголосила про нові зміни в своєму алгоритмі формування стрічки новин (detector.media).

Тепер система буде знижувати пости з посиланнями на сайти «низької якості», йдетсья у блозі соцмережі. Під це визначення потраплять сайти з малим обсягом контенту, дратуючим контентом, шкідливою або шокуючою рекламою. Зокрема, мова йде про спливаючі оголошення, рекламу для дорослих, рекламу товарів для боротьби з надлишковою вагою тощо. При цьому сайти з якісним контентом можуть отримати невеликий приріст реферального трафіку.

Перш ніж запровадити ці зміни, Facebook провела опитування серед користувачів. Воно виявило, що багатьом з них не подобається наявність у стрічці новин посилань, які ведуть на матеріали «що вводять в оману, мають сенсаційний характер, містять спам, включаючи публікації «для дорослих», «шокуючий контент».

Для того, аби втілити нові зміни в своєму алгоритмі, Facebook проаналізувала сотні тисяч веб-сторінок, визначаючи ті з них, які містять низькоякісний контент, та потім використала отримані дані для навчання системи штучного інтелекту. Вона буде сканувати нові посилання, якими люди діляться в стрічці та занижуватиме сайти-порушники. Крім того, вони не зможуть купувати рекламу в Facebook.

***

10.05.2017

Periscope запускает 360-градусные онлайн-трансляции на Android

В конце прошлого года компания Twitter объявила о поддержке 360-градусных онлайн-трансляций в сервисах Twitter и Periscope. После полугода тестирования эта функция стала общедоступной. В апреле сферические видео начали появляться в Periscope для iOS, а теперь они предлагаются пользователям Android-устройств. Для просмотра онлайн-трансляции пользователю неоходимо вращать смартфон вокруг себя или поворачивать картинку свайпами по экрану (InternetUA).

В то время как смотреть 360-градусные трансляции в Periscope могут все желающие, для создания такого контента потребуются специальные приспособления. На данный момент нативная поддержка Periscope Live 360 доступна только с 360-градусными камерами компании Insta360: Insta360 Nano для iOS и Insta360 Air для Android. Также трансляции можно вести с помощью камер Ricoh Theta S и Orah 4i, но для этого придётся использовать Periscope Producer.

***

10.05.2017

Telegram запустил голосовые звонки в приложении для Mac и Windows

Функция голосовых звонков стала доступна в альфа-версии Telegram Desktop. В предварительной версии доступны звонки другим пользователям, также можно посмотреть информацию о последних вызовах, они отображаются в специальной вкладке, на которую можно перейти из основного меню. Также предусмотрены настройки приватности для звонков (InternetUA).

Telegram запустил аудиозвонки через мобильное приложение в конце марта. Эта функция основана на той же технологии шифрования, что используется в секретных чатах мессенджера. Во время голосовых звонков на десктопе, как и в мобильной версии Telegram, демонстрируются четыре эмодзи, которые можно сравнить с собеседником, чтобы удостовериться в работе шифрования мессенджера.

Управление устройствами для ввода-вывода звука в Telegram для Mac и Windows отсутствует: звонок может идти через внешнюю аудиосистему при

подключённых наушниках, и изменить эту настройку у пользователя не получится.

***

10.05.2017
Огляд нової музики «ВКонтакте»: чи варто платити?

В останні роки слухати безкоштовно музику в онлайні стає все складніше. Тенденція впровадження абонплати за музичний контент добралася і до музики «ВКонтакте». Тепер слухати музику безкоштовно «ВКонтакте «можна буде тільки з рекламою і без можливості збереження її для оффлайн прослуховування в додатках для iOS і Android (Знай.ua).

Канал Rozetked підготував огляд нової музики «ВКонтакте» і спробував відповісти на питання «чи варто за неї платити?».

Нова музика «ВКонтакте» отримала оновлений інтерфейс, який став легше і трохи зручніше. У вкладці «рекомендації» на основі ваших музичних уподобань пропонується музика, яка може бути вам цікава.

До мінусів нової музики «ВКонтакте» можна віднести сильний розкид в якості: багато композицій з низькою якістю, відсутність обкладинок альбомів і плейлистів. Поки що це все та ж звалище користувача музики, що й раніше. Знайти можна практично все, але ось яка буде якість – питання.

Ще одним мінусом музики «ВКонтакте» можна сміливо вважати відсутність оновленого додатка ВК для iPad, як і нового додатка BOOM, в якому при оформленні підписки з'являється можливість зберігати музику для оффлайн прослуховування. Немає і окремих програм для Mac і Windows.

СОЦІАЛЬНІ МЕРЕЖІ ЯК ВИЯВ ФОРМУВАННЯ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА

11.05.2017
Крамченков vs. Сокур: реакція соцмереж

Сумчани у Facebook бурхливо відреагували на бійку у стінах мерії, коли побилися депутат міської ради Андрій Крамченков та лідер сумського осередку ГО «Східний корпус» Денис Сокур (SumyToday).

***

11.05.2017
«Україна рухається у правильному напрямку», – соцмережі відреагували на безвіз

Новина про затвердження радою ЄС безвізового режиму для України викликала ажіотаж у соціальних мережах. Користувачі радіють і сиплять жартами на цю тему (ZIK).

***

15.05.2017

Волонтери відправили листи 100 депутатам, аби ті підтримали армію

В рамках акції «Е-десятина» волонтери надіслали листи з пропозицією підтримати армію 100 депутатам Верховної Ради (ZIK).

Про це повідомляється на сторінці фонду «Повернись живим» у Facebook.

Волонтери зазначають, що ще сотню звернень топ-політикам надішлють до кінця травня.

Поки депутати думають, волонтери закликають громадян України підтримати армію особисто.

«Кожна гривня наближує нашу перемогу, і як показує досвід – прості люди часто можуть більше ніж політики», – написали організатори акції «Е-десятина».

***

16.05.2017

Ховайся, хто може, – реакція соцмережі на заборону «Одноклассников», «ВКонтакте» та «Яндекса»

Президент України Петро Порошенко підписав указ про нові санкції Ради національної безпеки і оборони України від 28 квітня 2017 року, які передбачають, зокрема, блокування доступу до соцмереж «ВКонтакте» і «Однокласники» (UaInfo).

Ось що про це пишуть у соцмережах:

«Скажіть, може бути, я щось пропустила? – Якщо блокують “ВКонтакте”, то Мінстець або хтось там ще на Банковій розробив свою, українську, молодіжну соцмережу з музикою, фільмами, бложиками і фоточками?», – обурено прокоментувала заборону керівник Одеського Кризового Медіа центру Олена Балаба.

«Не можу назвати це своєчасним рішенням, тому що, на мій погляд, це взагалі перше, що потрібно було зробити з початком агресії», – написала Аміна Окуєва.

«Запам’ятайте цей день, шановні мешканці ФБ. і проведіть його гідно. Тому що завтра сюди прийдуть Вконтакте і Однокласники. "І живі будуть заздрити мертвим», – написала ведуча програми Санден на Радіо «Аристократи» Анна Санден.

«Зараз будуть дикі крики про зраду і про обмеження свободи слова від вати і зраднюков)», – написала журналістка Катерина Золотарьова.

«Передбачаю жахливу ломку, що чекає на українську вату, яку лишили можливості верещати хором за російськими темниками. Нехай щастить!», – пише Олександр Онищенко.

«Скоро ваші мами і діти почнуть запитувати що таке проксі і VPN. Не ведіться, поступово заманюйте їх у Facebook.

Тут ми будемо їх привчати до політики, котиків, реалій життя зі зрадою і перемогою. А якщо вони будуть задавати багато питань, у нас завжди знайдеться відповідь – погугли», – пише Володимир Попов.

БІЗНЕС І СОЦІАЛЬНІ МЕРЕЖІ

26.04.2017

Facebook тестирует обложки с видео для Страниц брендов

Компания хочет добавить интерактива Страницам брендов и издателей. Сеть подтвердила, что тестирует функцию, которая позволит размещать видео на обложках. «Мы всегда искали возможность помочь брендам создавать вовлекающий опыт для аудитории», – отметили в Facebook. Впервые функцию заметили на странице драмы Netflix «Нарко». Во время конференции для разработчиков F8 компания объявила о том, что пользователи могут трансформировать статические профили благодаря сторонним приложеним (Marketing Media Review).

***

26.04.2017

Книжный креатив: сотрудники магазина «оживляют» книги в Instagram

Независимый книжный магазин во Франции буквально «оживил» книги в Instagram. К радости своих 21000 фолловеров Librairie Mollat регулярно размещает фото сотрудников и покупателей, которые являются продолжением обложек. Прекрасный пример увлекательного промо в сетях (Marketing Media Review).

***

26.04.2017

Intel и Facebook повысят производительность платформы глубокого обучения Caffe2

По оценкам экспертов, к 2020 году в мире будут работать более 50 миллиардов машин и устройств, способных подключаться к Интернету и обмениваться информацией между собой. Эти устройства будут генерировать

огромные объёмы данных, для анализа которых потребуются передовые системы искусственного интеллекта и глубокого обучения. Учитывая это, Intel и Facebook сотрудничают над увеличением производительности открытого фреймворка глубокого обучения Caffe2.

Докладніше

***

27.04.2017

Компания Twitter нарастила пользовательскую базу, но всё ещё остаётся убыточной

Компания Twitter опубликовала отчёт по итогам первого квартала 2017 финансового года. Выручка компании по итогам трёх месяцев составила 548 млн долларов против 595 млн годом ранее (InternetUA).

Twitter продолжает оставаться убыточной компанией. В прошедшем квартале чистый убыток составил 62 млн долларов против убытка в 80 млн в первом квартале прошлого года.

Однако есть и положительные моменты. К примеру, компания заявила, что ежемесячное количество активных пользователей увеличилось на 9 млн, до 328 млн человек. При этом ежедневное количество активных пользователей выросло на 14 %. Также на 17 % увеличилась выручка от продажи рекламы. Всё это привело к тому, что акции Twitter выросли на 10 %.

***

27.04.2017

Ольга Карпенко

Павел Дуров анонсировал запуск платежей в Telegram

Команда Telegram собирается запустить платформу для платежей в мессенджере с помощью ботов. Нововведение анонсировал основатель платформы Павел Дуров в Instagram. Он продемонстрировал черновик официального анонса для блога Telegram под названием «Платежи для ботов» в Stories. «Вкратце – платежное API для приема платежей в ботах, без комиссий от Telegram, зовут payment-провайдеров подключаться», – так нововведение описывают в канале «Telegram-маркетинг».

Докладніше

***

3.05.2017

Twitter начнет транслировать 12 новых каналов

Сервис микроблогов Twitter начнет предоставлять услуги по трансляции 12 новых каналов. Об этом сказано в заявлении компании (ЛІГАБізнесІнформ).

Среди новый партнеров Twitter – телеканал Bloomberg News, портал The Verge, пишущий о новинках IT, развлекательно-новостной портал BuzzFeed.

В частности, Bloomberg будет предоставлять свой live-контент в режиме 24/7, The Verge и BuzzFeed также будут показывать видеошоу. Часть предложений будет доступна уже в ближайшие дни.

Также Twitter будет показывать концерты, матчи Женской национальной баскетбольной ассоциации, турниры по гольфу, ряд других спортивных программ и мероприятий.

Финансовая сторона договоренностей пока не раскрывается.

***

4.05.2017
Илья Кабачинский
Google и Facebook контролируют 20 % мировых доходов с рекламы

Американские технологические компании Google и Facebook с миллиардной аудиторией пользователей, вместе получают свыше 20 % доходов на мировом рынке рекламы, сообщает CNBC. Суммарно это больше $100 млрд. Исследование провело агентство Zenith, которое составило список из 30 компаний.

Докладніше

***

2.05.2017
Спасти индустрию: как блокировка интернет-рекламы поможет Google и другим компаниям

В конце апреля появилась новость, что компания Google, возможно, занимается созданием блокировщика рекламы для собственного браузера Chrome. Новость более чем странная: зачем компании, которая зарабатывает на рекламе, ее блокировать? По всей видимости, масштабы сложностей с интерактивной рекламой достигли таких размеров, что на них обратили внимание сами издатели. В своей статье, журнал The Wired объяснил суть будущих изменений.

Докладніше

***

10.05.2017
Facebook проведет дешевый Wi-Fi в Индию

Компания Facebook Inc. планирует совместно с индийским мобильным оператором Bharti Airtel разместить 20 тысяч точек доступа Wi-Fi на территории Индии в ближайшие месяцы, говорится в пресс-релизе соцсети (Finance.Ua).

Пользователи смогут выбирать между суточным, недельным или месячным тарифами стоимостью около 10 рупий ($0,15) в сутки. Отмечается, что средний месячный доход индийцев составляет всего $160.

Facebook уже разместил 700 точек доступа в 4 индийских штатах.

Крупнейшие компании соревнуются между собой, чтобы привлечь новых пользователей и укрепить свое влияние на индийском рынке. Однако, в отличие от Facebook, главный конкурент компании на индийском рынке Google не берет плату за доступ в интернет. Google уже установила бесплатные точки доступа к интернету на сотне железнодорожных станций в разных регионах страны.

***

10.05.2017

Израильский стартап придумал робота, оптимально пишущего в Facebook

Стартапом Keywee разработан робот, отправляющий сообщения в Facebook, Instagram и Twitter (Русский Еврей).

По сообщению «Аруц шева», робот анализирует структуру контента и реакцию пользователей на публикации в сети и оформляет свои сообщения таким образом, что они вызывают больший интерес, чем сообщения, опубликованные людьми. Робот уже помог повысить трафик на новостях BBC, CNN, New York Times, AOL, Forbes и других сайтов.

Программное обеспечение может быть перестроено под те или иные возрастные и профессиональные требования. Так, выяснилось, что спортивные сообщения, опубликованные на спортивных сайтах под рубрикой «Если вы пропустили», снижают трафик на 10 %, а те же сообщения, опубликованные под той же рубрикой на новостных сайтах, повышают трафик на 25 %. Оказалось, что использование смайликов в сообщениях, связанных с модой, увеличивает трафик на 10 %. Система оценивает тысячи переменных и определяет оптимальный формат и контент сообщения.

***

16.05.2017

Як заборона російських соцмереж і програм позначиться на вітчизняному бізнесі *// І чи вдасться їх швидко замінити на «дозволені» аналоги*

Катерина Гребеник, Світлана Рябова, Віктор Гаценко

Президент Петро Порошенко розширив список юросіб, які перебувають під санкціями у зв’язку з окупацією Криму і війною на Донбасі. Цього разу список поповнився популярними соцмережами «Одноклассники», «ВКонтакте», поштовими сервісами Mail.ru і «Яндекс», цілою низкою російських ЗМІ. Крім того, санкції введені проти деяких ІТ-компаній, продукти яких дуже популярні в Україні: «Лаборатория Касперского», DrWeb,

«Софтлайн», ABBYY і «Абі Україна ЛТД» (продукти «1С», Abbyy FineReader, Abbyy Lingvo).

Докладніше

СОЦІАЛЬНІ МЕРЕЖІ І ПРОБЛЕМИ СУСПІЛЬНОЇ БЕЗПЕКИ

Інформаційно-психологічний вплив мережевого спілкування на особистість

26.04.2017

Группы смерти: опасная игра добралась до Великобритании

Анастасия Очеретнюк

Смертельная виртуальная игра, от которой в Украине гибнут подростки, добралась и до Великобритании. Об этом сообщает Daily Mail **(**podrobnosti.ua).

В обращении к родителям одна из школ Британии рассказывает о том, что игра «Синий кит» поощряет молодежь к выполнению ряда задач в течение 50 дней, начиная с пробуждения в ночное время и заканчивая самоубийством.

Стоит отметить, что «группы смерти» известны и в других странах Европы. О ней говорят в Латвии, Италии и даже в США.

***

4.05.2017

Залежність дітей від Інтернету: у Дніпрі відзнімуть соціальний відеоролик

У Дніпрі реалізується унікальний проект, спрямований на привернення уваги до проблеми зацикленості сучасних дітей на гаджетах, соціальних мережах «Ми з Інтернету». Про це під час прес-конференції в ІА «Мост-Дніпро» розповіла співзасновник громадської організації «Товариство підтримки талантів ZIRKA», керівник дитячої кіношколи ZIRKA Ніка Рудакова, передає Дніпроград з місця подій (Дніпроград).

«Наразі у нас виникає проблема пов’язана з розвитком емоціонального інтелекту та соціальною адаптацією. Близько 92 % дітей до 6 років вже користуються гаджетами, коли вони приходять в суспільство – садочок чи школу вони не знають як себе вести із людьми, вони не готові до комунікації та дружби. За допомогою відеоролику ми привернемо увагу до гострого браку спілкування в реальному світі і соціальної адаптованості молодого покоління», – розповіла Ніка Рудакова.

Режисер майбутньої кінострічки Ростислав Мельник розповів, що у відеоролику вони відобразять паралельну реальність, де усі спілкують лише за допомогою Інтернету.

«Таким чином ми покажемо молодому поколінню, що живе соцмережами, що вони втрачають частину свого справжнього життя. Іноді круто вийти на вулицю і побігати, подуріти, покататися на роликах. Адже справжня реальність краща – це великий кінотеатр 5D», – розповів Мельник.

Відеоролик планують відзняти протягом двох місяців, і вже на початку липня публікувати в Інтернеті та розповсюджувати по школах Дніпра.

***

11.05.2017

В сети появилась позитивная альтернатива суицидальному «Синему киту»

Бразильские специалисты по рекламе и графическому дизайну Ана Хоппе и Рафаэль Тилшер запустили в сети альтернативу смертельной игре «Синий кит» – позитивную игру «Розовый кит» (Обозреватель).

Участники «Розового кита» тоже выполняют 50 заданий, но в данном случае цель – помощь ближнему и достижение взаимопонимания с родственниками.

«Мы с Рафаэлем разговаривали о “Синемките” и о том, как интернет может очень быстро пропагандировать во всем мире что-то нехорошее, но мы в силах извлечь из этого урок. Мы захотели показать людям, что человек способен дарить миру любовь, получать и распространять ее», – говорит Хоппе.

О свои достижениях игроки отчитываются в соцсетях, используя хэштег #BallenaRosada. Издание отмечает, что игра предусматривает как серьезные задания (обзавестись новым другом или помочь жертве травли), так и забавные: обнять фрукт, разговаривать строчками из песен.

Авторы «Розового кита» отметили, что прежде чем распространить свою идею в сети, они обсудили ее с психологом. Вместе с тем Хоппе отмечает, что «Розовый кит» «играет вспомогательную роль, но не может быть курсом лечения».

Стоит отметить, что изначально «Розовый кит» предназначался для бразильских подростков в возрасте 13-17 лет, однако теперь к ней присоединились участники самых разных возрастов во всем мире.

***

10.05.2017

Instagram призывает открыто говорить о проблеме психического здоровья

В мае Instagram объединяет пользователей с помощью новой кампании #HereForYou, которая поощряет искать помощи тем, кто страдает от

психических заболеваний. Бренд запустил видео с тремя героями-инициаторами сообществ на платформе, которые призваны помочь нуждающимся. Ссылка в видео направляет зрителей к сайту, который помогает найти нужные ресурсы по проблеме в Instagram. В прошлом году сеть также представила новую функцию психологической поддержки, с помощью которой можно анонимно помочь любому, кто страдает от психических заболеваний. В рамках проекта Instagram объединился с другими организациями: Crisis Text Line, National Eating Disorder Association и Samaritans (Marketing Media Review).

***

11.05.2017
В сети обнаружили тайное общество любителей чужих селфи

В Twitter существует тайное общество Selfie Deck, члены которого ретвитят и лайкают селфи своих соратников ради взаимной популярности (IToboz.com).

По данным издания, изначально сообщество сформировалось в знак протеста против новой алгоритмической ленты Twitter, однако вскоре оно стало пристанищем для желающих сделать свои фотографии более популярными. Название Selfie Deck произошло от платформы TweetDeck для расширенного поиска информации в твитах. Члены тайного общества создают в TweetDeck отдельный раздел с аккаунтами своих соратников, после чего в обязательном порядке ретвитят и лайкают каждую их запись. Вступить в Selfie Deck можно только по приглашению одного из действующих членов, причем приоритет отдается владельцам аккаунтов с большим числом подписчиков из-за потенциальной возможности привлечь новых сторонников. Во вторник, 9 мая американец Картер Уилкерсон побил рекорд Twitter, набрав максимальное за историю соцсети количество ретвитов – 3434902. За месяц до этого Уилкерсон поинтересовался у американской сети быстрого питания Wendy’s, сколько ретвитов ему необходимо собрать, чтобы получить годовой запас курицы. Представители компании ответили, что ему потребуется 18 миллионов ретвитов, после чего Уилкерсон опубликовал скриншот сообщения и обратился к подписчиком с просьбой помочь набрать ретвитов.

Маніпулятивні технології

26.04.2017
Основатель Wikipedia начал борьбу с фейками

Основатель «Википедии» Джимми Уэйлс создал онлайн-платформу для проверки новостей, опубликованных в Сети, на их достоверность. Проект получил название Wikitribune (МедиаБизнес).

По замыслу Уэйлса, это будет бесплатный и свободный от рекламы сервис, существующий в первую очередь на пожертвования. Работать в Wikitribune будут как добровольцы, так и профессиональные журналисты, которые, в свою очередь, смогут получать за свою работу гонорар.

Журналисты и добровольцы будут создавать, проверять и одобрять новостные материалы, а также указывать источник информации. «Мы разрабатываем живой инструмент, который сможет предоставлять достоверную информацию с конкретными доказательствами для того, чтобы читатели смело составляли свое собственное мнение», – говорится на сайте платформы.

По данным Business Insider, Уэйлс уже запустил 30-дневную краудфандинговую кампанию, чтобы собрать средства для найма журналистов. Для начала Wikitribune надеется привлечь к сотрудничеству 10 журналистов, сам же Джимми Уэйлс займет посты руководителя проекта и его главного редактора.

***

27.04.2017

Google изменил алгоритм поиска для борьбы с фейками

Компания Google изменила алгоритмы работы своего интернет-поисковика в целях борьбы с распространением оскорбительного контента и фейков. Сообщение об этом было опубликовано в блоге компании (IToboz.com).

«Наши алгоритмы помогают определить надежные источники информации среди сотен миллиардов страниц в каталоге. Однако нам стало очевидно, что в незначительной доле ежедневных поисковых запросов (около 0,25 %) система выдает результаты с оскорбительным или вводящим в заблуждение контентом, а не тем, что ищут пользователи», – говорится в сообщении Google. Чтобы решить эту проблему и предотвратить распространение подобного рода контента, компания усовершенствовала методы оценки, а также обновила алгоритмы, чтобы система выдавала более надежную информацию. В частности, в Google ужесточили правила, касающиеся того, какую информацию считать нежелательной, отмечает ТАСС. В эту категорию вошли «вводящие в заблуждение данные, непредусмотренные оскорбительные результаты поиска, мистификации и безосновательные теории заговоров». Сотрудники компании будут отмечать страницы, на которых появляются публикации такого рода.

***

3.05.2017

Facebook визнала, що її платформу використовують для здійснення «штучного впливу»

Компанія Facebook опублікувала результати свого дослідження щодо поширення фейкових новин через її платформу. У ньому компанія визнала, що ризик використання платформи в маніпулятивних цілях досить високий.

Докладніше

***

27.04.2017

У штабі Навального повідомили про спроби АП використовувати топових відеоблогерів для дискредитації політика

Голова передвиборного штабу російського опозиціонера Олексія Навального Леонід Волков повідомив про спроби адміністрації президента РФ домовитися з топовими блогерами й адміністраторами популярних паблік «ВКонтакте» про розміщення інформації, що дискредитує Навального (LB.ua).

Про це він написав на своїй сторінці в Facebook.

За словами Волкова, представники адміністрації президента пропонують за розміщення «джинси» про Навального вдвічі більше, ніж за звичайну рекламу. «Щоправда, поки що безуспішно», – додав він.

Волков вважає, що блогери-мільйонники дорожать своєю репутацією і не будуть давати «заказуху» про Навального, який затребуваний серед їхньої аудиторії. «У цих умовах – це рівнозначне самогубству», – зазначив голова передвиборного штабу політика.

Саме тому, на думку Волкова, ролик, в якому Навального порівнювали з Гітлером, розмістили з анонімного аккаунта.

У бесіді з «Новою газетою» Леонід Волков зазначив, що представники АП почали спілкуватися з блогерами ще до анонсованої співрозмовниками телеканалу «Дождь» кампанії з дискредитації політика.

***

9.05.2017

Facebook дал инструкцию, как не попасться на фейковые новости

Компания Facebook разместила в крупнейших британских газетах инструкцию по выявлению недостоверных новостей (From-UA).

Такая инструкция появилась в The Guardian, The Daily Telegraph и The Times, говорится, что нужно внимательно проверять источник публикаций, скептически относиться к вызывающим заголовкам и проверять даты в материалах.

Полностью список советов по выявлению фейковых новостей выглядит так:

– Относитесь к заголовкам со скепсисом;
– Внимательно смотрите на URL;
– Ищите первоисточник;
– Обращайте внимание на необычное форматирование;

– Обратите внимание на фотографии;
– Проверяйте даты;
– Проверяйте доказательства;
– Ищите другие сообщения по теме;
– Не шутка ли эта история?
– Некоторые фейковые заметки – сознательная сатира.

Facebook в советах не упоминается, но на материале размещен логотип социальной сети. Аналогичные советы Facebook ранее неоднократно размещал и в онлайн-СМИ.

***

10.05.2017

Силовиков привлекут к расследованию поддельных аккаунтов в Facebook

Газета USA Today подвергается масштабной атаке спамеров, которые создают поддельные аккаунты в Facebook и делают их подписчиками издания. Во время чистки соцсети от ложных аккаунтов страница USA Today лишилась более 5 млн лайков, однако спамеры уже восполняют эту потерю. Газета просит ФБР расследовать ситуацию.

Докладніше

***

9.05.2017

Суд зобов'язав Facebook видаляти пости, які несуть «мову ворожнечі»

Про це повідомляє Kronen Zeitung (ESPRESO.TV).

Позов до суду проти Facebook подала Партія зелених Австрії, лідер якої Єва Главішніг постраждала від образливих повідомлень у соцмережі.

Суд вважає, що публікації про Главішніг чітко несуть «мову ненависті» та суперечать «стандартам спільноти».

Тож суд постановив, що Facebook має видаляти образливі пости не лише в Австрії, а й в усьому світі, зазначивши, що лише блокування такого контенту недостатньо.

«Це неймовірне досягнення», – прокоментував рішення суду спікер партії Дітер Брош. Він висловив сподівання, що Facebook змінить свою політику стосовно образливих публікацій, зважаючи на ймовірні позови у майбутньому.

***

10.05.2017

На Львівщині засудили юнака за пропаганду комунізму у соцмережах

На Львівщині засуджено юнака, який пропагував комуністичну ідеологію у соцмережах (Західна інформаційна корпорація).

Про це 10 травня інформує прес-служба прокуратури Львівської області.

За процесуального керівництва прокуратури Львівської області слідчим управлінням Головного управління національної поліції у Львівській області скеровано до суду обвинувальний акт відносно юнака, який вчинив кримінальне правопорушення, передбачене за ч.1 ст. 436-1 КК України (Виготовлення, поширення комуністичної, нацистської символіки та пропаганда комуністичного та націонал-соціалістичного (нацистського) тоталітарних режимів).

Обвинувачений з метою пропаганди комуністичної ідеології упродовж травня 2015 – квітня 2016 років розповсюджував через соціальну мережу Facebook фото та інші матеріали з символікою комуністичного режиму та загальновідомими гаслами того часу, що категорично заборонено Законом України «Про засудження комуністичного та націонал-соціалістичного (нацистського) тоталітарних режимів в Україні та заборону пропаганди їхньої символіки».

Враховуючи, що юнак визнав свою вину та сприяв слідству, прокуратурою укладено з ним угоду про визнання винуватості, яку 04.05.2017 затвердив суд. Юнаку призначено міру покарання у вигляді 2 років 6 місяців обмеження волі з випробувальним терміном в 1 рік.

***

11.05.2017

Die Hände nach oben: Втручатися у вибори у ФРН будуть за старою схемою

Вадим Довнар

Выборы в США и Франции роднит наличие хакерских взломов одного из кандидатов. Следующие важные выборы пройдут в Германии – ключевой европейской стране, которая определяет политику Евросоюза. И есть основания полагать, что там тоже будет использоваться тот же алгоритм.

Докладніше

Спецслужби і технології «соціального контролю»

26.04.2017

Интерпол обнаружил в Юго-Восточной Азии почти 9 тысяч хакерских серверов

В ходе операции по борьбе с киберпреступниками сотрудники Интерпола выявили в восьми странах в Юго-Восточной Азии 8,8 тысяч серверов,

служащих для различной киберкриминальной активности. Об этом сообщается на сайте международной полиции (InternetUA).

Согласно пресс-релизу, управляющие серверы использовались для распространения вредоносного и вымогательского ПО, проведения спам-кампаний и DDoS-атак. Все собранные сотрудниками Интерпола данные были переданы правоохранителям каждой из восьми стран (Китая, Индонезии, Малайзии, Филиппин, Сингапура, Таиланда и Вьетнама).

Интерпол также выявил 270 инфицированных вредоносным кодом web-сайтов (компрометация стала возможной из-за уязвимости в платформе, на которой работали ресурсы), сотни скомпрометированных правительственных порталов и ряд фишинговых ресурсов, связанных с киберпреступной группировкой в Нигерии.

***

27.04.2017

Школярі в Британії навчаються вести кібервійни

Дмитрий Евчин

На кіберзахист Об'єднаного Королівства Великої Британії стануть школярі. У Лондоні 14-річних юнаків та дівчат навчають вести кібервійни та відбивати хакерські атаки **(**podrobnosti.ua**)**.

«Думаю, сучасний світ потребує кібербезпеки. І ця галузь стрімко розвивається. Ми спостерігаємо технологічний стрибок, адже живемо в епоху інновацій. Приміром, люди створюють якийсь смарт-холодильник, але навіть не здогадуються, що його можна "хакнути"», – розповідає учасник кібертренінгів Отто Хіс.

Група кодерів, якою керує Хіс, дбає про захист безпілотників та роботу кейтерингових компаній. Фірми готують їжу, а машини доставляють її Лондоном офісним працівникам. Школярі захищають роботів від хакерських атак. Імовірно, в майбутньому вони гарантуватимуть безпеку і державних інституцій.

«Кіберзахисники потрібні, щоб відбивати хакерські атаки. Ця загроза реально існує, наш кіберпростір у небезпеці. Нам справді необхідні фахівці, і якомога скоріше», – наголошує організатор кібертренінгів Дайан Міллер.

Організатори шкільних IT тренінгів переконані: знання, здобуті тут, стануть у пригоді. Навіть якщо юнаки не отримають роботу в урядових компаніях з кіберзахисту.

***

27.04.2017

ФСБ Росії могла качати дані з України через нелегальний софт, – СБУ

У восьми компаніях провели обшуки в рамках операції з виявлення такого ПЗ, зокрема в компаніях «Укргазвидобування» і Dragon Capital

Федеральна служба безпеки Росії могла отримувати дані з України завдяки програмному забезпеченню «Стахановець», яке виявили у 8 компаніях, зокрема, в «Укргазвидобуванні» та Dragon Capital.

Докладніше

***

2.05.2017
У Росії заблокували месенджери BlackBerry, Imo і Line
Валентина Мартинюк

У Росії до списку заборонених ресурсів внесли адреси месенджерів BlackBerry, Imo і Line. У переліку також виявився аудіовізуальний чат Vchat, передає УНН з посиланням на ВВС (Інформаційне агентство «Українські Національні Новини»).

«Месенджери, які раніше відмовилися реєструватися у відомстві в статусі розповсюджувачів інформації, були внесені в реєстр заборонених сайтів з позначкою “Restricting”. Це означає, що в майбутньому Роскомнагляд буде блокувати всі сервісні IP-адреси і технічні домени сервісів», – йдеться в повідомленні.

Представник Роскомнадзора Вадим Ампелонский підтвердив внесення месенджерів у чорний список.

«Ми спільно з органами, які здійснюють оперативно-розшукову діяльність, планомірно наповнюємо реєстр організаторів поширення інформації. Ті, хто не реагує, виявляються під блокуванням», – сказав В.Ампелонский.

Варто зазначити, що раніше в квітні 2017 року на тих же підставах було заблоковано мобільний додаток Zello. Сервісом-рацією нерідко користувалися активісти, в тому числі далекобійники, під час координації протестних акцій.

***

4.05.2017
СБУ затримало п’ять адмінів груп у соцмережах

Співробітники СБУ затримали п’ять власників та адміністраторів антиукраїнських спільнот у соціальних мережах у різних регіонах країни (Корреспондент.net).

«За завданням своїх кураторів із російських спецслужб жителі Київської, Миколаївської, Дніпропетровської та Львівської областей поширювали напередодні травневих свят заклики до радикалізації суспільних акцій з нагоди 1,2,8 і 9 травня, а також намагалися використовувати соціальні мережі для ініціювання масових заворушень», – сказано в повідомленні СБУ.

У всіх випадках порушено кримінальні провадження, тривають невідкладні оперативно-слідчі дії.

***

5.05.2017

Кіберполіцією Слобожанщини ліквідовано злочинну групу шахраїв

Працівниками Слобожанського управління кіберполіції Департаменту кіберполіції НП України спільно працівниками ГУНП в Полтавській та Харківській областях, а також, батальйону поліції особливого призначення ГУНП в Полтавській області та прокуратурою Полтавської області, проведено міжрегіональну операцію із припинення діяльності та затримання активних учасників злочинної групи, у результаті якої одночасно проведено 10 санкціонованих обшуків на території Харківської та Полтавської областей.

Докладніше

***

4.05.2017

В Кременчуге СБУ задержала женщину за антиукраинскую пропаганду в соцсетях

Сотрудники Службы безопасности Украины в Кременчуге провели задержание женщины, которая вела антиукраинскую пропаганду и размещала сепаратистские материалы на своих страницах в социальных сетях. Об этом говорится в сообщении пресс-центра СБУ (Mignews.com.ua).

В ходе расследования было установлено, что указанное лицо является сторонницей «русского мира» и поддерживает политику Кремля. На своих страница в российских соцсетях она вела антиукраинскую пропаганду и размещала материалы, которые дискредитируют украинских военных и способствуют разжиганию межнациональной розни. Во время обыска по месту жительства правонарушительницы правоохранители изъяли компьютерную технику, а также доказательства ее сепаратистской деятельности.

По факту совершенного преступления возбуждено уголовное дело по части 2 статьи 110 Уголовного кодекса Украины – посягательство на территориальную целостность и неприкосновенность Украины, объединенное с разжиганием национальной или религиозной враждебности.

***

5.05.2017

Мешканця Чернігова судитимуть за антиукраїнські пости у соцмережі

Житель Чернігова постане перед судом за вчинення злочину проти основ національної безпеки України (Західна інформаційна корпорація).

Про це повідомила прес-служба прокуратури області.

Слідством установлено, що у грудні минулого року обвинувачений, перебуваючи за місцем свого проживання, в інтернет-мережі «ВКонтакте» за гроші розповсюджував матеріали із закликами до насильницької зміни чи повалення конституційного ладу або до захоплення державної влади та зміни меж території або державного кордону України.

Наразі обвинувальний акт у кримінальному провадженні направлено до суду для розгляду по суті.

Санкція інкримінованих статей передбачає максимальний термін покарання у виді позбавлення волі на термін від 5 до 10 років з конфіскацією майна або без такої.

***

11.05.2017

Путин подписал указ против анонимности в интернете

Президент России Владимир Путин подписал указ против анонимности в интернете и об урегулировании похожих на средства массовой информации сервисов. Об этом говорится в «Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы», текст которой доступен на сайте Кремля (Finance.Ua).

Теперь в течение полугода правительство России должно заняться поддержкой традиционных СМИ и урегулированием похожих на них сервисов. Речь идет о новостных агрегаторах, социальных сетях, интернет-телевидении, мессенджерах, а также о любых сайтах в интернете.

«Подобные меры необходимы для “формирования в России информационного пространства, учитывающего потребности граждан и общества в получении качественных и достоверных сведений”», – говорится в тексте.

В стратегии развитии информационного общества предлагается принять меры, которые бы исключили анонимность пользователей Сети и их «безответственность и безнаказанность». Кроме того, планируется создать специальную систему, гарантирующую «личную безопасность пользователей, конфиденциальность их информации».

Кроме того, Путин поручил чиновникам с 1 октября 2017 года разработать меры, которые позволили бы государственным органам перейти на российские средства шифрования, а также создать систему защиты российской инфраструктуры от кибератак.

***

11.05.2017

Роскомнадзор разблокировал китайский мессенджер WeChat

В России разблокирован сайт китайского мессенджера WeChat. Согласно сообщению министерства связи РФ, опубликованному в четверг, 11 мая,

компания-владелец WeChat предоставила контактные данные, необходимые для внесения в реестр организаторов распространения информации, и 10 мая с нее были сняты ограничения доступа (http://www.dw.com/).

***

11.05.2017

В США хотят ограничить «Касперского»: Он стал слишком распространен

Правительство США видит в продуктах «Лаборатории Касперского» угрозу для национальной инфраструктуры. Опасения вызывает то, что в «Лаборатории» работают бывшие российские военные, и то, что российские власти имеют доступ к любой информации на территории своей страны.

Докладніше

***

14.05.2017

Итальянское власти оштрафовали WhatsApp за сбор пользовательских данных

Своими действиями WhatsApp расстроил итальянцев (IGate).

Антимонопольные органы Италии наложили штраф в размере €3 миллионов на мессенджер WhatsApp. Об этом сообщило новостное агентство Reuters.

По мнению итальянцев, WhatsApp навязывал пользователям условия, обязывающие их соглашаться на передачу персональной информации материнской компании сервиса Facebook. В ведомстве отметили, что пользователей вынуждали передавать данные, указывая, что в противном случае они не смогут продолжать пользоваться приложением.

Reuters подчеркивает, что максимальное наказание за данное нарушение составляет €5 миллионов. Представители WhatsApp не стали комментировать ситуацию.

***

15.05.2017

Microsoft звинуватила спецслужби США в розповсюдженні вірусу WannaCry

У корпорації Microsoft заявили, що розповсюдження комп'ютерного вірусу WannaCry, який атакував комп'ютери в 150 країнах, стало можливим через викрадення хакерами даних у спецслужб США (Espreso.tv).

Про це повідомляє BBC.

Президент компанії Бред Сміт заявив, що викрадення даних про вразливі місця програмного забезпечення стало можливим через недбалість державних структур щодо заходів безпеки.

«Раніше ми вже бачили, як дані про вразливість системи, які збирало ЦРУ, з'явилися на WikiLeaks. Зараз вкрадені в АНБ дані про вразливість завдали удару користувачам по всьому світу», – наголосив Бред Сміт.

За словами Сміта, спецслужби мають не лише фіксувати дані про вразливість систем, але й передавати їх розробникам, щоб ті могли усувати недоліки та підвищувати безпеку комп'ютерних мереж.

«Кібератаки стають складнішими, немає іншого способу для користувачів захистити свою інформацію, окрім оновлення програмного забезпечення. Якщо провести паралелі зі звичайною зброєю, то рівноцінним сценарієм у даному випадку стала б крадіжка в американської армії ракет "Томагавк"», – додав президент Microsoft.

***

16.0.2017
Як в Україні блокуватимуть російські інтернет-сервіси

Президент України ввів в дію рішення РНБО щодо санкцій проти російських популярних інтернет-сервісів та соцмереж. DW з'ясовувала, як запрацюють нові санкції.

Докладніше

Проблема захисту даних. DDOS та вірусні атаки

26.04.2017
Facebook начал массово атаковать неизвестный вирус

Пользователи антивируса Webroot сообщили о массовом сбое работы компьютеров на Windows. Об этом сообщает lenta.ru, со ссылкой на издание ZDNet (МедиаБизнес).

По неизвестным причинам приложение после обновления начало отмечать системные фалы Windows как вредоносные и массово отправлять их в карантин. Это парализовало работу компьютеров пользователей, пользующихся антивирусом. Кроме того, сайт социальной сети Facebook также оказался недоступен, поскольку защита начала опознавать его как фишинговый ресурс.

В сети юзеры активно атакуют социальные сети Webroot: в Twitter антивируса пришли сотни сообщений о неполадке. В ответ компания зачем-то опубликовала памятку о вредоносном программном обеспечении.

Через некоторое время в Webroot сообщили, что сбой устранен, но тысячи пользователей остались с неработающей операционной системой. В частности, исправления ошибки до сих пор ожидают корпоративные клиенты.

Webroot – американская антивирусная программа, которой пользуются около 30 миллионов человек по всему миру. Согласно указанной на сайте информации, ее используют такие крупные компании как Cisco, Cellebrite и Virgin Media.

***

26.04.2017

Илья Кабачинский

Сервис Unroll.me очищает электронную почту от спама. А потом тихо продает ваши данные другим

Издание The New York Times 23 апреля опубликовало материал, в котором вскрылся неизвестный ранее момент из жизни скандальной компании Uber. Оказывается, что когда CEO Apple Тим Кук узнал о слежке за пользователями компанией Трэвиса Каланика, он пригрозил удалить Uber из App Store. Сам факт подобной встречи интересен уже тем, что Uber удалось сохранить бизнес за счет своего масштаба (если бы Apple удалила приложение сервиса, он бы потерял десятки миллионов пользователей), но многих заинтересовал другой момент. А именно компания Unroll.me.

Докладніше

***

26.04.2017

Kaspersky Lab исследует ботнет Hajime

Kaspersky Lab рассказала об активности зловреда Hajime, который в настоящее время энергично заражает устройства Интернета вещей и создает из них ботнет.

Докладніше

***

26.04.2017

Новый Android-троян крадёт пароли от приложений банков и социальных сетей

Компания ESET предупреждает о появлении новой вредоносной программы, нацеленной на мобильные устройства под управлением операционных систем Android (InternetUA).

Зловред, получивший название Android/Charger.B, был обнаружен в магазине Google Play. Троян замаскирован под приложение-фонарик Flashlight LED Widget. Но ничто не мешает злоумышленникам распространять программу

под видом других приложений и утилит. Кроме того, зловред с большой долей вероятности распространяется через неофициальные магазины Android-приложений.

После установки и запуска программа запрашивает права администратора устройства и разрешение открывать окна поверх других приложений. Далее троян отправляет на командный сервер информацию об устройстве, включая список установленных приложений, а также фотографию владельца, сделанную фронтальной камерой.

Главная задача зловреда – кража паролей от приложений банков и социальных сетей, в частности, Facebook и Instagram. Когда жертва запускает интересующее злоумышленников приложение, на экране появляется поддельное окно для ввода данных. Логины, пароли или данные банковских карт, введённые в фишинговом окне, будут отправлены злоумышленникам.

Троян может блокировать экран устройства, выводя сообщение о загрузке обновлений. Специалисты предполагают, что эта функция используется при краже средств со счёта.

***

26.04.2017

В 2016 году киберпреступность в Германии выросла на 80 %

Власти Германии зафиксировали свыше 82 тыс. случаев компьютерного мошенничества, шпионажа и других киберпреступлений в 2016 году. Это составляет на 80% больше подобных инцидентов по сравнению с предыдущим годом, сообщает Venture Beat (InternetUA).

Кроме того, немецкая полиция сообщает о 253 тыс. преступлений, совершенных при помощи Интернета, что демонстрирует рост на 3,6 % относительно 2015 года. Министр внутренних дел страны Томас де Мезьер должен в скором времени опубликовать доклад с обновленными данными в рамках ежегодной правительственной статистики.

***

26.04.2017

Любомир Левицкий запустил проект по борьбе с интернет-пиратством

В Украине 25 апреля был презентован социальный проект, направленный на борьбу с интернет-пиратством, #ДАЙШАНСМРІЇ. Автор проекта – режиссер Любомир Левицкий, сообщает Mediasat (Телекритика).

Цель проекта, по словам Левицкого, – повышение уровня осведомленности людей, не осознающих, что нелегальный просмотр фильма в Интернете приносит вред его создателям и делает невозможным создание новых лент. Проблема нарушения авторских прав является критической не

только для киноиндустрии, но и для других отраслей, в частности – музыкальной индустрии и IT.

Идея его создания возникла у режиссера после того, как в очередной раз его фильм сразу после выхода в прокат попал на пиратские онлайн-ресурсы, что привело к потере средств, которые должны пойти на создание следующей картины. А это, в свою очередь, тормозит развитие целого творческого пласта и исключает процесс создания новых рабочих мест в смежных отраслях.

Проект #ДАЙШАНСМРІЇ запускает при поддержке посольства США в Украине, Агентства США по международному развитию (USAID), Американской торговой палаты, Американского дома, Ассоциации музыкальной индустрии Украины и инициативы «Чистое небо».

Во время презентации были представлены три социальных ролика, посвященных борьбе с видео-, аудио- и IT-пиратством, которые будут распространяться на телевидении и в Интернете. Кроме того, в рамках #ДАЙШАНСМРІЇ предусматривается проведение образовательно-просветительских мероприятий, в рамках которых, в частности, интернет-пользователей будут знакомить с легальными ресурсами для просмотра кино и т.д.

***

27.04.2017

Вирус в Google Play заразил около 2 млн пользователей

Вредоносное программное обеспечение FalseGuide, спрятанное в приложения с руководствами по прохождению игр, заразило уже порядка 2 млн пользователей в Google Play. Об этом «Газете.Ru» сообщили в пресс-службе Check Point Software Technologies (InternetUA).

Первые 40 приложений, зараженных FalseGuide, были загружены в магазин в феврале 2017 года, но вскоре были обнаружены и удалены. На настоящий момент найдено еще пять новых приложений со зловредом, что дает основания полагать, что злоумышленники продолжают свою кампанию по заражению устройств пользователей.

При установке FalseGuide запрашивает права администратора устройства, а после создает скрытый ботнет из зараженных устройств. С помощью этого зловреда злоумышленники могут получить рутовый доступ к устройству, использовать его для DDoS-атак или для проникновения в защищенные сети.

***

27.04.2017

Больницы становятся любимой целью хакерских атак

Медицинские учреждения становятся новой целью киберпреступников, похищающих личные данные. Получая доступ к персональной медицинской информации, мошенники продают базы данных или вымогают деньги. Для

решения проблемы отрасли здравоохранения требуются совершенные инструменты и квалифицированные ИТ-кадры, способные противостоять угрозам.

Докладніше

***

27.04.2017

Выпускников предупреждают об активизации мошенников в соцсетях

В интернете активизировались мошенники, которые пытаются нажиться на ВНО (Донбасс. Комментарии).

В Украинском центре оценивания качества образования отметили, что через месяц стартует основная сессия внешнего независимого оценивания 2017 года. И уже в интернете, особенно в социальных сетях, наблюдается активизацию мошенников, которые за определенную плату предлагают «помощь» для успешной сдачи ВНО. В первую очередь речь идет о возможности приобрести готовые ответы к тестовым заданиям по различным предметам.

«Надлежащий уровень защиты информации на всех этапах подготовки и проведения внешнего независимого оценивания засвидетельствовано аттестатами соответствия. Поэтому настоятельно рекомендуем не пользоваться услугами мошенников, ведь вы непременно будете обмануты», – утверждают в УЦОКО.

***

27.04.2017

Обнаружены новые фишинговые сайты, которые обманывают украинцев

Специалисты Украинской межбанковской ассоциации членов платежных систем ЕМА обнаружили еще несколько фишинговых сайтов, которые нацелены на выманивание карточных данных украинцев, выдавая себя за сервисы денежных переводов и пополнений мобильного телефона (InternetUA).

Так, за последние две недели в ЕМА зафиксировали еще 8 таких сайтов. Их дизайн очень похож на дизайн легитимных веб-ресурсов, которые предоставляют перечисленные услуги. На самом деле, данные услуги они не предоставляют, а созданы лишь для того, чтобы заполучить карточные данные доверчивых пользователей.

Список фишинговых сайтов, выявленных за последние две недели:

http:// pay4mob .info/

http:// payformob .info/

http:// paynmob .info/

http:// popolnimob .info/

http:// pyaformob .info/
http:// popolnish .info/
http:// oplatiphone .info/
http:// popolninaphone .info/

***

27.04.2017

Антивирус Касперского – мина в киберполе Украины

Принимая во внимание, что Украина находится в состоянии гибридной войны с Российской Федерацией, встал вопрос о том, какое положение занимают в Украине до недавнего времени популярные, антивирусные решения российской «Лаборатории Касперского», какое отношение компания имеет к спецслужбам РФ и какие угрозы Национальной системе кибербезопасности может нести использование программ государства-агрессора.

Докладніше

***

2.05.2017

Жертвами 100-миллионного мошенничества оказались Facebook и Google

В прошлом месяце Министерство юстиции США обвинило уроженца Литвы в мошенничестве, умышленной краже личных данных и отмывании денег. Как выяснилось из документов, он обманными способами похитил у двух крупных технологических компаний более $100 миллионов, замаскировавшись под тайваньского производителя электроники. Сайт Fortune сообщил, что этими двумя компаниями оказались Facebook и Google (GFS).

Обе подтвердили Fortune, что их сотрудники стали жертвами мошенничества. Преступник, 48-летний Эвалдас Римасаускас (Evaldas Rimasauskas), подделывал адреса электронной почты, счета-фактуры и контракты, чтобы заставить Facebook и Google оплачивать поставки электроники. Деньги перечислялись на банковские счета в Литве, Латвии, Гонконге, Словении, Венгрии и Кипре.

В рассекреченных в прошлом месяце Министерством юстиции документах Facebook и Google описываются как «многонациональная корпорация, которая предоставляет доступ к социальной сети и сетевым сервисам», а также «многонациональная технологическая компания, специализирующаяся на интернет-сервисах и продуктах и имеющая штаб-квартиру в США». Под эти описания подпадают сотни предприятий, но в ретроспективе всё кажется довольно очевидным.

По словам представителей Facebook и Google, компании смогли компенсировать затраты после раскрытия преступления. Но ни одна не рассказала, сколько именно денег отправила на счета Римасаускаса.

***

2.05.2017

Роскомнадзор заблокував розсадник «піратства»

Користувачі знайшли спосіб обійти заборону на Rutracker (Знай.ua).

Роскомнадзор остаточно заблокує піратський ресурс Rutracker, яким активно користуються й українці.

Служба вже закрила доступ до «дзеркал» і службових серверів, які видають користувачам IP-адреси джерел для скачування файлів, пишуть російські ЗМІ.

У зв'язку з цим, завантаження контенту сповільнюється до критичної швидкості або взагалі зупиняється.

Компанія Pirate Pay, яка займається блокуванням піратських роздач, вже підготувала список «дзеркал» Rutracker. І незабаром вони перестануть працювати.

Варто відзначити, що сервіс вже раніше блокували. Однак перша спроба не увінчалася успіхом.

«Після блокування його відвідуваність на деякий час впала, але потім користувачі знайшли способи обходу заборон, і зараз сайт функціонує на повну силу», – зазначила гендиректор онлайн-кінотеатру Tvzavr Марина Суригіна.

***

2.05.2017

Доклад Verizon рассказал о распространении приложений-вымогателей

Популярность приложений-вымогателей у вирусописателей на подъёме, но хотя это давно известно, темпы распространения впечатляют. Статистика Data Breach Incident Report (DBIR) за 2017 от американского оператора мобильной связи Verizon говорит, что за прошлый год количество вымогателей выросло на 50 % (InternetUA).

Финансовые институты, медицинские учреждения и общественные организации чаще всего становятся мишенями вымогателей. Статистика собрана от 65 организаций, 42068 инцидентов и 1935 взломов в 84 странах. Медицинский центр Hollywood Presbyterian в прошлом году заплатил $17000 после блокировки вымогателями части сети. Позже в 2016 то же произошло с сетью больниц MedStar.

73 % атак являются финансово-мотивированными. 81 % взломов произошли при помощи украденных или слабых паролей, 66 % случаев установки вредоносных программ произошли через вложения в электронной почте.

Малые и средние организации становятся популярными целями. 61 % взломов были в компаниях менее чем с 1000 сотрудников против 53 % годом ранее.

***

3.05.2017

В Эфиопии появились терминалы, позволяющие загружать пиратские фильмы

Журналисты издания Torrent Freak рассказали о необычном бизнесе, который недавно был обнаружен одним из читателей ресурса: в обычном торговом центре в Эфиопии был замечен странный автомат, внешне напоминающий платежный терминал или же банкомат. Как оказалось при ближайшем рассмотрении, устройство открыто торгует нелегальным контентом (IToboz.com).

«В начале текущего года в All Mart (местный аналог магазинов Walmart) появился новый автомат. Фактически это просто монитор с USB-портом, но представленный в формате банкомата. Он называется SwiftMedia, – объясняет бдительный читатель. – По сути, вы приходите в очень крупный магазин, подходите к автомату и вставляете в него USB-накопитель. Включается экран, и вы можете выбрать фильмы из огромного архива». Стоит ли говорить, что ни о какой легальности контента, DRM-защите и авторских правах речи здесь не идет. Цены тоже мало напоминают расценки легитимных сервисов: подборки фильмов можно скачать за 25, 50 и 100 быр (1-3 долларов США), а отдельные кинокартины обойдутся всего в несколько десятков центов. В основном стоимость фильмов зависит от даты их выхода на экран. Обнаруживший странную машину читатель предполагает, что люди, которым принадлежит автомат, попросту качают торренты целыми днями, а затем добавляют их в каталог SwiftMedia, так как в автомате доступны даже новинки, недавно вышедшие на экраны кинотеатров (нужно полгать, что это лишь «экранки»). По его словам, в Эфиопии до подобной нелегальной деятельности никому нет дела, так как у правительства страны имеются куда более серьезные проблемы.

***

3.05.2017

Дилетанты массово воспользовались инструментами хакеров, связанных с АНБ

Хакерские инструменты аффилированной с АНБ группировки Equation Group начали использоваться для атак на простых пользователей. По всей видимости, работают хакеры-дилетанты, вооружившиеся этими эксплойтами. Общее количество заражений, по разным оценкам, находится в диапазоне от 15 до 41 тыс.

Докладніше

***

3.05.2017

Обнаружен новый троян OSX.Bella, который устанавливает бэкдор на Mac

По данным экспертов в области компьютерной безопасности, на macOS появился еще один опасный троян, похожий на недавно обнаруженный OSX.Dok и способный обходить GateKeeper. Новый зловред, получивший название OSX.Bella, ведет себя по-другому: после установки он запускает в ОС вредоносный скрипт (InternetUA).

Обнаруженный экспертами Malwarebytes троян устанавливается таким же путем, как OSX.Dok – маскируется под документ. Как только система будет заражена, на ОС ставится бэкдор под названием Bella.

OSX.Bella копирует /Users/Shared/AppStore.app и отображает предупреждение о том, что приложение повреждено. Зловред не предлагает пользователям обновить Mac, как в случае с OSX.Bella, а после запуска сразу же закрывается и удаляет себя из системы.

На первый взгляд кажется, что вредоносное ПО не представляет особой опасности, однако незаметно для пользователя запускается скрипт, написанный на Python. Исследователи обнаружили, что Bella получает доступ к сообщениям iMessage, функции «Найти iPhone», перехватывает пароли, данные с микрофона и камеры, а также умеет делать скриншоты.

***

4.05.2017

Компанія Google попереджає про шкідливу розсилку, замасковану під Google

Компанія Google попереджає користувачів поштового сервісу Gmail про шкідливість розсилки, замаскованої під сервіс Google Docs, яка почала надходити на електронні скриньки користувачів 3 травня (**Україна молода**).

Про це йдеться в повідомленні на сторінці сервісу в Twitter.

«Ми розслідуємо фішингові листи, які виглядають як Google Docs. Закликаємо вас не переходити за посиланнями і відзначати їх як фітинг», – йдеться в повідомленні.

Зокрема, у листі, автором якого може бути вказаний знайомий одержувача, пропонується відкрити документ в Google Docs.

При переході по посиланню відкривається вікно, у якому користувачу пропонують дозволити управляти своїми листами і контактами програмі, яка називається Google Docs (але не має відношення до Google і є шкідливою).

Як зазначає The Verge, розсилка відрізняється від звичайного фішингу тим, що не переводить користувача на сторінку, схожу на поштовий сервіс, а

діє всередині цього поштового сервісу, експлуатуючи існуючу можливість давати стороннім програмам доступ до акаунтів.

Як повідомили в Google, компанія вжила заходів для захисту користувачів. Зокрема, підроблені сторінки Google Docs були видалені, а акаунти-порушники відключені. Також в компанії відзначили, що працюють над тим, щоб запобігти такого роду підмінам у майбутньому.

***

4.05.2017

Україна уникла статусу головної піратської країни в звіті США

Україна зберегла статус «країна під пріоритетним наглядом» у щорічному звіті Офісу торгового представника США (2017 Special 301 Report) про стан захисту інтелектуальної власності у світі (LB.ua).

У звіті поряд з Україною такий статус отримали Китай, Індонезія, Таїланд, Індія, Алжир, Кувейт, Росія, Аргентина, Чилі та Венесуела. Всього в доповіді фігурують 34 країни. Статус Priority foreign country, або, як його ще називають, статус головної піратської країни в світі, цьогоріч не отримала жодна країна.

Залежно від тяжкості порушень, країни потрапляють в одну з трьох категорій: Watch list (країни під наглядом), Priority watch list (країни під першочерговим наглядом), або ж Priority foreign country (пріоритетна країна). Залежно від категорії, до країни можуть бути застосовані різні санкції, починаючи з двосторонніх консультацій, закінчуючи реальними економічними обмеженнями.

У нинішньому звіті експерти Офісу торгового представника США позитивно оцінили окремі заходи, які вжила Україна для поліпшення захисту прав інтелектуальної власності.

***

4.05.2017

Сайт інформагентства «ВолиньPost» три місяці зазнає хакерських атак – редакція

Сайт інформаційного агентства «ВолиньPost» повідомляє, що три місяці зазнає потужних DDoS-атак, які часто співпадали з важливими подіями у політичному житті міста, наприклад сесіями Луцької міської ради

Сайт інформагентства «ВолиньPost» три місяці зазнає хакерських атак – редакція (detector.media).

Про це повідомляється на сайті видання.

Остання потужна атака була 26 квітня, коли відбувалося чергове засідання ради. Технічна підтримка швидко стабілізувала роботу сайту.

Директор інформагентства «ВолиньPost» Юрій Сковорода повідомляє, що атаки мали різні типи, тому стосовно одних вдалося швидше налагодити протидію, щодо інших – зайняло трохи більше часу.

«Силами злагоджених професійних дій нашої техпідтримки наразі нам вдалось відбити всі атаки на сайт. Ми отримали досвід як діяти в таких ситуаціях, розуміючи, що атаки можуть продовжуватись. На основі отриманої інформації готові ділитися з іншими ЗМІ особливостями побудови алгоритмів захисту від базових видів DDOS-атак, залучивши відповідних спеціалістів галузі ІТ Луцька», – сказав він.

***

5.05.2017

На популярнейшем сайте обнаружили опасную «дыру»

Компания Digital Security, специализирующаяся на защите информации, обнаружила в соцсети Twitter опасную уязвимость. По словам специалистов, она позволяет публиковать записи от имени любого пользователя сервиса, при этом доступ к аккаунту жертвы не требуется. (ITоboz.com).

«Эта уязвимость особо опасна в связи с тем, что с ее помощью возможно разместить заведомо ложную информацию не в одном, а сразу в нескольких крупных аккаунтах (например, новостных изданий, политиков мирового уровня, звезд шоу-бизнеса и т.д.), причем проэксплуатировать её мог любой более ли менее продвинутый пользователь, – отмечают в компании. – Дезинформация такого рода может спровоцировать серьезные изменения в котировках акций, вызвать политическую нестабильность в крупном регионе, спровоцировать финансовые убытки ряда организаций, запустить кризисную волну в масштабах страны». Уязвимость была обнаружена сотрудником Digital Security Егором Жижиным более двух месяцев назад, однако эту информацию было решено не предавать огласке. Вместо этого данные об уязвимости были переданы в Twitter. Компания исправила ошибку, объявила эксперту благодарность и выплатила ему вознаграждение. Сам Жижин опубликовал подробное описание уязвимости на сайте Habrahabr.

***

9.05.2017

Найден ещё один способ слежки через мобильник – с помощью ультразвука

Учёные поделились новым методом слежки за владельцем смартфона с помощью технологии ultrasonic cross-device tracking, которая встраивается в рекламу (IT Новости).

Технология, встроенная в приложение, издает высокочастотные звуки, которые не слышит человеческое ухо, но воспринимает микрофон устройства. Как только смартфон получает сигнал, он запускает рекламный ролик,

представляющий собой программу, которая собирает всю информацию о владельце гаджета. За прошлый год американские специалисты нашли более 200 приложения для Android, способных воспринимать ультразвук втайне от пользователя. Благодаря этому ПО интернет-маркетологи могут эффективнее продвигать товары через рекламу в мобильных приложениях, считают исследователи.

***

11.05.2017
Хакеров РФ подозревают в атаке против Прибалтики

Российских программистов подозревают в хакерской атаке против энергетических систем стран Прибалтики. При этом Москва опровергает такие громкие обвинения (**Час Пик**).

Страны Прибалтики – Литва, Латвия и Эстония входят в одну энергетическую систему вместе с РФ, но с 2015 года эти государства трудятся над тем, чтобы прекратить это сотрудничество и войти другую энергетическую систему – с ЕС.

По информации международного агенства новостей Reuters, правонарушители в течение 2016-2017 годов спокойно вторгались в сети стран Прибалтики, «параллельно совершая более серьезные нападения на Украину».

Пресс-секретарь Президента Российской Федерации Владимира Путина Дмитрий Песков в интервью, которое он дал агентству Reuters отрицает все претензии в сторону России. «Это такая же клевета, как и все подобные обвинения», – прокомментировал Песков.

В свою очередь, секретарь СНБОУ Александр Турчинов разоблачил планы Президента РФ Владимира Путина по захвату стран Прибалтики, назвав военные учения «Запад-2017» подготовкой к захвату этих территорий.

***

11.05.2017
Трамп розпорядився посилити кібербезпеку

Американський президент Дональд Трамп підписав указ про зміцнення кібербезпеки. Про це заявив його радник з нацбезпеки Томас Боссерт, пишуть західні ЗМІ (Корреспондент.net).

За словами радника, указ має посилити захист федеральних мереж і важливих об’єктів американської інфраструктури від хакерських атак, а також посприяти дотриманню інтернет-користувачами низки правил.

Він зазначив, що це розпорядження Трампа не є реакцією на повідомлення про російські кібератаки.

«Це зроблено не через Росію, а для безпеки США», – відповів Боссерт на відповідне запитання, додавши, що Америку атакують не тільки хакери РФ.

***

12.05.2017
Обікрасти чи знеславити: небезпеки з соцмереж і як їх уникнути

Коли людина щось публікує в соцмережах чи навіть пише приватне повідомлення – це вже потенційна небезпека, кажуть спеціалісти. В чому ми занадто довіряємо соцмережам і чим ризикуємо, нехтуючи обережністю.
Докладніше

***

11.05.2017
Прохоров Кирил
Во «ВКонтакте» опять обнаружены «вирусные» сообщения

В социальной сети «ВКонтакте» найден вредоносный код, который распространяется под видом бесплатных ключей для антивируса Dr.Web (IT новости).
Как пишет источник, анонимные сообщения предлагают бесплатно скачать лицензионные ключи. Как правило ссылки ведут на файловый хостинг RGhost. При загрузке архива вирус отправляет найденную на инфицированном компьютере информацию. Программное обеспечение способно открывать веб-страницы, перезагружать или выключать компьютер, передавать и получать скриншоты экрана, выводить текстовые сообщения. Наиболее опасной функцией является встроенный кейлоггер, запоминающий порядок клавиш.

***

11.05.2017
Рекламные компании следят за нами через наши смартфоны

Современные Android-смартфоны могут следить за пользователем и слушать все происходящее вокруг.
Докладніше

***

11.05.2017
Кибератака нарушила работу ряда французских СМИ

Кибератака на французскую компанию по оптимизации производительности сайтов Cedexis спровоцировала временные перебои в работе таких СМИ, как Monde и Figaro, передает Reuters (ITоboz.com).
По словам представителей компании-провайдера, сервера Cedexis подверглись «беспрецедентной и сложно организованной» DDoS-атаке, после чего наблюдались нарушения в работе сайтов французских изданий Monde, Figaro, 20 Minutes, L'Obs и телерадиокомпании France Télévisions. В данный

момент последствия кибератаки устранены, по факту инцидента проходит проверка.

***

11.05.2017

Ученые превратили антивирусы в оружие для кибератак

Команда исследователей двух университетов Германии разработала метод, позволяющий превратить сканирующий движок антивирусной программы в инструмент для кибератак (IToboz.com).

Атаки базируются на способности антивирусов обнаруживать вредоносное ПО, основываясь на сигнатурах. Данный метод работы антивирусных решений предполагает рассмотрение файла или пакета согласно словарю известных вредоносов, составленному авторами антивируса. Если какой-либо участок кода просматриваемой программы соответствует известной сигнатуре в словаре, антивирус либо удалит файл, либо отправит в карантин. По словам исследователей, злоумышленник может изъять сигнатуры из санирующего движка или понять принцип их работы и использовать антивирус для уничтожения хранящихся на атакуемой системе файлов. Если внедрить копию сигнатуры вредоносного ПО в легитимный файл, антивирусная программа примет его за вредонос и удалит (в лучшем случае поместит в карантин). Таким образом злоумышленник может саботировать работу целого предприятия. Исследователям удалось получить сигнатуры вредоносного ПО из пяти сканирующий движков. Один из них – движок с открытым исходным кодом ClamAV, а остальные четыре разработаны неназванными коммерческими предприятиями. Эксперты использовали сигнатуры для осуществления трех типов атак: прикрытия угадывания паролей путем удаления журналов приложений, удаления электронных писем пользователей и упрощения атак путем удаления файлов cookie браузера.

***

14.05.2017

Министры финансов G7 объявили войну киберпреступности

Растущую опасность для экономики представляет киберпреступность, и борьба с ней должна иметь приоритетный характер (InternetUA).

Об этом было заявлено 13 мая на встрече министров финансов стран G7 в итальянском городе Бари, передает «Укринформ».

Как подчеркнул по окончании встречи глава финансового ведомства Италии Пьер Карло Падоан, на ней достигнуты «договоренности по многим вопросам, в том числе о том, чтобы вести борьбу с киберпреступностью, что, к сожалению, весьма актуально сейчас».

По его словам, в настоящее время экспертам, специализирующимся на теме киберпреступности, поручено проанализировать складывающуюся

ситуацию и сделать выводы о возможных угрозах. Результаты этой работы будут оцениваться на саммите глав государств и правительств стран «большой семерки» в июне 2017 года.

***

15.05.2017
Пик хакерской атаки в Европе пройден - Европол

Рост числа жертв массированной хакерской атаки в Европе приостановился. Об этом заявил представитель полицейской организации Европейского Союза в понедельник, 15 мая, в Гааге (ЧАС.UA).

«Очевидно, что количество пострадавших не увеличивается. Ситуация в Европе, как кажется, стабилизировалась. Это – успех», – отметил он.

Сотрудник Европола увязал эту тенденцию с тем, что владельцы компьютеров и системные администраторы, по всей видимости, наконец, выполнили «свое домашнее задание» и установили программные обновления, позволяющие защититься от вредоносной программы WannaCry.

Между тем в полицейской службе ЕС считают, что пока рано утверждать, кто стоит за атакой.

***

15.05.2015
Илья Кабачинский
WCry, раунд 2: массовые кибератаки могут повториться

Днем 12 мая вирус-вымогатель WannaCry заразил тысячи компьютеров по всему миру. За несколько дней число пострадавших выросло до 200 000 в 150 странах. Как сообщает Motherboard, создатели вируса обновили его и научили обходить домен iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com, к которому ранее WCry был привязан.

Докладніше

***

16.05.2017
Уязвимость браузера Edge позволяет красть пароли

Специалист по информационной безопасности Мануэль Кабальеро обнаружил уязвимость в коде веб-браузера Microsoft Edge в системе Windows 10. Она даёт злоумышленникам возможность получить доступ к паролям и куки-файлам на компьютере, предоставляя неавторизованный доступ к сайтам вроде Facebook и Twitter (InternetUA).

Проблема кроется внутри правила ограничения домена (Same Origin Policy, SOP) в браузере Edge. Как оказалось, реализация этого механизма специалистами Microsoft оставляет желать лучшего, поскольку эта уязвимость в

нём является уже третьей. Два прежде найденных метода злоупотребления этим правилом до сих пор не были закрыты в обновлениях операционной системы Windows 10.

Последняя уязвимость, если верить исследователю, является самой быстрой и прямолинейной среди всех трёх. Кабальеро также выразил неудовлетворение непостоянным циклом обновлений браузера Microsoft Edge по сравнению с конкурентами вроде Google Chrome и Mozilla Firefox.

В качестве доказательства существования уязвимости и возможности использовать её Кабальеро опубликовал видео на YouTube, а также статью в своём блоге.

Это открытие было сделано через несколько дней после того, как компания Google в рамках своего проекта Zero обнаружила в Windows 10 уязвимость, степень тяжести которой описала словом «вопиющая». Она была закрыта Microsoft в течение суток.

***

16.05.2017

Експерти звинувачують у створенні вірусу WannaCry хакерів КНДР

Дослідники виявили ідентичний код у системі вірусу WannaCry та програмах хакерів Lazarus Group, які пов'язані з владою Північної Кореї (Espreso.tv).

Про це заявив дослідник з питань безпеки Google Ніл Мехта, повідомляє The Hill.

Він пояснив, що виявив велику кількість комп'ютерних кодів в ранній версії WannaCry, які були ідентичні тим кодам, що використовують хакери Lazarus Group. Мехта в результаті розповсюдив «дорожню карту», за допомогою якої можна виявити ці коди.

Після цього спеціалісти «Лабораторії Касперського» зауважили, що ці коди були усунені з більш пізньої версії програми. На їхню думку, хакери роблять це для того, щоб замісти сліди свого злочину.

Зазначимо, Lazarus Group найбільш відома тим, що у 2014 році зламала компанію Sony Pictures, щоб бойкотувати вихід стрічки «Інтерв'ю», у якому висміюється очільник Північної Кореї Кім Чен Ин. Ці хакери останнім часом також були пов'язані з низкою пограбувань цифрових банків. Зокрема, вони вкрали $81 мільйон у центрального банку Бангладеш.

***

16.05.2017

Украинцев массово обворовывают через подставные сайты

Количество мошеннических сайтов в Украине в 2016 году выросло в 4,5 раза (174 фишинговых ресурса в 2016 году против 38 – в 2015 году). И мошенники продолжают набирать обороты. Только за первый квартал этого

года специалистами Ассоциации EMA уже было выявлено 54 фишинговых веб-ресурса.

Докладніше

ДОДАТКИ

Додаток 1

26.04.2017

Intel и Facebook повысят производительность платформы глубокого обучения Caffe2

По оценкам экспертов, к 2020 году в мире будут работать более 50 миллиардов машин и устройств, способных подключаться к Интернету и обмениваться информацией между собой. Эти устройства будут генерировать огромные объёмы данных, для анализа которых потребуются передовые системы искусственного интеллекта и глубокого обучения. Учитывая это, Intel и Facebook сотрудничают над увеличением производительности открытого фреймворка глубокого обучения Caffe2 (InternetUA).

Большинство вычислительных нагрузок, связанных с глубоким обучением, включают в себя непосредственно обучение (training) и построение логических выводов (inference). Для обучения обычно требуется многочасовая или даже многодневная работа. Логические выводы, как правило, осуществляются за миллисекунды или секунды и зачастую являются частью более объёмного процесса. Хотя вычислительная нагрузка при построении логических выводов намного меньше, чем при обучении, логические выводы строятся по намного более объёмному набору данных. Поэтому совокупный объём вычислительных ресурсов, необходимых для построения логического вывода, вероятнее всего, будет несопоставимо больше, чем ресурсы, необходимые для обучения.

Для повышения эффективности платформы Caffe2 специалисты Intel и Facebook работают над интеграцией средств Intel MKL – библиотеки математических функций Math Kernel Library. Она обеспечит максимальную производительность процессоров Intel при построении логических выводов.

Кроме того, повышению быстродействия будет способствовать появление общедоступных чипов Intel Xeon следующего поколения под кодовым названием Skylake. В них будут представлены 512-битные инструкции умножения-сложения с однократным округлением Fused Multiply Add (FMA) в рамках 512-битного семейства векторных инструкций Intel AVX-512, что обеспечивает значительный прирост производительности по сравнению с прежними 256-битными инструкциями AVX2, реализованными в процессорах Haswell/Broadwell как в задачах по обучению, так и в задачах по построению логических выводов. Использование 512-битных инструкций FMA позволяет фактически удвоить количество операций с плавающей точкой, которое

выполняет процессор Skylake за одну секунду, и значительно увеличить скорость матричной арифметики одинарной точности, используемой в свёрточных и рекуррентных нейронных сетях.

(вгору)

Додаток 2

27.04.2017
Ольга Карпенко
Павел Дуров анонсировал запуск платежей в Telegram

Команда Telegram собирается запустить платформу для платежей в мессенджере с помощью ботов. Нововведение анонсировал основатель платформы Павел Дуров в Instagram. Он продемонстрировал черновик официального анонса для блога Telegram под названием «Платежи для ботов» в Stories. «Вкратце – платежное API для приема платежей в ботах, без комиссий от Telegram, зовут payment-провайдеров подключаться», – так нововведение описывают в канале «Telegram-маркетинг» (AIN.UA).

Согласно сообщению, пользователи мессенджера смогут покупать любые вещи через Telegram-ботов. «Представьте мир, где вы сможете заказать пиццу или заплатить за пару туфель, нажав всего несколько кнопок в Telegram. Чтобы сделать это возможным, сегодня мы запускаем Bot Payments – способ для ботов принимать платежи от пользователей по всему миру», – обещают в анонсе.

В мессенджере новой версии у ботов появится кнопка «Оплатить». Если пользователь нажмет на нее, его попросят предоставить данные банковской карты (бот будет просить эту информацию только однажды). После этого, как обещает команда Telegram, платежи с помощью ботов можно будет совершать в два клика.

Платежи будут работать без комиссии: каждый платеж будет направляться напрямую от пользователя к разработчикам бота. Принимая платеж от пользователя, разработчик сможет выбрать между несколькими системами биллинга, которые пользователь уже пробовал, или выбрать систему с самой низкой комиссией.

Создатели мессенджера также подчеркивают, что не будут хранить у себя данные банковских карт, но будут модерировать платежных ботов. «Мы будем делать то, чем занимается каждый шериф – убивать плохих ботов и награждать хороших значками», – говорится в сообщении.

По данным того же канала «Telegram-маркетинг», первым партнером Telegram может стать сервис Stripe, который в Украине не работает. Поэтому функция в Украине может запуститься с опозданием.

(вгору)

Додаток 3

4.05.2017
Илья Кабачинский

Google и Facebook контролируют 20 % мировых доходов с рекламы

Американские технологические компании Google и Facebook с миллиардной аудиторией пользователей, вместе получают свыше 20 % доходов на мировом рынке рекламы, сообщает CNBC. Суммарно это больше $100 млрд. Исследование провело агентство Zenith, которое составило список из 30 компаний (AIN.UA).

По данным агентства Zenith, компания Google за последний год заработала на рекламе $79,4 млрд, а Facebook – $26,9 млрд. Обе компании – технологические гиганты, работающие в Интернете, и не представленные в традиционных медиа. Тройку лидеров замыкает компания Comcast, заработавшая на рекламе $12,9 млрд за последний год. В отличие от первых двух, Comcast получает деньги и от телевизионной рекламы.

Первая десятка выглядит следующим образом:

1Alphabet (Google).
2Facebook.
3Comcast.
4Baidu.
5The Walt Disney Company.
621st Century Fox.
7CBS Corporation.
8iHeartMedia Inc.
9Microsoft.
10Bertelsmann.

Больше всего в списке американских компаний из-за размера рекламного рынка США – он крупнейший в мире. Сервис Twitter занимает 30 место, но показывает лучшую динамику: с 2012 по 2016 год рост рекламных доходов составил 734 %. За последний квартал выручка составила $548 млн. В рейтинге пока только три китайских компании – Baidu, CCTV и Tencent, компания-владелец мессенджера WeChat.

Чтобы наращивать свои доходы, компания Google уже задумывается о возможности продажи телевизионной рекламы.

(вгору)

Додаток 4

2.05.2017

Спасти индустрию: как блокировка интернет-рекламы поможет Google и другим компаниям

В конце апреля появилась новость, что компания Google, возможно, занимается созданием блокировщика рекламы для собственного браузера Chrome. Новость более чем странная: зачем компании, которая зарабатывает на рекламе, ее блокировать? Причина есть – Google хочет блокировать рекламу, «которая приносит пользователю негативный опыт». Громоздкие, медленные и

раздражающие рекламные объявления, заполонившие сайты, уже давно стали проблемой. По всей видимости, масштабы сложностей с интерактивной рекламой достигли таких размеров, что на них обратили внимание сами издатели. В своей статье, журнал The Wired объяснил суть будущих изменений. Редакция AIN.UA приводит адаптивный перевод материала (AIN.UA).

Коалиция за лучшую рекламу (The Coalition for Better Ads) – альянс издательских, технологических и рекламных компаний – хочет сохранить рекламную отрасль довольно оригинальным способом: фактически, «убив» одну из ее частей. Компании, входящие в коалицию, намерены, помимо прочих идей, обсудить возможность предустановки в браузеры избирательного блокировщика рекламы. Цель – очищение сети от наиболее навязчивых типов рекламы, которые автоматически воспроизводят звук, занимают слишком большую часть экрана или заставляют пользователей ждать, чтобы их закрыть.

Впервые об идее сообщил The Wall Street Journal: по сведениям издания, блокировщик рекламы будет не только встроен в Google Chrome, но и включен по умолчанию.

Представители Google отказались комментировать новость, отметив лишь, что компания действительно тесно сотрудничала с коалицией, чтобы изучить, как Google и другие члены альянса могут поддерживать высокие стандарты рекламы.

Адвокат Коалиции Стюарт Ингис не любит называть возможные изменения блокировкой рекламы, поскольку известные программы-блокировщики неизбирательны и касаются всех объявлений в сети. По его словам, члены альянса начнут активное обсуждение конкретных предложений по борьбе с навязчивой рекламой в ближайшие недели, но внедрение возможных решений займет от полугода до года. «Очевидно, что справиться с проблемой помогут браузеры, будь то Google, Microsoft или Apple. И насколько мне известно, Google еще не принял никаких решений», – отмечает адвокат.

«Какое бы решение ни приняла Коалиция, Google не будет действовать в одностороннем порядке», – уверен Ингис. «Форматы рекламы, подлежащие блокировке, будут определены членами альянса на основе результатов исследований и мнения пользователей о рекламе, которую они считают наиболее надоедливой. Если новый подход будет разработан, его, скорее всего, внедрит целый ряд браузеров».

На первый взгляд, кажется странным, что компании, зарабатывающие на рекламе, могут поддержать, пусть и частичную, ее блокировку, но такое решение продиктовано четкими намерениями. Так, согласно опросам Interactive Advertising Bureau, около 26 % всех интернет-пользователей уже установили блокировщики рекламы на свои компьютеры, а 10 % пользуются ими даже на смартфонах. Основная причина популярности таких приложений в том, что реклама делает сайты медленными и усложняет навигацию. Если же представителям рекламной индустрии удастся удержать пользователей от инсталляции блокировщиков (или суметь убедить отключить их) и самим

начать борьбу с наиболее навязчивой рекламой – возможно, это поможет сохранить больше рекламных доходов.

В прошлом месяце Коалиция за лучшую рекламу опубликовала исследование, показывающее, какие форматы рекламы больше всего раздражают пользователей. На основе полученных данных, альянс разработал «Стандарты лучшей рекламы» (Better Ads Standards), которые станут основой для работы по уменьшению количества плохих объявлений и продвижению хороших.

Усилия коалиции будут направлены на то, чтобы вернуть доверие интернет-пользователей, убедив компании отказаться от некачественных объявлений в сети. «Важную роль в этом должны сыграть рекламодатели и покупатели рекламы, которым стоит выбирать для сотрудничества издателей и рекламные сети, использующие форматы рекламы, полностью соответствующие требованиям альянса» – считает Джон Монтгомери, исполнительный вице-президент агентства GroupM, члена коалиции и крупнейшего покупателя рекламы в мире. Часть ответственности за реализацию идеи ляжет и на разработчиков браузеров, таких как Google и Microsoft, которые смогут блокировать не только навязчивую рекламу, но и объявления, нарушающие разработанные принципы.

Вполне возможно, что такие меры станут еще большей темой для споров, чем просто избирательная блокировка рекламы, но вместе с тем, они могут принести результат. По оценкам StatCounter, около 53 % юзеров в прошлом месяце использовали Google Chrome. Немногие компании захотят рисковать половиной рекламных просмотров, запуская объявления, которые будут нарушать новые стандарты. По словам Стюарта Ингиса, если коалиция пойдет по этому пути, она разработает конкретный перечень причин и условий для блокировки сайтов, кроме того будет введена процедура апелляции для издателей, которые посчитают, что попали под запрет несправедливо.

В то же время, альянс пытается разрешить только часть проблем с интернет-рекламой. Помимо того, что объявления могут доставлять массу неприятных эмоций пользователям, они могут быть опасными. Так, в прошлом году некоторые сайты и топовые онлайн-издания (например, The New York Times) ошибочно отображали рекламные объявления, содержавшие опасный код, который запускал установку вредоносных программ на компьютеры посетителей. Это был далеко не единичный случай – жалобы на такие инциденты периодически появляются уже в течение нескольких лет. Кроме того, многие AdTech-компании пытаются собирать информацию о пользователях, вероятно, нарушая при этом политики конфиденциальности.

Нет ничего удивительного в том, что юзеры устанавливают блокировщики рекламы не только для того, чтобы облегчить загрузку страниц, а и чтобы обезопасить себя. Но факт остается фактом – до тех пор, пока сфера диджитал-рекламы не будет обеспечивать полную безопасность для пользователей, блокировщики рекламы по-прежнему будут актуальны.

(вгору)

Додаток 5

16.05.2017

Як заборона російських соцмереж і програм позначиться на вітчизняному бізнесі *// І чи вдасться їх швидко замінити на «дозволені» аналоги*

Катерина Гребеник, Світлана Рябова, Віктор Гаценко

Президент Петро Порошенко розширив список юросіб, які перебувають під санкціями у зв'язку з окупацією Криму і війною на Донбасі. Підставою для указу стало рішення РНБО від 28 квітня, яке глава держави ввів у дію своїм указом (Mind).

Цього разу список поповнився популярними соцмережами «Одноклассники», «ВКонтакте», поштовими сервісами Mail.ru і «Яндекс», цілою низкою російських ЗМІ. Крім того, санкції введені проти деяких IT-компаній, продукти яких дуже популярні в Україні: «Лаборатория Касперского», DrWeb, «Софтлайн», ABBYY і «Абі Україна ЛТД» (продукти «1С», Abbyy FineReader, Abbyy Lingvo).

Санкції введені й проти юридичних осіб – дочірніх компаній цих IT- та медіагігантів, зареєстрованих в Україні. Серед обмежень, що накладені на фігурантів списку, блокування активів на території України, обмеження щодо фінансових операцій, заборона на виведення капіталів, заборона на видачу їм ліцензій і дозволів, заборона на надання телеком-послуг і користування телеком-мережами загального користування, а також заборона інтернет-провайдерам надавати користувачам мереж доступ до заблокованих сайтів. Указ набирає чинності з дня опублікування.

Як «санкційні» компанії відреагували на указ президента?

Компанії, що потрапили під блокування, дали дуже стримані коментарі щодо указу президента. Mind вдалося поговорити з деякими з них – у цілому складається враження, що фігуранти списку поки не оцінили повною мірою обстановку і визначають лінію поведінки.

Офіційні позиції звучать помірно оптимістично. «"ВКонтакте" – найпопулярніша соціальна мережа в Україні, кожен місяць ресурс відвідують 16 млн жителів країни. Ми вважаємо, що інтернет за своєю суттю не має кордонів. Ми захищали і захищатимемо інтереси всіх наших користувачів і партнерів», – написав на своїй сторінці «ВКонтакте» глава з комунікацій українського офісу компанії Влад Леготкін.

У Mail.Ru Group заявили, що в першій половині вівторка, 16 травня, спостерігалося «драматичне зростання трафіку» на заборонені сайти, зокрема поштовий сервіс Mail.Ru, і що таке рішення передусім вдарить по громадянам України. Аудиторію заблокованих платформ група оцінила в 25 млн осіб.

«У нашій роботі нічого не зміниться, ми будемо продовжувати надавати всі сервіси нашим користувачам у всіх країнах, а існуючі можливості спеціальних сервісів дозволять продовжити використовувати наші інтернет-

ресурси. Наших співробітників, партнерів і клієнтів на території України ми хочемо запевнити, що всі зобов'язання Mail.Ru Group будуть виконуватися перед ними в повному обсязі. Оскільки частка українського бізнесу в структурі виручки Mail.Ru Group незначна, ми не бачимо причин для коригування наших фінансових планів, і продовжимо активно розвиватися на ринку в різних напрямках», – йдеться в повідомленні групи. У «Яндекс» оцінили свою українську аудиторію в 11 млн користувачів щомісяця.

На українському сайті «1С» з'явився коментар про те, що на даний момент змін у роботі сервісу немає. «Указ Президента стосується тільки окремих юридичних осіб. Програма «1С:Підприємство» повністю працездатна, технічна підтримка працює у штатному режимі, всі інформаційно-методологічні ресурси доступні для користування. Партнери «1С:Франчайзі» продовжують надавати послуги з оновлення продуктів і інформаційно-технологічної підтримки користувачів програмних продуктів «1С:Підприємства», – йдеться в коментарі.

Чи є технічні можливості блокування і що думають з цього приводу провайдери?

Багато опитаних Mind українських клієнтів заблокованих компаній сумніваються, що технічно можливо зробити блокування сайтів провайдерами. «Не впевнений, що в Україні є технічна можливість реалізації цього рішення», – говорить Олександр Колб, засновник агентства інтернет-маркетингу Promodo. Глава Української асоціації директ-маркетингу Валентин Калашніков уточнює, що заблокувати сайти легко – але не менш легко обійти це блокування через анонімайзери (сервіси, що приховують інформацію про комп'ютер або користувача в мережі від віддаленого сервера).

«Обійти будь-яке блокування через сайти, що доступні будь-якому користувачеві, сьогодні не є проблемою», – підтверджує Олександр Карпов, директор ЕМА – Української міжбанківської асоціації членів платіжних систем.

Провайдери поки не вирішили, як вони будуть діяти в даному випадку. «Питання, звичайно, неоднозначне. Наші юристи поки вивчають указ. Як тільки у нас буде готова позиція, ми її озвучимо», – зазначила Наталя Клітна, віце-президент Асоціації правовласників і постачальників контенту.

Співвласник інтернет-провайдера «Тріолан» Вадим Сидоренко сказав у коментарі виданню «Економічна правда», що він поки не бачить можливості того, як можна реалізувати вимогу щодо блокування. Тому що, по-перше, є можливість його обійти і через VPN, proxy тощо. По-друге, тому що провайдери не аналізують структуру трафіку в мережі й просто не знають, як виділяти, що потрібно блокувати, а що – ні.

Проте телеком-оператор і провайдер інтернету «Укртелеком» у коментарі виданню «Ліга» повідомив, що вже почав виконувати указ. «Процес досить складний і вимагає певного часу, з огляду на значну кількість ресурсів. Роботи вже розпочато. Вони будуть проводитися поетапно і, за попередньою оцінкою фахівців, триватимуть від декількох днів до тижня», – цитує видання прес-службу оператора.

Олександр Данченко, народний депутат, глава комітету ВР з питань інформатизації та зв'язку, вважає, що хоч заборона і є правильною за суттю, її реалізація виконана невірно. «Інтернет-провайдери взагалі до цього не причетні, адресувати вимоги щодо блокування потрібно не ним. Як відомо, вони не підключені безпосередньо до ресурсів, а отримують трафік від транзитних компаній. Загалом таких компаній в Україні сім або вісім; чотири з них російські. Їх назви, юридичні адреси в Україні СБУ добре відомі. Ось з ними і потрібно було б розбиратися. Транзитним операторам легше забезпечувати блокування доступу. І потрібно розібратися з серверами «ВКонтакте» в Україні, які тут є», – каже нардеп.

Які аспекти впливу нинішніх обмежень на бізнес в Україні?

Чи не найбільше занепокоєння у бізнес-спільноти викликав пункт про блокування «1С» – програми для ведення бухгалтерського обліку. «1С» – це продукт, який належить російській компанії ABBYY, саме вона потрапила до списку заблокованих юросіб.

«1С» вже давно збиралися вносити до списку забороненого ПЗ, але 95% компаній в Україні використовують її як систему обліку. Так що поки складно сказати, як це буде. На мою думку, це нонсенс», – каже Дмитро Зарахович, керуючий партнер національного сервісу з грошових переказів UAPAY.

У дочірньому підприємстві «Еврософтпром», що володіє правами на програмні продукти «1С» в Україні, підтверджують, що коло потерпілих може бути дуже широким. «Постраждає 300 000 легальних користувачів «1С», а також від 30 до 60% піратських, незареєстрованих користувачів. Плюс працівники 500 франчайзингових компаній, у кожній працюють в середньому 22 людини. 11 000 осіб втратять роботу. У великих компаніях працюють від 50 до 100 співробітників», – зазначає Вадим Мазур, директор компанії.

Та драматизувати ситуацію, можливо, рано. У компанії IntelTech, яка є партнером мережі «1С: Франчайзі» і займається консалтингом, впровадженням та супроводом програми «1С», вважають, що указом напряму не заборонено користування програмою. «Програмне забезпечення «1С:Підприємство» не є об'єктом санкцій, його використання не заборонене. Ми продовжуємо свою діяльність з обслуговування та техпідтримки ваших інформаційних систем відповідно до укладених раніше договорів», – йдеться в повідомленні компанії, розісланому клієнтам.

Сам програмний продукт під санкції не підпадає. Справа в тому, що в Україні ABBYY працює переважно за системою франчайзингу: сертифіковані компанії, зареєстровані в країні, займаються установкою ПЗ, техпідтримкою і навчанням персоналу. Ймовірно, сам продукт і технологія не є об'єктом санкцій, і користувачі зможуть продовжити ними користуватися. Проблеми можуть виникнути, наприклад, з оновленням, або якщо податкова відмовиться приймати звітність, що згенерована в «1С» (хоча можливість це перевірити досить примарна, кажуть учасники ринку).

«Великої кризи з тим бізнесом, який користувався офлайновими рішеннями, тим самим «1С», гадаю, не буде. Вони продовжуватимуть

обслуговуватися. Правда, інтеграцію з іншими сервісами всередині компанії, якісь поновлення вже не зможуть робити», – вважає Калашніков.

Чи є реальні альтернативи «1С» на ринку?

Теоретично так, наприклад, розробки німецької компанії SAP, продукти IBM або Microsoft. З першою трохи знайомі в Україні, однак її продуктами користуються переважно великі компанії.

«Тут питання ціни, не всі зможуть собі це дозволити. З чого складається ця ціна? По-перше, плата за призначену для користувача ліцензію, по-друге – витрати на міграцію даних, по-третє – на навчання персоналу і/або тимчасове падіння їх продуктивності», – пояснює підприємець, знайомий з особливостями цих систем.

Є шанс запропонувати щось ринку і в українських творців софта. «Упевнений, у цілому українська IT-галузь завдяки цьому рішенню отримає чудовий поштовх до розвитку. Не секрет, що з боку російських товарів має місце агресивне просування, і досі споживачам було дешевше користуватися російським продуктом. Тепер український IT отримає шанс», – прогнозує Калашніков.

«ВКонтакте», «Яндекс» і «Мейл.ру» – переділ медіабізнесу?

Прихильники блокування сайтів російських соцмереж і поштових сервісів упевнені, що рішення президента є правильним з точки зору забезпечення інформаційної безпеки України. «В цілому потрібно не обмежуватися блокуванням, а розробити повноцінну стратегію державної контрпропаганди. А так ми щось блокуємо, а інформаційної альтернативи у нас як не було, так і немає», – уточнює Данченко.

Експерт зі стратегічних комунікацій НГО «Інформаційна безпека» Тетяна Попова згодна з тим, що рішення прибрати з українського інформаційного простору сайти з агітацією агресора – слушне. «Однак реалізовувати його потрібно було через суд. Упевнена, в суді легко було б довести, що там є хейтинг, дезінформація, заклики до насильства і повалення існуючого ладу та інші речі, що суперечать українському законодавству. А так президент поставив під сумнів легітимність свого рішення і взяв на себе негатив громадської думки, якого можна було б уникнути», – говорить Попова.

Однак блокування соцмереж, а також «Мейл.ру» і «Яндекса», які є великими медіакомпаніями, має й інший аспект: вплив на величезну кількість приватних підприємців, дрібних і середніх компаній, чий бізнес замкнений на електронну комерцію або діджитал-контент.

Варто відзначити, що навіть через три роки від початку війни з РФ російські сайти займають домінуючі позиції щодо залучення користувачів і охопленням аудиторії в українському сегменті інтернету. Так, у 2016 році vk.com стабільно посідав другу-третю сходинку рейтингу найпопулярніших сайтів (популярнішим був тільки google), yandex, mail.ru і odnoklassniki знаходяться на 4-5-6 місцях і випереджають за охопленням аудиторії ukr.net і facebook .

«Це шлях країн третього світу. Потрібно блокувати контент, а не платформу. Сотні тисяч фрілансерів ведуть бізнес через ВК. Тут в Україні. І ФБ не має і половини тих можливостей, які дає ВК для анонсування та розкрутки», – написав у мережі facebook український письменник і підприємець Максим Кідрук.

Бізнесу в цій ситуації залишається лише поспівчувати, тому що він зіткнеться з місяцями перехідного періоду і величезною конкуренцією за увагу аудиторії у кабінетах рекламників, погоджується Олексій Ткачук, SMM-директор в Getbob digital agency і автор блогу про Instagram – dnative.ru. «На білоруському ринку вартість залучення одного передплатника в брендові спільноти на facebook зараз на рівні 40-50 центів, а facebook у нас пасе задніх за охопленням аудиторії, і конкуренція в ньому практично відсутня. Якщо ж весь бізнес в єдиному пориві вирішить надолужувати втрачені позиції в facebook – це призведе до підвищення CPC/CPM в кілька разів, що стане ще одним ударом, який багато хто може і не пережити », – прогнозує він.

«Заборона соціальних мереж найбільше вдарить по малому і мікробізнесу. Адже соцмережі – основний канал продажів: сайти в основному потрібні для того, аби продемонструвати свій товар. «ВКонтакте» – це молодіжна цільова аудиторія, facebook – більше бізнес-аудиторія. Які втрати несе бізнес? Наприклад, аудит, розробка стратегії просування сторінки в середньому коштує від 600 доларів на місяць. Мінімальна вартість роботи smm-фахівця починається від 6 000 гривень на місяць. Це базові витрати – без реклами, оплати послуг фотографа тощо», – каже Тетяна Петренко, фахівець з SMM.

«Для нас першочерговим є навіть не питання доступності сайтів, а питання про те, як оплачувати рекламу. Ми – великі партнери і для «Яндекс», і для «Мейл.ру», і для «ВКонтакте». Якщо буде знайдено технічну можливість блокування сайтів – звичайно, трафік буде обрізаний, користувачі перейдуть на інші ресурси», – прогнозує Олександр Колб.

Як розраховуватися з контрагентами зі списку?

Юрист Лідія Климків вважає, що, згідно з постановою Нацбанку, можливість розрахунків обмежена. «Швидше за все, розраховуватися (отримати заборгованість або розплатитися за боргами) не вдасться з тими контрагентами, до яких застосовано санкції у вигляді а) обмеження торгових операцій; б) зупинення виконання економічних і фінансових зобов'язань», – зазначає юрист.

Так, за її словами, якщо українська компанія надає або отримує рекламні послуги через «Яндекс» і має договір на послуги з цим «Яндексом» (але тільки з тим «Яндексом», який є компанією зі списку), то у неї можуть бути проблеми як з боку держорганів України, так і на рівні розрахунків. Те ж саме стосується рекламних бюджетів у соцмережі «ВКонтакте». «Оскільки санкції поширюються лише на компанії зі списку, виникає питання: чи можна буде співпрацювати з якимись посередниками. Аналіз законодавства говорить, що таке можливо. Тому компанії, що опинилися під санкціями, швидше за все,

шукатимуть шляхів реструктуризації своїх каналів дистрибуції і ланцюжки підписання договорів з компаніями в Україні», – робить висновок Климків.

Керівник аналітичного відділу консалтингової компанії «Медіа ресурси Менеджмент» Артем Вакалюк упевнений, що рішення про блокування сайтів російських соцмереж і медіакомпаній призведе до перерозподілу рекламних бюджетів в інтернеті. «Узагалі це блокування саме для українських медіа може мати позитивний ефект. З ринку штучно прибираються декілька дійсно великих гравців. А оскільки святе місце не порожніє – своє встигнуть «схопити» й українські сервіси, що пропонують схожі послуги», – зазначає експерт.

(вгору)

Додаток 6

3.05.2017

Facebook визнала, що її платформу використовують для здійснення «штучного впливу»

Компанія Facebook опублікувала результати свого дослідження щодо поширення фейкових новин через її платформу. У ньому компанія визнала, що ризик використання платформи в маніпулятивних цілях досить високий (detector.media).

У документі, випущеному Facebook, окремо виділено поняття «штучного впливу» (false amplifier), який здійснюється через створення фейкових акаунтів у соцмережі та цілеспрямоване поширення через них певного контенту: викривлених новин, мемів, спаму, тощо.

«Відбувається створення груп або сторінок з певним наміром поширювати сенсаційні чи упереджені новини, які часто містять спотворені факти, аби вони відповідали певному наративу. Іноді ці сторінки включають в себе якийсь відсторонений контент, аби відволікти увагу від їхньої реальної мети», – йдеться у звіті компанії.

штучного впливу можуть координувати свої дії в написанні коментарів чи в розподілі «лайків» до публікацій. При цьому в Facebook підкреслили, що мова йде не про активність ботів, а реальних людей.

«Ми помітили, що більшість штучного впливу здійснюється не за допомогою автоматизованих процесів, а скоординованими людьми, які керують підставними акаунтами. Ми спостерігали за активністю цих фейкових акаунтів: ці дії могли виконувати лише люди з певним рівнем володіння мовними навичками і базовими знаннями про п

,

який вони публікують, що створює деяке враження про автоматизацію процесу», – йдеться у звіті Facebook.

Автори дослідження стверджують, що зусилля щодо поширення фейкових новин під час президентської виборчої кампанії в США в 2016 році були «статистично дуже малі у порівнянні із загальною активністю в сфері політичних питань

.

,

присвяченого виборам та громадській активності на Facebook, йдеться у звіті.

Автори звіту також відзначають, що цей тип активності часто використовується для отримання економічної вигоди. Модель роботи схожа з тією, яку використовували підлітки з невеликого македонського містечка – вони адміністрували роботу десятків сайтів з поширення фейкових новин, монетизуючи трафік та просуваючи певні новини чи меседжі за гроші.

Facebook планує боротися із явищем «штучного впливу» придіялючи більше уваги поведінці акаунтів у мережі, натомість менше зважаючи на контент, який акаунти поширюють. Для цього компанія буде використовувати нові аналітичні методи, в тому числі машинне навчання. Так, наприклад, соцмережа почала відслідковувати патерни активності фейкових акаунтів. При цьому, аналізувати контент на цих сторінках не було необхідності, зазначає Facebook.

Facebook вказує, що цей новий підхід допоміг їй деактивувати 30000 фейкових акаунтів напередодні президентських виборів у Франції. Компанія планує надалі розвивати свої інструменти, аби зменшити ризики маніпуляцій в інформаційному просторі, йдеться у висновках дослідження.

Reuters звертає увагу, що компанія кардинально змінила свою позицію: у листопаді минулого року CEO Facebook Марк Цукерберг назвав вплив фейкових новин у соцмережі на результати президентських виборів у США божевіллям.

(вгору)

Додаток 7

10.05.2017

Силовиков привлекут к расследованию поддельных аккаунтов в Facebook

Газета USA Today подвергается масштабной атаке спамеров, которые создают поддельные аккаунты в Facebook и делают их подписчиками издания. Во время чистки соцсети от ложных аккаунтов страница USA Today лишилась более 5 млн лайков, однако спамеры уже восполняют эту потерю. Газета просит ФБР расследовать ситуацию (Internetua).

Атака на USA Today

Газета USA Today, которая страдает от обилия поддельных аккаунтов среди своих подписчиков в Facebook, попросила Федеральное бюро

расследований США (ФБР) расследовать эту ситуацию. В прошлом месяце Facebook провел крупную чистку соцсети, удалив множество учетных записей, за которыми не стояли реальные пользователи. USA Today сообщает, что после этого она лишилась примерно трети подписчиков. Ранее страница газеты имела 15,2 млн лайков, после чистки их осталось 9,5 млн.

На днях Facebook сообщил USA Today, что в соцсети продолжается подозрительная активность, связанная с ее страницей. Газета остается главной мишенью спамеров, создающих поддельные аккаунты – она привлекает около 1 тыс. таких «подписчиков» в день. Facebook проинформировал USA Today, что может удалить ещё около 3 млн. лайков с ее страницы. После этого медиахолдинг Gannett Company, материнская компания газеты, решил обратиться в ФБР. Пока неизвестно, согласится ли бюро провести расследование.

По словам Шабнама Шаика (Shabnam Shaik), руководителя технической программы Facebook, ни одно другое издание публицистического характера не подвергается такому массовому наступлению со стороны спамеров. USA Today не может сказать определенно, почему именно она стала мишенью атаки. Соцсеть также не может понять причины происходящего. Для сравнения: во время апрельской чистки известное британское издание The Guardian лишилось всего 20 тыс. подписчиков, оказавшихся ложными. В то время как USA Today и связанные с ней издания потеряли в общей сложности 12 млн. лайков. USA Today – это первая общенациональная ежедневная газета в США, основанная в 1982 г. Ежедневный бумажный тираж составляет 959 тыс. копий, ежедневное количество читателей – около 7 млн.

Поддельные аккаунты в Facebook

Создание «неаутентичных» аккаунтов, которые лайкают страницы медиаизданий с целью распространения спама и ложной информации – это обычная практика спамеров. Спамеры подписываются на издания, чтобы «пустые» учетные записи выглядели более безопасными, когда контактируют с реальными пользователями.

Facebook сообщает, что продолжает борьбу с ложными аккаунтами. Компания применяет специальное ПО, которое их удаляет, а также блокирует новых подписчиков из Бангладеш, где высока активность спамеров. При этом соцсеть утверждает, что эти меры не содержат риска для реальных учетных записей.

Ежемесячная аудитория Facebook насчитывает около 1,94 млрд пользователей. По оценкам компании, примерно 1 % месячной активности в соцсети приходится на аккаунты, за которыми не стоит реальное лицо или организация. Это поддельные аккаунты спамеров, а также страницы, которые создаются пользователями для их домашних животных и т. п. Большая часть таких страниц создается за пределами США.

При этом поддельные учетные записи – вовсе не безобидная вещь, пишет USA Today. В апреле 2017 г. стало известно, что в Пакистане 10 студентов пытали и убили своего сокурсника, студента журфака Машала Хана (Mashal

Khan), который якобы осмелился богохульствовать на своей странице в Facebook. Товарищ Хана, который перенес побои по тому же обвинению, выжил и был госпитализирован. Перед смертью Хан утверждал, что аккаунт в соцсети был поддельным – его создал кто-то из его друзей.

(вгору)

Додаток 8

11.05.2017

Die Hände nach oben: Втручатися у вибори у ФРН будуть за старою схемою

Вадим Довнар

Выборы в США и Франции роднит наличие хакерских взломов одного из кандидатов. Следующие важные выборы пройдут в Германии – ключевой европейской стране, которая определяет политику Евросоюза. И есть основания полагать, что там тоже будет использоваться тот же алгоритм (LB.ua).

Факт вмешательства России в ход президентских выборов во Франции продемонстрировал, что Кремль не намерен не только отказываться от политики раскола Европы, но и менять стратегию привнесения «контролируемого хаоса» на интересующие Москву территории. Ближайшая цель – Германия, где уже в сентябре нынешнего года пройдут выборы канцлера.

Не стучали, но открылось

Накануне второго тура президентских выборов во Франции, как известно, кто-то слил в Интернет десятки тысяч внутренней переписки и других документов предвыборного штаба кандидата Эмануэля Макрона. The Guardian, ссылаясь на исследования нескольких работающих в сфере кибербезопасности компаний сообщило, что кибератаки «на Макрона» и штаб Демпартии США во время избирательной кампании Хиллари Клинтон связаны и имеют отношение к России. Сразу две компании, занимающиеся кибербезопасностью – Flashpoint из Нью-Йорка и Trend Micro из Токио – пришли к выводу, что ко взлому причастна группа хакеров, известная как Advanced Persistent Threat 28, Fancy Bear или Pawn Storm, и связанная с ГРУ РФ.

Собственно, непосредственно хакерская атака скорее всего была намного раньше выборов, а пользователь под ником EMLEAKS лишь выложил переписку и нужные сфабрикованные материалы в открытый доступ в веб-приложении Pastebin, позволяющим анонимно загружать отрывки текста или исходного кода и делиться этими данными с другими пользователями.

Знакомые уши Москвы концентрируются на Берлине

Напомним, скандалы, связанные со взломом закрытой документации политиков, возникали и до президентских выборов в США и Франции. И всегда в осуществлении этих атак подозревалась Россия. Еще с 2015 года, полагают многие аналитики, Кремль взял на вооружение тактику управляемого хаоса в Европе. Стали открываться факты вложения им гигантских средств в

различных лоббистов своих интересов: от бывших президентов до крайне правых или левых организаций. В частности, ни у кого уже не вызывает сомнения ставка Кремля на победу Ле Пен и ее финансирование из РФ. Как бесспорным представляется инициатор хакерских вмешательств во внутренние дела США, Голландии и Германии. Поэтому не стоит удивляться географии терактов в Европе – Париж, Ницца, Берлин.

В то же время, как пишет издание Monde, однозначно говорить о причастности России к инциденту со штабом Макрона пока сейчас нельзя: «Установление ответственных за кибератаки представляет собой длительный и комплексный процесс, который займет много дней или недель». В общем, сакраментальное – «а вы докажите».

Пока же будет идти официальное расследование, Кремль, упиваясь своей безнаказанностью, может спокойно заниматься следующим «клиентом». Не сложно догадаться, что им уже стала канцлер Германии Ангела Меркель. Впрочем, «Гибридная война» против нее ведется с 2015 года с момента утверждения политиком четкой позиции по Украине и констатации, что антироссийские санкции сняты не будут до выполнения Россией требований международного сообщества.

Между тем, приближаются выборы в ФРГ, и не нужно быть пророком, чтобы утверждать, что в преддверии голосования снова случится какой-то «вброс» или даже серия «вбросов» ранее похищенной путем хакерских атак информации, разумеется, с «поправками и изменениями» для указания правильного хода мысли читателей – немецкого электората, которые дополнительно будут «полироваться» другими «гибридными» формами и методами. И хотя руководитель разведки Германии Ханс-Георг Маассен предостерег Кремль от таких действий, но похищенная в 2015 году российским ГРУ вследствие хакерского нападения на Бундестаг информация должна в ближайшее время «всплыть».

Ноу-хау? И так сойдет

В условиях неизменности кремлевской стратегии на раскол Европы актуальным становится вопрос противодействия попыткам россиян вмешаться во внутренние дела других стран. По мнению уже экс-директора ФБР Джеймса Коми, высказанным им в интервью CNN накануне повторных слушаний в Сенате США относительно вмешательства России в президентские выборы США, нужно разговаривать с людьми: «Самое эффективное противодействие попыткам россиян вмешаться во внутренние процессы – рассказать людям обо всех их методах и приемах воздействия на сознание, чтобы они потеряли свою эффективность в дальнейшем».

Так вот, возвращаясь к случаю кибернападения на штаб Макрона, отметим, что технология и формы провокации, которую российские спецслужбы применили во Франции, ими уже применялись. В 2013 году, когда Кремль и президент Сирии Башар Асад «отмазывались» от очередной химической атаки против мирного населения.

Тогда, напомним, хаккер под ником JAsIrX взломал почту британской частной военной корпорации Britam Defense , которая обеспечивает охрану нефтедобывающих фирм в Ираке, и выложил ссылки на архивы со взломанной почтой этой компании в веб-приложении Pastebin. Далее «ведущие российские аналитики блогосферы» мгновенно проанализировали данные архивы и…вскрыли «новый мировой заговор» против России. Его, как утверждалось, организовали Великобритания, США и Катар, а осуществить должны были украинцы – сотрудники Britam Defense.

Как и в случае со штабом Макрона в выложенной документации среди настоящих документов фигурировали сфабрикованные письма. Причем, фальсификаторы прокололись на том, что обрабатывали свои поделки в русскоязычных версиях приложений.

«Иранское» и «сирийское» письма, как доказали специалисты, являлись поддельными и полностью сфабрикованными.

Что же касается Britan Defence, то, оказалось, что продемонстрированное взломщиками − настоящие внутренние документы компании. Однако они не несли никакой сенсационной нагрузки, а выложены были только для подтверждения аутентичности двух упомянутых писем.

Между тем, какой-никакой результат фальсификаторами был получен. Украина на несколько дней оказалась в эпицентре очередной информационной провокации. Дескать, смотрите, какие алчные эти «хохлы»-наемники, на все готовы ради твердой валюты.

Как мы видим, никаких ноу-хау российские спецслужбы не изобретают. Методы их шаблонны и достаточно известны, да и наблюдать их можно не только в случае со вмешательством в ход выборов в иностранных государствах.

Так что французским расследователям недавнего инцидента в штабе Макрона стоило бы также обратиться за помощью к британцам, которые вероятно разложили полностью российскую провокацию в 2013 году с использованием Britam Defense.

Кроме того, как заявил глава Агентства национальной безопасности США Майк Роджерс на Комитете Сената по вопросам вооруженных сил, спецслужбы США предупреждали Францию о российских хакерах, которые атаковали штаб тогдашнего кандидата в президенты страны Эммануэля Макрона.

(вгору)

Додаток 9

27.04.2017

ФСБ Росії могла качати дані з України через нелегальний софт, – СБУ

У восьми компаніях провели обшуки в рамках операції з виявлення такого ПЗ, зокрема в компаніях «Укргазвидобування» і Dragon Capital

Федеральна служба безпеки Росії могла отримувати дані з України завдяки програмному забезпеченню «Стахановець», яке виявили у 8 компаніях, зокрема, в «Укргазвидобуванні» та Dragon Capital (iPress.ua).

Відповідне програмне забезпечення містить засоби негласного контролю і зняття інформації, про які власники-клієнти могли й не знати, – заявив начальник апарату голови СБУ Олександр Ткачук на брифінгу 27 квітня, інформує «Українська правда».

26 квітня у восьми компаніях провели обшуки в рамках операції з виявлення такого ПЗ, зокрема в компаніях «Укргазвидобування» і Dragon Capital.

«Ці обшуки не були пов'язані з основним напрямком діяльності цих компаній, а були пов'язані саме з тим, що Служба документувала використання спеціального програмного забезпечення, за допомогою якого здійснюється віддалений контроль і зняття інформації», – сказав Ткачук.

За даними СБУ, приблизно 300 компаній на території України на сьогодні використовують таке програмне забезпечення. Ще з 2016 року використання цього програмного продукту заборонено, бо його визнали спеціальним технічним засобом.

«В рамках кримінального провадження СБУ задокументовано, що компанія-розробник цього програмного продукту співпрацює з Федеральною службою безпеки Російської Федерації.

Після обшуків у 8 компаніях виявлено докази того, що «більше тисячі ліцензій на цей програмний продукт використовувалися на комп'ютерах цих компаній», але СБУ не вилучала всі комп'ютери.

У компанії «Укргазвидобування» вилучили 1 сервер та 5 клієнтських машин, а у Dragon Capital вилучили 1 сервер і 3 клієнтських комп'ютери. Цього достатньо, щоб призначити експертизи, сказав Ткачук.

(вгору)

Додаток 10

5.05.2017
Кіберполіцією Слобожанщини ліквідовано злочинну групу шахраїв

Працівниками Слобожанського управління кіберполіції Департаменту кіберполіції НП України спільно працівниками ГУНП в Полтавській та Харківській областях, а також, батальйону поліції особливого призначення ГУНП в Полтавській області та прокуратурою Полтавської області, проведено міжрегіональну операцію із припинення діяльності та затримання активних учасників злочинної групи, у результаті якої одночасно проведено 10 санкціонованих обшуків на території Харківської та Полтавської областей (Сайт Департаменту Кіберполіції України).

Так, кіберполіцейськими виявлено та задокументовано злочинну групу з ознаками організованості, учасники якої, починаючи з вересня 2016 року до

березня цього року шахрайським шляхом заволоділи 46 банківськими картками громадян, а в подальшому несанкціоновано втрутились у роботу електронно-обчислювальних машин (комп'ютерів) АТ «Ощадбанк» і за допомогою системи WEB-банкінг «Ощад 24/7», перепрев'язували їх до мобільного телефону учасника злочинної групи, та вчиняли заволодіння грошовими коштами громадян в значних розмірах. У результаті вжитих заходів встановлено, що особи, які входять до складу злочинної групи, здійснюють телефонні дзвінки з території виправної колонії (розташованої на тимчасово окупованій території Луганської області) із прихованого номеру телефону та, представляючись працівниками поліції, під приводом не притягнення близької особи до відповідальності, вимагають переказати грошові кошти в розмірі від 2 тис. доларів США на карти АТ «Ощадбанк». У подальшому, отримані злочинним шляхом грошові кошти, знімались через банкомати АТ «Ощадбанк» в Полтавській та Харківській областях, а також, з використанням терміналів ПАТ КБ «ПриватБанк» розподілялися серед учасниками злочинної групи. Крім того, значна сума грошових коштів, отриманих шахраями, з використанням сервісу переказу коштів «Western Union» конвертувалася в російські рублі та обготівковування на території так званої «ЛНР». Також, встановлено, що учасники злочинної групи під час вчинення протиправних дій відрекомендовувалися потерпілим керівниками Державної фіскальної служби України у різних областях України та співробітниками банків з метою заволодіння грошовими коштами підприємців і громадян. На сьогодні, задокументовано більше 300 епізодів злочинної діяльності групи, які заподіяли шкоду громадянам на суму понад 4 млн. грн. У ході проведення обшуків вилучено комп'ютерну техніку, мобільні термінали, понад 70 сім-карт різних мобільних операторів, котрі використовувалися як фінансові номери, грошові кошти, понад 400 чеків із банкоматів з підтвердженням успішного зняття грошових коштів, чорнові записи з номерами карт та пін-кодами до них, а також чорнові записи з підрахунками отриманих злочинним шляхом коштів та 50 банківських карток АТ «Ощадбанк» та КБ «Приватбанк», на які постраждалі переказували грошові кошти. На разі, на 17 підконтрольних шахраям банківських рахунків, відкритих в ПАТ КБ «ПриватБанк», накладено арешт та заблоковано кошти у сумі близько 1 млн. грн. Крім того, накладено арешти на 48 банківських карт емітованих АТ «Ощадбанк». Учасників злочинної групи затримано у порядку ст. 208 КПК України за підозрою в скоєнні злочинів, передбачених ч. 3 ст. 190 КК України.

(вгору)

Додаток 11

11.05.2017

В США хотят ограничить «Касперского»: Он стал слишком распространен

Правительство США видит в продуктах «Лаборатории Касперского» угрозу для национальной инфраструктуры. Опасения вызывает то, что в «Лаборатории» работают бывшие российские военные, и то, что российские власти имеют доступ к любой информации на территории своей страны (InternetUA).

Меморандум Комитета по разведке

Власти США опасаются, что российские спецслужбы могут использовать «Лабораторию Касперского», чтобы шпионить за американцами и саботировать работу ключевых инфраструктурных систем страны. Об этом сообщило издание ABC News. Власти обеспокоены тем, что продукция российской компании широко используется в США, причем не только в частном, но и в коммерческом, а также государственном сегменте. Например, антивирусы «Лаборатории» используются в Федеральном бюро тюрем. Кроме того, на территории США продаются ноутбуки, на которых предустановлено ПО российской компании.

Обеспокоенность возможной угрозой, исходящей от «Лаборатории», была высказана в секретном меморандуме, который был направлен в прошлом месяце директору Национальной разведки Дэну Коутсу (Dan Coats) и генеральному прокурору Джеффу Сешнсу (Jeff Sessions). Документ был подготовлен Комитетом по разведке Сената США. Комитет убедительно просит принять меры в связи с потенциальным риском, который несет в себе широкая распространенность продуктов «Лаборатории» на американском рынке. Это расценивается как вопрос национальной безопасности.

Проблема персонала

Американские чиновники обеспокоены тем, что некоторые руководители «Лаборатории» ранее работали на российские разведывательные и военные структуры. Например, директор компании по правовым вопросам Игорь Чекунов в свое время работал в пограничной службе России, которая отчитывается перед органами госбезопасности. Исполнительный директор Андрей Тихонов был подполковником российской армии, где занимался информационными технологиями.

Глава «Лаборатории» Евгений Касперский отвечает на это, что оба сотрудника пришли в компанию более 20 лет назад, и что он на 100% уверен в отсутствии у них связей с правительством.

Мнения американских чиновников

По словам Эрика Розенбаха (Eric Rosenbach), который до января 2017 г. был помощником министра обороны США по вопросам кибербезопасности, «многие люди в сообществе национальной безопасности чувствуют себя некомфортно» из-за возможных связей «Лаборатории» с российской разведкой.

Того же мнения придерживается Майкл Карпентер (Michael Carpenter), который до января 2017 г. занимал должность заместителя помощника министра обороны по Украине, России и Евразии. По его словам, «широко известным фактом» является то, что «Лаборатория» может представлять угрозу для национальной инфраструктуры США. Бывший заместитель министра

энергетики Лиз Шервуд-Рэндэлл (Liz Sherwood-Randall) отмечает, что давно исследует возможную угрозу для энергосетей со стороны «Лаборатории».

Доступ к данным в России

Министерство обороны США обеспокоено также тем, что российская система оперативно-розыскных мероприятий позволяет властям на законном основании ознакомиться с любыми данными, которые идут через российские сети. Министерство отмечает, что для этого необходим судебный ордер, однако, по его данным, в России этим часто пренебрегают. В ответ на это Евгений Касперский уверяет, что его компания предоставляет властям какие-либо данные только и исключительно на основании судебного ордера.

Кроме того, если клиент не хочет, чтобы его данные, даже в анонимной форме, передавались через Россию, он может отказаться от услуг компании. Наконец, предприятия и госорганы могут установить у себя локальный центр «Лаборатории», чтобы их данные не покидали пределов компании или страны. В ответ на предположение, что через свои продукты «Лаборатория» может получить доступ ко всем файлам пользователя, Касперский заметил, что это трудно осуществимо технически.

Отношения с ФБР

В 2016 г. Федеральное бюро расследований (ФБР) высказало ряд опасений насчет «Лаборатории» представителям индустрии, в том числе, Координационному совету подсектора электричества – организации, в которую входят главы энергетических компании Северной Америки. По данным ABC News, в феврале 2017 г. Министерство внутренней безопасности США направило американским спецслужбам секретный доклад, касающийся «Лаборатории». В настоящий момент ФБР выясняет, в каких отношениях находится «Лаборатория» с российским правительством.

Источники ABC News сообщают, что несколько лет назад ФБР предлагало Евгению Касперскому стать информатором бюро, но он отказался. Сам Касперский этот факт отрицает. «Лаборатория» заявляет, что глава компании действительно встречался с представителями ФБР и других спецслужб, но только ради обсуждения вопросов борьбы с киберпреступностью.

(вгору)

Додаток 12

16.0.2017

Як в Україні блокуватимуть російські інтернет-сервіси

Президент України ввів в дію рішення РНБО щодо санкцій проти російських популярних інтернет-сервісів та соцмереж. DW з’ясовувала, як запрацюють нові санкції (DW.COM).

16 травня на сайті президента України був опублікований указ про введення в дію рішення Ради національної безпеки і оборони України (РНБО) від 28 квітня «Про застосування персональних спеціальних економічних та

інших обмежувальних заходів (санкцій)». Серед 468 юридичних осіб щодо яких продовжуються або вводяться нові обмеження – 81 IT-компанія, зокрема популярні російські інтернет-сервіси «Яндекс» та Mail.ru, соціальні мережі «ВКонтакте» та «Одноклассники» (обидва контролюються Mail.ru Group).

Трирічні санкції щодо них передбачають блокування українських активів, обмеження торговельних операцій, заборону на виведення коштів за межі України, припинення виконання економічних і фінансових зобов'язань, та головне – блокування інтернет-провайдерами доступу до цих ресурсів.

Реакція компаній

Згідно з квітневим дослідженням компанії Kantar TNS CMeter, ці ресурси є одними з найпопулярніших серед української інтернет-аудиторії: зокрема «ВКонтакте» на третьому місці і має охоплення у 78,7 відсотка. Майже півмільйона підписників має сторінка президента України у цій популярній російській соцмережі.

Рішення РНБО та президента стало справжньою несподіванкою для інтернет-компаній та їх українських представництв. «Це рішення вдарить насамперед по самих користувачах – громадянах України. Близько 25 мільйонів жителів України спілкуються зі своїми друзями в Україні і в усьому світі; тепер вони будуть позбавлені цих зв'язків», – йдеться в заяві Mail.Ru Group.

Директор зі зв'язків із громадськістю головного офісу "Яндекс" у Москві Очір Манджиков в коментарі DW заявив, що компанія ще розробляє план дій щодо подальшої роботи в Україні, зазначивши, що їх сервісами користуються понад 11 мільйонів українських юзерів.

Наслідки для користувачів

Блокування російських ресурсів означатиме, що абоненти українських провайдерів не зможуть вільно отримувати доступ до електронної пошти Mail.Ru, не зможуть користуватись поштою, пошуком чи картами від «Яндексу», обмінюватись фотографіями чи спілкуватись в «Одноклассниках» чи слухати музику «ВКонтакте». Однак до практичного застосування санкцій ще далеко, зазначають експерти.

Першим про плани щодо виконання рішення РНБО заявив найбільший український інтернет-провайдер «Укртелеком». «Процес досить складний і вимагає певного часу, з огляду на значну кількість ресурсів», – заявив директор з корпоративних комунікацій компанії Михайло Шуранов, зазначивши що роботи триватимуть від кількох діб до тижня.

Водночас, Олександр Федієнко, голова правління найбільшого галузевого об'єднання інтернет-провайдерів – Інтернет асоціації України – каже, що для термінового блокування російських соцмереж в провайдерів просто немає ресурсів на переоснащення мереж.

А голова галузевої асоціації «Телекомунікаційна палата України» Тетяна Попова вважає, що блокування не є ефективним засобом захисту інформаційної безпеки держави. «Будь-який вид блокування не так важко впровадити і не важко обійти – є врешті VPN, TOR та інші інструменти», – пояснила вона у розмові з DW.

Туманні юридичні перспективи

Натомість, опитані DW експерти зазначають, що юридичні перспективи впровадження рішення РНБО незрозумілими. «Українське законодавство донедавна передбачало блокування інтернет-ресурсів тільки за рішенням суду. Підписаний нещодавно президентом закон "Про підтримку кінематографії" запроваджує процедуру досудового блокування для піратських сайтів. Якихось механізмів блокування ресурсів, які є у санкційному списку немає», – констатує Попова.

Рішення президента входить у колізію із діючим законодавством, визнає голова парламентського комітету з питань інформатизації та зв'язку Олександр Данченко (фракція «Самопомочі»). «Законні підстави для блокування інтернет-ресурсів передбачає законопроект, розроблений кіберполіцією. Але він ще не пройшов необхідного обговорення з ринком і не зареєстрований у парламенті. В цьому вигляді перспективи його прийняття нульові», – сказав він у розмові з DW.

Інтернет-цензура чи відповідь на інформаційну війну?

Публікація указу голови держави викликала бурхливу дискусію, розділивши експертне середовище на тих, хто вважає блокування російських соцмереж дієвим інструментом захисту інформаційного простору і тих, хто назвав рішення РНБО кроком до впровадження цензури. «З інтернет-цензурою потрібно бути обережним. Це викличе багато критики і в наших міжнародних партнерів, і всередині країни. Будуть аналогії з політикою, яку проводить Росія», – заявив агенції УНІАН директор Центру прикладних політичних досліджень «Пента» Володимир Фесенко.

Натомість політтехнолог, засновник «Українського інституту майбутнього» Тарас Березовець рішення підтримав. «Істерична реакція показує, як росіянам сьогодні зробили боляче. Росія хотіла гібридну війну, вона її отримала. Розкажіть тепер, як все було марно», – написав Березовець на своїй сторінці у мережі Facebook, до якої, як очікують, почнеться тепер масова «міграція» українських користувачів з російських соцмереж.

(вгору)

Додаток 13

26.04.2017

Илья Кабачинский

Сервис Unroll.me очищает электронную почту от спама. А потом тихо продает ваши данные другим

Издание The New York Times 23 апреля опубликовало материал, в котором вскрылся неизвестный ранее момент из жизни скандальной компании Uber. Оказывается, что когда CEO Apple Тим Кук узнал о слежке за пользователями компанией Трэвиса Каланика, он пригрозил удалить Uber из App Store. Сам факт подобной встречи интересен уже тем, что Uber удалось сохранить бизнес за счет своего масштаба (если бы Apple удалила приложение

сервиса, он бы потерял десятки миллионов пользователей), но многих заинтересовал другой момент. А именно компания Unroll.me (AIN.UA).

Оказалось, что компания Uber следила за водителями и клиентами Lyft через покупку информации у агентства Slice Inteligence. Та, в свою очередь, получала данные за счет сервиса Unroll.me, купленного в 2011 году. Как он работает?

Unroll.me – это сервис для очистки электронного ящика. Пользователю необходимо дать доступ к своему аккаунту в одной из популярных почтовых служб, после чего Unroll.me просканирует содержимое и укажет на спам, рассылки и другой не самый важный контент. В несколько кликов пользователь может отписаться от ненужной информации и очистить электронный ящик. Несколько лет назад сервис рекомендовали все ключевые издания Америки, в том числе и The New York Times.

Сервис бесплатен, но бесплатного, как известно, ничего нет. Unroll.me сканировал почту пользователей и потом мог продавать с нее информацию другим компаниям по запросу. В самой компании заверили, что все данные передаются исключительно анонимно, но пользователей такой ответ, очевидно, не устроил: согласие на подобное никто вроде как не давал.

Что интересно, руководитель компании Slice Inteligence Джоджо Эдайя даже принес пользователям свои извинения. Правда, виновным он себя не признал: ему было обидно за то, что некоторые пользователи пожелали удалить сервис, а не по причине тайной перепродажи данных:

«Наши пользователи – сердце нашей компании и сервиса. И это был настоящий удар смотреть на то, что их расстроила информация с объяснением нашего способа монетизации бесплатного сервиса», — Джоджо Эдайя, CEO Slice.

К дискуссии также подключилась основательница Unroll.me Перри Чейс, которая сейчас уже не работает в компании, но решила не стоять в стороне:

«Поверьте мне, сервис, которые очищает от лишнего мусора почты миллионов людей, делает это БЕСПЛАТНО только из-за того, что мы придумали способ его монетизации. И да, продажа данных – это единственный вариант для заработка подобных сервисов», – Перри Чейс, основательница Unroll.me.

На самом деле сервис Unroll.me уведомлял пользователей, что продает их данные, просто пользовательское соглашение никто не читал: видимо чтиво на 5000 слов интересно не всем. Правда, пользователи быстро нашли скрытый обман: возможно на 15-й странице текста пользователя и уверяют, что могут продать его данные, но при первой регистрации Unroll.me обещает «не трогать ваши личные данные».

Сам руководитель компании не принес извинений за продажу информации сторонним лицам. И, судя по всему, компания не прекратит этого делать в будущем.

(вгору)

Додаток 14

26.04.2017
Kaspersky Lab исследует ботнет Hajime

Kaspersky Lab рассказала об активности зловреда Hajime, который в настоящее время энергично заражает устройства Интернета вещей и создает из них ботнет (ITnews).

На данный момент под контролем Hajime находятся почти 300 тысяч гаджетов по всему миру. Потенциально все они готовы выполнять команды злоумышленников, однако реальная цель Hajime до сих остается неизвестной.

В переводе с японского Hajime означает «начало». Первые признаки активности этого зловреда были замечены в октябре 2016 года. Наибольшее число зараженных устройств сейчас зафиксировано в Иране – около 20 %. Следом идут Бразилия (9 %) и Вьетнам (8 %).

Исследователи отмечают, что в Hajime нет функций, позволяющих осуществлять атаки; на данный момент зловред содержит только модуль, отвечающий за его распространение. Для заражения устройств Hajime использует разные техники, но чаще отдает предпочтение брутфорс-атакам, то есть методу подбора пароля через перебирание возможных комбинаций. После успешного заражения зловред предпринимает меры для сокрытия своего присутствия на устройстве.

Hajime не слишком избирателен – он готов заразить любой гаджет, подключенный к Интернету. Однако в числе его жертв все же преобладают видеозаписывающие устройства, веб-камеры и роутеры. Примечательно, что зловред избегает некоторых сетей, среди них, в частности, сети General Electric, Hewlett-Packard, почтовой службы США и Министерства обороны США.

«Самая большая интрига Hajime – это его цель. Ботнет быстро растет, а для чего до сих пор неизвестно. Мы не заметили присутствия Hajime в каких-либо атаках или другой вредоносной активности. Тем не менее не стоит недооценивать угрозу. Мы рекомендуем всем владельцам устройств Интернета вещей сменить пароли на гаджетах, при этом выбирать сложные комбинации, которые нелегко угадать, а также по возможности обновить ПО от производителя», – отметил Константин Зыков, старший аналитик Kaspersky Lab.

(вгору)

Додаток 15

27.04.2017
Больницы становятся любимой целью хакерских атак

Медицинские учреждения становятся новой целью киберпреступников, похищающих личные данные. Получая доступ к персональной медицинской информации, мошенники продают базы данных или вымогают деньги. Для решения проблемы отрасли здравоохранения требуются совершенные

инструменты и квалифицированные ИТ-кадры, способные противостоять угрозам (InternetUA).

Кибератаки – новая реальность медицины

Эксперты все чаще фиксируют активность киберпреступников в медицинской отрасли. Одна из стран, где в настоящее время проблема похищения данных из больниц стоит особенно остро – Новая Зеландия. С середины 2015 по середину 2016 г. Национальный центр кибербезопасности Новой Зеландии зарегистрировал 338 инцидентов с попытками нарушения информационной безопасности, из них 169 – на государственные службы, в том числе учреждения здравоохранения. Для сравнения, годом ранее было зафиксировано всего 190 подобных инцидентов.

ИТ-специалисты предупреждают, что кибератаки – это новая реальность, в которой будут вынуждены функционировать государственные органы как потенциальные мишени таких нападений. При этом с каждым годом число кибератак будет возрастать.

Медицинские данные как ценный товар

Чаще всего для атаки на больницы и поликлиники используются вредоносное программное обеспечение ransomware (софт для вымогательства) и другие программы. Такое ПО устанавливается на компьютер жертвы и хранит данные в заложниках до момента оплаты выкупа. Люди стремятся сохранить в тайне информацию о состоянии здоровья. Медицинский центр, потерявший такие данные, рискует получить судебные иски и понести крупные финансовые потери.

Учреждения здравоохранения становятся мишенью, в том числе из-за наличия достаточных финансовых средств для оплаты выкупа. По данным ФБР США, в 2016 г. киберпреступники с помощью вымогательства получили от учреждений здравоохранения более $150 млн.

Главная проблема – отсутствие кадров

Возрастающее количество кибератак на государственные службы также является следствием дефицита квалифицированных ИТ-кадров. Высокие зарплаты ИТ-специалистов в частном секторе приводят к тому, что государственные органы теряют высококлассных сотрудников, способных бороться с киберугрозами.

Системный инженер Fortinet Юрий Захаров отметил важную роль квалифицированного персонала в борьбе с киберпреступностью: «В настоящее время все более широкое распространение получают так называемые целенаправленные атаки, когда целью злоумышленников становятся определенные организации и информация. За такими атаками чаще всего стоят подготовленные и технически грамотные люди, целью которых является получение реального дохода методом шантажа и вымогательства. Организации здравоохранения, как и другие специализированные компании, оперирующие персональными данными и личной информацией клиентов, должны грамотно и своевременно обеспечивать необходимый и достаточный уровень защиты информации от хищения или нелегитимного доступа посторонних лиц. Помимо

современных технических средств противодействия целенаправленным атакам у компаний должен быть грамотный и квалифицированный персонал».

(вгору)

Додаток 16

27.04.2017
Антивирус Касперского – мина в киберполе Украины

Не секрет, что большинство ИТ компаний вынуждены сотрудничать со спецслужбами своих стран. Яркий пример тому – информация, обнародованная Эдвардом Сноуденом о государственной программе США «PRISM». Когда на активное сотрудничество вынуждены были пойти многие крупные компании, предоставив компетентным органам доступ к серверам Microsoft, Google, Yahoo, Facebook, YouTube, Skype. Принимая во внимание, что Украина находится в состоянии гибридной войны с Российской Федерацией, встал вопрос о том, какое положение занимают в Украине до недавнего времени популярные, антивирусные решения российской «Лаборатории Касперского», какое отношение компания имеет к спецслужбам РФ и какие угрозы Национальной системе кибербезопасности может нести использование программ государства-агрессора («Информационное Сопротивление).

Напомню, что в сентябре 2015 года Украина ввела санкции против ряда российских компаний, в число которых попал и известный разработчик антивирусного программного обеспечения «Лаборатория Касперского». Санкции касались запрета осуществления государственных закупок и использования органами государственной власти антивирусных продуктов «Лаборатории Касперского» производства российских коммерческих структур.

Только спустя год, в сентябре 2016 года, санкционный список был расширен и в нем среди прочих оказалась украинская дочерняя компания «Лаборатория Касперского Украина». Это значит, что до недавнего времени находящаяся под санкциями российская компания могла свободно осуществлять свою деятельность в Украине через дочернюю структуру. По некоторым данным, антивирусные продукты российских компаний были установлены на компьютерах Верховной Рады Украины, Государственной налоговой администрации, Фонда госимущества, Пенсионного фонда, Минобороны, Минобразования, ГПУ, Минсоцполитики, ЦИК, СБУ и др.

В декабре 2016 года «Общество с ограниченной ответственностью Лаборатория Касперского Украина» сообщило о ликвидации компании по решению владельца. На этой ноте и должна была закончиться история путешествия российской компании по киберпространству Украины. Но не все так просто – «дело партии» продолжает жить…

К сожалению, санкции распространяются только на государственный сектор Украины. И пока Госспецсвязь, согласно Плану реализации Стратегии Кибербезопасности Украины на 2017 год, только пытается внедрять меры по ограничению использования программного обеспечения государства-агрессора

на объектах критической инфраструктуры, физические лица и коммерческие организации спокойно продолжают использовать российский софт, в том числе, и антивирусные решения «Касперского».

На просторах украинского интернета свободно живет ресурс «kaspersky[dot]ua» с доменным именем в сегменте «.ua» и интерфейсом на украинском языке. На этом сайте приведен список довольно известных украинских IT компаний, которые являются партнерами российской антивирусной фирмы. Большинство из этих компаний на своих корпоративных сайтах открыто рекламируют и реализуют продукты «Касперского».

Чем же так опасна «Лаборатория Касперского» и ее продукты для украинского киберпространства в условиях гибридной войны с Россией?

Известный факт, что в 2014 году российским хакерам накануне президентских выборов в Украине удалось взломать компьютер системного администратора Центральной избирательной комиссии с помощью трояна. Злоумышленники установили программу, которая делала снимки экрана компьютера, фиксировала пароли, набранные с клавиатуры, и отправляла информацию на удаленный сервер. В дальнейшем, полученная информация была использована для попытки дискредитации избирательной системы Украины. Интересно, что на компьютере системного администратора ЦИК был установлен все тот же антивирус «Касперского», который по несчастливой случайности или преднамеренно не смог увидеть угрозу. А может, антивирус сам сгенерировал эту угрозу...?

В сети неоднократно появлялась информация о близкой дружбе «Лаборатории Касперского» и ее руководителя с уполномоченными службами Российской Федерации. В обзоре американской информационной компании Bloomberg излагаются утверждения о том, что с 2012 года фирма проводит замену своего руководящего состава на сотрудников близких к ФСБ Российской Федерации. Также лаборатория активно помогает спецслужбам РФ в вопросах анализа и расследования инцидентов, а так же проводит консультации в области информационной безопасности.

В тоже время Евгений Касперский, основатель и руководитель одноименной фирмы, еженедельно посещает банные комплексы с представителями разведслужб Российской Федерации. Так же следует обратить внимание на интересный факт из официальной биографии Евгения Касперского. Будущий топ-менеджер антивирусной лаборатории в 1987 году окончил 4-й (технический) факультет Высшей школы КГБ (в настоящее время факультет известен как Институт криптографии, связи и информатики Академии ФСБ России). Как пишут в книгах, «КГБистов бывших не бывает».

Также из доклада Bloomberg следует, что «Лаборатория Касперского» собирает конфиденциальные данные с устройств пользователей, которых насчитывается около 400 млн. по всему миру, и передает информацию в ФСБ по требованию. Такими сведениями с агентством на условиях анонимности поделились шесть действующих и бывших сотрудников фирмы.

Таким образом, физические лица и украинские коммерческие предприятия, конечные пользователи продукции «Касперского» за собственные деньги предоставляют полный доступ к своей системе, приложениям, файлами и даже действиям.

Ведь антивирус «Касперского» работает в системе с наивысшим приоритетом и его работа не может, в достаточной степени, быть ограничена или контролироваться внешним программным обеспечением. Антивирус сканирует любые файлы и может передавать информацию на удаленный сервер. Но даже если перехватить эту информацию, определить содержимое вряд ли удастся. Вся передача осуществляется в зашифрованном виде.

Таким образом, если брать во внимание, что множество элементов критической инфраструктуры, телекоммуникаций и других ключевых объектов Украины принадлежат частным компаниям, становится явным, к каким угрозам для Национальной системы кибербезопасности может привести за собой дальнейшее использование программного обеспечения производства страны-агрессора, а тем более продуктов компаний, замеченных в профессиональных связях с ФСБ.

Надеюсь, что Госспецсвязи и другим соответствующим органам все же удастся ограничить использование российского софта не только в государственном секторе, но и среди других субъектов, имеющих отношение к критической инфраструктуре и информационным системам.

(вгору)

Додаток 17

3.05.2017

Дилетанты массово воспользовались инструментами хакеров, связанных с АНБ

Хакерские инструменты аффилированной с АНБ группировки Equation Group начали использоваться для атак на простых пользователей. По всей видимости, работают хакеры-дилетанты, вооружившиеся этими эксплойтами. Общее количество заражений, по разным оценкам, находится в диапазоне от 15 до 41 тыс (InternetUA).

Серьезные инструменты попали в руки хакеров-дилетантов

На протяжении последних месяцев хакерская группировка Shadow Brokers публиковала в открытом доступе инструменты печально знаменитой Equation Group – еще одной хакерской группировки, которая, по мнению экспертов по безопасности, может быть связана с Агентством национальной безопасности США (АНБ). Как минимум два из этих инструментов уже активно используются дилетантами для проведения атак.

Эксперт по безопасности Дэн Тентлер (Dan Tentler), основатель компании Phobos Group, заявил изданию The Register, что ему удалось выявить несколько десятков тысяч машин с признаками заражения бэкдором Doublepulsar,

разработанным Equation. Этот бэкдор, в свою очередь, устанавливается с помощью другого инструмента тех же разработчиков – эксплойта Eternalblue.

Данный эксплойт атакует сервисы сетевого протокола для удаленного доступа SMB в версиях Windows от XP до Server 2008 R2 – при условии, что данные сервисы доступны извне.

Microsoft устранила соответствующую уязвимость в SMB Server (MS17-010) в марте 2017 г. Патч был выпущен для операционных систем Windows, начиная с Vista SP2 и до Windows Server 2016 включительно. Патчи для XP и Server 2003 не выпускались, поскольку их Microsoft уже сняла с поддержки.

Масштабы проблемы

По словам Тентлера, в минувший четверг он с помощью поисковика Shodan.io выявил более 15 тыс. заражений, четыре пятых из которых приходятся на IP-адреса на территории США. С каждым новым сканированием количество заражений растет. Систему, атакованную Doublepulsar, можно опознать по ответу на специальный PING-запрос к порту 445.

По заверению Тентлера, рост числа заражений означает, что хакеры-дилетанты и недоучки вооружились чужими инструментами и начали заражать все вокруг. Причем 15 тыс. заражений – это еще и «нижний порог» оценки. Коллега Тентлера по цеху, эксперт Роберт Грэм (Robert Graham) обнаружил более 41 тыс. зараженных хостов, и это, скорее всего, не конец.

«Ничего неожиданного в том, что дилетанты схватились за бывшие "игрушки" Equation, нет, – говорит Ксения Шилак, директор по продажам компании SEC-Consult Рус. – Но это очень неприятное развитие событий: дилетант, вооруженный эффективным инструментом взлома, опасней, чем дилетант безоружный. Количество успешных заражений, в целом, тоже неудивительно: пользовательская "беззаботность" в отношении кибербезопасности – это объективный фактор, с которым приходится считаться: и отрасли киберзащиты, и разработчикам ПО».

«Чужие игрушки»

В 2015 г. «Лаборатория Касперского» опубликовала исследование, посвящённое EquationGroup, в котором указывалось, что эта группа «много лет взаимодействует с другими влиятельными группировками, например с теми, что стоят за Stuxnet и Flame, причем каждый раз с позиции превосходства: Equation всегда получала доступ к эксплойтам нулевого дня раньше других групп».

Группировка TheShadowBrokersв августе 2016 г. объявила о том, что ей удалось похитить ряд инструментов EquationGroup, и попыталась выставить их на аукцион. Поскольку желающих платить за кота в мешке не нашлось, «брокеры» начали публиковать эти эксплойты в общем доступе (это дает основание полагать, что распространение данного инструментария и было основной целью «брокеров»).

Эксперты, проанализировавшие опубликованные Shadow Brokers эксплойты, сошлись в высокой оценке качества вредоносных программ Equation. Как нетрудно заметить, они до сих пор оказываются весьма

эффективны, несмотря на то, что вендоры ПО оперативно выпускают патчи для всех уязвимостей, к которым у Equationбыли эксплойты.

(вгору)

Додаток 18

12.05.2017

Обікрасти чи знеславити: небезпеки з соцмереж і як їх уникнути

Коли людина щось публікує в соцмережах чи навіть пише приватне повідомлення – це вже потенційна небезпека, кажуть спеціалісти. В чому ми занадто довіряємо соцмережам і чим ризикуємо, нехтуючи обережністю.

Про це пишуть Версії з посиланням на 24 (Версії.if.ua: Щоденна інтернет-газета).

Про ризики, пов'язані з ситуацією, коли соцмережа знає про тебе все і навіть більше, вже писали страшні книги і знімали жахаючі фільми. Але відмовлятися від користування соцмережами ніхто і не думає. Є принаймні кілька причин, чому: це зручно, швидко і майже безкоштовно. Але загрози від них таки є.

Розказати (не) все

У Департаменті кіберполіції Національної поліції України відзначили: багато користувачів соціальних мереж публікують і зберігають на своїх сторінках майже всю інформацію про своє життя (де навчались, працювали чи працюють, близьких родичів, знайомих, свої уподобання). В історії залишають діалоги інтимного характеру та світлини, доступ до яких закритий (начебто) для інших користувачів. Але всі ці дані – простий спосіб для шахраїв використати вашу довірливість.

Кіберполіцією все частіше фіксуються випадки зламу сторінок в соціальних мережах, коли власників сторінки шантажують можливим розсиланням фото інтимного змісту між користувачами, які знаходяться в статусі «Друзі». Тому ми рекомендуємо не розміщати таку інформацію в мережі Інтернет, аби не стати жертвою вимагачів чи шахраїв, які використовують методи соціальної інженерії, – наголосили кіберполіцейські.

Програміст Макс Фрай розповів: нещодавно у популярній соцмережі «ВКонтакте» припустилися помилки, і всім користувачам відкрився доступ до адмінпанелі цієї соцмережі. І люди отримали доступи – можливість банити групи тощо.

Немає гарантії, що в якийсь момент не станеться помилки і не відкриється доступ до особистих повідомлень. А оскільки вони не шифруються – це вже небезпечно. Будь-яка інформація, яку людина додає в свої соцмережі – фото, повідомлення – може бути небезпечною, – уточнив фахівець.

Причому способів, як саме використати отриману інформацію у незаконних оборудках, можна вигадати чимало. Все залежить від фантазії зловмисника. Наприклад, можна отримати телефон людини і таким чином –

доступ до інтернет-банкінгу. Власне, відзначають у кіберполіції, доступ до ваших грошей через інтернет – найбільш ласий шматок для шахраїв.

Що не можна довіряти соцмережам

Макс Фрай наполегливо радить не вносити у профіль соцмережі особисті дані, наприклад, адресу місця проживання.

Це ненормально – давати таку інформацію, аж до вулиці і номеру будинку та квартири. Я б не писав важливу інформацію у повідомленнях. Якщо для спілкування з друзями, на загальні теми – це нормально. Для чогось важливішого, від чого залежить ваша робота і бізнес, я би використотував те, що нині набрало обертів, це месенджери з шифруванням, як Telegram, наприклад, – уточнив програміст.

Чи були прецеденти, що якусь робочу інформацію крали – звісно ж були, каже експерт. Зламати можна все, що завгодно. Питання в тому – кому і для чого це потрібно. Питання у сумі і наскільки людина важлива, щоб її профіль зламати. Чим вищий статус має користувач у реальному житті – тим небезпечніші для нього соцмережі.

А як же налаштування конфіденційності, якими апелюють до користувачів розробники соцмереж, обіцяючи всезагальне благо? Макс Фрай переконує, що насправді їх роблять для того, щоб більше отримувати грошей. Чим більше інформація закрита в середині соцмережі – тим дорожче її розробники можуть продати. Вони максимально захищають дані користувачів не заради самих користувачів, а заради того, аби потім на цьому заробляти. Це одна з причин, чому так багато розбіжностей у їхніх налаштуваннях. А користувачу експерт радить не публікувати інформацію, яка може вплинути на його життя.

Якщо вам є, що приховувати, і потрібно опублікувати інформацію, яку хтось не повинен бачити – краще її не публікувати взагалі. Тому що якщо комусь це треба – побачать, – наголосив експерт.

Втім, за словами програміста, українців не можна назвати найнедбалішими користувачами. У всьому світі батьки, наприклад, часто реєструють у соцмережах дітей, вказуючи при цьому всю інформацію. (Згадайте деякі Інстаграми модних чи музичних діток).

Людина ще ходить в дитсадок, а в соцмережі вже є повна інформація про неї. Це дуже погано, – відзначив Фрай.

Він нагадав: «“ВКонтакті” колись був пункт при реєстрації з вимогою підтвердити, що користувач має більше 18 років. Тепер його прибрали. У ФБ така автентифікація чисто номінальна – адже дату народження можна вписати, яку заманеться. Тому виглядає – реєструватися неповнолітнім тепер можна. Але вся відповідальність лягає на батьків».

Соцмережі і закон

Чи може поліція знайти щось у соцмережі і використати це на законних підставах проти людини? Так – кажуть експерти.

10 травня у Львові людину засудили на 2 роки, за те, що вона упродовж кількох місяців публікувала нацистську символіку, пропагувала. Це вже прецедент, – розповів Фрай.

Існує інший бік медалі – чи може закон захистити від того, щоб, наприклад, ваші фото з соцмережі не зміг використовувати будь-хто?

Тут маємо «вилку» у законі: згідно з ст. 300 ЦК України фізична особа має право на індивідуальність. Відповідно до ст. 308 ЦК України фотографія, інші художні твори, на яких зображено фізичну особу, можуть бути публічно показані, відтворені, розповсюджені лише за згодою цієї особи.

Але – ви добровільно розповсюджуєте власні фотографії у мережі. А ставши членом мережі, укладаєте:

1) публічний договір, в якому одна сторона, підприємець взяла на себе обов'язок здійснювати продаж товарів, виконання робіт або надання послуг кожному, хто до неї звернеться (роздрібна торгівля, перевезення транспортом загального користування, послуги зв'язку, медичне, готельне, банківське обслуговування тощо), (ст. 633 ЦКУкраїни), тобто договір із власником сайту, умови якого встановлюються однаковими для всіх споживачів;

2) договір приєднання, умови якого встановлені однією із сторін у формулярах або інших стандартних формах, який може бути укладений лише шляхом приєднання другої сторони до запропонованого договору в цілому. Друга сторона не може запропонувати свої умови договору. Таким чином, ви погоджуєтеся із певними умовами і не можете висунути свої до адміністратора сайту (ст. 634 ЦК України).

Тому, якщо справа дійде до суду, все залежатиме від доказів, які будуть представлені.

Які соцмережі найбезпечніші

Тут все досить відносно, відзначив Макс Фрай. Все залежить від підходу розробників і бюджету. Є такі програми, що називаються Bug Bounty, коли людина, що знаходить у програмі чи системі якийсь баг (помилку, дефект), то не користається нею, а повідомляє розробника і йому за це розробник платить. За словами програміста, така можливість є і у ВК, і в Facebook. Втім, Макс Фрай назвав Фейсбук ризикованішим через його масштабність. У ФБ було вже кілька випадків, коли людям у особисті повідомлення приходили підозрілі посилання та відео і через помилку в коді при натисканні на це посилання воно розсилалось усім «френдам». А ці посилання та відео містили шкідливий код.

Захиститися від такого заздалегідь не можливо. Коли вже знаєш про подібну ймовірність, коли вже когось «зламують», тоді вже пишуть рекомендації і як себе поводити з такими вірусами, – уточнив експерт.

Рекомендації для убезпечення акаунту в соцмережах

Максимально у всіх сервісах варто встановлювати двохфакторну авторизацію: окрім логіна й пароля – ще й смс з кодом. Навіть якщо вас зламали і якимось чином отримали ваш пароль, то зловмисники не зможуть увійти у ваш профіль без доступу до вашого телефону. Це для звичайних користувачів. Для тих, хто має справу з більш серйозною інформацією – варто

не вказувати при реєстрації мейл та номер телефону, про який всі знають. Краще зареєструвати новий е-мейл та номер телефону і використовувати їх виключно для входу в соцмережу. Останнє, що і так мали би всі знати та досі нехтують – якщо вам в пошту приходить будь-який файл від незнайомого користувача – не можна його відкривати, адже це найпростіший спосіб маскування для вірусів.

(вгору)

Додаток 19

11.05.2017

Рекламные компании следят за нами через наши смартфоны

То, о чем мы сейчас расскажем, скорее всего, вам не понравится. Современные Android-смартфоны могут следить за пользователем и слушать все происходящее вокруг. Это не секрет (Украинский телекоммуникационный портал).

А что, если ваш смартфон проверяет, слушаете ли вы ту или иную рекламу и отправляет эти данные тем, кто эту рекламу создает?

Увы, это очень и очень вероятно. Существует компания, которая этим занимается, и более 200 Android-приложений, нарушающих вашу конфиденциальность.

Компания Silverpush разработала технологию мониторинга для рекламной индустрии. Суть в том, что в рекламных роликах проигрываются ультразвуковые маячки, которые не различимы для человеческого уха, но могут быть зафиксированы с помощью микрофона, например, с помощью микрофона смартфона.

Маячки проигрываются на частоте от 18 до 20 кГц, когда вы смотрите или слушаете рекламу.

Приложение на вашем телефоне слышит их и сообщает в Silverpush о том факте, что реклама была вами прослушана. Но кто станет ставить такое приложение на свой смартфон?

Исследователи из немецкого технического университета в Брауншвейге обнаружили программное обеспечение от Silverpush в 234 приложениях для Android.

Эти приложения установили уже несколько миллионов раз, и они скрыто слушают все, что происходит вокруг вас. В 2015 году таких приложений было всего 5, но, кажется, идея понравилась рекламщикам.

Приложения не просто слушают, стараясь уловить ультразвуковые маячки. Они передают провайдеру информацию о прослушанной рекламе и о пользователе, что позволяет лучше изучить аудиторию и охват рекламы. Разумеется, все это делается без разрешения пользователей.

Вам стоит знать, что активисты в вопросах защиты гражданских прав всячески осуждают действия Silverpush. Антивирусная программа Avira классифицирует их софт как вредоносный.

К сожалению, эксперты отказались опубликовать список следящих приложений, однако они сообщили, что некоторые из приложений выпущены известными компаниями. Кажется, нужно быть осторожнее не только в выборе производителя смартфона, но и в выборе приложений.

(вгору)

Додаток 20

15.05.2015
Илья Кабачинский
WCry, раунд 2: массовые кибератаки могут повториться

Днем 12 мая вирус-вымогатель WannaCry заразил тысячи компьютеров по всему миру. За несколько дней число пострадавших выросло до 200 000 в 150 странах. Злоумышленники успели получить более $42 000 от жертв, но эксперту по безопасности Дэриену Хассу удалось замедлить его распространение. Впрочем, как уверяют эксперты, уже с сегодняшнего дня можно ожидать новых массовых атак (AIN.UA).

Как сообщает Motherboard, создатели вируса обновили его и научили обходить домен iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com, к которому ранее WCry был привязан. Именно это и стало 13 мая основной причиной снижения активности распространения вируса. Впрочем, уже с 15 мая атаки на компьютеры по всему миру могут возобновиться с прежней силой.

Напомним, вирус-вымогатель появляется на компьютерах пользователей после открытия фишинговой рассылки: письма приходят от имени известных компаний, на которые могут реагировать пользователи. За разблокировку компьютера требуют от $300, а в случае неуплаты за 7 дней он удаляет всю информацию с компьютера пользователя.

Вирус активен только на компьютерах с Windows. Представители компании Microsoft выпустили обновление, которое защищает компьютеры от атаки еще в марте, но те, кто его не установил, могут пострадать. Также компания оперативно представила меры защиты даже для тех версий Windows, которые уже не поддерживаются. В частности, Windows XP.

От атаки хакеров пострадали не только обычные пользователи, но и целые компании. По всему миру закрывались банки, фабрики, даже больницы, сотрудников компаний просили более осторожно подходить к открытию писем от незнакомых людей.

Согласно последним данным, всего атака повлияла на 10 000 организаций и 200 000 людей в 150 странах мира. Злоумышленники неплохо заработали. Как сообщало издание Quartz 14 мая, хакреам удалось получить более $23 000 в качестве выкупа от жертв. Уже 15 мая The Guardian опубликовал более свежие данные: $42 000. Больше всего зараженных компьютеров оказалось в России.

Как себя защитить?

Самый простой способ – установить все актуальные обновления от Microsoft. Уязвимость впервые обнаружили еще в феврале 2017 года, а уже в

марте компания представила обновление для Windows, которое блокирует распространение вируса. У пользователей легальной версии Windows обновления устанавливаются автоматически, но стоит все же проверить наличие последний версий. Если у вас более старая версия Windows, защиту для нее можно найти здесь.

Также компания внесла информацию о вирусе WCry в собственный бесплатный антивирус Windows Defender. Его можно скачать и установить себе на компьютер. Если у вас уже есть антивирус от сторонней компании, стоит проверить наличие последних обновлений и убедиться, что там есть защита от WCry. Чтобы не беспокоиться за сохранность своих данных, стоит также сделать их резервную копию.

Главное, что необходимо помнить: вирус сам по себе не активируется. Чтобы он запустился, пользователь должен произвести некоторое действие. В частности, открыть письмо и кликнуть по ссылке. Поэтому излишняя внимательность не повредит. Ранее под прикрытием «ПриватБанка» подобный вирус распространялся и в Украине. Благо пользователи оперативно заметили подвох.

(вгору)

Додаток 21

16.05.2017

Украинцев массово обворовывают через подставные сайты

Количество мошеннических сайтов в Украине в 2016 году выросло в 4,5 раза (174 фишинговых ресурса в 2016 году против 38 – в 2015 году). И мошенники продолжают набирать обороты (InternetUA).

Только за первый квартал этого года специалистами Ассоциации ЕМА уже было выявлено 54 фишинговых веб-ресурса.

Большая часть сайтов имитирует сервисы для пополнения мобильного телефона или совершения денежного перевода.

Если тенденция сохранится, то к концу этого года количество мошеннических сайтов может перевалить за двести, говорят эксперты.

Несмотря на то, что многие банковские и небанковские сервисы электронных платежей предупреждают своих пользователей о фишинговых сайтах, большое количество украинцев до сих пор не знают о рисках фишинга. По данным ЕМА, только 66% наших владелец карт не станут пользоваться непроверенным веб-ресурсом, о котором нет информации в интернет. Остальные об этом мало задумываются.

Важно помнить, что все без исключения фишинговые сайты предлагают пользователям несуществующие услуги с низкими комиссиями. Но веб-ресурсы мошенников лишь имитируют сервисы для совершения платежей онлайн.

В целом, все фишинговые сайты в Украине можно разделить на несколько видов:

– Сайты, имитирующие сервисы для пополнения мобильного.
– Сайты, имитирующие сервисы для совершения денежных переводов.
– Веб-ресурсы, которые «предлагают» обе услуги.
– Сайты-подделки под известные веб-сервисы электронных платежей.
– Сайты, рекламирующие подработки в Интернет.
– Веб-ресурсы, «продающие» дешевые авиабилеты.

На каждом фишинговом сервисе (как и на любом легитимном веб-сервисе) есть платежная форма, которую пользователь заполняет, указывая конфиденциальные данные своей карты: срок действия карты и трехзначный код безопасности карты (или код CVV2 /CVC2).

Позже мошенники попытаются использовать добытые конфиденциальные данные карты клиента, чтобы украсть деньги с его счета.

Определять фишинговый сайт с двухфазным переводом денег с карты на карту надо по тем же признакам, что и «обычный» фишинговый веб-ресурс:

– У такого сервиса отсутствует репутация – о нем нет информации в интернет (или она носит отрицательный характер).

– Сайт отечественного сервиса зарегистрирован сроком на 1 год и на домене ниже уровня.ua (для регистрации сервиса на этом домене требуется прохождение сложной процедуры, а мошенники выбирают домены с регистрацией без ограничений, это .ru, .com.ua, .in.ua, .pp.ua, .kiev.ua, .dp.ua,. te.ua, .org, .net, .com, .info, .biz, .top, .in, .cc и т.д.).

– В текстах сайта есть ошибки, опечатки, неточности.
– Название сайта не соответствует названию в его адресной строке.

Еще одна особенность отечественного фишингового мошенничества – геоблокирование.

Преступники используют специальные IP-фильтры для того, чтобы на страницу фишингового ресурса могли попасть только пользователи из Украины.

То есть, преступники работают на конкретную «целевую аудиторию» и одновременно «скрываются» от мониторинга международных организаций для выявления фишинговых сайтов.

(вгору)

Соціальні мережі

як чинник інформаційної безпеки

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

Упорядник **Терещенко** Ірина Юріївна

Редактор О. Федоренко

Свідоцтво про державну реєстрацію КВ № 5358 від 03.08.2001 р.

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